PUMPCON
2014

When Vulnerability Disclosure Gets Ugly

Oct 10, 2014

All materials posted at samsclass.info and free to use

Sam Bowne

@sambowne

I teach Ethical Hacking at City College San Francisco. My statements are my own, not official positions of CCSF.

San Francisco

http://samsclass.info

Twitter page

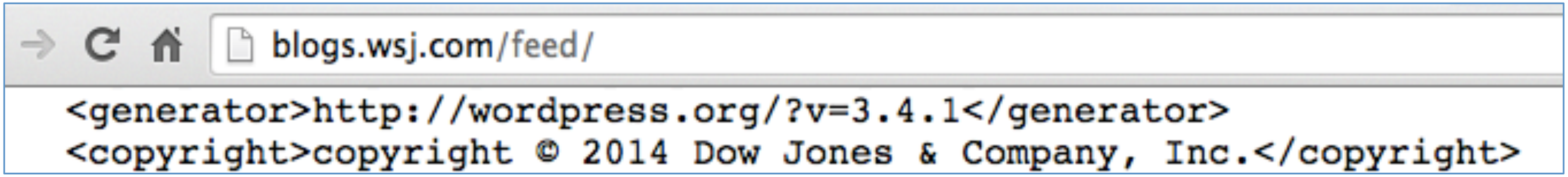
All materials posted at samsclass.info and free to use

Obvious Security Problems
Cold Calls

All materials posted at samsclass.info and free to use

Old Wordpress Version

- Wall Street Journal
  - Wordpress version from 2012
  - Ty Ryan Satterfield (@I_am_ryan_S)

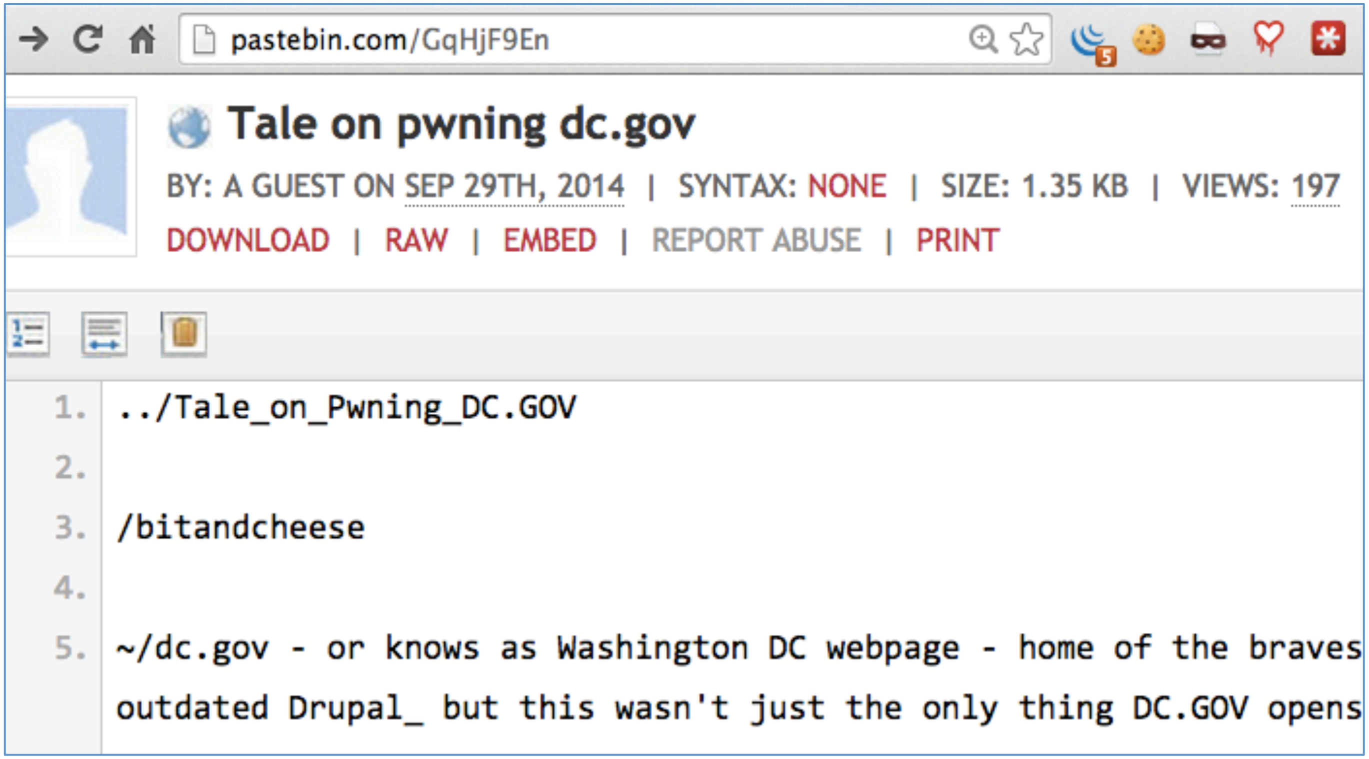


blogs.wsj.com/feed/

```
<generator>http://wordpress.org/?v=3.4.1</generator>
<copyright>copyright © 2014 Dow Jones & Company, Inc.</copyright>
```

All materials posted at samsclass.info and free to use

SQLi on Pastebin

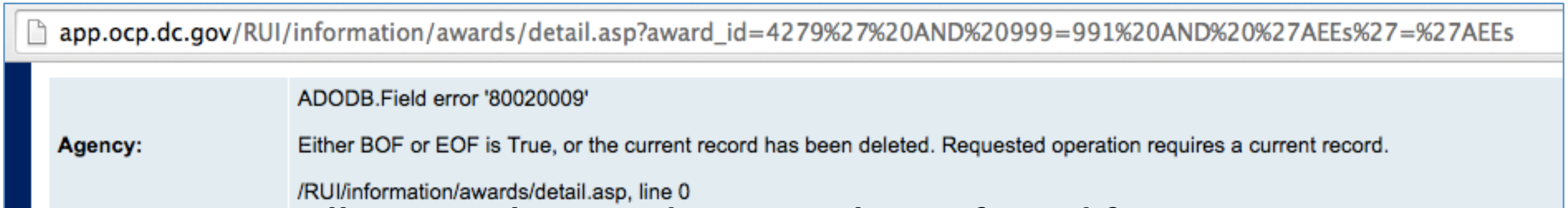


pastebin.com/GqHjF9En

Tale on pwning dc.gov

BY: A GUEST ON SEP 29TH, 2014 | SYNTAX: NONE | SIZE: 1.35 KB | VIEWS: 197

```
../Tale_on_Pwning_DC.GOV

/bitandcheese

~/dc.gov - or knows as Washington DC webpage - home of the braves
outdated Drupal_ but this wasn't just the only thing DC.GOV opens
```

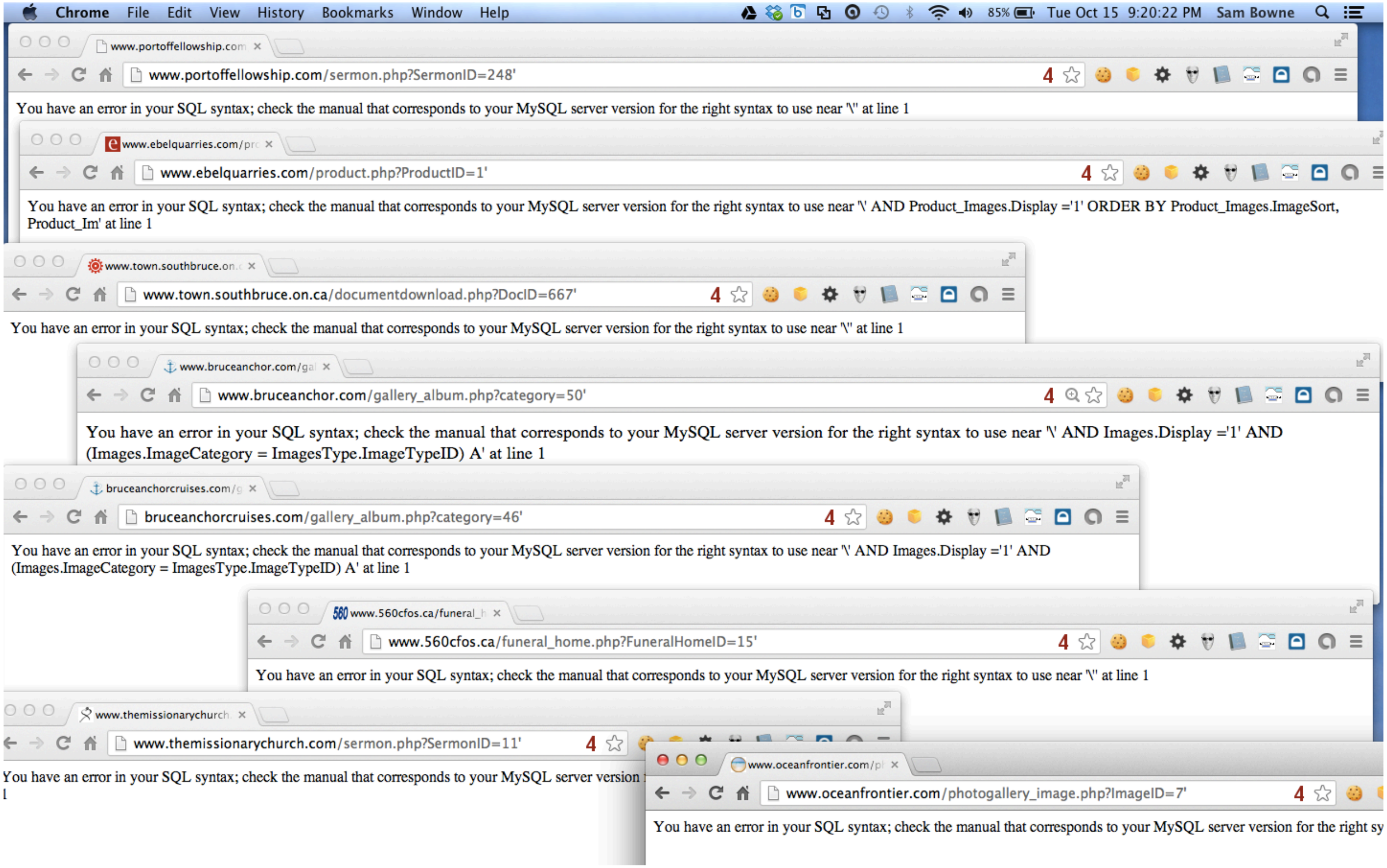


app.ocp.dc.gov/RUI/information/awards/detail.asp?award_id=4279%27%20AND%20999=991%20AND%20%27AEEs%27=%27AEEs

Agency:

```
ADODB.Field error '80020009'

Either BOF or EOF is True, or the current record has been deleted. Requested operation requires a current record.

/RUI/information/awards/detail.asp, line 0
```

Websmart, Inc. and 100,000 Vulnerable Websites



www.portoffellowship.com/sermon.php?SermonID=248'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1

www.ebelquarries.com/product.php?ProductID=1'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\' AND Product_Images.Display ='1' ORDER BY Product_Images.ImageSort, Product_Im' at line 1

www.town.southbruce.on.ca/documentdownload.php?DocID=667'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1

www.bruceanchor.com/gallery_album.php?category=50'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\' AND Images.Display ='1' AND (Images.ImageCategory = ImagesType.ImageTypeID) A' at line 1

bruceanchorcruises.com/gallery_album.php?category=46'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\' AND Images.Display ='1' AND (Images.ImageCategory = ImagesType.ImageTypeID) A' at line 1

www.560cfos.ca/funeral_home.php?FuneralHomeID=15'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1

www.themissionarychurch.com/sermon.php?SermonID=11'

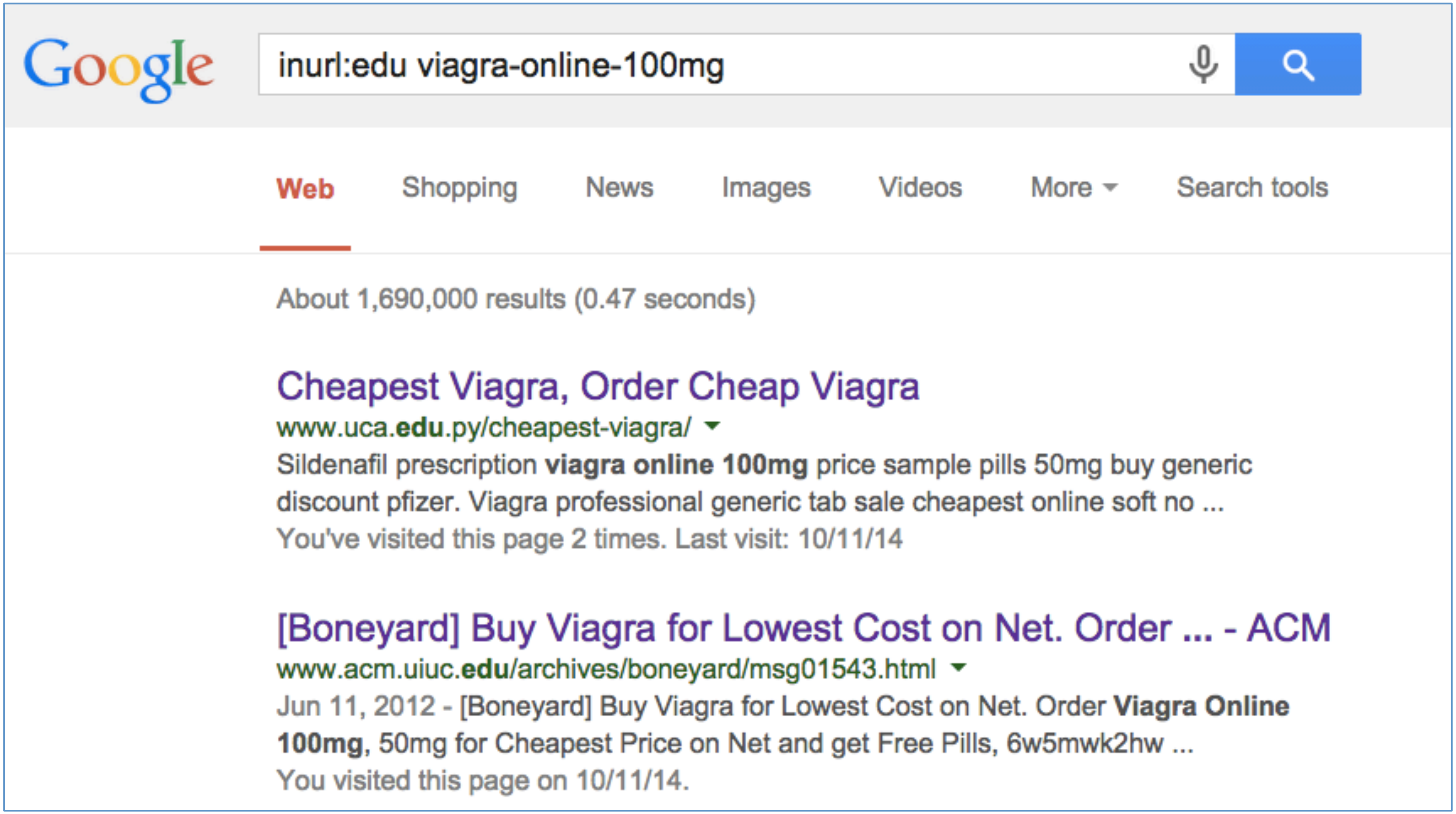
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version
1

www.oceanfrontier.com/photogallery_image.php?ImageID=7'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right sy

