

This document is made available through the declassification efforts  
and research of John Greenewald, Jr., creator of:

# The Black Vault

---



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

**Discover the Truth** at: **<http://www.theblackvault.com>**



POSTAL REGULATORY COMMISSION  
Washington, DC 20268-0001

Office of the Secretary

March 31, 2017

Mr. John Greenewald  
[REDACTED]

**RE: FOIA 17-17**

Dear Mr. Greenewald,

This letter is in response to your February 17, 2017 email, requesting the following records:

- A copy of records, electronic or otherwise, of all after action reports, damage assessments, incident reports, and any communications concerning the SQL injection cyber incident/intrusion Documents in the file(s) related to those proceedings.

After a review of the relevant agency records, the Commission searched and found the attached documents responsive to your request. In addition, attached to this letter is a Vaughn Index, to correlate each withheld portion with the specific Freedom of Information Act (FOIA) exemption and the nondisclosure justification.

You may appeal this response by filing an appeal within one year, in the following ways.

By filing an appeal at the following address:

Ruth Ann Abrams, Chief FOIA Officer  
Postal Regulatory Commission  
901 New York Avenue, Suite 200  
Washington, DC 20268-00001  
Email: [ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)

Additionally, the Office of Government Information Services (OGIS) was created by way of a 2007 amendment to the FOIA to provide mediation services to resolve disputes between FOIA requesters and federal agencies as a non-exclusive alternative to litigation. Using the OGIS for mediation does not affect your right to pursue litigation. You may contact OGIS in any of the following ways:

Office of Government Information Services National Archives and Records Administration  
8610 Adelphi Road, Room 2510  
College Park, MD 20740-6001  
Email: [ogis@nara.gov](mailto:ogis@nara.gov)  
Tel: 301-837-1996/Fax: 301-837-0348  
Toll-Free: 1-877-684-6448

If you need further assistance or would like to discuss any aspect of your request, please do not hesitate to contact the Commission's FOIA Public Liaison, Ann Fisher in any of the following ways:

Postal Regulatory Commission  
FOIA Public Liaison  
901 New York Avenue NW, Suite 200  
Washington, DC 20268-0001  
Email: [FOIA@prc.gov](mailto:FOIA@prc.gov)  
Tel: 202-789-6800

I hope that you find this information useful.

Sincerely,

A handwritten signature in black ink, appearing to read "Ruth Ann Abrams", with a long horizontal flourish extending to the right.

Ruth Ann Abrams  
Chief FOIA Officer

---

Enclosure

**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 24, 2017 3:07 PM  
**To:** soc@us-cert.gov  
**Cc:** Support; RUBLE, STACY L  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

Greetings SOC,

I apologize for the delay in responding. In response to the subject incident, PRC IT staff have taken the following actions:

- 1) Scanned the website for all known vulnerabilities
- 2) Scanned the website using (b) (5) for web site scan policy template
- 3) Scanned the website using (b) (5)

All above scan reports show no vulnerabilities related to SQLi as reported. Additionally, our MTIPs perimeter defense has not detected any traffic that would indicate a SQLi type vulnerability - inbound or outbound.

At this point, we have completed our analysis and find no evidence of an intrusion or referenced vulnerability. Please let me know if US CERT requires any further action from the PRC.

Thanks,  
Lee

---

A. Lee Martin  
Info Tech Manager  
Postal Regulatory Commission  
901 New York Ave., NW Ste 200 W  
Washington, DC 20268  
Office: (202) 789-5470  
Cell: (202) 816-9027

-----Original Message-----

From: Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
Sent: Tuesday, January 10, 2017 1:11 PM  
To: Support <support@prc.gov>; Martin, Lee <Lee.Martin@prc.gov>  
Cc: Christine.Sahlin@us-cert.gov  
Subject: US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)



(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration  
Center (NCCIC) Department of Homeland Security

888-282-0870

SOC@us-cert.gov

www.us-cert.gov

Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,

Christine Sahlin

Incident Management Analyst

NCCIC Hunt & Incident Response Team

Desk: 850.452.6907

Email: Christine.sahlin@us-cert.gov

**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 24, 2017 2:34 PM  
**To:** 'Brian A. Lemaster'  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

OK, I looked up (b) (5) and that is a generic plugin for SQLi, but I will use your response about using the Web Site Template.

-----Original Message-----

**From:** Brian A. Lemaster [mailto:lemaster@tecodo.com]  
**Sent:** Tuesday, January 24, 2017 2:25 PM  
**To:** Martin, Lee <Lee.Martin@prc.gov>  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

I'll have to look and find out. I ran site against all Plugins, Web Site Template

Brian A. Lemaster  
Chief Technology Officer  
Tecodo, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, Virginia 20171  
Direct: +1 571.388.7106  
Office: +1 703.788.6704  
<http://www.tecodo.com>

This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.

-----Original Message-----

**From:** Martin, Lee [mailto:Lee.Martin@prc.gov]  
**Sent:** Tuesday, January 24, 2017 1:23 PM  
**To:** Brian A. Lemaster <lemaster@tecodo.com>  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

Can you tell me what plugin we used and I will reference that.

-----Original Message-----

**From:** Brian A. Lemaster [mailto:lemaster@tecodo.com]  
**Sent:** Tuesday, January 24, 2017 1:19 PM  
**To:** Martin, Lee <Lee.Martin@prc.gov>  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

You may want to ask if they can rescan and/or assist with testing.

Brian A. Lemaster  
Chief Technology Officer  
Tecodo, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, Virginia 20171  
Direct: +1 571.388.7106  
Office: +1 703.788.6704  
<http://www.tecodo.com>

This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.

-----Original Message-----

From: Martin, Lee [mailto:Lee.Martin@prc.gov]  
Sent: Tuesday, January 24, 2017 1:15 PM  
To: Brian A. Lemaster <lemaster@tecodo.com>  
Subject: FW: US-CERT Incident number INC000010106204 PRC

Hey Brian,

(b) (5)

A large black rectangular redaction box covering the body of the email.

-----Original Message-----

From: Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
Sent: Tuesday, January 10, 2017 1:11 PM  
To: Support <support@prc.gov>; Martin, Lee <Lee.Martin@prc.gov>  
Cc: Christine.Sahlin@us-cert.gov  
Subject: US-CERT Incident number INC000010106204 PRC

(b) (5)

A large black rectangular redaction box covering the body of the email.

(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration  
Center (NCCIC) Department of Homeland Security  
888-282-0870  
SOC@us-cert.gov  
www.us-cert.gov  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: Christine.sahlin@us-cert.gov

**Martin, Lee**

---

**From:** Brian A. Lemaster <lemaster@tecodo.com>  
**Sent:** Tuesday, January 10, 2017 4:16 PM  
**To:** Martin, Lee  
**Subject:** RE: INC000010106204 PRC

(b) (5)

will run the test you sent and let you know what I find.

Brian A. Lemaster  
Chief Technology Officer  
Tecodo, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, Virginia 20171  
Direct: +1 571.388.7106  
Office: +1 703.788.6704  
<http://www.tecodo.com>

This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.

-----Original Message-----

**From:** Martin, Lee [mailto:Lee.Martin@prc.gov]  
**Sent:** Tuesday, January 10, 2017 4:06 PM  
**To:** Brian A. Lemaster <lemaster@tecodo.com>  
**Subject:** FW: INC000010106204 PRC

OK, so finally DHS got back to me and there is a possibility the prc.gov web site may have a SQL injection vulnerability. Can you scan the web site using the correct plugin and see if it will detect this?

(b) (5)

Lee

-----Original Message-----

**From:** Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
**Sent:** Tuesday, January 10, 2017 3:00 PM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Cc:** soc@us-cert.gov; jonathan.homer@hq.dhs.gov  
**Subject:** RE: INC000010106204 PRC

Mr. Martin,

(b) (5)



RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: Christine.sahlin@us-cert.gov

-----Original Message-----

From: Martin, Lee [mailto:Lee.Martin@prc.gov]  
Sent: Tuesday, January 10, 2017 12:39 PM  
To: SOC  
Cc: ABRAMS, RUTH A  
Subject: Ref: INC000010106204 PRC

Greetings SOC,

I have received notification for the above ref. security incident and have several questions before I can proceed:

(b) (5)



\* Our scans do not indicate compromise or notification of any malware existing on our site. Can you give me more information on what our next steps should be?

Thanks,

Lee

---

A. Lee Martin

Info Tech Manager

Postal Regulatory Commission

901 New York Ave., NW Ste 200 W

Washington, DC 20268

Office: (202) 789-5470

Cell: (202) 816-9027



**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 10, 2017 3:40 PM  
**To:** Christine.Sahlin@us-cert.gov; ABRAMS, RUTH A  
**Cc:** soc@us-cert.gov; jonathan.homer@hq.dhs.gov  
**Subject:** RE: INC000010106204 PRC

Thank you for the follow up information Christine, we will scan our system for SQL injection vulnerabilities and follow up with the SOC once completed.

-----Original Message-----

From: Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
Sent: Tuesday, January 10, 2017 3:00 PM  
To: Martin, Lee; ABRAMS, RUTH A  
Cc: soc@us-cert.gov; jonathan.homer@hq.dhs.gov  
Subject: RE: INC000010106204 PRC

Mr. Martin,

(b) (5)



RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: Christine.sahlin@us-cert.gov

-----Original Message-----

From: Martin, Lee [mailto:Lee.Martin@prc.gov]  
Sent: Tuesday, January 10, 2017 12:39 PM  
To: SOC  
Cc: ABRAMS, RUTH A  
Subject: Ref: INC000010106204 PRC

Greetings SOC,

I have received notification for the above ref. security incident and have several questions before I can proceed:



(b) (5)



Thanks,

Lee

---

A. Lee Martin

Info Tech Manager

Postal Regulatory Commission

901 New York Ave., NW Ste 200 W

Washington, DC 20268

Office: (202) 789-5470

Cell: (202) 816-9027

**Martin, Lee**

---

**From:** Christine.Sahlin@us-cert.gov  
**Sent:** Tuesday, January 10, 2017 3:00 PM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Cc:** soc@us-cert.gov; jonathan.homer@hq.dhs.gov  
**Subject:** RE: INC000010106204 PRC

Mr. Martin,

(b) (5)



RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: Christine.sahlin@us-cert.gov

-----Original Message-----

**From:** Martin, Lee [mailto:Lee.Martin@prc.gov]  
**Sent:** Tuesday, January 10, 2017 12:39 PM  
**To:** SOC  
**Cc:** ABRAMS, RUTH A  
**Subject:** Ref: INC000010106204 PRC

Greetings SOC,

I have received notification for the above ref. security incident and have several questions before I can proceed:

(b) (5)



Thanks,

Lee

---

A. Lee Martin

Info Tech Manager

Postal Regulatory Commission

901 New York Ave., NW Ste 200 W

Washington, DC 20268

Office: (202) 789-5470

Cell: (202) 816-9027

**Martin, Lee**

---

**From:** Brian A. Lemaster <lemaster@tecodo.com>  
**Sent:** Tuesday, January 10, 2017 2:08 PM  
**To:** Support; Martin, Lee  
**Subject:** Re: US-CERT Incident number INC000010106204 PRC

Will do

Get [Outlook for iOS](#)

---

**From:** Martin, Lee <Lee.Martin@prc.gov>  
**Sent:** Tuesday, January 10, 2017 2:07:09 PM  
**To:** Support  
**Subject:** FW: US-CERT Incident number INC000010106204 PRC

All,

I've been working with US CERT to get their incident notifications sent to the support group. That said, I've requested more information concerning this incident. The info below is vague, so let's hope they respond with something more meaning full that we can act on.

(b) (5)

I'll let you know once I get more info.

Thanks,  
Lee

-----Original Message-----

**From:** Christine.Sahlin@us-cert.gov [<mailto:Christine.Sahlin@us-cert.gov>]  
**Sent:** Tuesday, January 10, 2017 1:11 PM  
**To:** Support; Martin, Lee  
**Cc:** Christine.Sahlin@us-cert.gov  
**Subject:** US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)

(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration Center (NCCIC)  
Department of Homeland Security  
888-282-0870  
SOC@us-cert.gov  
[www.us-cert.gov](http://www.us-cert.gov)  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: Christine.sahlin@us-cert.gov

**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 10, 2017 2:07 PM  
**To:** Support  
**Subject:** FW: US-CERT Incident number INC000010106204 PRC

All,

I've been working with US CERT to get their incident notifications sent to the support group. That said, I've requested more information concerning this incident. The info below is vague, so let's hope they respond with something more meaning full that we can act on.

(b) (5)

I'll let you know once I get more info.

Thanks,  
Lee

-----Original Message-----

From: Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
Sent: Tuesday, January 10, 2017 1:11 PM  
To: Support; Martin, Lee  
Cc: Christine.Sahlin@us-cert.gov  
Subject: US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)

(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration  
Center (NCCIC) Department of Homeland Security  
888-282-0870  
SOC@us-cert.gov  
www.us-cert.gov  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: Christine.sahlin@us-cert.gov

M8

**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 10, 2017 1:39 PM  
**To:** SOC@us-cert.gov  
**Cc:** ABRAMS, RUTH A  
**Subject:** Ref: INC000010106204 PRC

Greetings SOC,

I have received notification for the above ref. security incident and have several questions before I can proceed:

(b) (5)



Thanks,  
**Lee**

---

**A. Lee Martin#**  
*Info Tech Manager*  
*Postal Regulatory Commission*  
*901 New York Ave., NW Ste 200 W*  
*Washington, DC 20268*  
*Office: (202) 789-5470*  
*Cell: (202) 816-9027*



**Martin, Lee**

---

**From:** Christine.Sahlin@us-cert.gov  
**Sent:** Tuesday, January 10, 2017 1:11 PM  
**To:** Support; Martin, Lee  
**Cc:** Christine.Sahlin@us-cert.gov  
**Subject:** US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration  
Center (NCCIC) Department of Homeland Security  
888-282-0870  
SOC@us-cert.gov

www.us-cert.gov  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: Christine.sahlin@us-cert.gov

**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Monday, January 09, 2017 12:55 PM  
**To:** Brian A. Lemaster  
**Subject:** Junk Mail Filter

Hey Brian,

US CERT sent and incident alert on Fri afternoon to [Support@prc.gov](mailto:Support@prc.gov) and I didn't receive anything. Can you check the junk\spam mail filter to see if the message is captured there?

Thanks,

**Lee**

---

**A. Lee Martin#**

*Info Tech Manager*

*Postal Regulatory Commission*

*901 New York Ave., NW Ste 200 W*

*Washington, DC 20268*

*Office: (202) 789-5470*

*Cell: (202) 816-9027*

**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Friday, January 06, 2017 2:23 PM  
**To:** RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: DHS info

Stacy, Ruth Ann,

Followed up with my DHS contact just now and the notification is still scheduled to go out via email by COB today. It is now pending DHS Sr. Leadership approval before being distributed. Again, they aren't allowed to talk details over the phone, but she did say that this incident affected 30 + agencies and that is not considered catastrophic. Basically, once notified, we'll need to do forensics, review logs, scans looking for traces\impact of the details in the report and next steps should we have been compromised.

(b) (5)



I'll let you know the min. I hear something and am able to analyze their report. Let me know if there are any questions.

Thanks,  
Lee

---

**From:** RUBLE, STACY L  
**Sent:** Friday, January 06, 2017 11:38 AM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Subject:** RE: DHS info

thanks

---

**From:** Martin, Lee  
**Sent:** Friday, January 06, 2017 11:38 AM  
**To:** RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: DHS info

Stacy,

Still haven't received anything from the Incident Response staff from DHS. The person that called yesterday told me that they will contact me by the end of today once the report has been completed. I will contact them this afternoon.

Lee

---

**From:** RUBLE, STACY L  
**Sent:** Friday, January 06, 2017 11:34 AM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Subject:** DHS info

Lee, Ruth Ann, what came of the DHS information you were to receive yesterday?  
Thanks, Stacy

Stacy L. Ruble  
Secretary and Chief Administrative Officer



**Postal Regulatory Commission**

901 New York Ave NW – Suite 200 W – Washington, DC 20268  
202.789.6800 [stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)

*Notice:* This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.

**Martin, Lee**

---

**From:** soc@us-cert.gov  
**Sent:** Tuesday, February 21, 2017 8:39 AM  
**To:** Support  
**Subject:** US-CERT Incident number INC000010106204 -

PRC,

At this time, there is not further action required. We will notify you if this changes.

Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration Center (NCCIC) Department of Homeland Security  
888-282-0870  
SOC@us-cert.gov  
www.us-cert.gov  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Email Attachment :

**Martin, Lee**

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 10:15 AM  
**To:** soc@us-cert.gov  
**Cc:** Support  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC  
  
**Importance:** High

Greeting SOC,

Just following up on my earlier message regarding subject incident. Please advise if you require any follow on actions.

Regards, Lee

---

A. Lee Martin  
Info Tech Manager  
Postal Regulatory Commission  
901 New York Ave., NW Ste 200 W  
Washington, DC 20268  
Office: (202) 789-5470  
Cell: (202) 816-9027

-----Original Message-----

**From:** Martin, Lee  
**Sent:** Tuesday, January 24, 2017 3:07 PM  
**To:** soc@us-cert.gov  
**Cc:** Support <support@prc.gov>; RUBLE, STACY L <stacy.ruble@prc.gov>  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

Greetings SOC,

I apologize for the delay in responding. In response to the subject incident, PRC IT staff have taken the following actions:

- 1) Scanned the website for all known vulnerabilities
- 2) Scanned the website using (b) (5) for web site scan policy template
- 3) Scanned the website using (b) (5)

All above scan reports show no vulnerabilities related to SQLi as reported. Additionally, our MTIPs perimeter defense has not detected any traffic that would indicate a SQLi type vulnerability - inbound or outbound.

At this point, we have completed our analysis and find no evidence of an intrusion or referenced vulnerability. Please let me know if US CERT requires any further action from the PRC.

Thanks,  
Lee

---

A. Lee Martin  
Info Tech Manager  
Postal Regulatory Commission  
901 New York Ave., NW Ste 200 W  
Washington, DC 20268  
Office: (202) 789-5470  
Cell: (202) 816-9027

-----Original Message-----

From: Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
Sent: Tuesday, January 10, 2017 1:11 PM  
To: Support <support@prc.gov>; Martin, Lee <Lee.Martin@prc.gov>  
Cc: Christine.Sahlin@us-cert.gov  
Subject: US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)





(b) (5)

Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration  
Center (NCCIC) Department of Homeland Security  
888-282-0870

SOC@us-cert.gov

www.us-cert.gov

Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,

Christine Sahlin

Incident Management Analyst

NCCIC Hunt & Incident Response Team

Desk: 850.452.6907

Email: Christine.sahlin@us-cert.gov

RuthAnn

**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

**From:** it-services On Behalf Of (b) (6)  
**Sent:** Thursday, February 16, 2017 10:16 AM  
**To:** PRC-PAGR  
**Subject:** Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:  
Submitted values are:

message type: Question  
Subject : Postal Regulatory Commission  
First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)

## ABRAMS, RUTH A

---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
 Ann

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

From: it-services On Behalf Of (b) (6)

Sent: Thursday, February 16, 2017 10:16 AM

To: PRC-PAGR

Subject: Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:

Submitted values are:

message type: Question

Subject : Postal Regulatory Commission

First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number (b) (6)

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)



**ABRAMS, RUTH A**

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 11:38 AM  
**To:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Will do. I will let you know what I find out.

---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
 Ann

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

From: it-services On Behalf Of (b) (6)

Sent: Thursday, February 16, 2017 10:16 AM

To: PRC-PAGR

Subject: Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:

Submitted values are:

message type: Question

Subject : Postal Regulatory Commission

First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number (b) (6)

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)

**ABRAMS, RUTH A**

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 1:39 PM  
**To:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission  
**Attachments:** The Postal Regulatory Commission Report.pdf

All,

See the information and attachment I received from the source:

Hello Mr.Adams,

My name is (b) (6) and I'd like to apologize for the delayed response to your inquiry. On January 5, 2017, I submitted the accompanying report to MS-ISAC NCCIC Partner Liaison Center for Internet Security, and I was assured that information successfully delivered to all affected organizations including Postal Regulatory Commission.

The report includes the identified SQLi vulnerability, which was offered for sale by the Russian cybercriminal known as Rasputin. In the case, you have any follow-up questions, please don't hesitate to reach out to us at any time.

Respectfully,

(b) (6)



---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
Ann

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission



Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

**From:** it-services On Behalf Of (b) (6)  
**Sent:** Thursday, February 16, 2017 10:16 AM  
**To:** PRC-PAGR  
**Subject:** Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:  
Submitted values are:

message type: Question  
Subject : Postal Regulatory Commission  
First name\*: (b) (6)  
Last Name\*: (b) (6)  
Email Address: (b) (6)  
phone number: (b) (6)  
address1: ADDRESS 1  
address2: ADDRESS 2  
city: CITY  
state: STATE  
zipcode\*: (b) (6)  
comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)

**ABRAMS, RUTH A**

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 2:13 PM  
**To:** ABRAMS, RUTH A; FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Ruth Ann,

I'm not sure what the source information mean that was given to us. Can you please draft me a response so that I can apply to the reporter that made the original inquiry.

Thank you!

---

**From:** ABRAMS, RUTH A  
**Sent:** Thursday, February 16, 2017 1:40 PM  
**To:** ADAMS, GAIL Z; FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,  
Thank you for the source information. We will look it over. However, the IT team scanned the system and no vulnerability was identified.  
Ruth Ann

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 1:39 PM  
**To:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

All,

See the information and attachment I received from the source:

Hello Mr.Adams,

My name is (b) (6) and I'd like to apologize for the delayed response to your inquiry. On January 5, 2017, I submitted the accompanying report to MS-ISAC NCCIC Partner Liaison Center for Internet Security, and I was assured that information successfully delivered to all affected organizations including Postal Regulatory Commission.

The report includes the identified SQLi vulnerability, which was offered for sale by the Russian cybercriminal known as Rasputin. In the case, you have any follow-up questions, please don't hesitate to reach out to us at any time.

Respectfully,

(b) (6)



---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
Ann

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

From: it-services On Behalf Of (b) (6)

Sent: Thursday, February 16, 2017 10:16 AM

To: PRC-PAGR

Subject: Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:

Submitted values are:

message type: Question

Subject : Postal Regulatory Commission

First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number (b) (6)

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)



**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 9:25 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Google Alert - Postal Regulatory Commission

All,

I did another vulnerability scan on the web site last night using plugins that the vendor recommended specifically to identify SQL injections and the results were negative. Also, I am looking for another SQL injection scanner to validate our internal results, but at this point I believe that this is a false positive. Our scans results did not show this vulnerability. The vulnerability scanner the Commission uses is an industry \ Gov't standard and is 1 of the tools being implemented Gov't wide under the CDM program. I have high confidence that we would have found it if it existed in our environment.

Lee

---

**From:** ADAMS, GAIL Z  
**Sent:** Friday, February 17, 2017 9:05 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Google Alert - Postal Regulatory Commission

This story is spreading. See Infosecurity Magazine article below. Do we have a response for the reporter who originally inquired?

---

**From:** Google Alerts [<mailto:googlealerts-noreply@google.com>]  
**Sent:** Friday, February 17, 2017 9:02 AM  
**To:** ADAMS, GAIL Z  
**Subject:** Google Alert - Postal Regulatory Commission

Google Alerts

## Postal Regulatory Commission

Daily update · February 17, 2017

NEWS

### Hacker 'Rasputin' Probes Top Unis and Governments for SQLi Bugs

Infosecurity Magazine

Victims include the universities of Oxford and Cambridge as well as the US Postal Regulatory Commission and National Oceanic and Atmospheric ...



Flag as irrelevant

**ABRAMS, RUTH A**

---

**From:** ABRAMS, RUTH A  
**Sent:** Thursday, February 16, 2017 1:40 PM  
**To:** Martin, Lee (Lee.Martin@prc.gov)  
**Cc:** RUBLE, STACY L (stacy.ruble@prc.gov)  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission  
**Attachments:** The Postal Regulatory Commission Report.pdf

Lee,  
Let's discuss.

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 1:39 PM  
**To:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

All,

See the information and attachment I received from the source:

Hello Mr.Adams,

My name is (b) (6) and I'd like to apologize for the delayed response to your inquiry. On January 5, 2017, I submitted the accompanying report to MS-ISAC NCCIC Partner Liaison Center for Internet Security, and I was assured that information successfully delivered to all affected organizations including Postal Regulatory Commission.

The report includes the identified SQLi vulnerability, which was offered for sale by the Russian cybercriminal known as Rasputin. In the case, you have any follow-up questions, please don't hesitate to reach out to us at any time.

Respectfully,

(b) (6)



---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
Ann

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

**From:** it-services On Behalf Of Eleanor  
**Sent:** Thursday, February 16, 2017 10:16 AM  
**To:** PRC-PAGR  
**Subject:** Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:  
Submitted values are:

message type: Question  
Subject : Postal Regulatory Commission  
First name\*: (b) (6)



Last Name\*: (b) (6)

Email Address: (b) (6)

phone number

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)

**ABRAMS, RUTH A**

---

**From:** ABRAMS, RUTH A  
**Sent:** Thursday, February 16, 2017 11:25 AM  
**To:** Martin, Lee (Lee.Martin@prc.gov)  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Please reach out DHS and find out if the source of information is the email report we never received.

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

**From:** it-services On Behalf Of Eleanor  
**Sent:** Thursday, February 16, 2017 10:16 AM  
**To:** PRC-PAGR  
**Subject:** Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:

Submitted values are:

message type: Question

Subject : Postal Regulatory Commission

First name\*: Eleanor

Last Name\*: Lamb

Email Address: elamb@meritalk.com

phone number: 703-883-9000, ext. 127

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: 22314

comments:

Hello,

My name is Eleanor Lamb and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

Eleanor

**ABRAMS, RUTH A**

---

**From:** ABRAMS, RUTH A  
**Sent:** Thursday, February 16, 2017 1:40 PM  
**To:** ADAMS, GAIL Z; FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,  
Thank you for the source information. We will look it over. However, the IT team scanned the system and no vulnerability was identified.  
Ruth Ann

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 1:39 PM  
**To:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

All,  
  
See the information and attachment I received from the source:  
  
Hello Mr.Adams,  
  
My name is Andrei Barysevich, and I'd like to apologize for the delayed response to your inquiry. On January 5, 2017, I submitted the accompanying report to MS-ISAC NCCIC Partner Liaison Center for Internet Security, and I was assured that information successfully delivered to all affected organizations including Postal Regulatory Commission.  
  
The report includes the identified SQLi vulnerability, which was offered for sale by the Russian cybercriminal known as Rasputin. In the case, you have any follow-up questions, please don't hesitate to reach out to us at any time.