All materials posted at samsclass.info and free to use

Pharma Infections at Colleges



inurl:edu viagra-online-100mg

About 1,690,000 results (0.47 seconds)

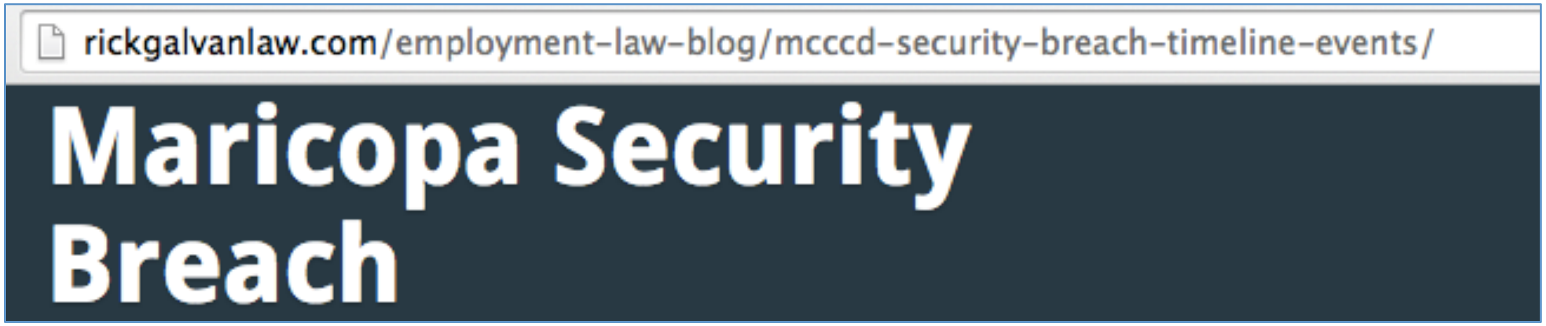
Cheapest Viagra, Order Cheap Viagra
www.uca.**edu**.py/cheapest-viagra/
Sildenafil prescription **viagra online 100mg** price sample pills 50mg buy generic discount pfizer. Viagra professional generic tab sale cheapest online soft no ...
You've visited this page 2 times. Last visit: 10/11/14

[Boneyard] Buy Viagra for Lowest Cost on Net. Order ... - ACM
www.acm.uiuc.**edu**/archives/boneyard/msg01543.html
Jun 11, 2012 - [Boneyard] Buy Viagra for Lowest Cost on Net. Order **Viagra Online 100mg**, 50mg for Cheapest Price on Net and get Free Pills, 6w5mwk2hw ...
You visited this page on 10/11/14.

All materials posted at samsclass.info and free to use

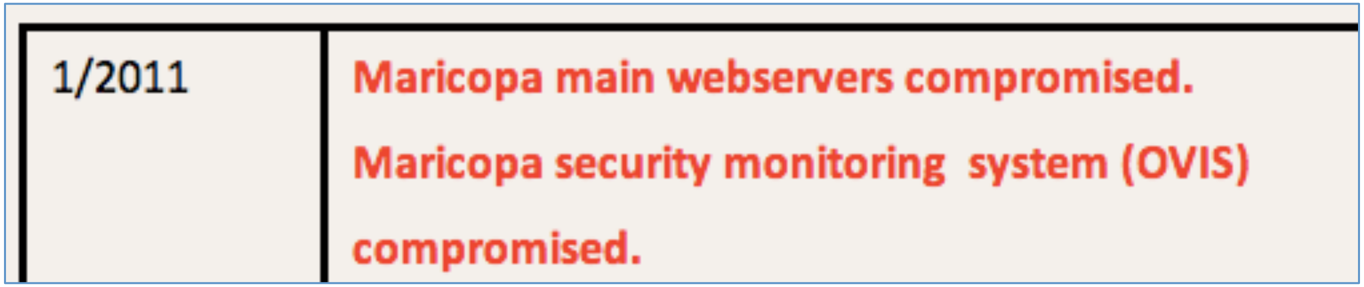
19 Colleges Infected with Pharma

- 5 Fixed within a few weeks
- 7 Fixed within 8 months
- 7 Still Infected on 7-19-14
- http://samsclass.info/125/proj11/subtle-infect.htm#19more

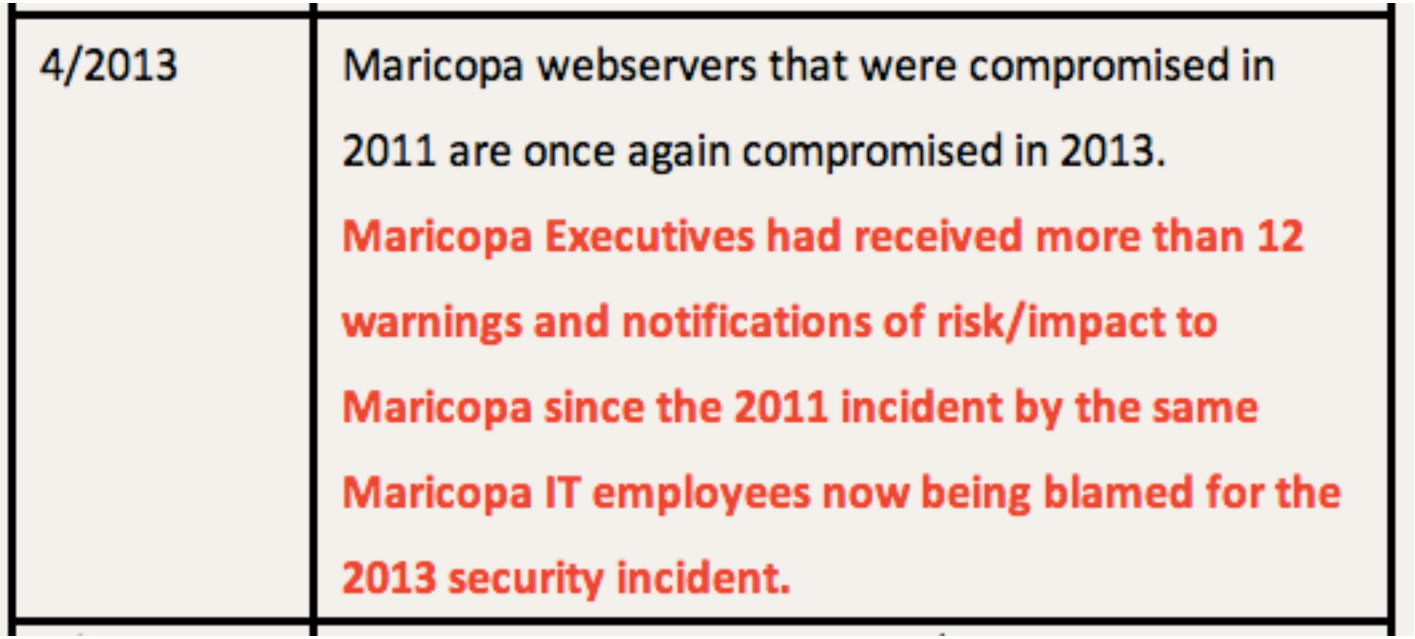


rickgalvanlaw.com/employment-law-blog/mcccd-security-breach-timeline-events/

Maricopa Security Breach

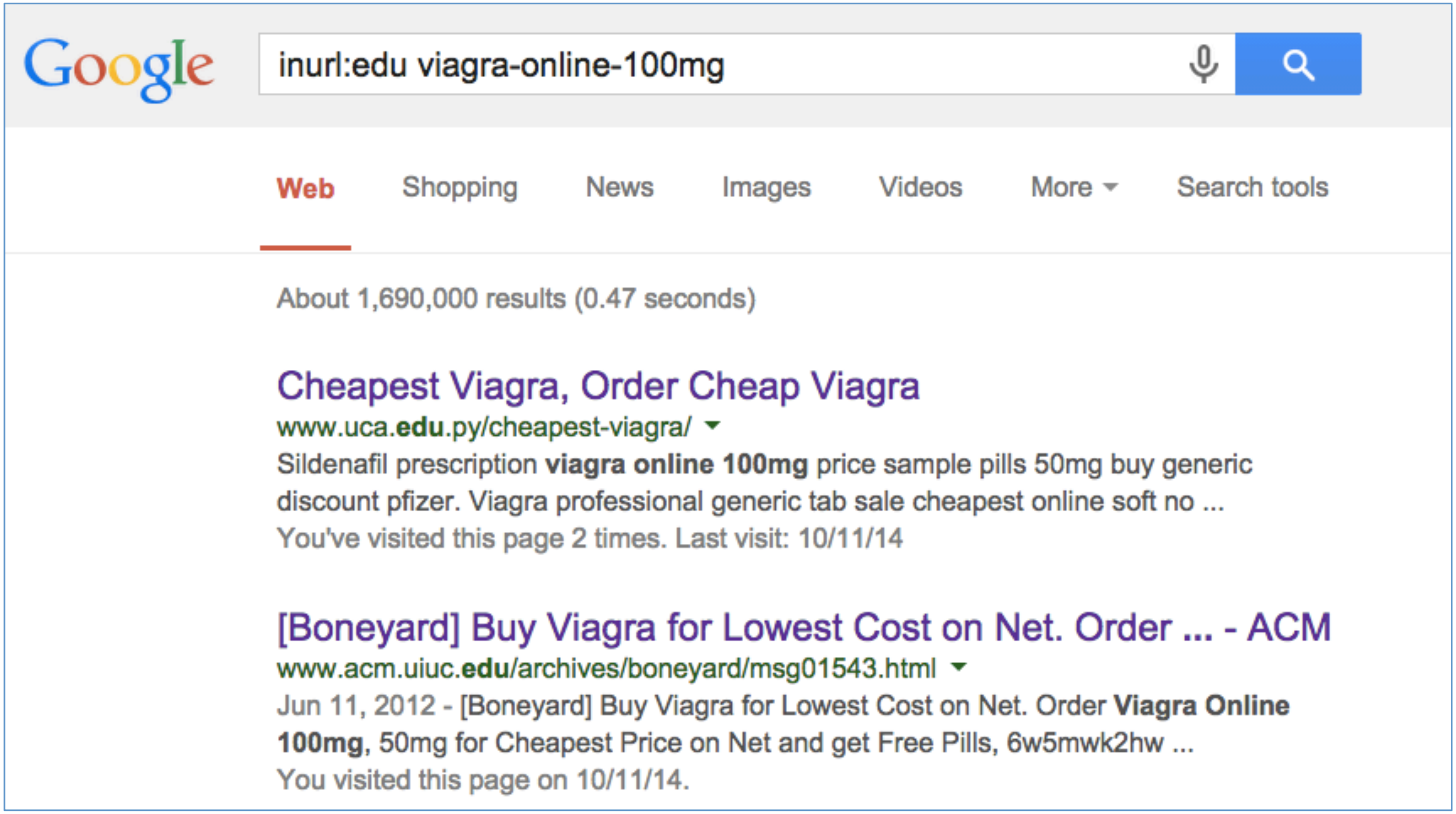


1/2011	Maricopa main webservers compromised. Maricopa security monitoring system (OVIS) compromised.



4/2013	Maricopa webservers that were compromised in 2011 are once again compromised in 2013. Maricopa Executives had received more than 12 warnings and notifications of risk/impact to Maricopa since the 2011 incident by the same Maricopa IT employees now being blamed for the 2013 security incident.

Infections at UC Santa Cruz



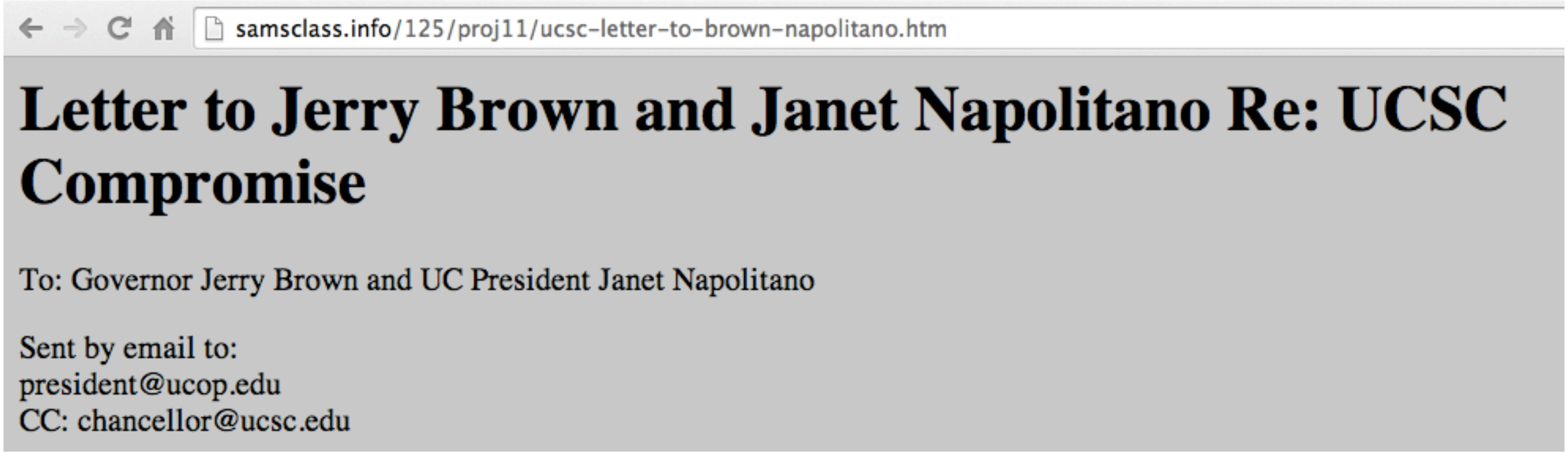
inurl:edu viagra-online-100mg

About 1,690,000 results (0.47 seconds)

Cheapest Viagra, Order Cheap Viagra
www.uca.**edu**.py/cheapest-viagra/
Sildenafil prescription **viagra online 100mg** price sample pills 50mg buy generic discount pfizer. Viagra professional generic tab sale cheapest online soft no ...
You've visited this page 2 times. Last visit: 10/11/14

[Boneyard] Buy Viagra for Lowest Cost on Net. Order ... - ACM
www.acm.uiuc.**edu**/archives/boneyard/msg01543.html
Jun 11, 2012 - [Boneyard] Buy Viagra for Lowest Cost on Net. Order **Viagra Online 100mg**, 50mg for Cheapest Price on Net and get Free Pills, 6w5mwk2hw ...
You visited this page on 10/11/14.