Respectfully,

**Andrei Barysevich**  
*Director of Advanced Collection*

Recorded Future  
+1 347 439 9330  
[andrei@recordedfuture.com](mailto:andrei@recordedfuture.com)  
[LinkedIn](#) | [Twitter](#)

---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

**ABRAMS, RUTH A**

---

**From:** ABRAMS, RUTH A  
**Sent:** Thursday, February 16, 2017 1:40 PM  
**To:** ADAMS, GAIL Z; FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,  
Thank you for the source information. We will look it over. However, the IT team scanned the system and no vulnerability was identified.  
Ruth Ann

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 1:39 PM  
**To:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

All,  
  
See the information and attachment I received from the source:  
  
Hello Mr.Adams,  
  
My name is (b) (6) and I'd like to apologize for the delayed response to your inquiry. On January 5, 2017, I submitted the accompanying report to MS-ISAC NCCIC Partner Liaison Center for Internet Security, and I was assured that information successfully delivered to all affected organizations including Postal Regulatory Commission.

The report includes the identified SQLi vulnerability, which was offered for sale by the Russian cybercriminal known as Rasputin. In the case, you have any follow-up questions, please don't hesitate to reach out to us at any time.

Respectfully,

(b) (6)



---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
Ann

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

**From:** it-services On Behalf Of (b) (6)  
**Sent:** Thursday, February 16, 2017 10:16 AM  
**To:** PRC-PAGR  
**Subject:** Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:  
Submitted values are:

message type: Question

Subject : Postal Regulatory Commission

First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number (b) (6)

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: 22314

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

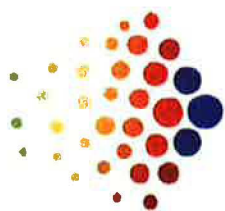
Thanks very much.

Best,

(b) (6)

**CONFIDENTIAL**

(b) (6)



**Recorded Future**



## **Executive Summary**

(b) (6)



**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 10:15 AM  
**To:** soc@us-cert.gov  
**Cc:** Support  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

**Importance:** High

Greeting SOC,

Just following up on my earlier message regarding subject incident. Please advise if you require any follow on actions.

Regards, Lee

---

A. Lee Martin  
Info Tech Manager  
Postal Regulatory Commission  
901 New York Ave., NW Ste 200 W  
Washington, DC 20268  
Office: (202) 789-5470  
Cell: (202) 816-9027

-----Original Message-----

**From:** Martin, Lee  
**Sent:** Tuesday, January 24, 2017 3:07 PM  
**To:** soc@us-cert.gov  
**Cc:** Support <support@prc.gov>; RUBLE, STACY L <stacy.ruble@prc.gov>  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

Greetings SOC,

I apologize for the delay in responding. In response to the subject incident, PRC IT staff have taken the following actions:

- 1) Scanned the website for all known vulnerabilities
- 2) Scanned the website using (b) (5) for web site scan policy template
- 3) Scanned the website using (b) (5)

All above scan reports show no vulnerabilities related to SQLi as reported. Additionally, our MTIPs perimeter defense has not detected any traffic that would indicate a SQLi type vulnerability - inbound or outbound.

At this point, we have completed our analysis and find no evidence of an intrusion or referenced vulnerability. Please let me know if US CERT requires any further action from the PRC.

Thanks,  
Lee

---

A. Lee Martin  
Info Tech Manager  
Postal Regulatory Commission  
901 New York Ave., NW Ste 200 W  
Washington, DC 20268  
Office: (202) 789-5470  
Cell: (202) 816-9027

-----Original Message-----

From: [Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov) [mailto:[Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov)]  
Sent: Tuesday, January 10, 2017 1:11 PM  
To: Support <[support@prc.gov](mailto:support@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
Cc: [Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov)  
Subject: US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration Center  
(NCCIC) Department of Homeland Security  
888-282-0870

SOC@us-cert.gov  
www.us-cert.gov  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: [Christine.sahlin@us-cert.gov](mailto:Christine.sahlin@us-cert.gov)

**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 24, 2017 3:07 PM  
**To:** soc@us-cert.gov  
**Cc:** Support; RUBLE, STACY L  
**Subject:** RE: US-CERT Incident number INC000010106204 PRC

Greetings SOC,

I apologize for the delay in responding. In response to the subject incident, PRC IT staff have taken the following actions:

- 1) Scanned the website for all known vulnerabilities
- 2) Scanned the website using (b) (5) for web site scan policy template
- 3) Scanned the website using (b) (5)

All above scan reports show no vulnerabilities related to SQLi as reported. Additionally, our MTIPs perimeter defense has not detected any traffic that would indicate a SQLi type vulnerability - inbound or outbound.

At this point, we have completed our analysis and find no evidence of an intrusion or referenced vulnerability. Please let me know if US CERT requires any further action from the PRC.

Thanks,  
Lee

---

A. Lee Martin  
Info Tech Manager  
Postal Regulatory Commission  
901 New York Ave., NW Ste 200 W  
Washington, DC 20268  
Office: (202) 789-5470  
Cell: (202) 816-9027

-----Original Message-----

**From:** Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
**Sent:** Tuesday, January 10, 2017 1:11 PM  
**To:** Support <support@prc.gov>; Martin, Lee <Lee.Martin@prc.gov>  
**Cc:** Christine.Sahlin@us-cert.gov  
**Subject:** US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)

(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration Center  
(NCCIC) Department of Homeland Security  
888-282-0870  
[SOC@us-cert.gov](mailto:SOC@us-cert.gov)  
[www.us-cert.gov](http://www.us-cert.gov)  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: [Christine.sahlin@us-cert.gov](mailto:Christine.sahlin@us-cert.gov)

**ABRAMS, RUTH A**

---

**From:** Brian A. Lemaster <lemaster@tecodo.com>  
**Sent:** Tuesday, January 10, 2017 2:08 PM  
**To:** Support; Martin, Lee  
**Subject:** Re: US-CERT Incident number INC000010106204 PRC

Will do

[Get Outlook for iOS](#)

---

**From:** Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Sent:** Tuesday, January 10, 2017 2:07:09 PM  
**To:** Support  
**Subject:** FW: US-CERT Incident number INC000010106204 PRC

All,

I've been working with US CERT to get their incident notifications sent to the support group. That said, I've requested more information concerning this incident. The info below is vague, so let's hope they respond with something more meaning full that we can act on.

(b) (5)



I'll let you know once I get more info.

Thanks,  
Lee

-----Original Message-----

**From:** [Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov) [<mailto:Christine.Sahlin@us-cert.gov>]  
**Sent:** Tuesday, January 10, 2017 1:11 PM  
**To:** Support; Martin, Lee  
**Cc:** [Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov)  
**Subject:** US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)





(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration Center (NCCIC)  
Department of Homeland Security  
888-282-0870  
[SOC@us-cert.gov](mailto:SOC@us-cert.gov)  
[www.us-cert.gov](http://www.us-cert.gov)  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: [Christine.sahlin@us-cert.gov](mailto:Christine.sahlin@us-cert.gov)

**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 10, 2017 2:07 PM  
**To:** Support  
**Subject:** FW: US-CERT Incident number INC000010106204 PRC

All,

I've been working with US CERT to get their incident notifications sent to the support group. That said, I've requested more information concerning this incident. The info below is vague, so let's hope they respond with something more meaning full that we can act on.

(b) (5)



I'll let you know once I get more info.

Thanks,  
Lee

-----Original Message-----

From: [Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov) [mailto:[Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov)]

Sent: Tuesday, January 10, 2017 1:11 PM

To: Support; Martin, Lee

Cc: [Christine.Sahlin@us-cert.gov](mailto:Christine.Sahlin@us-cert.gov)

Subject: US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)



(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration Center  
(NCCIC) Department of Homeland Security

888-282-0870

[SOC@us-cert.gov](mailto:SOC@us-cert.gov)

[www.us-cert.gov](http://www.us-cert.gov)

Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,

Christine Sahlin

Incident Management Analyst

NCCIC Hunt & Incident Response Team

Desk: 850.452.6907

Email: [Christine.sahlin@us-cert.gov](mailto:Christine.sahlin@us-cert.gov)

**ABRAMS, RUTH A**

---

**From:** Christine.Sahlin@us-cert.gov  
**Sent:** Tuesday, January 10, 2017 1:11 PM  
**To:** Support; Martin, Lee  
**Cc:** Christine.Sahlin@us-cert.gov  
**Subject:** US-CERT Incident number INC000010106204 PRC

PRC,

(b) (5)



Respectfully,

US-CERT Security Operations Center (US-CERT SOC) National Cybersecurity & Communications Integration Center  
(NCCIC) Department of Homeland Security  
888-282-0870  
[SOC@us-cert.gov](mailto:SOC@us-cert.gov)  
[www.us-cert.gov](http://www.us-cert.gov)  
Twitter: @USCERT\_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: [Christine.sahlin@us-cert.gov](mailto:Christine.sahlin@us-cert.gov)

**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 10:09 AM  
**To:** Wang, Lily  
**Cc:** Brian A. Lemaster; ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

More documentation from MS on how to protect from SQL injections.

<https://msdn.microsoft.com/en-us/library/ms998271.aspx>

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily <lily.wang@prc.gov>  
**Cc:** Brian A. Lemaster <lemaster@tecodeo.com>; ABRAMS, RUTH A <ruth.a.abrams@prc.gov>  
**Subject:** Potential Website Vulnerability  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. He is a link that will help you determine the right and wrong way to make data base calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee

**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily  
**Cc:** Brian A. Lemaster; ABRAMS, RUTH A  
**Subject:** Potential Website Vulnerability  
**Attachments:** The Postal Regulatory Commission Report.pdf  
  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. Here is a link that will help you determine the right and wrong way to make database calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee



**ABRAMS, RUTH A**

---

**From:** Wang, Lily  
**Sent:** Friday, February 17, 2017 10:26 AM  
**To:** Martin, Lee  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

Lee,

(b) (5)

Thanks

Lily

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily  
**Cc:** Brian A. Lemaster; ABRAMS, RUTH A  
**Subject:** Potential Website Vulnerability  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. Here is a link that will help you determine the right and wrong way to make data base calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee

**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 10:34 AM  
**To:** Wang, Lily  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

Lily,

(b) (5)

Please take care of this ASAP.

Thank You

**From:** Wang, Lily  
**Sent:** Friday, February 17, 2017 10:26 AM  
**To:** Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>  
**Subject:** RE: Potential Website Vulnerability

Lee,

(b) (5)

Thanks

Lily

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily  
**Cc:** Brian A. Lemaster; ABRAMS, RUTH A  
**Subject:** Potential Website Vulnerability  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. He is a link that will help you determine the right and wrong way to make data base calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee

**ABRAMS, RUTH A**

---

**From:** Wang, Lily  
**Sent:** Friday, February 17, 2017 10:38 AM  
**To:** Martin, Lee  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

Lee,

(b) (5)

Lily

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 10:34 AM  
**To:** Wang, Lily  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

Lily,

(b) (5)

Please take care of this ASAP.

Thank You

**From:** Wang, Lily  
**Sent:** Friday, February 17, 2017 10:26 AM  
**To:** Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>  
**Subject:** RE: Potential Website Vulnerability

Lee,

(b) (5)

Thanks

Lily

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily

**Cc:** Brian A. Lemaster; ABRAMS, RUTH A  
**Subject:** Potential Website Vulnerability  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. Here is a link that will help you determine the right and wrong way to make data base calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee

**ABRAMS, RUTH A**

---

**From:** Brian A. Lemaster <lemaster@tecodo.com>  
**Sent:** Friday, February 17, 2017 11:03 AM  
**To:** Martin, Lee; Wang, Lily  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

(b) (5)



Brian A. Lemaster  
Chief Technology Officer  
Tecodo, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, Virginia 20171  
Direct: +1 571.388.7106  
Office: +1 703.788.6704  
<http://www.tecodo.com>

*This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.*

**From:** Martin, Lee [<mailto:Lee.Martin@prc.gov>]  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily <[lily.wang@prc.gov](mailto:lily.wang@prc.gov)>  
**Cc:** Brian A. Lemaster <lemaster@tecodo.com>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>  
**Subject:** Potential Website Vulnerability  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. He is a link that will help you determine the right and wrong way to make data base calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee



**ABRAMS, RUTH A**

---

**From:** Wang, Lily  
**Sent:** Friday, February 17, 2017 12:01 PM  
**To:** Brian A. Lemaster; Martin, Lee  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

Lee,  
Here is updates.

1. SQL select statement on (b) (5) was correct, I did not find any miscodes.

(b) (5)



Continue working and will keep you updates. Thanks

Brian, Thank you for the inputting.

Lily

---

**From:** Brian A. Lemaster [<mailto:lemaster@tecodo.com>]  
**Sent:** Friday, February 17, 2017 11:03 AM  
**To:** Martin, Lee; Wang, Lily  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

(b) (5)



Brian A. Lemaster  
Chief Technology Officer  
Tecodo, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, Virginia 20171  
Direct: +1 571.388.7106  
Office: +1 703.788.6704  
<http://www.tecodo.com>

*This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.*

**From:** Martin, Lee [mailto:Lee.Martin@prc.gov]  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily <lily.wang@prc.gov>  
**Cc:** Brian A. Lemaster <lemaster@tecodo.com>; ABRAMS, RUTH A <ruth.a.abrams@prc.gov>  
**Subject:** Potential Website Vulnerability  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. Here is a link that will help you determine the right and wrong way to make data base calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee

**ABRAMS, RUTH A**

---

**From:** Wang, Lily  
**Sent:** Friday, February 17, 2017 4:38 PM  
**To:** Martin, Lee  
**Cc:** ABRAMS, RUTH A; Brian A. Lemaster  
**Subject:** RE: Potential Website Vulnerability

Lee,

(b) (5)



Thank you for patience.

Lily

---

**From:** Wang, Lily  
**Sent:** Friday, February 17, 2017 12:01 PM  
**To:** Brian A. Lemaster; Martin, Lee  
**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

Lee,

Here is updates.

1. SQL select statement on (b) (5) was correct, I did not find any miscodes.

(b) (5)



Continue working and will keep you updates. Thanks

Brian, Thank you for the inputting.

Lily

---

**From:** Brian A. Lemaster [<mailto:lemaster@tecodo.com>]  
**Sent:** Friday, February 17, 2017 11:03 AM  
**To:** Martin, Lee; Wang, Lily

**Cc:** ABRAMS, RUTH A  
**Subject:** RE: Potential Website Vulnerability

(b) (5)



Brian A. Lemaster  
Chief Technology Officer  
Tecodo, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, Virginia 20171  
Direct: +1 571.388.7106  
Office: +1 703.788.6704  
<http://www.tecodo.com>

*This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.*

**From:** Martin, Lee [<mailto:Lee.Martin@prc.gov>]  
**Sent:** Friday, February 17, 2017 9:50 AM  
**To:** Wang, Lily <[lily.wang@prc.gov](mailto:lily.wang@prc.gov)>  
**Cc:** Brian A. Lemaster <[lemaster@tecodo.com](mailto:lemaster@tecodo.com)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>  
**Subject:** Potential Website Vulnerability  
**Importance:** High

Lily, our web site is being reported by the media as being vulnerable to a SQL injection vulnerability. We've scanned our website using (b) (5) and have not identified that this vulnerability exists, however we need to validate these results by every means possible. So, I need you look through the web site source code and verify that all database queries are parameterized. Here is a link that will help you determine the right and wrong way to make data base calls:

<https://blog.codinghorror.com/give-me-parameterized-sql-or-give-me-death/>

Scan (b) (5) this page first as it was identified as being SQLi vulnerable in the attached report and let me know what you find out. Once you completed that page, please proceed with all other DB calls throughout the web site. This is high priority and needs to be completed ASAP.

Please let me know if you have any problems accomplishing this request.

Thx, Lee

**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Friday, January 06, 2017 11:38 AM  
**To:** RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: DHS info

Stacy,

Still haven't received anything from the Incident Response staff from DHS. The person that called yesterday told me that they will contact me by the end of today once the report has been completed. I will contact them this afternoon.

Lee

---

**From:** RUBLE, STACY L  
**Sent:** Friday, January 06, 2017 11:34 AM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Subject:** DHS info

Lee, Ruth Ann, what came of the DHS information you were to receive yesterday?  
Thanks, Stacy

Stacy L. Ruble  
Secretary and Chief Administrative Officer

**Postal Regulatory Commission**

901 New York Ave NW – Suite 200 W – Washington, DC 20268  
202.789.6800 [stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)

*Notice:* This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.



**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Friday, January 06, 2017 2:23 PM  
**To:** RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: DHS info

Stacy, Ruth Ann,

Followed up with my DHS contact just now and the notification is still scheduled to go out via email by COB today. It is now pending DHS Sr. Leadership approval before being distributed. Again, they aren't allowed to talk details over the phone, but she did say that this incident affected 30 + agencies and that is not considered catastrophic. Basically, once notified, we'll need to do forensics, review logs, scans looking for traces\impact of the details in the report and next steps should we have been compromised.

(b) (5)



I'll let you know the min. I hear something and am able to analyze their report. Let me know if there are any questions.

Thanks,  
Lee

---

**From:** RUBLE, STACY L  
**Sent:** Friday, January 06, 2017 11:38 AM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Subject:** RE: DHS info

thanks

---

**From:** Martin, Lee  
**Sent:** Friday, January 06, 2017 11:38 AM  
**To:** RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: DHS info

Stacy,

Still haven't received anything from the Incident Response staff from DHS. The person that called yesterday told me that they will contact me by the end of today once the report has been completed. I will contact them this afternoon.

Lee

---

**From:** RUBLE, STACY L  
**Sent:** Friday, January 06, 2017 11:34 AM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Subject:** DHS info

Lee, Ruth Ann, what came of the DHS information you were to receive yesterday?  
Thanks, Stacy

Stacy L. Ruble  
Secretary and Chief Administrative Officer



**Postal Regulatory Commission**

901 New York Ave NW – Suite 200 W – Washington, DC 20268  
202.789.6800 [stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)

*Notice:* This transmission may be privileged and may contain confidential information intended only for the person(s) named above. Any other distribution, re-transmission, copying or disclosure is strictly prohibited. If you have received this transmission in error, please notify me immediately by telephone or return email and delete this file from your system.



**ABRAMS, RUTH A**

---

**From:** Martin, Lee  
**Sent:** Tuesday, January 10, 2017 3:40 PM  
**To:** Christine.Sahlin@us-cert.gov; ABRAMS, RUTH A  
**Cc:** soc@us-cert.gov; jonathan.homer@hq.dhs.gov  
**Subject:** RE: INC000010106204 PRC

Thank you for the follow up information Christine, we will scan our system for SQL injection vulnerabilities and follow up with the SOC once completed.

-----Original Message-----

**From:** Christine.Sahlin@us-cert.gov [mailto:Christine.Sahlin@us-cert.gov]  
**Sent:** Tuesday, January 10, 2017 3:00 PM  
**To:** Martin, Lee; ABRAMS, RUTH A  
**Cc:** soc@us-cert.gov; jonathan.homer@hq.dhs.gov  
**Subject:** RE: INC000010106204 PRC

Mr. Martin,

The vulnerable path represents that there is a possible SQL injection vulnerability on that website link.

Here are links to US-CERT documents regarding SQL injection vulnerabilities:

<https://www.us-cert.gov/security-publications/sql-injection>

<https://www.us-cert.gov/security-publications/practical-identification-sql-injection-vulnerabilities-0>

RS,  
Christine Sahlin  
Incident Management Analyst  
NCCIC Hunt & Incident Response Team  
Desk: 850.452.6907  
Email: [Christine.sahlin@us-cert.gov](mailto:Christine.sahlin@us-cert.gov)

-----Original Message-----

**From:** Martin, Lee [mailto:Lee.Martin@prc.gov]  
**Sent:** Tuesday, January 10, 2017 12:39 PM  
**To:** SOC  
**Cc:** ABRAMS, RUTH A  
**Subject:** Ref: INC000010106204 PRC

Greetings SOC,

I have received notification for the above ref. security incident and have several questions before I can proceed:

(b) (5)



Thanks,

Lee

---

A. Lee Martin

Info Tech Manager

Postal Regulatory Commission

901 New York Ave., NW Ste 200 W

Washington, DC 20268

Office: (202) 789-5470

Cell: (202) 816-9027

**RUBLE, STACY L**

---

**From:** ABRAMS, RUTH A  
**Sent:** Tuesday, January 10, 2017 4:01 PM  
**To:** RUBLE, STACY L  
**Cc:** Martin, Lee  
**Subject:** DHS notification - SQL injection vulnerability

Stacy,

We received the promised notification from DHS. An issue was found at another agency, which prompted them to scan all agencies for the vulnerability. We were notified that we may have a SQL injection vulnerability (which means that we may be vulnerable to having malicious code injected into our system through the website).

Lee and Brian are scanning the website to look for any SQL injections using the tools we currently have. Lee will let us know if we need to procure any additional tools. We estimate that we can close out this notification within 2 weeks. It is a priority items so may be closed out sooner than this.

With kindest regards,

Ruth Ann Abrams  
Deputy Secretary



**Postal Regulatory Commission**

901 New York Ave NW – Suite 200 W – Washington, DC 20268  
202.789.6843 – [ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)

**RUBLE, STACY L**

---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 10:56 AM  
**To:** TAUB, ROBERT G; RUBLE, STACY L  
**Cc:** ADAMS, GAIL Z; BOSTON, APRIL E  
**Subject:** FYI: Article reporting we were hacked by Russian

## The Recorded Future Blog

### Russian-Speaking Hacker Breaches Over 60 Universities and Government Agencies

Posted in

- [Cyber Threat Intelligence](#)

by Levi Gundert on February 15, 2017

#### Key Takeaways

- Rasputin's latest victims include over 60 (combined total) prominent universities and federal, state, and local U.S. government agencies.
- Rasputin, a Russian-speaking and notorious financially-motivated cyber criminal, continues to locate and exploit vulnerable web applications via a proprietary SQL Injection (SQLi) tool.
- In November 2016, Rasputin penetrated the U.S. Election Assistance Commission (EAC) via SQLi.
- 15 plus years of SQLi attacks, and going strong; this prolific vulnerability remains one of the most popular exploits for opportunistic actors due to its ongoing success rate.
- Economic incentives are required to change the behavior that facilitates SQLi vulnerabilities either through penalties established by government regulations (sticks) or tax abatement incentives (carrots) for compliance.

In December 2016, Recorded Future collaborated with law enforcement on the [U.S. Election Assistance Commission \(EAC\) hack and subsequent database sale](#) — committed by an actor Recorded Future named Rasputin.

The EAC database breach was the result of SQL Injection (SQLi), an attack that is technically easy, but expensive to defend. Recorded Future continues to monitor Rasputin's campaigns, which are now sequentially targeting specific industry

verticals. These are intentional targets of choice based on the organization's perceived investment in security controls and the respective compromised data value. Additionally, these databases are likely to contain significant quantities of users and potentially associated personally identifiable information (PII).

Rasputin's latest victims include the following U.S. government and international universities. Recorded Future notified all of the below organizations with relevant breach details.



Geographic locations of Rasputin's latest U.S. education and government victims.

## U.S. University Victims

- Cornell University
- VirginiaTech
- University of Maryland, Baltimore County
- University of Pittsburgh
- New York University
- Rice University
- University of California, Los Angeles
- Eden Theological Seminary

- Arizona State University
- NC State University
- Purdue University
- Atlantic Cape Community College
- University of the Cumberlands
- Oregon College of Oriental Medicine
- University of Delhi
- Humboldt State University
- The University of North Carolina at Greensboro
- University of Mount Olive
- Michigan State University
- Rochester Institute of Technology
- University of Tennessee
- St. Cloud State University
- University of Arizona
- University at Buffalo
- University of Washington

## **UK University Victims**

- University of Cambridge
- University of Oxford
- Architectural Association School of Architecture
- University of Chester
- University of Leeds
- Coleg Gwent
- University of Glasgow
- University of the Highlands and Islands
- University of the West of England
- The University of Edinburgh

## **U.S. Government Victims (Cities)**

- City of Springfield, Massachusetts
- City of Pittsburgh, Pennsylvania
- Town of Newtown, Connecticut
- City of Alexandria, Virginia
- City of Camden, Arkansas
- City of Sturgis, Michigan

## **U.S. Government Victims (States)**

- Texas Board of Veterinary Medical Examiners
- Oklahoma State Department of Education
- The South Carolina Public Employee Benefit Authority
- Rhode Island Department of Education
- District Columbia Office of Contracting and Procurement
- District Columbia Office of the Chief Financial Officer
- Alaska Department of Natural Resources
- County of Santa Rosa, Florida
- York County, Pennsylvania
- Virginia Department of Environmental Quality
- State of Oklahoma
- Alaska Division of Retirement and Benefits

- Louisiana Department of Education
- Madison County, Alabama
- Washington State Arts Commission
- West Virginia Department of Environmental Protection

## **Federal Agencies**

- Postal Regulatory Commission
- U.S. Department of Housing and Urban Development
- Health Resources and Services Administration
- National Oceanic and Atmospheric Administration

## **Other**

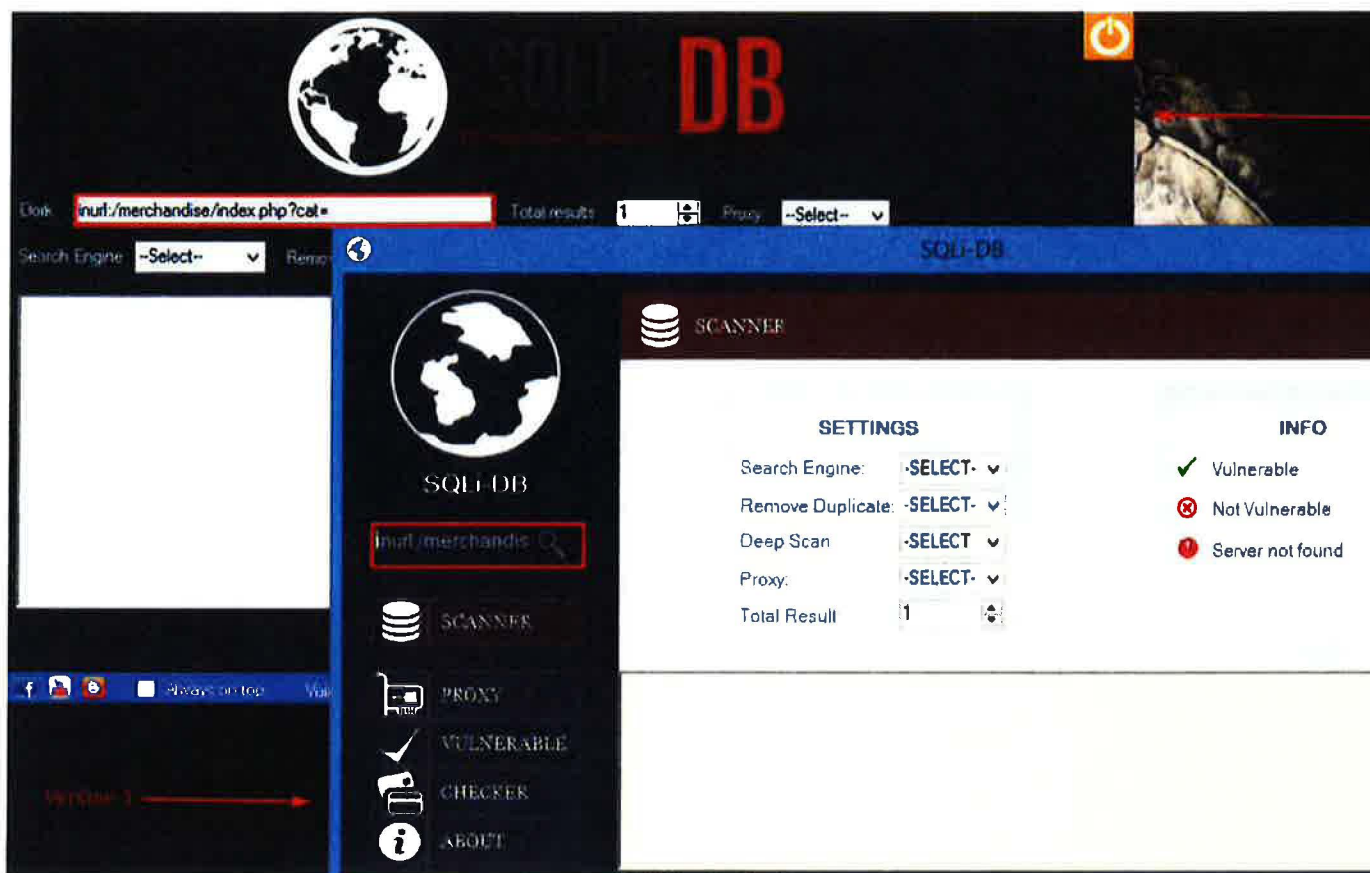
- Fermi National Accelerator Laboratory
- Child Welfare Information Gateway

## **What's the Deal With SQLi?**

SQL injection has been around since databases first appeared on the internet.