All materials posted at samsclass.info and free to use



samsclass.info/125/proj11/ucsc-letter-to-brown-napolitano.htm

Letter to Jerry Brown and Janet Napolitano Re: UCSC Compromise

To: Governor Jerry Brown and UC President Janet Napolitano

Sent by email to:
president@ucop.edu
CC: chancellor@ucsc.edu

- UCSC cleaned their server
- Re-infected a week later
- NEED ROOT CAUSE ANALYSIS

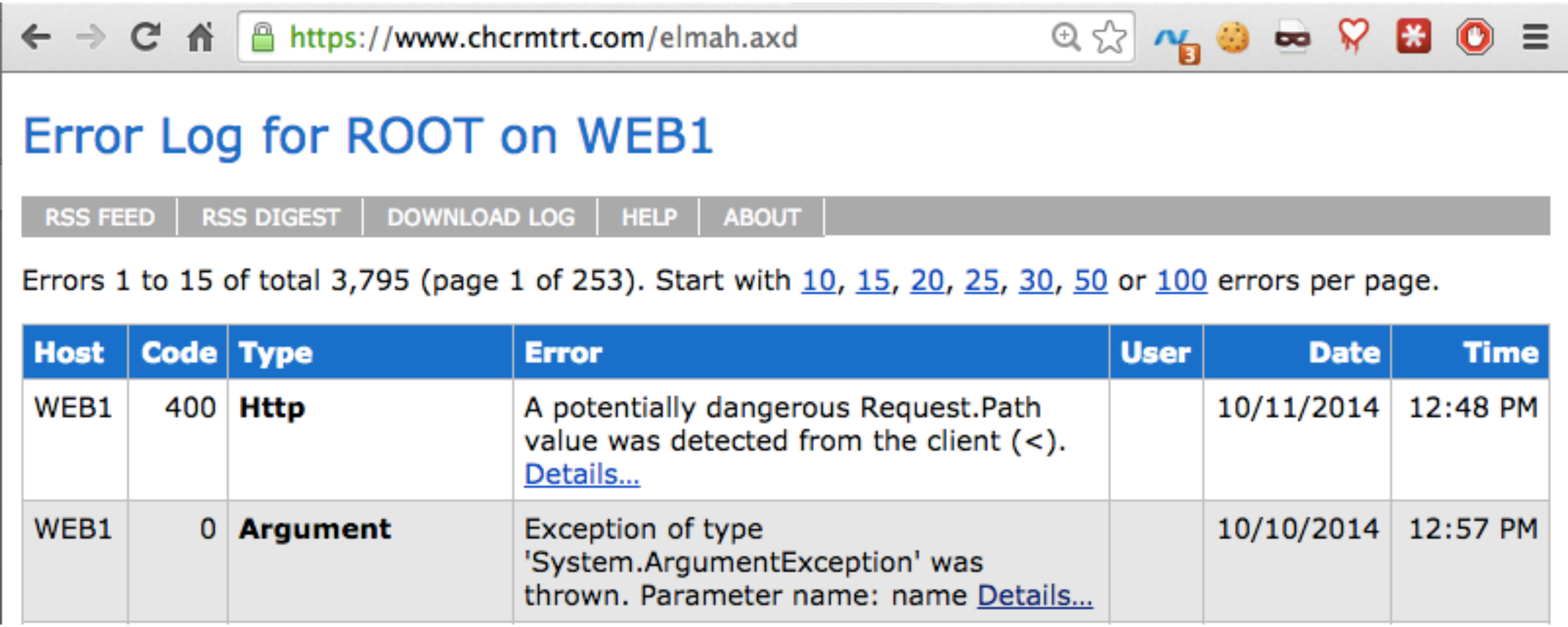
Many More Pharma Infections

- Dozens of other schools, businesses, foreign sites, etc.
- http://samsclass.info/125/proj11/subtle-infect.htm#19more

Exposed Data

Exposed Error Logs

- Can leak cookies
- Even when secured by HTTPS



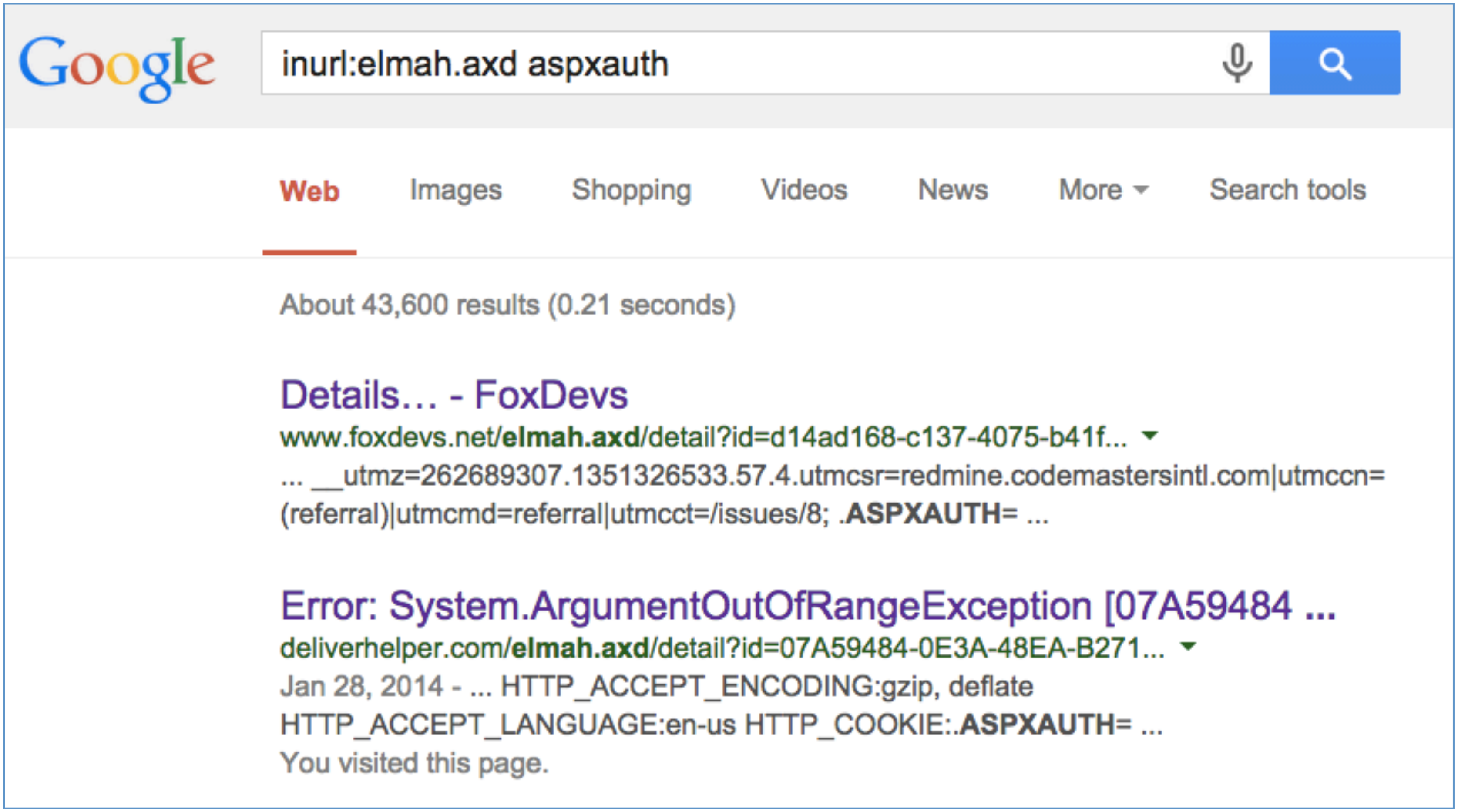
Error Log for ROOT on WEB1

Errors 1 to 15 of total 3,795 (page 1 of 253). Start with 10, 15, 20, 25, 30, 50 or 100 errors per page.

Host	Code	Type	Error	User	Date	Time
WEB1	400	**Http**	A potentially dangerous Request.Path value was detected from the client (<). Details...		10/11/2014	12:48 PM
WEB1	0	**Argument**	Exception of type 'System.ArgumentException' was thrown. Parameter name: name Details...		10/10/2014	12:57 PM

All materials posted at samsclass.info and free to use

Google Dork for Exposed ELMAH Pages



inurl:elmah.axd aspxauth

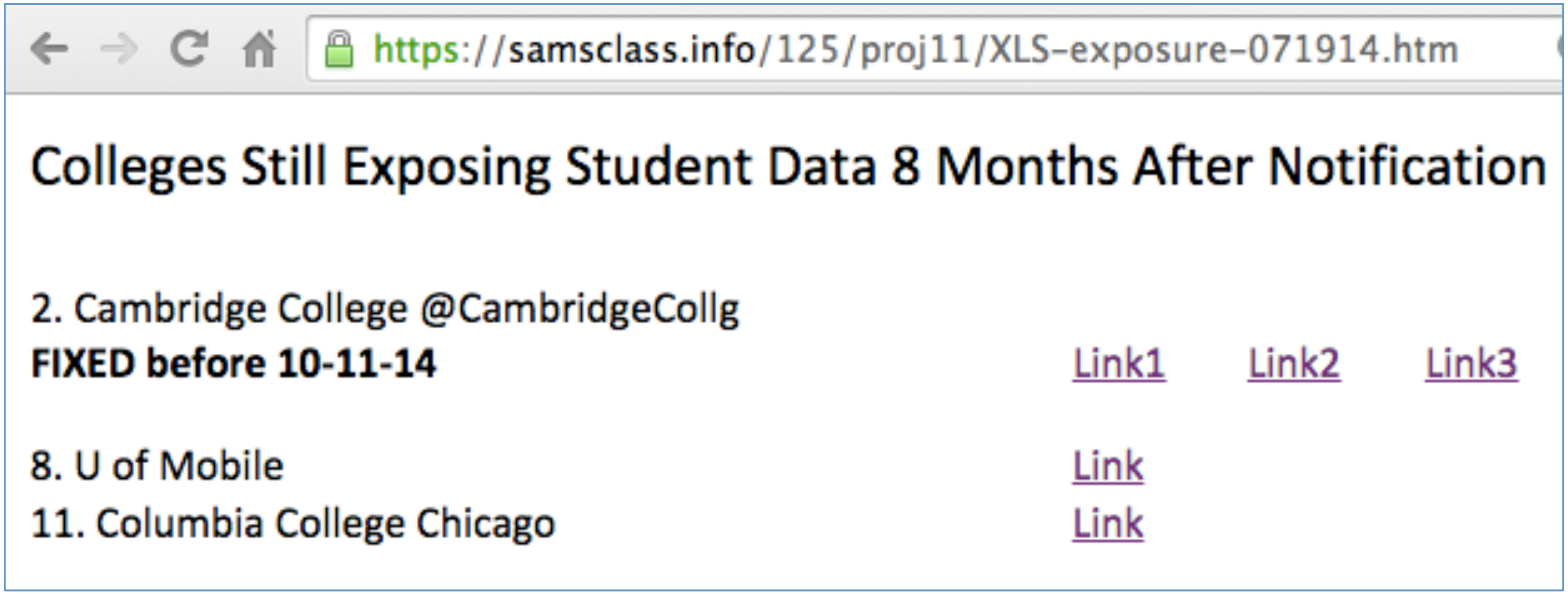
About 43,600 results (0.21 seconds)

Details… - FoxDevs
www.foxdevs.net/**elmah.axd**/detail?id=d14ad168-c137-4075-b41f...
... __utmz=262689307.1351326533.57.4.utmcsr=redmine.codemastersintl.com|utmccn=(referral)|utmcmd=referral|utmcct=/issues/8; .**ASPXAUTH**= ...

Error: System.ArgumentOutOfRangeException [07A59484 ...
deliverhelper.com/**elmah.axd**/detail?id=07A59484-0E3A-48EA-B271...
Jan 28, 2014 - ... HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_ACCEPT_LANGUAGE:en-us HTTP_COOKIE:.**ASPXAUTH**= ...
You visited this page.