When a user is allowed to interact directly with a database, through an application in a web browser, without checking or sanitizing the input before the database executes the instruction(s), a SQL injection vulnerability exists.



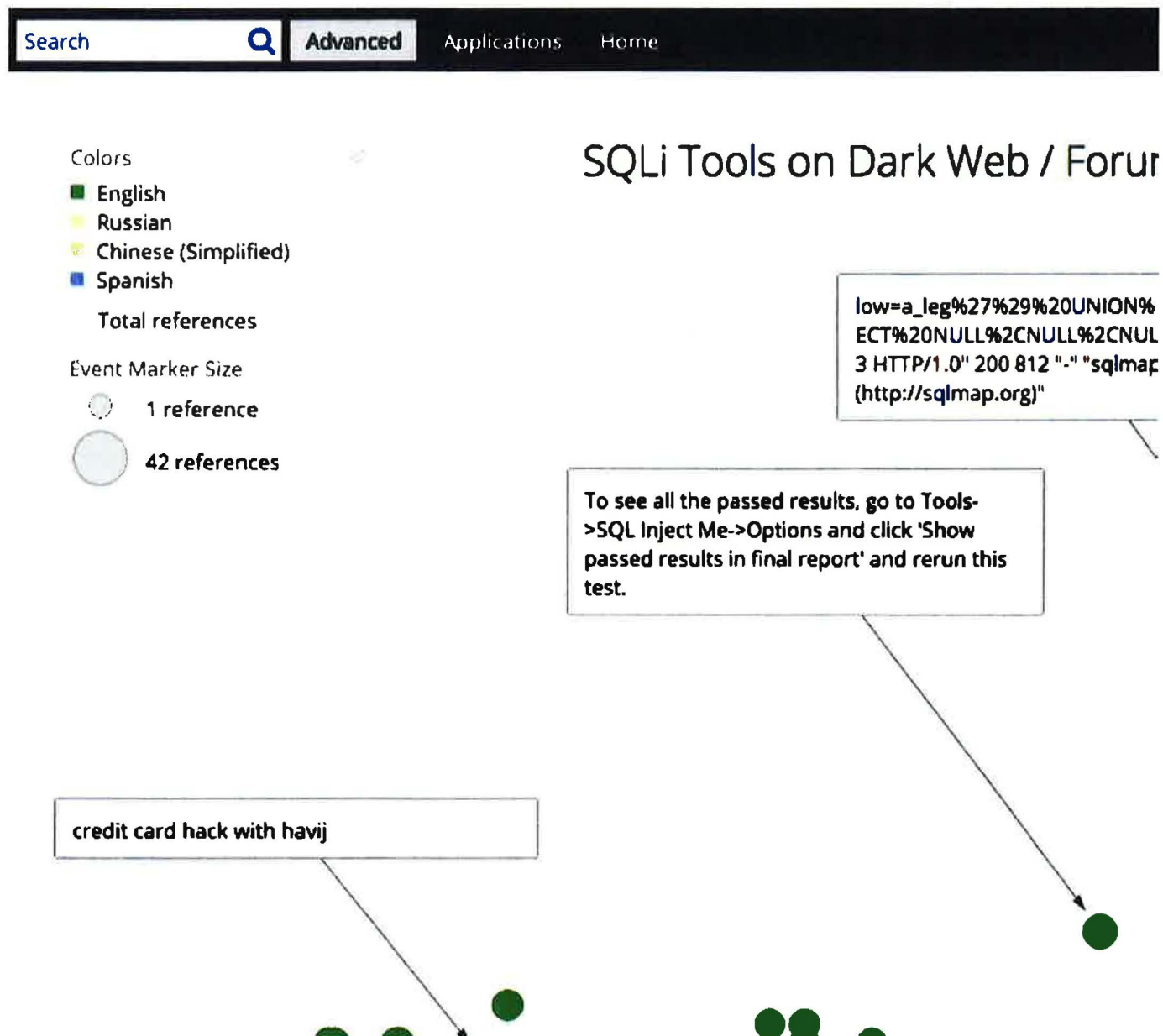


Opportunistic threat actors don't need any specific technical knowledge or skill to find vulnerable websites. Free tools — like Havij, Ashiyane SQL Scanner, SQL Exploiter Pro, SQLi Hunter, SQL Inject Me, SQLmap, SQLSentinel, SQLninja, etc. — automate the identification and exploitation of vulnerable websites and associated databases through “point and click” menus.

These SQLi scanners help security teams find SQL flaws, but they also help adversaries find the the same flaws.

Rasputin is an outlier in that he's allegedly using a proprietary SQLi tool that he developed himself. Financial profits motivate actors like Rasputin, who have

technical skills to create their own tools to outperform the competition in both identifying and exploiting vulnerable databases. North American and Western European databases contain information on customers or users that are historically valued at a premium in the underground economy. Buyer demand typically centers on access to American, Canadian, or UK database access.



A recent example of a SQLi scanner's results appeared at [pastebin.com/Qzjs8iKt](https://pastebin.com/Qzjs8iKt) (recently deleted, but always available in Recorded Future). Here's a sample of the file (select details redacted to protect potentially uninformed victims):

#### Cached Document

Title Untitled  
Author A Guest  
Downloaded Jan 22, 2017, 23:54  
Original URL <http://pastebin.com/Qzjs8iKt>

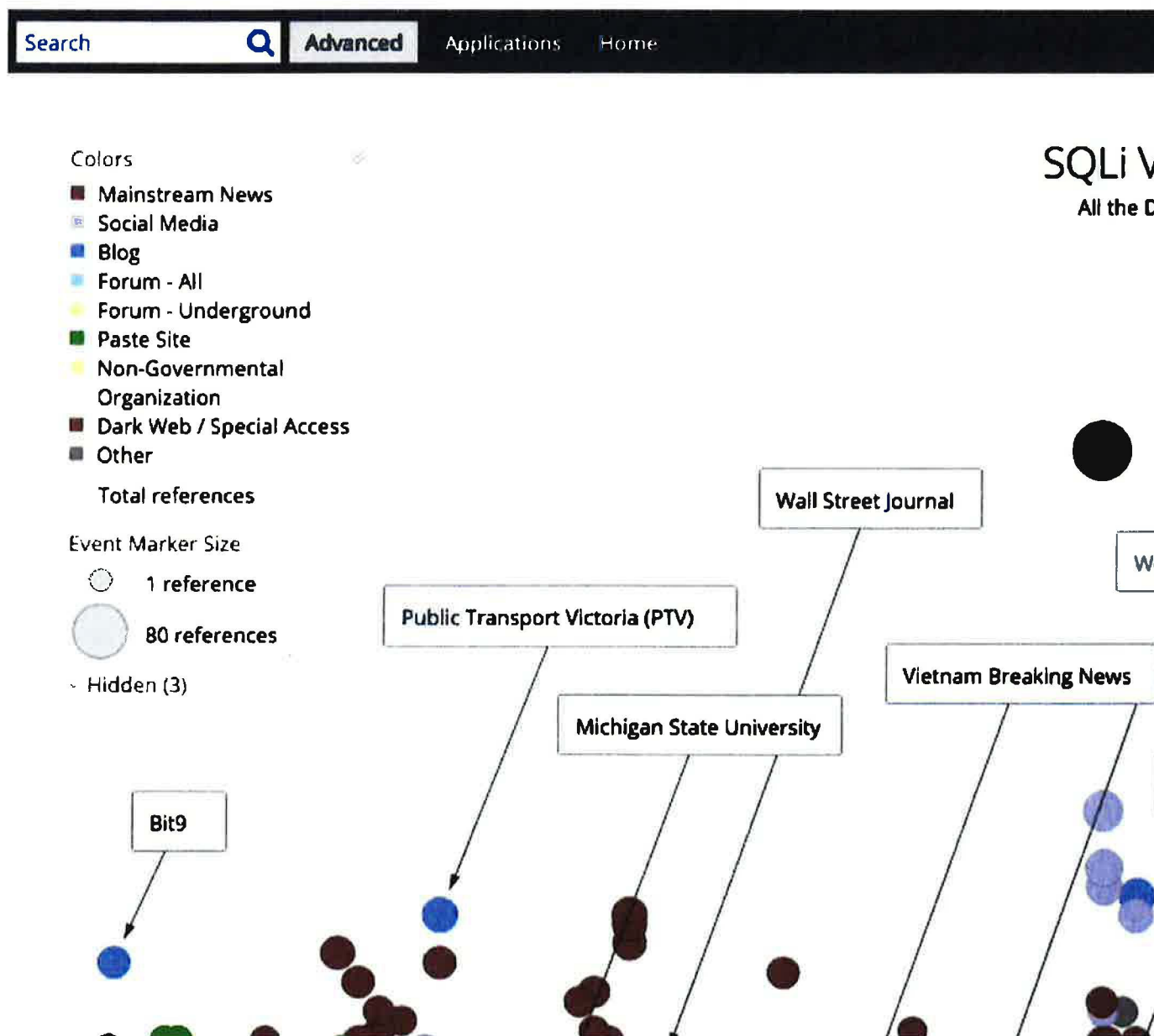
☰ ☰ Translate All

```
1. [ SQL VULN FOUND ] http://      mea.com/site/index.php/site/SupportResource?pic
2. [ SQL VULN FOUND ] http://      .net/647/c7ev_sid=10&ev_ltx=sl:Fremdsprachen lerne
3. [ SQL VULN FOUND ] http://      xt.com/file-extension/ASP%27
4. [ SQL VULN FOUND ] http://      foods.com/en/chicken_detail.asp?productID
5. [ SQL VULN FOUND ] http://      posture.com/_site/products.php?cat=04%27
6. [ SQL VULN FOUND ] http://[ POSSIBLE BLIND ] http://www.      avej.com/index.php;
7. [ SQL VULN FOUND ] http://      gold.com/PG_compare/compare.asp?PG_lng=GB%27
8. [ SQL VULN FOUND ] http://      ntik.com/visprodukt.asp?id=8465&katId=2%27
9. [ SQL VULN FOUND ] http://      ntik.com/visprodukt.asp?id=8470&katId=3%27
10. [ SQL VULN FOUND ] http://      ntik.com/visprodukt.asp?id=8473&katId=3%27
11. [ SQL VULN FOUND ] https://      ports.com/websiteinfo.asp?CartId={2D6F4E-
12. [ SQL VULN FOUND ] http://      .      ano.com/php/download.php?file=pdf/dm/DM-FD000
13. [ SQL VULN FOUND ] http://      .      ano.com/php/download.php?file=pdf/dm/DM-SG000
14. [ SQL VULN FOUND ] http://      .      ano.com/php/download.php?file=pdf/dm/DM-WH000
15. [ SQL VULN FOUND ] https://secure.      -ichiba.com/top/cart/asp/cart.asp;
16. [ SQL VULN FOUND ] https://www.      fense.com/cart/addtocart.asp?cartid=125%27
17. [ SQL VULN FOUND ] https://www.      ec.com/Home/Index%27
18. [ SQL VULN FOUND ] https://_      phin.com/%27
19. [ SQL VULN FOUND ] http://testphp.      b.com/listproducts.php?cat=1%27
```

Amazingly, SQLi vulnerabilities are simple to prevent through coding best practices.

[Over 15 years of high-profile data breaches](#) have done little to prevent poorly programmed web applications and/or third-party software from being used by government, enterprises, and academia. Some of the most publicized data breaches were the result of SQLi including large corporations like Heartland Payment Systems, HBGary Federal, Yahoo!, LinkedIn, etc.

The evidence suggests economics play a role in causation for this troubling trend. The problem and solution are well understood, but solutions may require expensive projects to improve or replace vulnerable systems. These projects are often postponed until time and/or budget is available, until it's too late to prevent SQLi victimization.



Where Do We Go From Here?



Until organizations have an incentive (carrots or sticks) to properly audit internal and vendor code before production use, this problem will continue into the foreseeable future.