All materials posted at samsclass.info and free to use

Exposed Student Data



https://samsclass.info/125/proj11/XLS-exposure-071914.htm

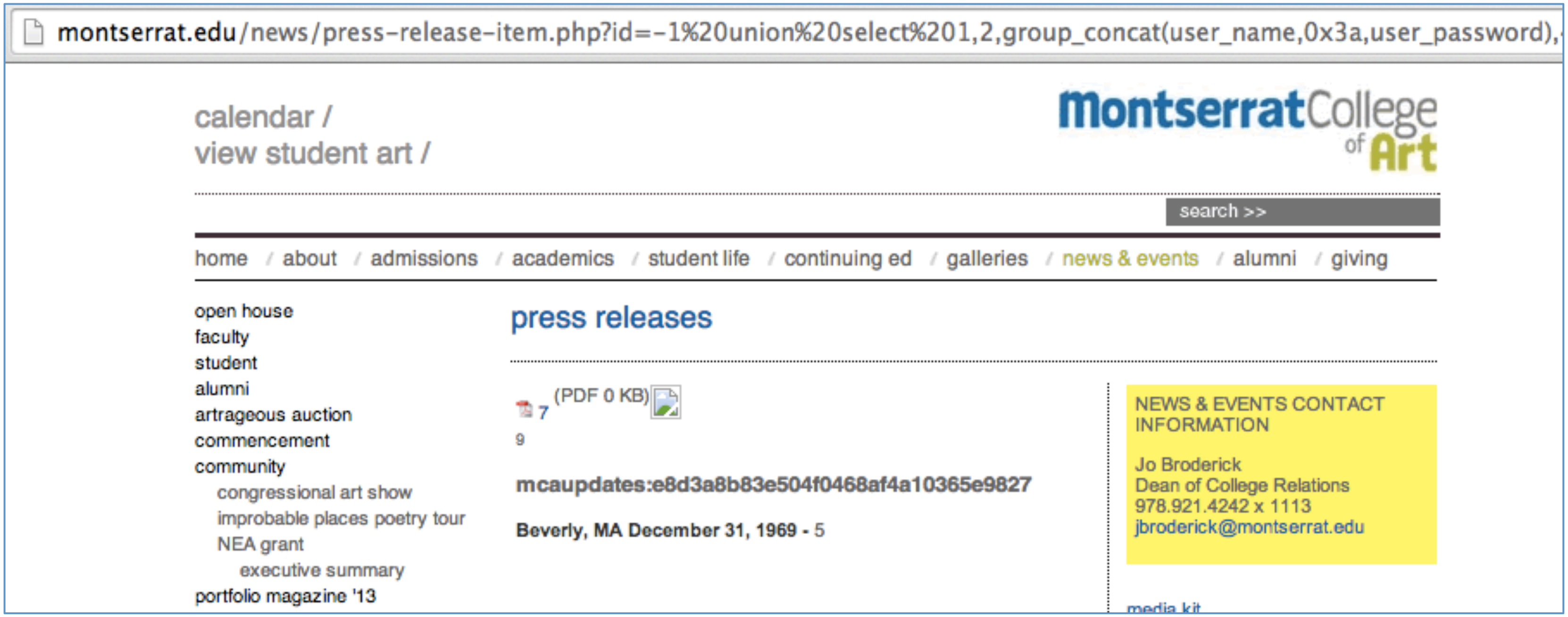
Colleges Still Exposing Student Data 8 Months After Notification

2. Cambridge College @CambridgeCollg
FIXED before 10-11-14 Link1 Link2 Link3

8. U of Mobile Link
11. Columbia College Chicago Link

All materials posted at samsclass.info and free to use

Exposed Password Hash



montserrat.edu/news/press-release-item.php?id=-1%20union%20select%201,2,group_concat(user_name,0x3a,user_password),

press releases

7 (PDF 0 KB)

9

mcaupdates:e8d3a8b83e504f0468af4a10365e9827

Beverly, MA December 31, 1969 - 5

NEWS & EVENTS CONTACT INFORMATION

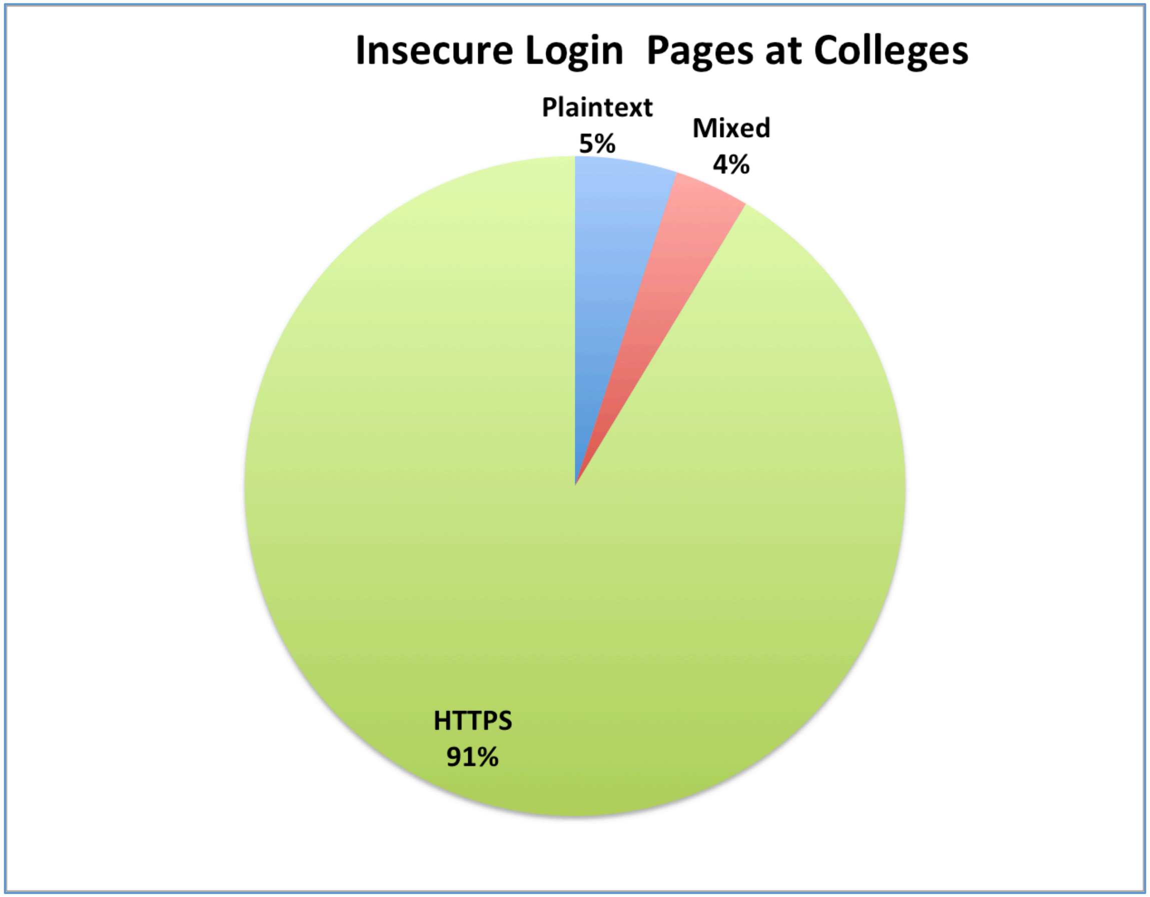
Jo Broderick
Dean of College Relations
978.921.4242 x 1113
jbroderick@montserrat.edu

All materials posted at samsclass.info and free to use

Plaintext Login Pages at Colleges

Insecure Login Pages at Colleges

90 colleges notified in Dec, 2013



All materials posted at samsclass.info and free to use

Big Names

- Cornell
- Johns Hopkins
- Stanford
- UC Berkeley

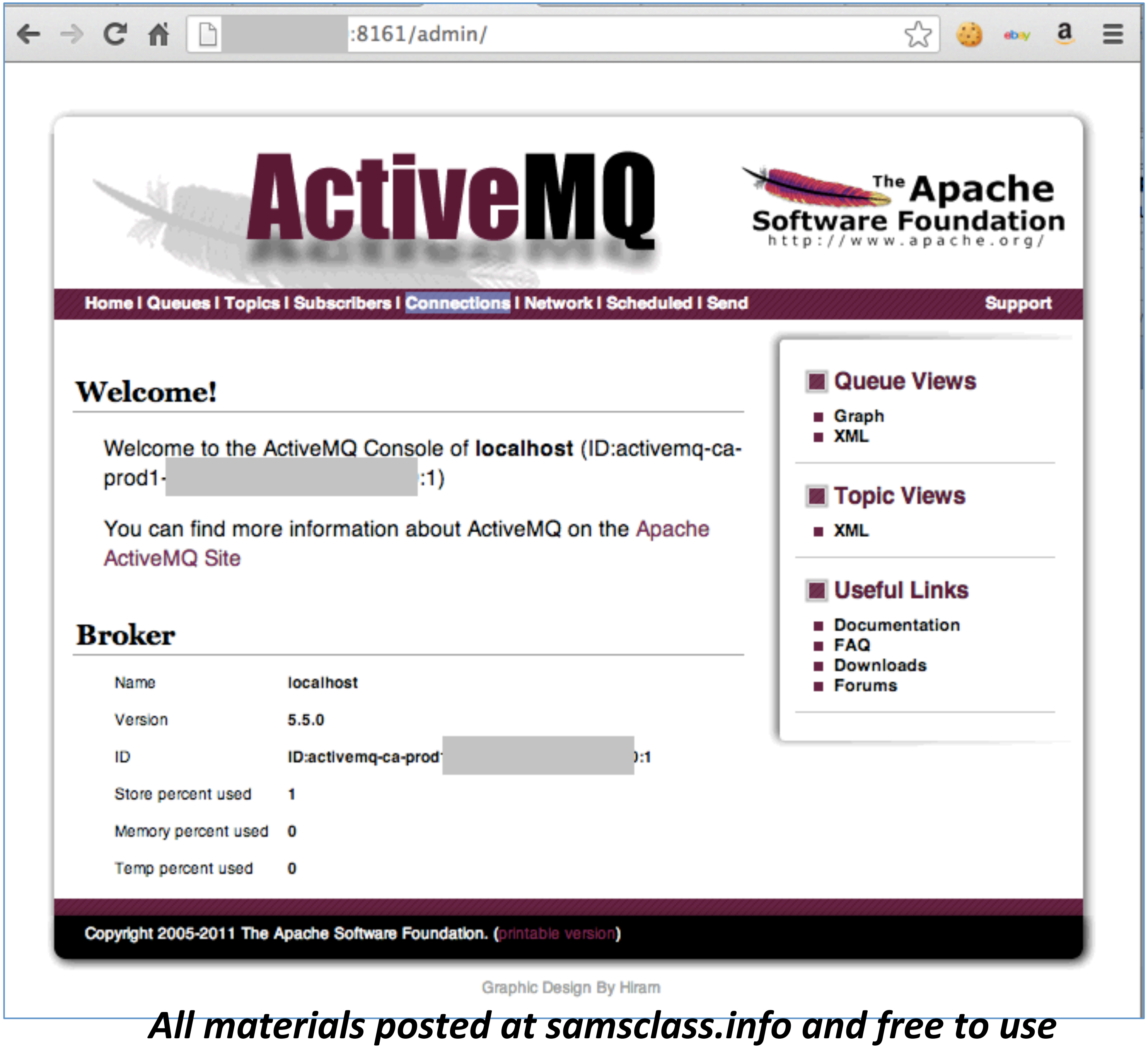
Results

- 7 months after notification:
- 16/57 plaintext login pages fixed or improved (28%)
- 8/33 mixed login pages fixed or improved (24%)

Other Problems

ActiveMQ

- Free open-source middleware from Apache
- A Defcon talk said it was often insecure, so I looked on SHODAN to see



[redacted]:8161/admin/

Home | Queues | Topics | Subscribers | Connections | Network | Scheduled | Send   Support

Welcome!

Welcome to the ActiveMQ Console of **localhost** (ID:activemq-ca-prod1-[redacted]:1)

You can find more information about ActiveMQ on the Apache ActiveMQ Site

Broker

Name	localhost
Version	5.5.0
ID	ID:activemq-ca-prod[redacted]):1
Store percent used	1
Memory percent used	0
Temp percent used	0

Queue Views

- Graph
- XML

Topic Views

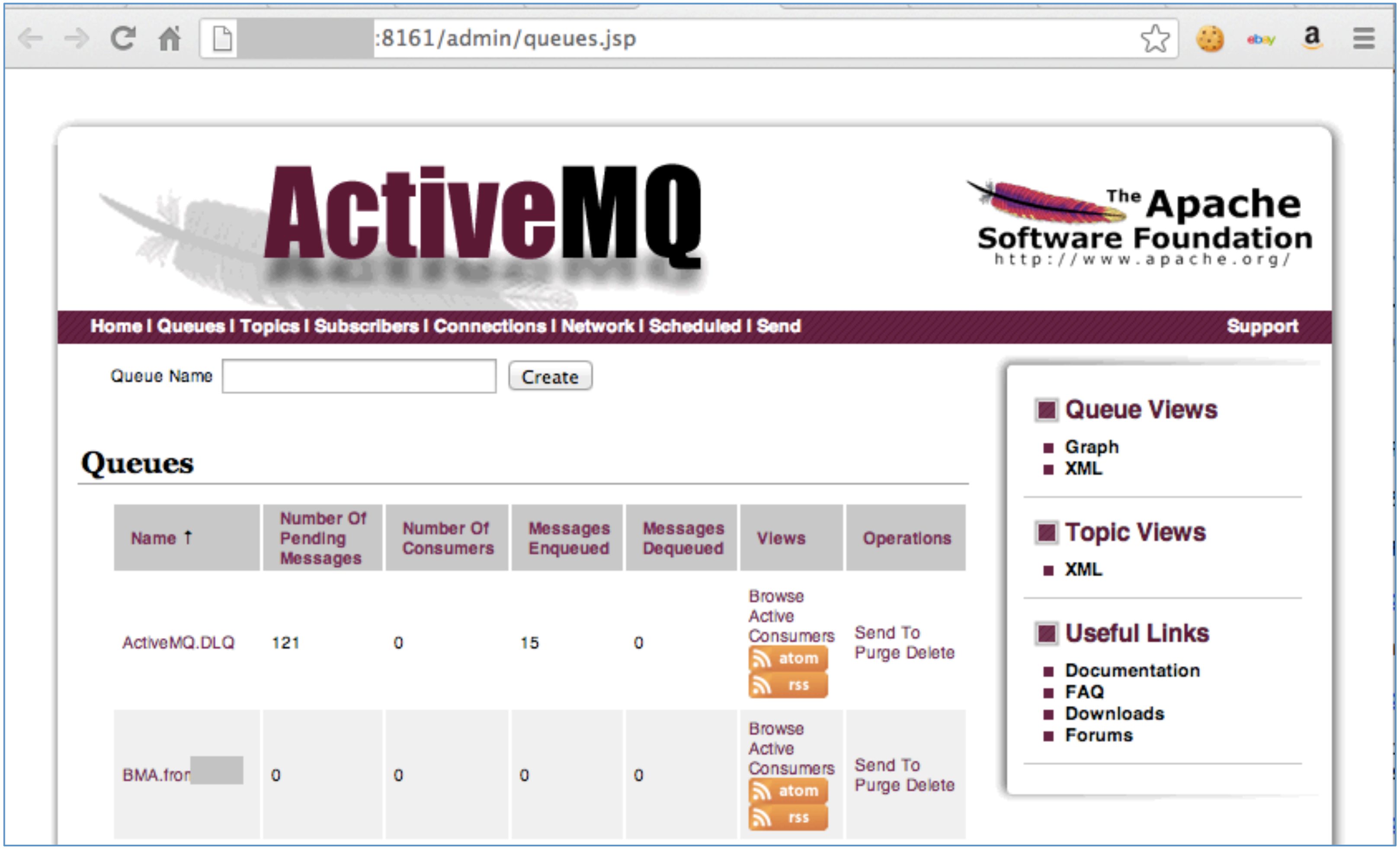
- XML

Useful Links

- Documentation
- FAQ
- Downloads
- Forums

Copyright 2005-2011 The Apache Software Foundation. (printable version)

Graphic Design By Hiram



[redacted]:8161/admin/queues.jsp

Home | Queues | Topics | Subscribers | Connections | Network | Scheduled | Send   Support

Queue Name [ ] Create

Queues

Name ↑	Number Of Pending Messages	Number Of Consumers	Messages Enqueued	Messages Dequeued	Views	Operations
ActiveMQ.DLQ	121	0	15	0	Browse Active Consumers atom rss	Send To Purge Delete
BMA.fron[redacted]	0	0	0	0	Browse Active Consumers atom rss	Send To Purge Delete

Queue Views

- Graph
- XML

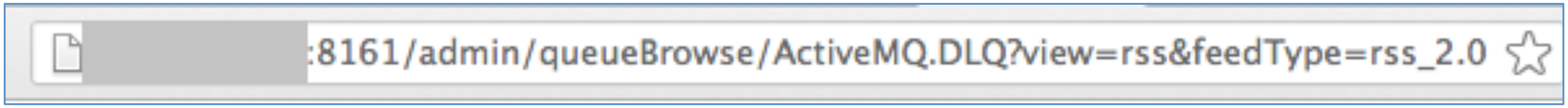
Topic Views

- XML

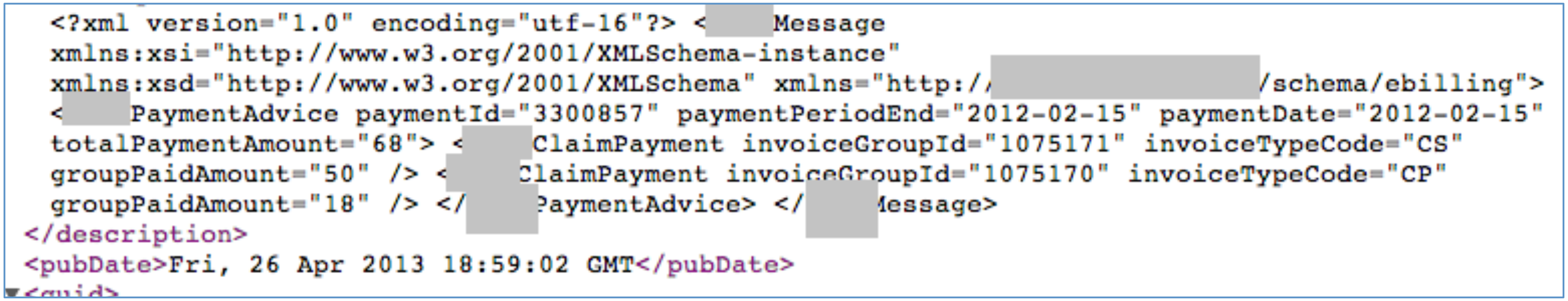
Useful Links

- Documentation
- FAQ
- Downloads
- Forums

Real Check Data?

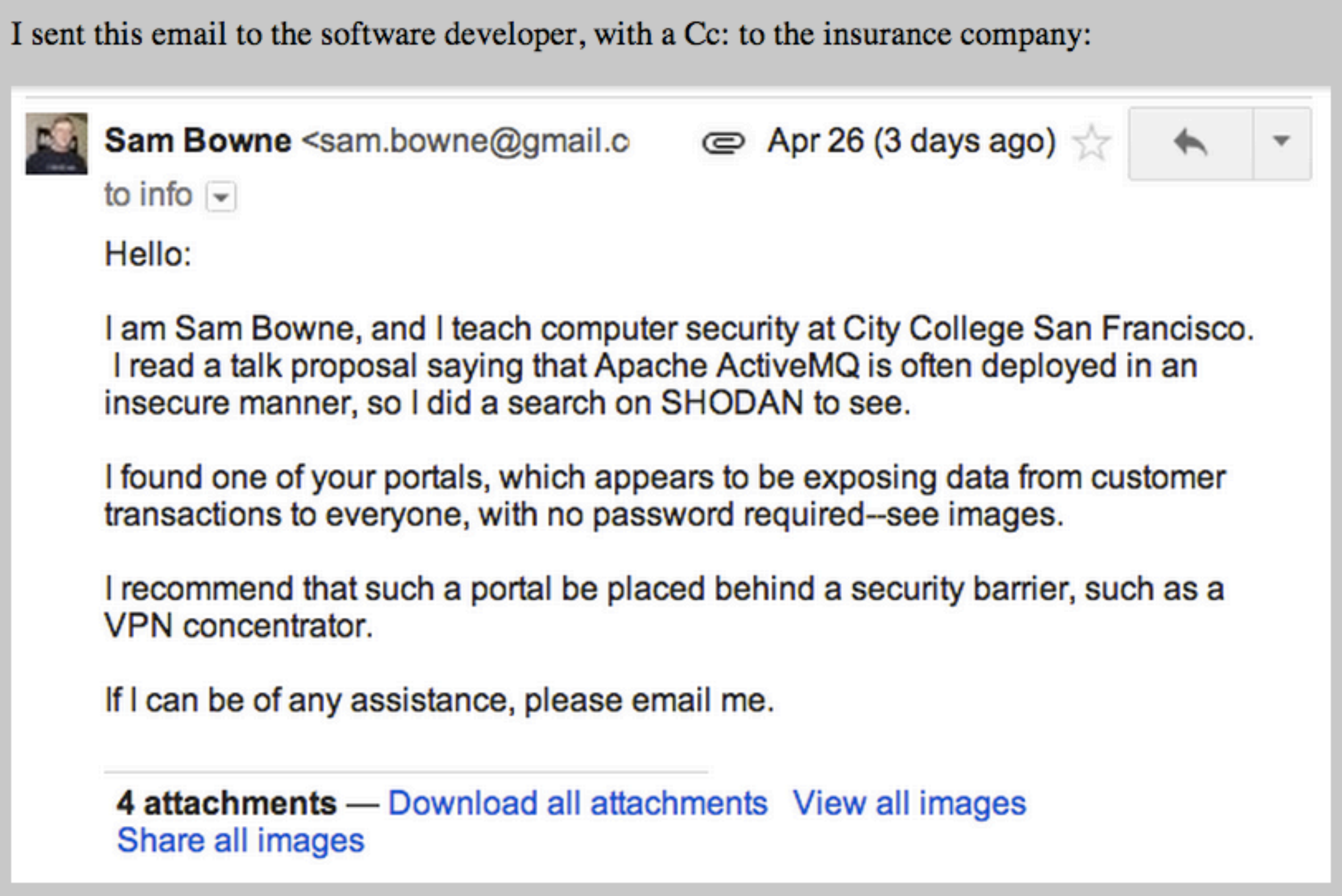


[redacted]:8161/admin/queueBrowse/ActiveMQ.DLQ?view=rss&feedType=rss_2.0



```
  <?xml version="1.0" encoding="utf-16"?> <[redacted]Message
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://[redacted]/schema/ebilling">
  <[redacted]PaymentAdvice paymentId="3300857" paymentPeriodEnd="2012-02-15" paymentDate="2012-02-15"
  totalPaymentAmount="68"> <[redacted]ClaimPayment invoiceGroupId="1075171" invoiceTypeCode="CS"
  groupPaidAmount="50" /> <[redacted]ClaimPayment invoiceGroupId="1075170" invoiceTypeCode="CP"
  groupPaidAmount="18" /> </[redacted]PaymentAdvice> </[redacted]Message>
</description>
<pubDate>Fri, 26 Apr 2013 18:59:02 GMT</pubDate>
▼<guid>
```

I sent this email to the software developer, with a Cc: to the insurance company:



Sam Bowne <sam.bowne@gmail.c

Apr 26 (3 days ago)

to info

Hello:

I am Sam Bowne, and I teach computer security at City College San Francisco. I read a talk proposal saying that Apache ActiveMQ is often deployed in an insecure manner, so I did a search on SHODAN to see.

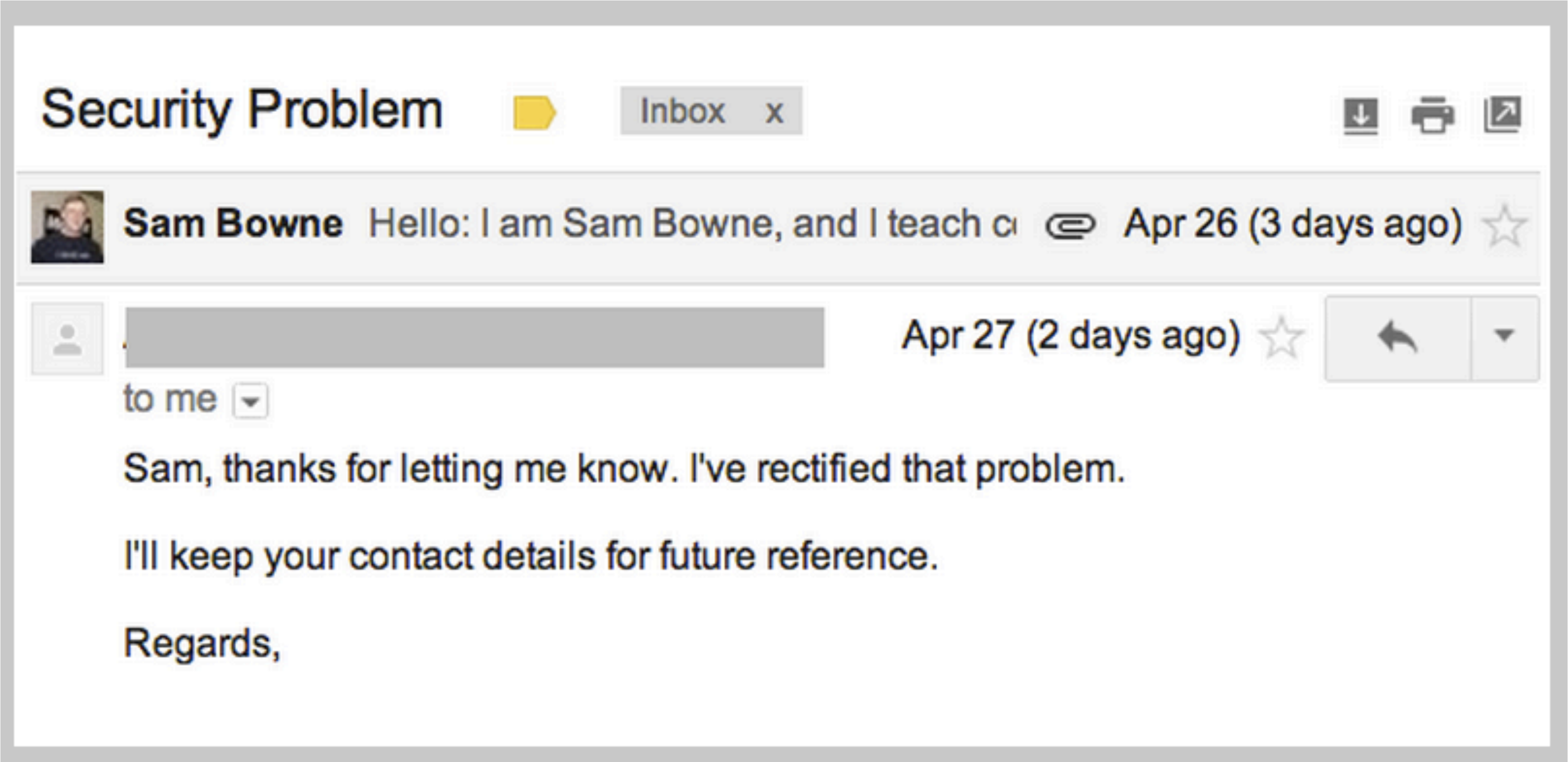
I found one of your portals, which appears to be exposing data from customer transactions to everyone, with no password required--see images.

I recommend that such a portal be placed behind a security barrier, such as a VPN concentrator.

If I can be of any assistance, please email me.

4 attachments — Download all attachments View all images Share all images

All materials posted at samsclass.info and free to use



Security Problem

Sam Bowne Hello: I am Sam Bowne, and I teach c Apr 26 (3 days ago)

[redacted] Apr 27 (2 days ago)

to me

Sam, thanks for letting me know. I've rectified that problem.

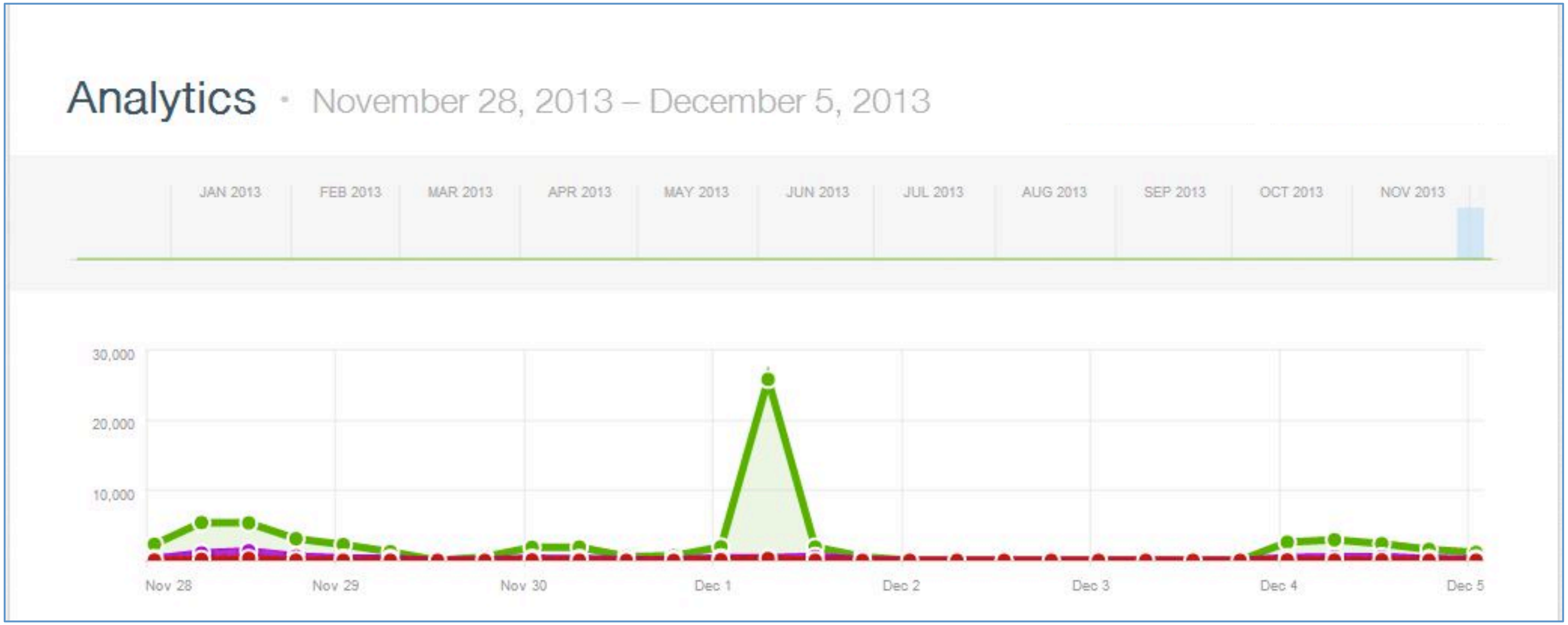
I'll keep your contact details for future reference.