Raising awareness among developers is worthwhile and [OWASP](#) continues to perform a valuable community service through education, but eradicating SQLi vulnerabilities will likely require stiff penalties for inaction. An opt-in program for partial corporate tax abatement could be a starting point. Program participation should require quarterly code audits by an approved vendor. Robust governance, risk, and compliance (GRC) programs (e.g., financial services companies) already mandate periodic code reviews, but all verticals need some type of incentive regardless of specific industry regulations. Unfortunately, government fines and/or loss from lawsuits may be the only incentives to prioritize code audits.

## Conclusion

Cyber criminals continue to find, exploit, and sell access to vulnerable databases, targeting web applications by industry vertical, as demonstrated by Rasputin's latest victims. Even the most prestigious universities and U.S. government agencies are not immune to SQLi vulnerabilities.

This well established, but easy-to-remediate problem (though often costly), continues to vex public and private sector organizations. Economics must be addressed to fully eradicate this issue. Despite the government's penchant for

employing sticks to modify behavior, perhaps it's time to offer financial carrots to address and fully eradicate this issue.

Trending Threat Insights Delivered to Your Inbox for Free

CYBER DAILY  
Over 23,000 Subscribers

Sign up for the Cyber Daily and receive trending threat insights every day by email.

- Top Threat Actors
- Top Vulnerabilities
- Top Malware
- Top Suspicious IP Addresses

SUBSCRIBE

CYBER DAILY  
Over 23,000 Subscribers

Trending Threat Insights Delivered to Your Inbox for Free

SUBSCRIBE

RSS Twitter Facebook LinkedIn YouTube Google+

#### Recent Posts

- [Russian-Speaking Hacker Breaches Over 60 Universities and Government Agencies](#)By Levi Gundert on February 15, 2017
- [Combining Technical, Open, and Dark Web Sources of Threat Intelligence for the First Time](#)By Nagraj Seshadri on February 13, 2017
- [Fall in Love With Threat Intelligence at RSA](#)By RFSID on February 10, 2017
- [Why Threat Intelligence Teams Fail \(And What You Can Do About It\)](#)By RFSID on February 9, 2017
- [6 Corporate Security Risks Where Threat Intelligence Can Help](#)By RFSID on February 7, 2017

#### Company

- 
- 
- 
- 
- 

#### For Customers

**Ann Fisher**  
**Director, Public Affairs & Government Relations**  
Postal Regulatory Commission  
901 New York Avenue, NW  
Suite 200  
Washington, DC 20268-0001  
Telephone: 202-789-6803  
Ann.Fisher@prc.gov  
www.prc.gov

NOTICE: This e-mail message and any attachments transmitted with it contains confidential and proprietary information intended solely for the use of the addressee in its interactions with the Postal Regulatory Commission.



**RUBLE, STACY L**

---

**From:** ADAMS, GAIL Z  
**Sent:** Friday, February 17, 2017 9:05 AM  
**To:** RUBLE, STACY L; ABRAMS, RUTH A; Martin, Lee  
**Cc:** FISHER, ANN C  
**Subject:** FW: Google Alert - Postal Regulatory Commission

This story is spreading. See Infosecurity Magazine article below. Do we have a response for the reporter who originally inquired?

---

**From:** Google Alerts [<mailto:googlealerts-noreply@google.com>]  
**Sent:** Friday, February 17, 2017 9:02 AM  
**To:** ADAMS, GAIL Z  
**Subject:** Google Alert - Postal Regulatory Commission

Google Alerts

## Postal Regulatory Commission

Daily update · February 17, 2017

NEWS

### Hacker 'Rasputin' Probes Top Unis and Governments for SQLi Bugs

Infosecurity Magazine

Victims include the universities of Oxford and Cambridge as well as the US **Postal Regulatory Commission** and National Oceanic and Atmospheric ...



Flag as irrelevant

You have received this email because you have subscribed to **Google Alerts**.

[Unsubscribe](#)



Receive this alert as RSS feed

[Send Feedback](#)

**RUBLE, STACY L**

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 2:13 PM  
**To:** ABRAMS, RUTH A; FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Ruth Ann,

I'm not sure what the source information mean that was given to us. Can you please draft me a response so that I can apply to the reporter that made the original inquiry.

Thank you!

---

**From:** ABRAMS, RUTH A  
**Sent:** Thursday, February 16, 2017 1:40 PM  
**To:** ADAMS, GAIL Z; FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,  
Thank you for the source information. We will look it over. However, the IT team scanned the system and no vulnerability was identified.  
Ruth Ann

---

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 1:39 PM  
**To:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

All,

See the information and attachment I received from the source:

Hello Mr.Adams,

My name is (b) (6) and I'd like to apologize for the delayed response to your inquiry. On January 5, 2017, I submitted the accompanying report to MS-ISAC NCCIC Partner Liaison Center for Internet Security, and I was assured that information successfully delivered to all affected organizations including Postal Regulatory Commission.

The report includes the identified SQLi vulnerability, which was offered for sale by the Russian cybercriminal known as Rasputin. In the case, you have any follow-up questions, please don't hesitate to reach out to us at any time.

Respectfully,

(b) (6)



---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
Ann

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

From: it-services On Behalf Of (b) (6)

Sent: Thursday, February 16, 2017 10:16 AM

To: PRC-PAGR

Subject: Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:

Submitted values are:

message type: Question

Subject : Postal Regulatory Commission

First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number (b) (6)

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)

**RUBLE, STACY L**

---

**From:** FISHER, ANN C  
**Sent:** Friday, February 17, 2017 9:26 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Google Alert - Postal Regulatory Commission

Thanks Lee. Could you or Ruth Ann boil that down to a sentence that Gail can share with the media?

---

**From:** Martin, Lee  
**Sent:** Friday, February 17, 2017 9:25 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Google Alert - Postal Regulatory Commission

All,

I did another vulnerability scan on the web site last night using plugins that the vendor recommended specifically to identify SQL injections and the results were negative. Also, I am looking for another SQL injection scanner to validate our internal results, but at this point I believe that this is a false positive. Our scans results did not show this vulnerability. The vulnerability scanner the Commission uses is an industry \ Gov't standard and is 1 of the tools being implemented Gov't wide under the CDM program. I have high confidence that we would have found it if it existed in our environment.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Friday, February 17, 2017 9:05 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Google Alert - Postal Regulatory Commission

This story is spreading. See Infosecurity Magazine article below. Do we have a response for the reporter who originally inquired?

---

**From:** Google Alerts [<mailto:googlealerts-noreply@google.com>]  
**Sent:** Friday, February 17, 2017 9:02 AM  
**To:** ADAMS, GAIL Z  
**Subject:** Google Alert - Postal Regulatory Commission

Google Alerts

## Postal Regulatory Commission

Daily update · February 17, 2017

NEWS

## Hacker 'Rasputin' Probes Top Unis and Governments for SQLi Bugs

Infosecurity Magazine

Victims include the universities of Oxford and Cambridge as well as the US Postal Regulatory Commission and National Oceanic and Atmospheric ...



Flag as irrelevant

You have received this email because you have subscribed to **Google Alerts**.

[Unsubscribe](#)



[Receive this alert as RSS feed](#)

[Send Feedback](#)



**FISHER, ANN C**

---

**From:** ABRAMS, RUTH A  
**Sent:** Friday, February 17, 2017 1:02 PM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** Re: Draft Response to reporter regarding hacking

Looks good. Thanks.

Sent from my iPhone

On Feb 17, 2017, at 12:39 PM, ADAMS, GAIL Z <[gail.adams@prc.gov](mailto:gail.adams@prc.gov)> wrote:

Thanks Ruth Ann. I just added the word "to" before "continues."

---

**From:** ABRAMS, RUTH A  
**Sent:** Friday, February 17, 2017 12:24 PM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; Martin, Lee; RUBLE, STACY L  
**Subject:** RE: Draft Response to reporter regarding hacking

See edit below. Thanks!

---

**From:** ADAMS, GAIL Z  
**Sent:** Friday, February 17, 2017 12:09 PM  
**To:** ABRAMS, RUTH A; Martin, Lee; RUBLE, STACY L  
**Cc:** FISHER, ANN C  
**Subject:** Draft Response to reporter regarding hacking

Ruth Ann,

Please review and let me know if OSA is ok with this response. Feel free to edit any way necessary.

Thank you

The Commission regularly scans all of its systems to identify and protect against potential vulnerabilities. Our internal controls have found no evidence of hacking to any of the Commission's systems. The Commission continues to harden its systems from malicious actors in order to protect the confidentiality, integrity, and availability of our information systems.

<image001.jpg>

**Gail Z. Adams**

Communications Specialist

Postal Regulatory Commission



**FISHER, ANN C**

---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 11:23 AM  
**To:** Martin, Lee; ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Gail,

Please contact (b) (6) the author of the article that says we were hacked, and let him know we found no evidence of this. See if he will provide you with the source name. It wasn't clear to me from the article.

Thanks,  
 Ann

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

From: it-services On Behalf Of (b) (6)

Sent: Thursday, February 16, 2017 10:16 AM

To: PRC-PAGR

Subject: Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:

Submitted values are:

message type: Question

Subject : Postal Regulatory Commission

First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number (b) (6)

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)

**FISHER, ANN C**

---

**From:** FISHER, ANN C  
**Sent:** Thursday, February 16, 2017 10:56 AM  
**To:** TAUB, ROBERT G (robert.taub@prc.gov); RUBLE, STACY L  
**Cc:** ADAMS, GAIL Z; BOSTON, APRIL E  
**Subject:** FYI: Article reporting we were hacked by Russian

## The Recorded Future Blog

### Russian-Speaking Hacker Breaches Over 60 Universities and Government Agencies

Posted in

- [Cyber Threat Intelligence](#)

by Levi Gundert on February 15, 2017

#### Key Takeaways

- Rasputin's latest victims include over 60 (combined total) prominent universities and federal, state, and local U.S. government agencies.
- Rasputin, a Russian-speaking and notorious financially-motivated cyber criminal, continues to locate and exploit vulnerable web applications via a proprietary SQL Injection (SQLi) tool.
- In November 2016, Rasputin penetrated the U.S. Election Assistance Commission (EAC) via SQLi.
- 15 plus years of SQLi attacks, and going strong; this prolific vulnerability remains one of the most popular exploits for opportunistic actors due to its ongoing success rate.
- Economic incentives are required to change the behavior that facilitates SQLi vulnerabilities either through penalties established by government regulations (sticks) or tax abatement incentives (carrots) for compliance.

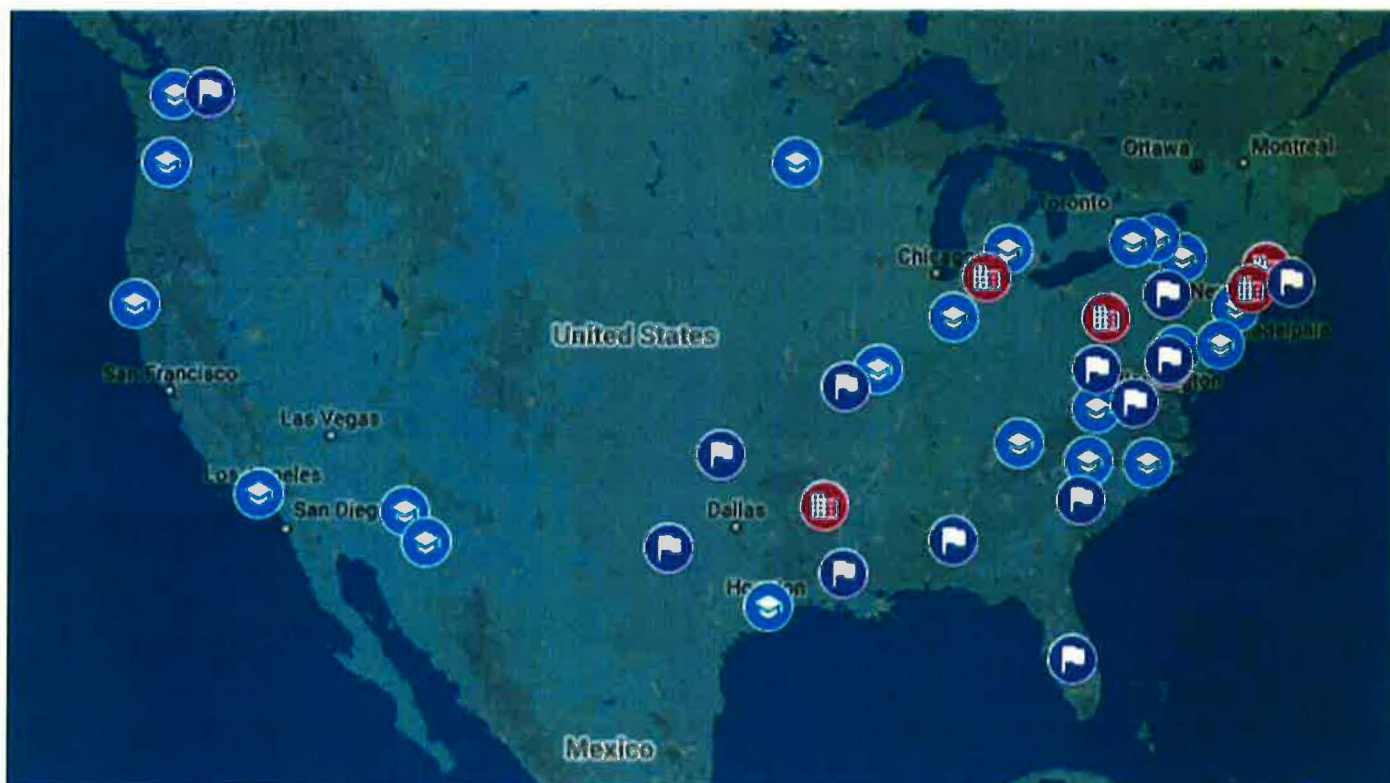
In December 2016, Recorded Future collaborated with law enforcement on the [U.S. Election Assistance Commission \(EAC\) hack and subsequent database sale](#) —

committed by an actor Recorded Future named Rasputin.