Regards,

All materials posted at samsclass.info and free to use

Wordpress Bots

>2000 WordPress Bots

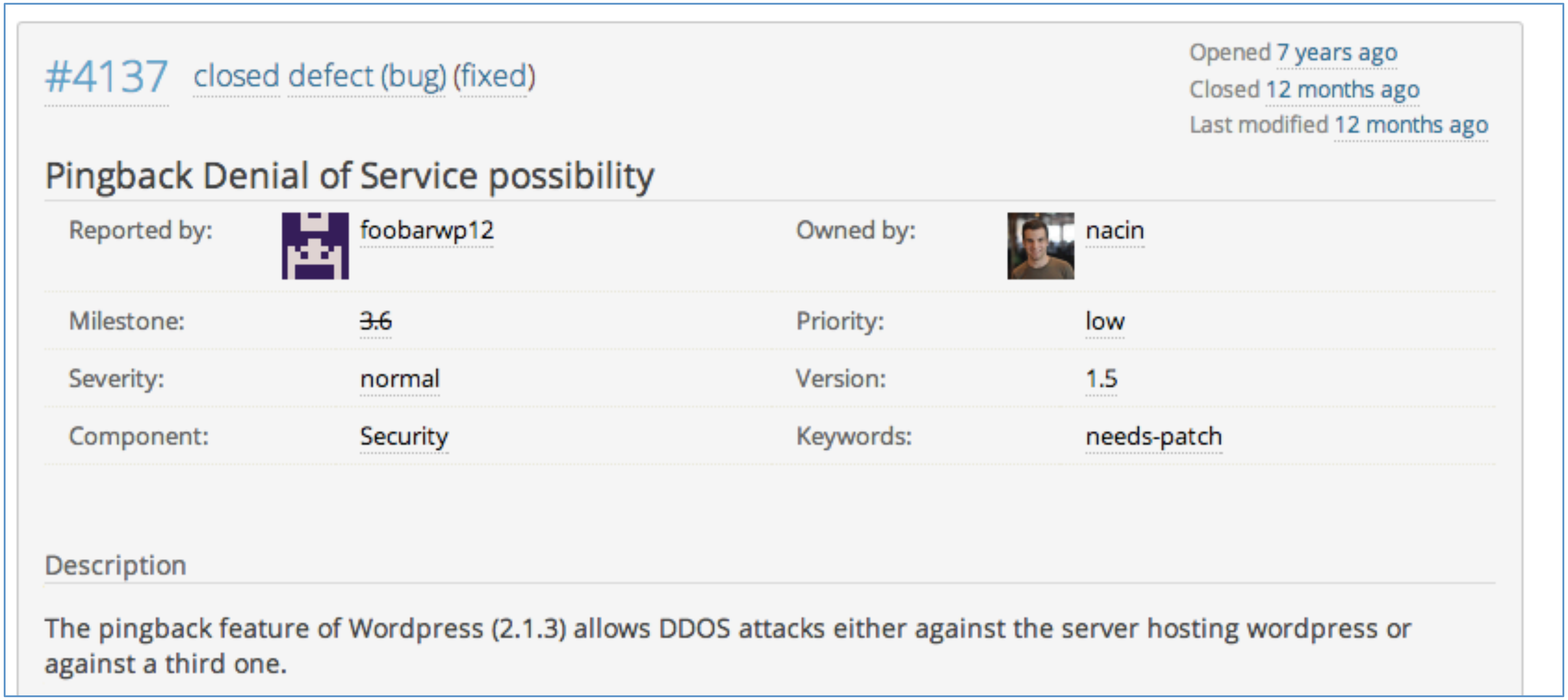


Analytics · November 28, 2013 – December 5, 2013

- Thanks to Steven Veldkamp

All materials posted at samsclass.info and free to use

WordPress Has Known for 7 Years



#4137 closed defect (bug) (fixed)

Opened 7 years ago
Closed 12 months ago
Last modified 12 months ago

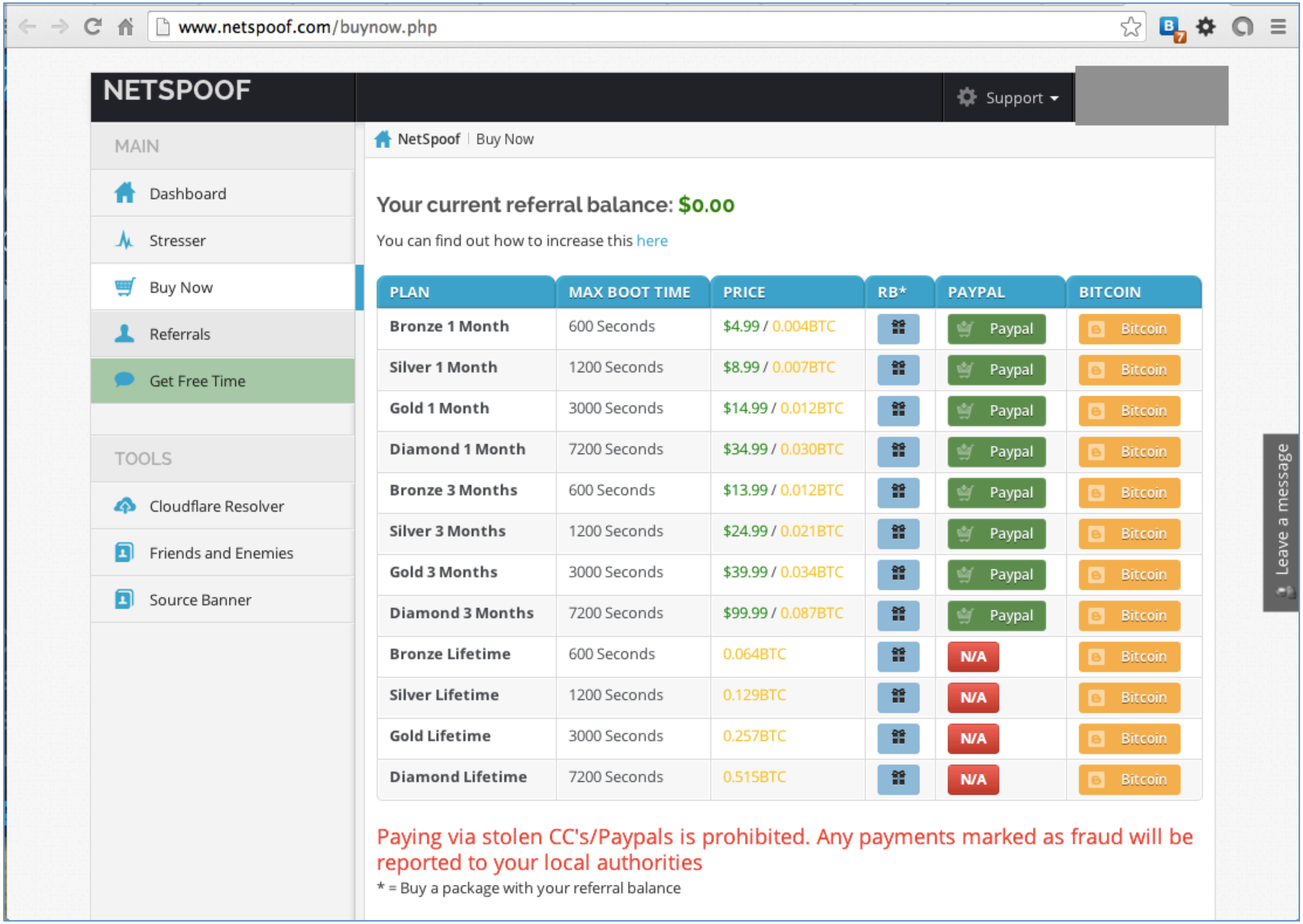
Pingback Denial of Service possibility

Reported by:	foobarwp12	Owned by:	nacin
Milestone:	~~3.6~~	Priority:	low
Severity:	normal	Version:	1.5
Component:	Security	Keywords:	needs-patch

Description

The pingback feature of Wordpress (2.1.3) allows DDOS attacks either against the server hosting wordpress or against a third one.

All materials posted at samsclass.info and free to use



[redacted]

Your current referral balance: $0.00

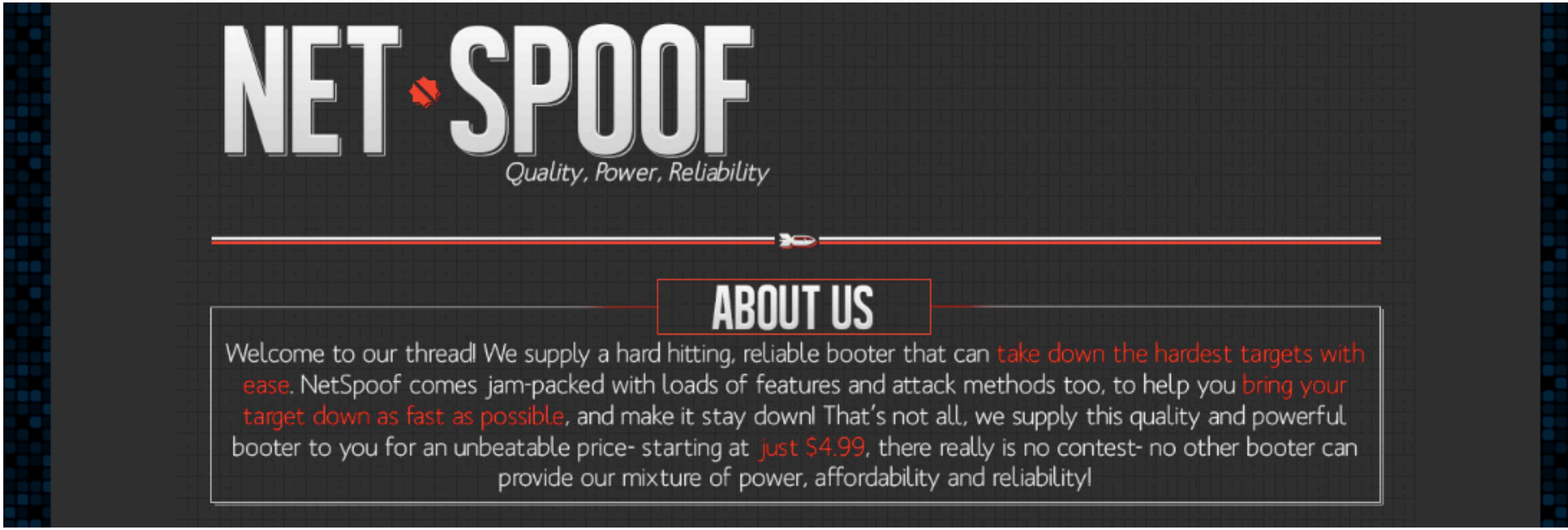
You can find out how to increase this here

PLAN	MAX BOOT TIME	PRICE	RB*	PAYPAL	BITCOIN
Bronze 1 Month	600 Seconds	$4.99 / 0.004BTC	🎁	Paypal	Bitcoin
Silver 1 Month	1200 Seconds	$8.99 / 0.007BTC	🎁	Paypal	Bitcoin
Gold 1 Month	3000 Seconds	$14.99 / 0.012BTC	🎁	Paypal	Bitcoin
Diamond 1 Month	7200 Seconds	$34.99 / 0.030BTC	🎁	Paypal	Bitcoin
Bronze 3 Months	600 Seconds	$13.99 / 0.012BTC	🎁	Paypal	Bitcoin
Silver 3 Months	1200 Seconds	$24.99 / 0.021BTC	🎁	Paypal	Bitcoin
Gold 3 Months	3000 Seconds	$39.99 / 0.034BTC	🎁	Paypal	Bitcoin
Diamond 3 Months	7200 Seconds	$99.99 / 0.087BTC	🎁	Paypal	Bitcoin
Bronze Lifetime	600 Seconds	0.064BTC	🎁	N/A	Bitcoin
Silver Lifetime	1200 Seconds	0.129BTC	🎁	N/A	Bitcoin
Gold Lifetime	3000 Seconds	0.257BTC	🎁	N/A	Bitcoin
Diamond Lifetime	7200 Seconds	0.515BTC	🎁	N/A	Bitcoin

Paying via stolen CC's/Paypals is prohibited. Any payments marked as fraud will be reported to your local authorities