The EAC database breach was the result of SQL Injection (SQLi), an attack that is technically easy, but expensive to defend. Recorded Future continues to monitor Rasputin's campaigns, which are now sequentially targeting specific industry

verticals. These are intentional targets of choice based on the organization's perceived investment in security controls and the respective compromised data value. Additionally, these databases are likely to contain significant quantities of users and potentially associated personally identifiable information (PII).

Rasputin's latest victims include the following U.S. government and international universities. Recorded Future notified all of the below organizations with relevant breach details.



Geographic locations of Rasputin's latest U.S. education and government victims.

## U.S. University Victims

- Cornell University
- VirginiaTech
- University of Maryland, Baltimore County

- University of Pittsburgh
- New York University
- Rice University
- University of California, Los Angeles
- Eden Theological Seminary
- Arizona State University
- NC State University
- Purdue University
- Atlantic Cape Community College
- University of the Cumberland
- Oregon College of Oriental Medicine
- University of Delhi
- Humboldt State University
- The University of North Carolina at Greensboro
- University of Mount Olive
- Michigan State University
- Rochester Institute of Technology
- University of Tennessee
- St. Cloud State University
- University of Arizona
- University at Buffalo
- University of Washington

## **UK University Victims**

- University of Cambridge
- University of Oxford
- Architectural Association School of Architecture
- University of Chester
- University of Leeds
- Coleg Gwent
- University of Glasgow
- University of the Highlands and Islands
- University of the West of England
- The University of Edinburgh

## **U.S. Government Victims (Cities)**

- City of Springfield, Massachusetts
- City of Pittsburgh, Pennsylvania
- Town of Newtown, Connecticut
- City of Alexandria, Virginia
- City of Camden, Arkansas
- City of Sturgis, Michigan

## **U.S. Government Victims (States)**

- Texas Board of Veterinary Medical Examiners
- Oklahoma State Department of Education
- The South Carolina Public Employee Benefit Authority
- Rhode Island Department of Education
- District Columbia Office of Contracting and Procurement
- District Columbia Office of the Chief Financial Officer
- Alaska Department of Natural Resources

- County of Santa Rosa, Florida
- York County, Pennsylvania
- Virginia Department of Environmental Quality
- State of Oklahoma
- Alaska Division of Retirement and Benefits
- Louisiana Department of Education
- Madison County, Alabama
- Washington State Arts Commission
- West Virginia Department of Environmental Protection

## **Federal Agencies**

- Postal Regulatory Commission
- U.S. Department of Housing and Urban Development
- Health Resources and Services Administration
- National Oceanic and Atmospheric Administration

## **Other**

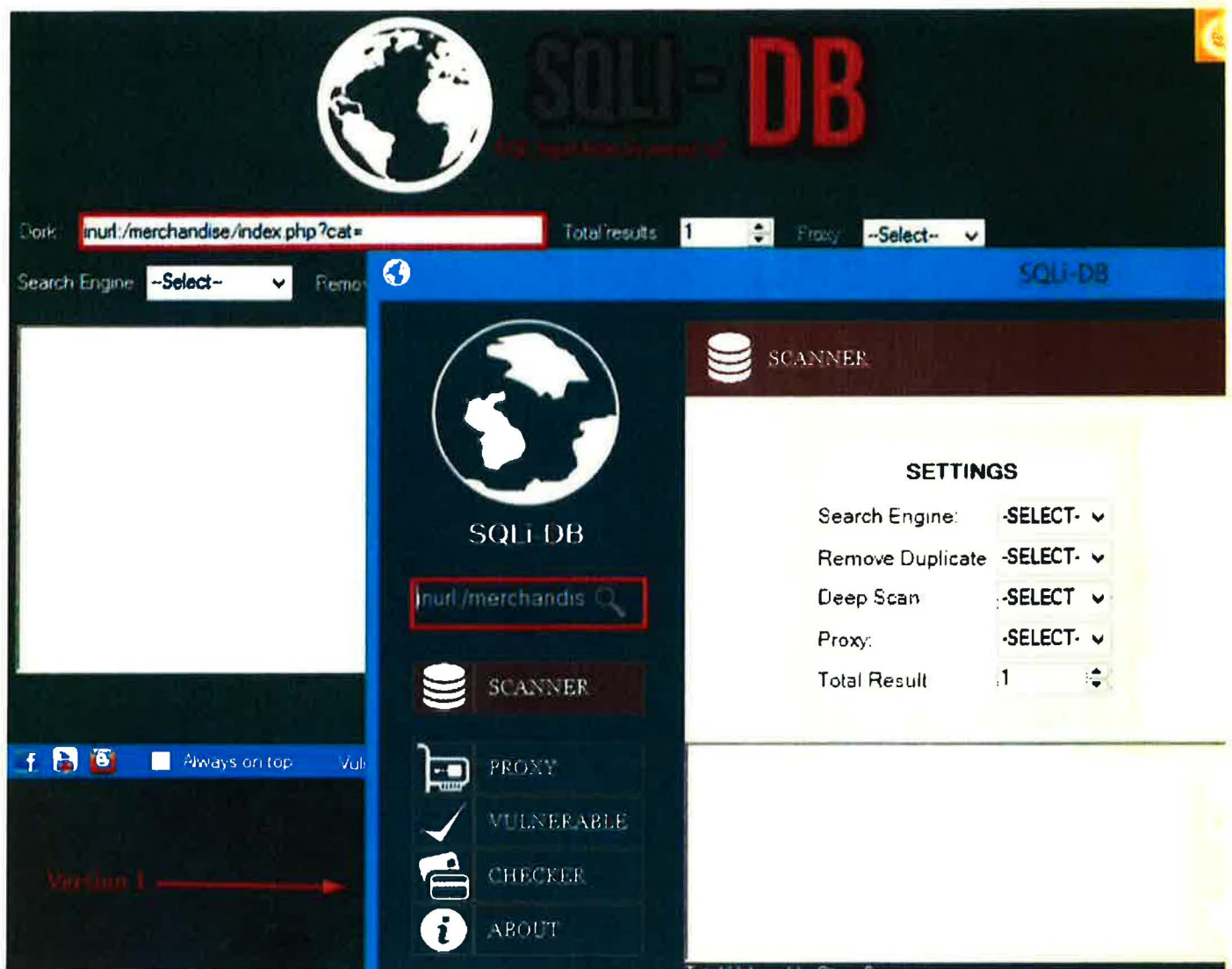
- Fermi National Accelerator Laboratory
- Child Welfare Information Gateway

## **What's the Deal With SQLi?**

SQL injection has been around since databases first appeared on the internet.

When a user is allowed to interact directly with a database, through an application in a web browser, without checking or sanitizing the input before the database executes the instruction(s), a SQL injection vulnerability exists.





Opportunistic threat actors don't need any specific technical knowledge or skill to find vulnerable websites. Free tools — like Havij, Ashiyane SQL Scanner, SQL Exploiter Pro, SQLi Hunter, SQL Inject Me, SQLmap, SQLSentinel, SQLninja, etc. — automate the identification and exploitation of vulnerable websites and associated databases through “point and click” menus.

These SQLi scanners help security teams find SQL flaws, but they also help adversaries find the the same flaws.



Rasputin is an outlier in that he's allegedly using a proprietary SQLi tool that he developed himself. Financial profits motivate actors like Rasputin, who have technical skills to create their own tools to outperform the competition in both identifying and exploiting vulnerable databases. North American and Western European databases contain information on customers or users that are historically valued at a premium in the underground economy. Buyer demand typically centers on access to American, Canadian, or UK database access.

## Colors

- English
- Russian
- Chinese (Simplified)
- Spanish

## Total references

## Event Marker Size

- 1 reference
- 42 references

## SQLi Tools on Dark Web / Forum

low=a\_leg%27%29%20UNION%  
ECT%20NULL%2CNULL%2CNUL  
3 HTTP/1.0" 200 812 "-" "sqlmap  
(http://sqlmap.org)"

To see all the passed results, go to Tools-  
>SQL Inject Me->Options and click 'Show  
passed results in final report' and rerun this  
test.

credit card hack with havij

Feb 2015 Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2016 Feb  
Feb 14 2015 2 year

Report

A recent example of a SQLi scanner's results appeared at [pastebin.com/Qzjs8iKt](https://pastebin.com/Qzjs8iKt) (recently deleted, but always available in Recorded Future). Here's a sample of the file (select details redacted to protect potentially uninformed victims):

#### Cached Document

Title: Untitled

Author: A Guest

Downloaded: Jan 22, 2017, 23:54

Original URL: <http://pastebin.com/Qzjs8iKt>

☰ ☰ Translate All

```
1. [ SQL VULN FOUND ] http://      mea.com/site/index.php/site/SupportResource?pid=232%27
2. [ SQL VULN FOUND ] http://      .net/647/c?ev_sid=10&ev_ltx-sl:Fremdsprachen+lernen&ev_lx=kw&
3. [ SQL VULN FOUND ] http://      xt.com/file-extension/ASP%27
4. [ SQL VULN FOUND ] http://      foods.com/en/chicken_detail.asp?productID=44%27
5. [ SQL VULN FOUND ] http://      posture.com/_site/products.php?cat=04%27
6. [ SQL VULN FOUND ] http://[ POSSIBLE BLIND ] http://www.      avej.com/index.php?pg=home_de
7. [ SQL VULN FOUND ] http://      gold.com/PG_compare/compare.asp?PG_lng=GB%27
8. [ SQL VULN FOUND ] http://      ntik.com/visprodukt.asp?id=8465&katId=2%27
9. [ SQL VULN FOUND ] http://      ntik.com/visprodukt.asp?id=8470&katId=3%27
10. [ SQL VULN FOUND ] http://      ntik.com/visprodukt.asp?id=8473&katId=3%27
11. [ SQL VULN FOUND ] https://      ports.com/websiteinfo.asp?CartId={2D6F4E-FEVERESTB49
12. [ SQL VULN FOUND ] http://      .ano.com/php/download.php?file=pdf/dm/DM-FD0002-04-ENG.pc
13. [ SQL VULN FOUND ] http://      .ano.com/php/download.php?file=pdf/dm/DM-SC0003-00-ENG.pc
14. [ SQL VULN FOUND ] http://      .ano.com/php/download.php?file=pdf/dm/DM-WH0002-07-ENG.pc
15. [ SQL VULN FOUND ] https://secure.      -ichiba.com/top/cart/asp/cart.asp%27
16. [ SQL VULN FOUND ] https://www.      fense.com/cart/addtocart.asp?cartid=125%27
17. [ SQL VULN FOUND ] https://www.      cc.com/Home/Index%27
18. [ SQL VULN FOUND ] https://_      phin.com/%27
19. [ SQL VULN FOUND ] http://test.php.      b.com/listproducts.php?cat=1%27
20. [ SQL VULN FOUND ] http://www.      den.com/side.php?pg=743%27
```

CLOSE

Amazingly, SQLi vulnerabilities are simple to prevent through coding best practices. [Over 15 years of high-profile data breaches](#) have done little to prevent poorly programmed web applications and/or third-party software from being used by government, enterprises, and academia. Some of the most publicized data

breaches were the result of SQLi including large corporations like Heartland Payment Systems, HBGary Federal, Yahoo!, LinkedIn, etc.

The evidence suggests economics play a role in causation for this troubling trend. The problem and solution are well understood, but solutions may require expensive projects to improve or replace vulnerable systems. These projects are often postponed until time and/or budget is available, until it's too late to prevent SQLi victimization.