* = Buy a package with your referral balance

All materials posted at samsclass.info and free to use



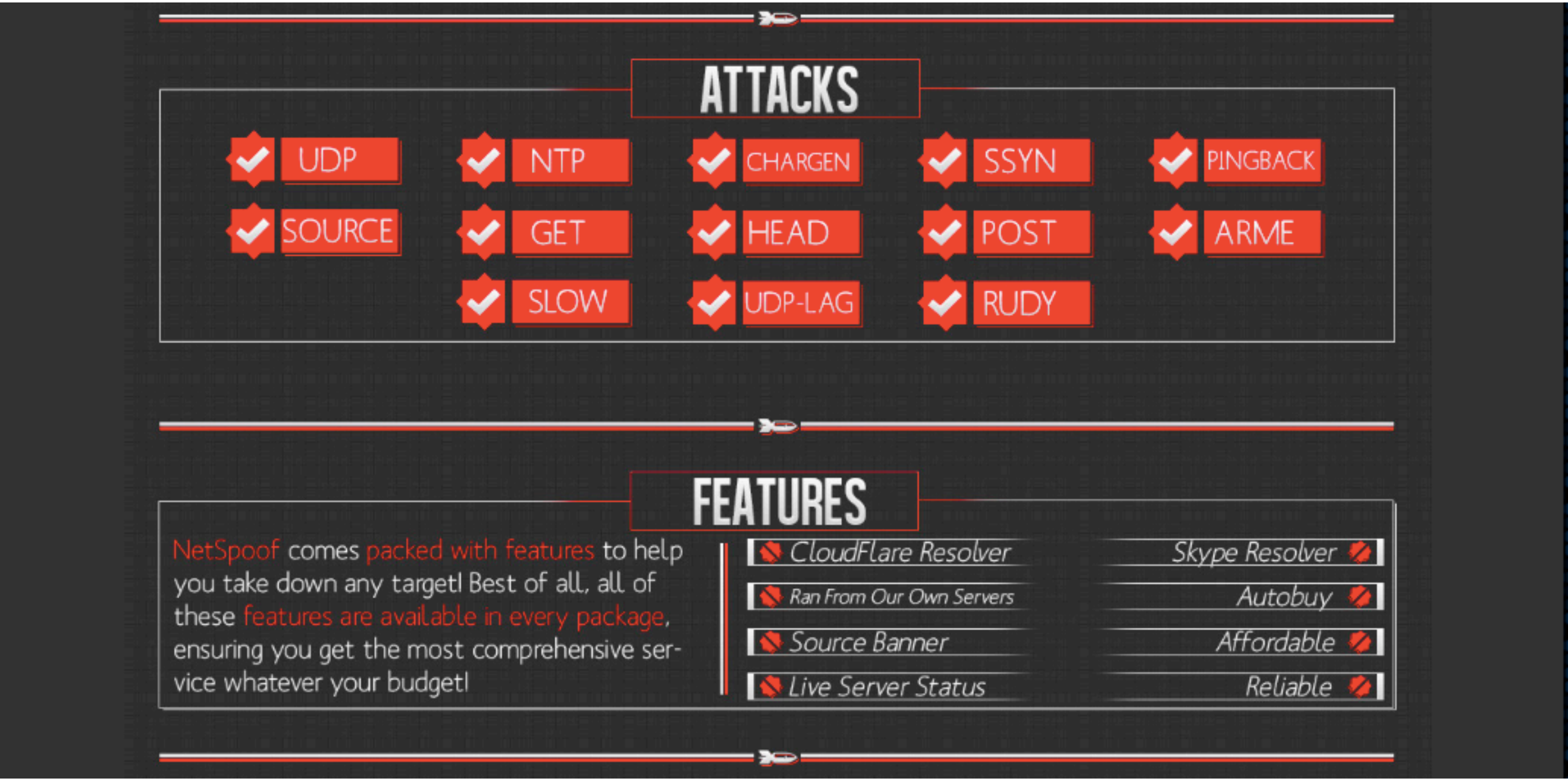
NET SPOOF

Quality, Power, Reliability

ABOUT US

Welcome to our thread! We supply a hard hitting, reliable booter that can take down the hardest targets with ease. NetSpoof comes jam-packed with loads of features and attack methods too, to help you bring your target down as fast as possible, and make it stay down! That's not all, we supply this quality and powerful booter to you for an unbeatable price- starting at just $4.99, there really is no contest- no other booter can provide our mixture of power, affordability and reliability!

All materials posted at samsclass.info and free to use



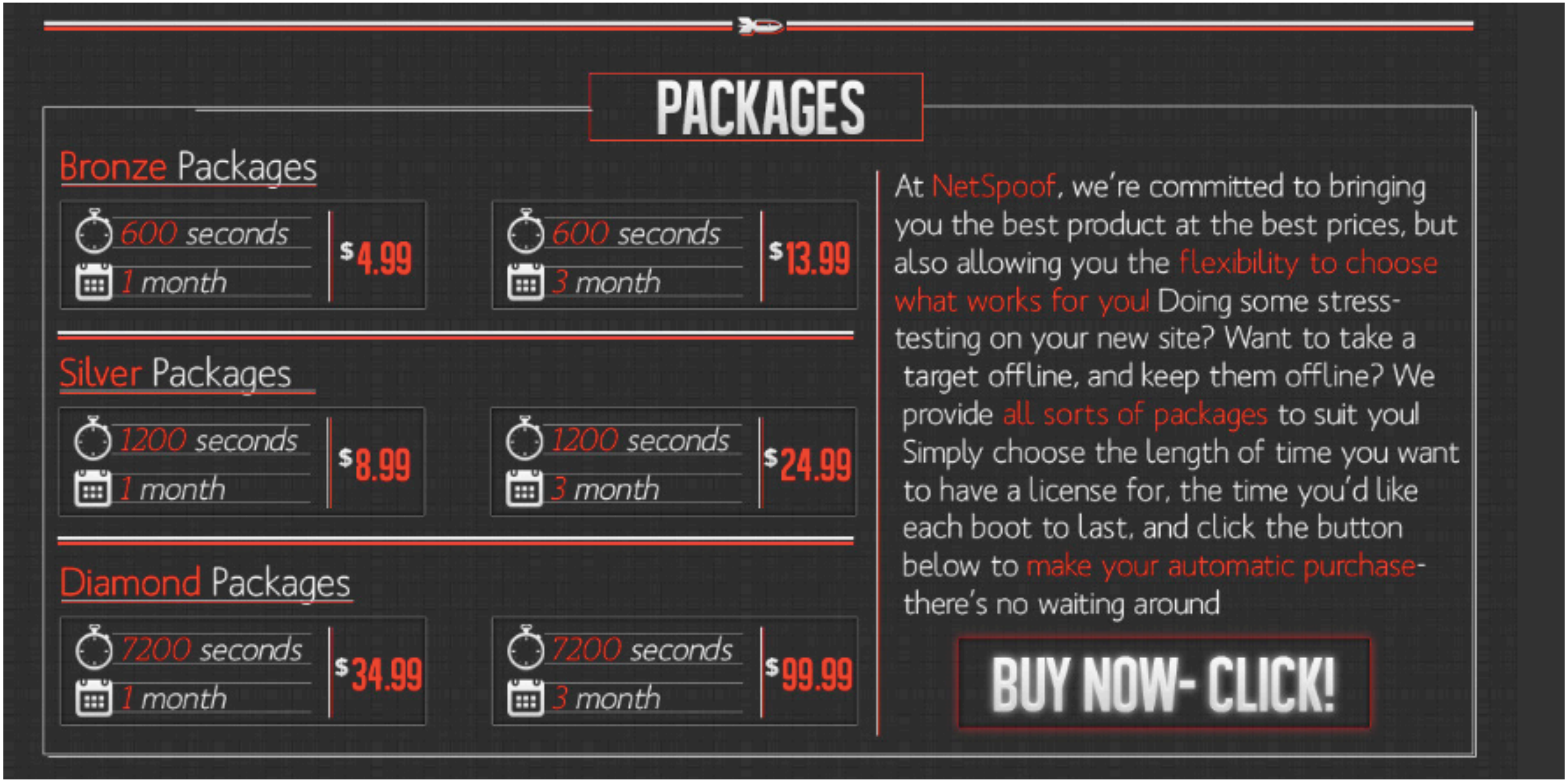
ATTACKS

- ✓ UDP
- ✓ SOURCE
- ✓ NTP
- ✓ GET
- ✓ SLOW
- ✓ CHARGEN
- ✓ HEAD
- ✓ UDP-LAG
- ✓ SSYN
- ✓ POST
- ✓ RUDY
- ✓ PINGBACK
- ✓ ARME

FEATURES

NetSpoof comes packed with features to help you take down any target! Best of all, all of these features are available in every package, ensuring you get the most comprehensive service whatever your budget!

- CloudFlare Resolver
- Ran From Our Own Servers
- Source Banner
- Live Server Status
- Skype Resolver
- Autobuy
- Affordable
- Reliable



PACKAGES

Bronze Packages

600 seconds 1 month	$4.99		600 seconds 3 month	$13.99

Silver Packages

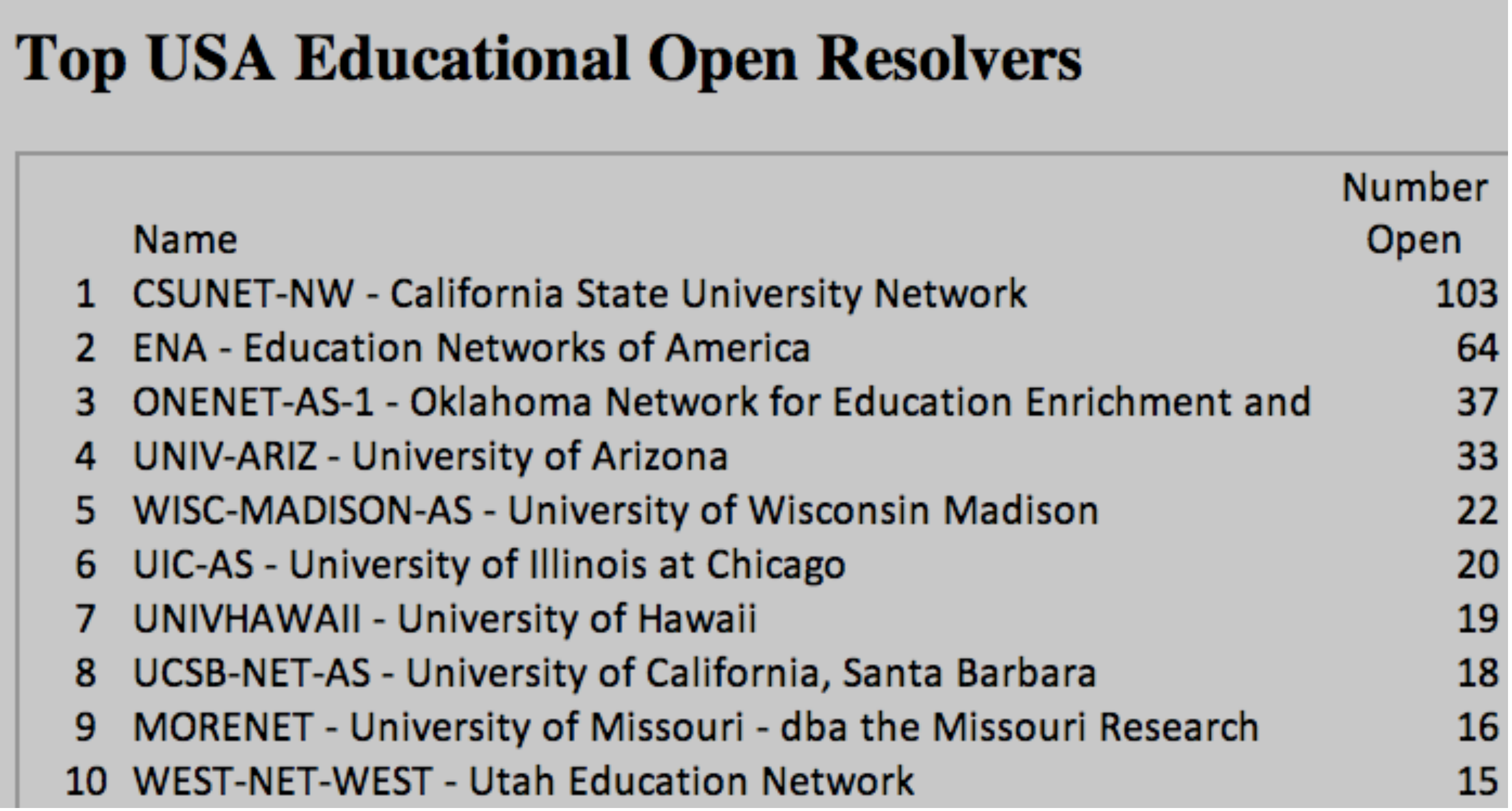
1200 seconds 1 month	$8.99		1200 seconds 3 month	$24.99

Diamond Packages

7200 seconds 1 month	$34.99		7200 seconds 3 month	$99.99

At NetSpoof, we're committed to bringing you the best product at the best prices, but also allowing you the flexibility to choose what works for you! Doing some stress-testing on your new site? Want to take a target offline, and keep them offline? We provide all sorts of packages to suit you! Simply choose the length of time you want to have a license for, the time you'd like each boot to last, and click the button below to make your automatic purchase- there's no waiting around