Colors

- Mainstream News
- Social Media
- Blog
- Forum - All
- Forum - Underground
- Paste Site
- Non-Governmental Organization
- Dark Web / Special Access
- Other

Total references

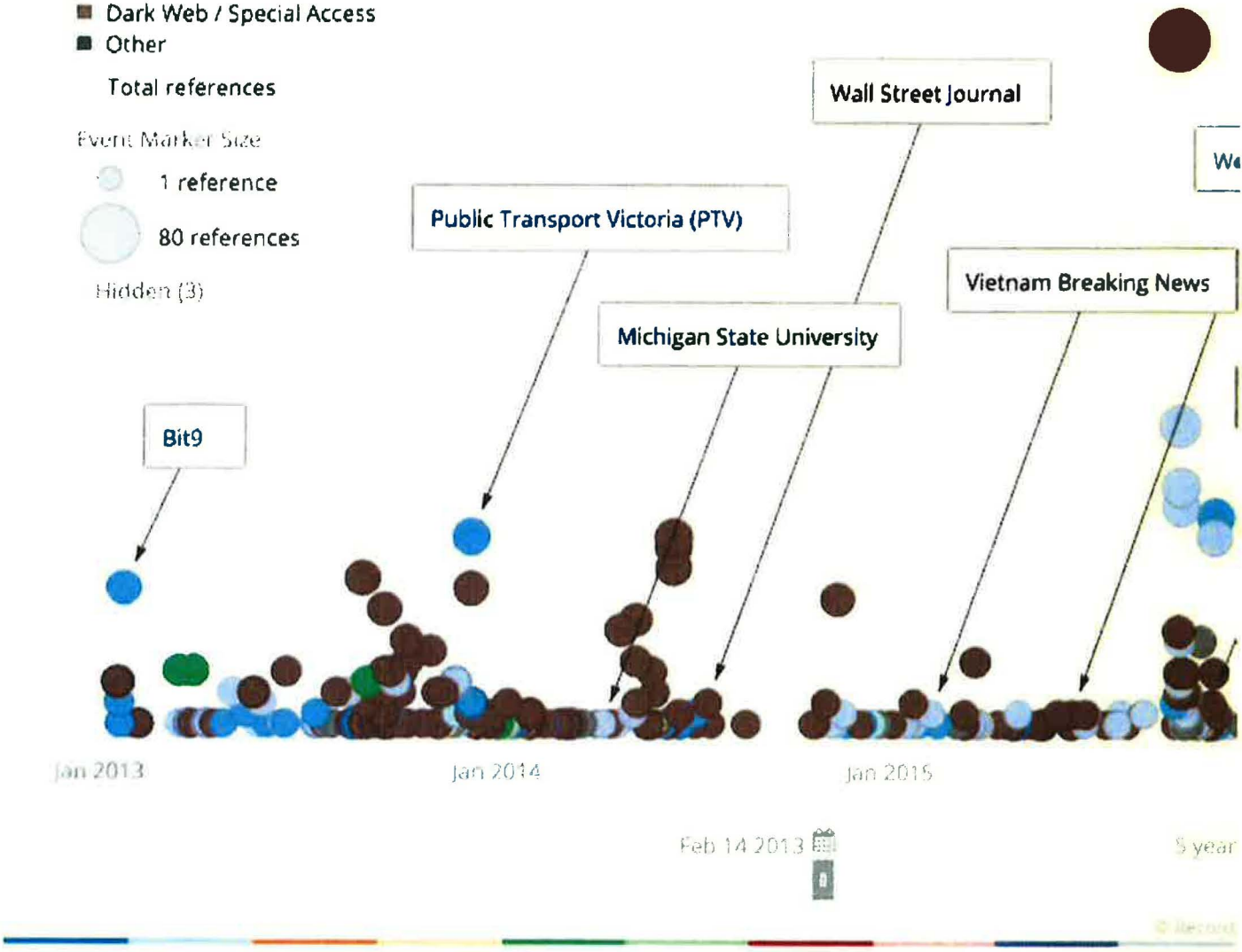
Event Marker Size

- 1 reference
- 80 references

Hidden (3)

SQLi V

All the Dr



Where Do We Go From Here?



Until organizations have an incentive (carrots or sticks) to properly audit internal and vendor code before production use, this problem will continue into the foreseeable future.

Raising awareness among developers is worthwhile and [OWASP](#) continues to perform a valuable community service through education, but eradicating SQLi vulnerabilities will likely require stiff penalties for inaction. An opt-in program for partial corporate tax abatement could be a starting point. Program participation should require quarterly code audits by an approved vendor. Robust governance, risk, and compliance (GRC) programs (e.g., financial services companies) already mandate periodic code reviews, but all verticals need some type of incentive regardless of specific industry regulations. Unfortunately, government fines and/or loss from lawsuits may be the only incentives to prioritize code audits.

## Conclusion

Cyber criminals continue to find, exploit, and sell access to vulnerable databases, targeting web applications by industry vertical, as demonstrated by Rasputin's latest victims. Even the most prestigious universities and U.S. government agencies are not immune to SQLi vulnerabilities.

This well established, but easy-to-remediate problem (though often costly), continues to vex public and private sector organizations. Economics must be addressed to fully eradicate this issue. Despite the government's penchant for

employing sticks to modify behavior, perhaps it's time to offer financial carrots to address and fully eradicate this issue.



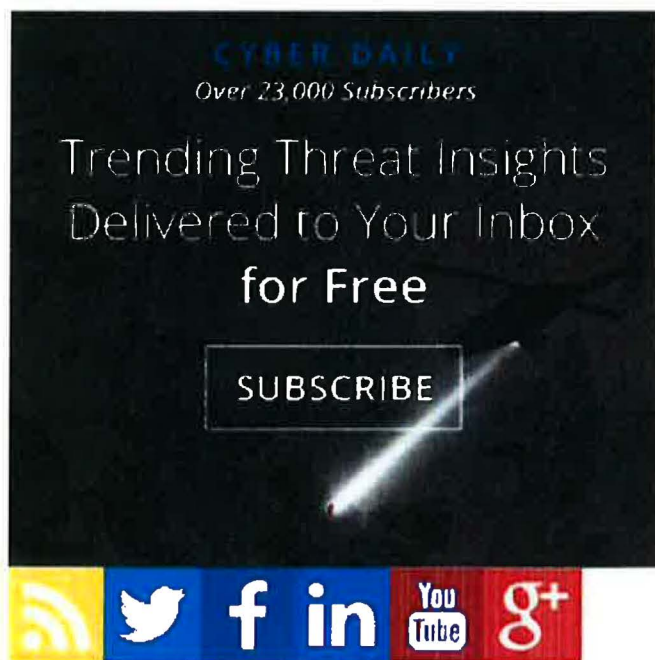
Trending Threat Insights Delivered to Your Inbox **for Free**

**CYBER DAILY**  
Over 23,000 Subscribers

Sign up for the **Cyber Daily** and receive trending threat insights every day by email.

- Top Threat Actors
- Top Vulnerabilities
- Top Malware
- Top Suspicious IP Addresses







**SUBSCRIBE**



**CYBER DAILY**  
Over 23,000 Subscribers

Trending Threat Insights Delivered to Your Inbox **for Free**

**SUBSCRIBE**

#### Recent Posts

- [Russian-Speaking Hacker Breaches Over 60 Universities and Government Agencies](#) By Levi Gundert on February 15, 2017
- [Combining Technical, Open, and Dark Web Sources of Threat Intelligence for the First Time](#) By Nagraj Seshadri on February 13, 2017
- [Fall in Love With Threat Intelligence at RSA](#) By RFSID on February 10, 2017
- [Why Threat Intelligence Teams Fail \(And What You Can Do About It\)](#) By RFSID on February 9, 2017
- [6 Corporate Security Risks Where Threat Intelligence Can Help](#) By RFSID on February 7, 2017



**Company**

- 
- 
- 
- 
- 

**For Customers**

**Ann Fisher**

**Director, Public Affairs & Government Relations**

Postal Regulatory Commission

901 New York Avenue, NW

Suite 200

Washington, DC 20268-0001

Telephone: 202-789-6803

Ann.Fisher@prc.gov

[www.prc.gov](http://www.prc.gov)

NOTICE: This e-mail message and any attachments transmitted with it contains confidential and proprietary information intended solely for the use of the addressee in its interactions with the Postal Regulatory Commission.

**ADAMS, GAIL Z**

---

**From:** (b) (6)  
**Sent:** Thursday, February 16, 2017 1:13 PM  
**To:** ADAMS, GAIL Z  
**Cc:** (b) (6)  
**Subject:** Re: Russian-Speaking Hacker Breaches Over 60 Universities and Government Agencies - Postal Regulatory Commission Inquiry  
**Attachments:** The Postal Regulatory Commission Report.pdf; ATT00001.htm

Hello Mr.Adams,

My name is (b) (6) and I'd like to apologize for the delayed response to your inquiry. On January 5, 2017, I submitted the accompanying report to MS-ISAC NCCIC Partner Liaison Center for Internet Security, and I was assured that information successfully delivered to all affected organizations including Postal Regulatory Commission.

The report includes the identified SQLi vulnerability, which was offered for sale by the Russian cybercriminal known as Rasputin. In the case, you have any follow-up questions, please don't hesitate to reach out to us at any time.

Respectfully,

(b) (6)



**ADAMS, GAIL Z**

---

**From:** (b) (6)  
**Sent:** Thursday, February 16, 2017 12:02 PM  
**To:** ADAMS, GAIL Z  
**Cc:** (b) (6)  
**Subject:** Re: Russian-Speaking Hacker Breaches Over 60 Universities and Government Agencies - Postal Regulatory Commission Inquiry

Gail,

Thank you for reaching out. I forwarded your inquiry to our threat research team. They'll follow up as soon as possible.

I'm adding my colleague (b) (6) to the thread should you have questions in the meantime.

My best,

(b) (6)

On Thu, Feb 16, 2017 at 11:59 AM, ADAMS, GAIL Z <[gail.adams@prc.gov](mailto:gail.adams@prc.gov)> wrote:

Hello,

My name is Gail Adams with the Postal Regulatory Commission. I'm writing regarding an article that is appearing on your website titled "Russian-Speaking Hacker Breaches Over 60 Universities and Government Agencies." (<https://www.recordedfuture.com/recent-rasputin-activity/#>) The Postal Regulatory Commission is on the list as one of the Federal government agencies that were hacked.

I would like to speak with the author of this article to discuss further. We have no evidence of the Postal Regulatory Commission being hacked.

I look forward to speaking with the author, (b) (6) or someone else from your organization to gather more information.

I can be reached at [202-789-6829](tel:202-789-6829) or by responding to this email at [gail.adams@prc.gov](mailto:gail.adams@prc.gov).

Thank you,

Gail



**Gail Z. Adams**  
Communications Specialist

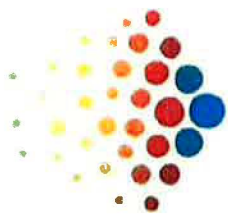
Postal Regulatory Commission  
901 New York Avenue NW, Suite 200  
Washington, DC 20268  
Telephone: [202-789-6829](tel:202-789-6829)  
[gail.adams@prc.gov](mailto:gail.adams@prc.gov)  
[www.prc.gov](http://www.prc.gov)  
*Follow us on Twitter: @PostalRegulator*

--  
(b) (6)



**CONFIDENTIAL**

(b) (6)



**Recorded Future**

## **Executive Summary**

(b) (6)





**ADAMS, GAIL Z**

---

**From:** Martin, Lee  
**Sent:** Thursday, February 16, 2017 11:11 AM  
**To:** ADAMS, GAIL Z; RUBLE, STACY L; ABRAMS, RUTH A  
**Cc:** FISHER, ANN C  
**Subject:** RE: Form submission from: Contact the Postal Regulatory Commission

Hi Gail, the report is incorrect. The PRC was not affected by the SQLi hack referenced in this article. Not sure of the source of their info, but we've scanned our system(s) for this vulnerability and it doesn't exist.

Lee

**From:** ADAMS, GAIL Z  
**Sent:** Thursday, February 16, 2017 10:47 AM  
**To:** RUBLE, STACY L <[stacy.ruble@prc.gov](mailto:stacy.ruble@prc.gov)>; ABRAMS, RUTH A <[ruth.a.abrams@prc.gov](mailto:ruth.a.abrams@prc.gov)>; Martin, Lee <[Lee.Martin@prc.gov](mailto:Lee.Martin@prc.gov)>  
**Cc:** FISHER, ANN C <[Ann.Fisher@prc.gov](mailto:Ann.Fisher@prc.gov)>  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Ruth Ann,

I need to respond to this reporter asap. Is this information correct about the PRC being hacked recently? Does the IT team have any insight into this?

---

**From:** PRC-PAGR  
**Sent:** Thursday, February 16, 2017 10:43 AM  
**To:** ADAMS, GAIL Z  
**Cc:** FISHER, ANN C; ANASIEWICZ, LEONA T  
**Subject:** FW: Form submission from: Contact the Postal Regulatory Commission

Hi Gail,

I received the email below from a reporter.

Deb

-----Original Message-----

**From:** it-services On Behalf Of (b) (6)  
**Sent:** Thursday, February 16, 2017 10:16 AM  
**To:** PRC-PAGR  
**Subject:** Form submission from: Contact the Postal Regulatory Commission

Submitted on Thursday, February 16, 2017 Submitted by user:  
 Submitted values are:

message type: Question  
 Subject : Postal Regulatory Commission  
 First name\*: (b) (6)

Last Name\*: (b) (6)

Email Address: (b) (6)

phone number

address1: ADDRESS 1

address2: ADDRESS 2

city: CITY

state: STATE

zipcode\*: (b) (6)

comments:

Hello,

My name is (b) (6) and I write for MeriTalk, an online publication based outside of D.C. that covers IT at the Federal and local levels. I'm interested in following up about a report from Recorded Future (linked here: <https://www.recordedfuture.com/recent-rasputin-activity/>) stating that PRC was one of over 60 that had been hacked recently.

Do you have a comment on their report?

Thanks very much.

Best,

(b) (6)

**ADAMS, GAIL Z**

---

**From:** (b) (6)  
**Sent:** Friday, February 17, 2017 1:38 PM  
**To:** ADAMS, GAIL Z  
**Subject:** RE: Postal Regulatory Commission

Hi Gail,

Thanks for the email. Do you have any idea what could've prompted the authors of the report to name the PRC as one of the agencies that was hacked? Even if their findings were not true, do you have any idea where they came from?

Thanks.

Best,

(b) (6)

(b) (6)

**From:** ADAMS, GAIL Z [<mailto:gail.adams@prc.gov>]  
**Sent:** Friday, February 17, 2017 1:28 PM  
**To:** (b) (6)  
**Subject:** Postal Regulatory Commission

Hello (b) (6)

We received your inquiry regarding a story recently published naming the Postal Regulatory Commission as one of the federal agencies recently hacked.

The Commission regularly scans all of its systems to identify and protect against potential vulnerabilities. Our internal controls have found no evidence of hacking to any of the Commission's systems. The Commission continues to harden its systems from malicious actors in order to protect the confidentiality, integrity, and availability of our information systems.

Please don't hesitate to let me know if you have any further questions.

Thank you,

Gail



**Gail Z. Adams**

Communications Specialist

Postal Regulatory Commission

901 New York Avenue NW, Suite 200

Washington, DC 20268

Telephone: 202-789-6829

[gailadams@prc.gov](mailto:gailadams@prc.gov)

[www.prc.gov](http://www.prc.gov)

***Follow us on Twitter: @PostalRegulator***