Open DNS Resolvers at Colleges

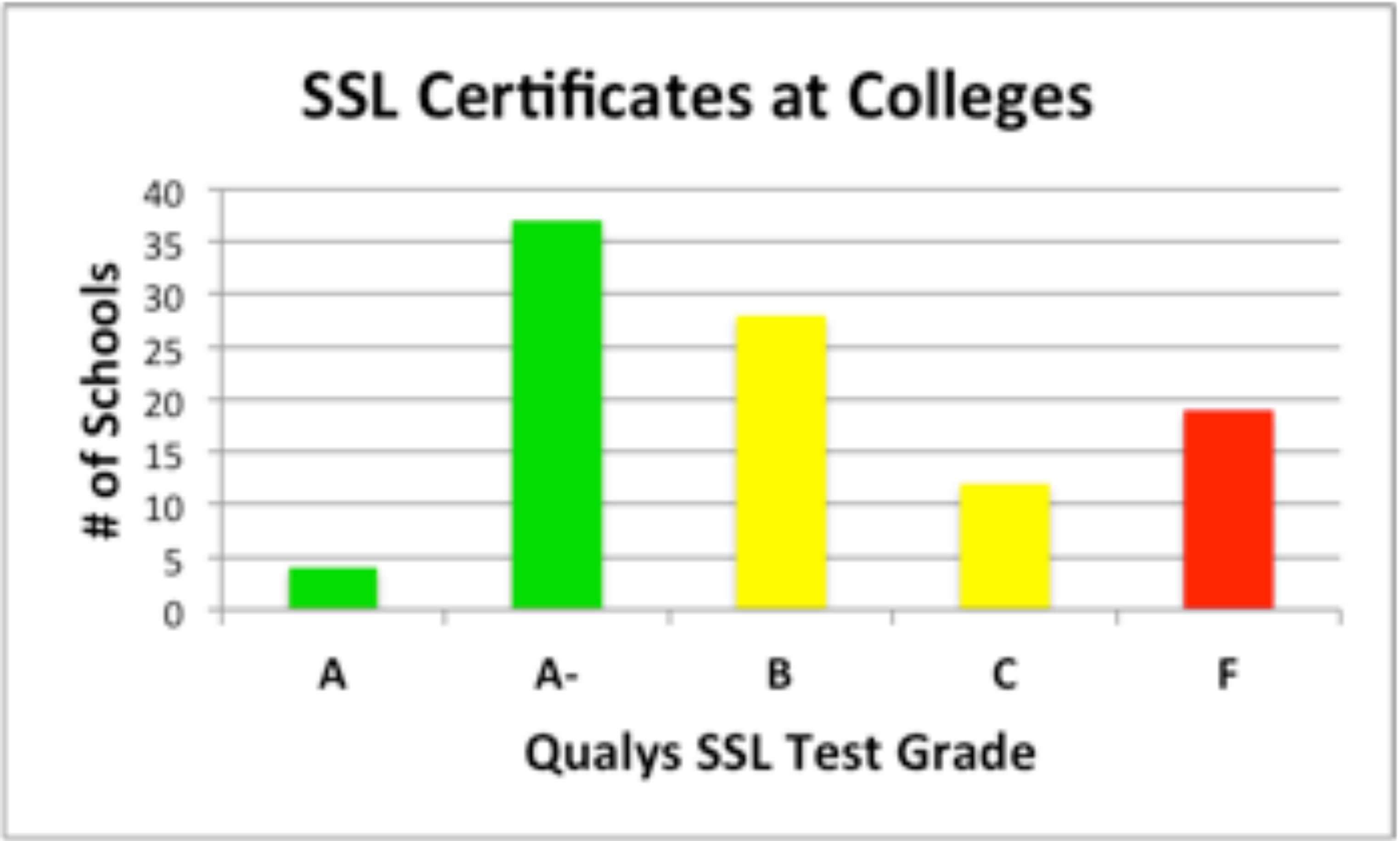


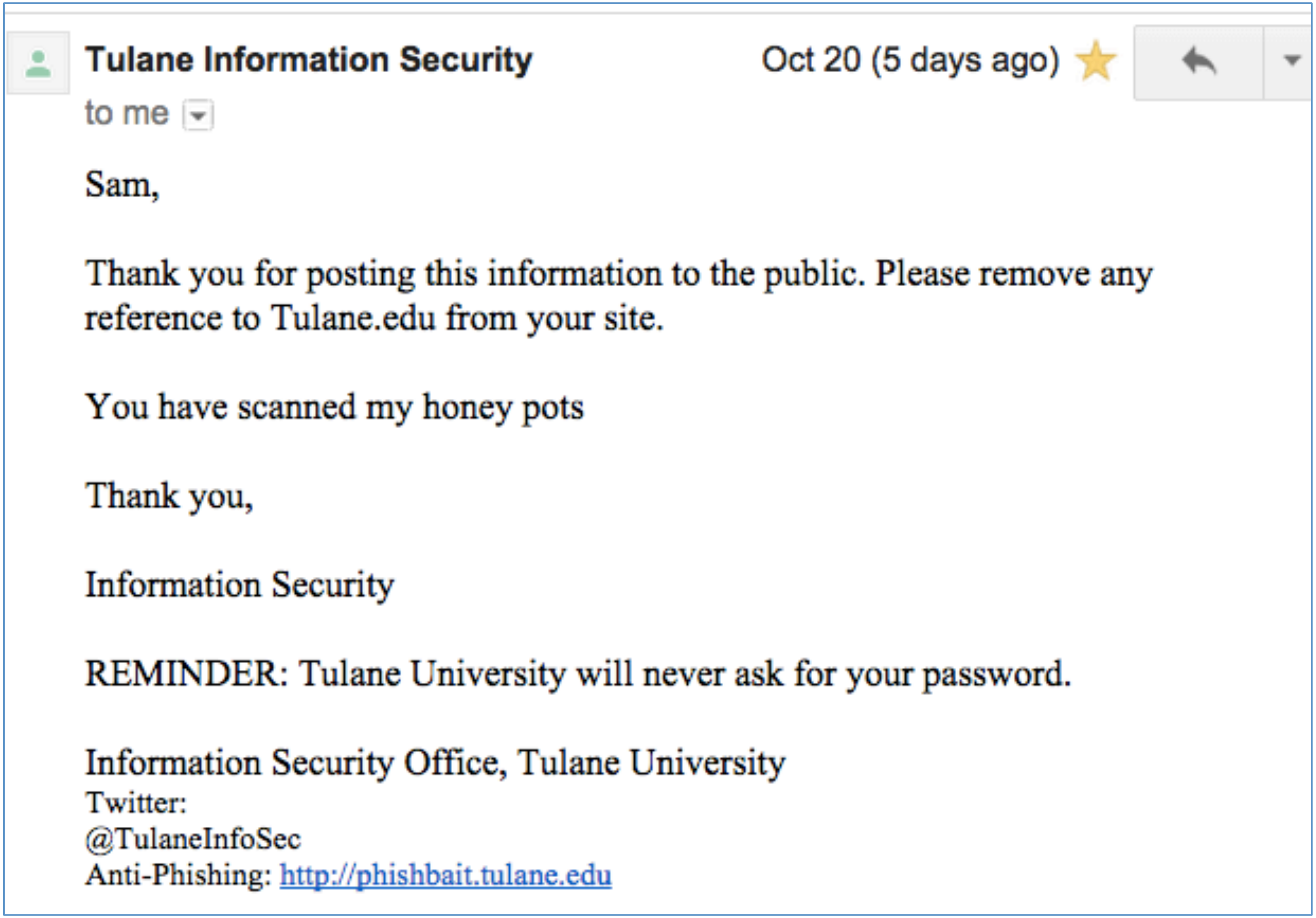
Top USA Educational Open Resolvers

		Number
	Name	Open
1	CSUNET-NW - California State University Network	103
2	ENA - Education Networks of America	64
3	ONENET-AS-1 - Oklahoma Network for Education Enrichment and	37
4	UNIV-ARIZ - University of Arizona	33
5	WISC-MADISON-AS - University of Wisconsin Madison	22
6	UIC-AS - University of Illinois at Chicago	20
7	UNIVHAWAII - University of Hawaii	19
8	UCSB-NET-AS - University of California, Santa Barbara	18
9	MORENET - University of Missouri - dba the Missouri Research	16
10	WEST-NET-WEST - Utah Education Network	15

Results

- Seven months after notification
- 38% decrease in open resolvers, from a total of 682 to 421


SSL Certificates at Colleges
# of Schools
40
35
30
25
20
15
10
5
0
A
A-
B
C
F
Qualys SSL Test Grade



Sam,

Thank you for posting this information to the public. Please remove any reference to Tulane.edu from your site.

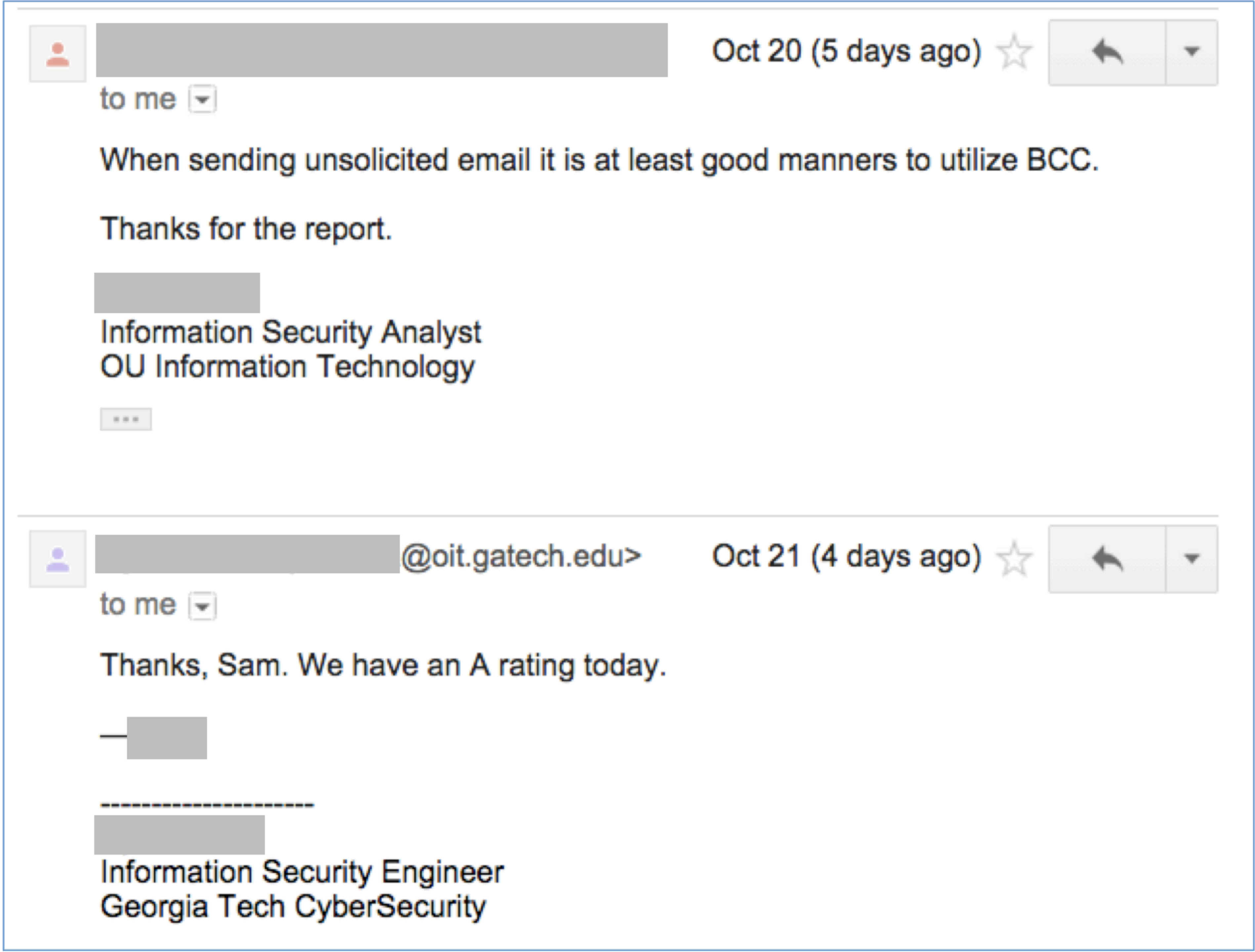
You have scanned my honey pots

Thank you,

Information Security

REMINDER: Tulane University will never ask for your password.

Information Security Office, Tulane University
Twitter:
@TulaneInfoSec
Anti-Phishing: http://phishbait.tulane.edu



[redacted] Oct 20 (5 days ago)

to me

When sending unsolicited email it is at least good manners to utilize BCC.

Thanks for the report.

[redacted]
Information Security Analyst
OU Information Technology

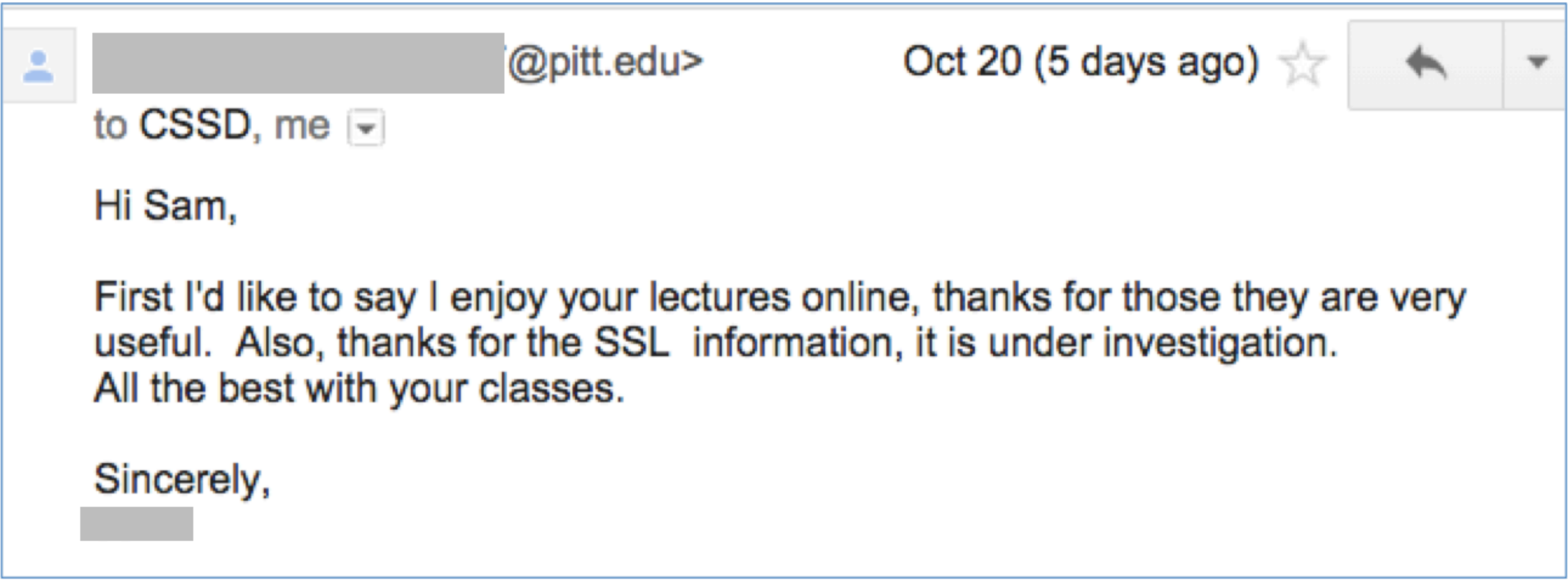
[redacted]@oit.gatech.edu> Oct 21 (4 days ago)

to me

Thanks, Sam. We have an A rating today.

—[redacted]

[redacted]
Information Security Engineer
Georgia Tech CyberSecurity



[redacted]@pitt.edu> Oct 20 (5 days ago)

to CSSD, me

Hi Sam,

First I'd like to say I enjoy your lectures online, thanks for those they are very useful. Also, thanks for the SSL information, it is under investigation.
All the best with your classes.

Sincerely,
[redacted]

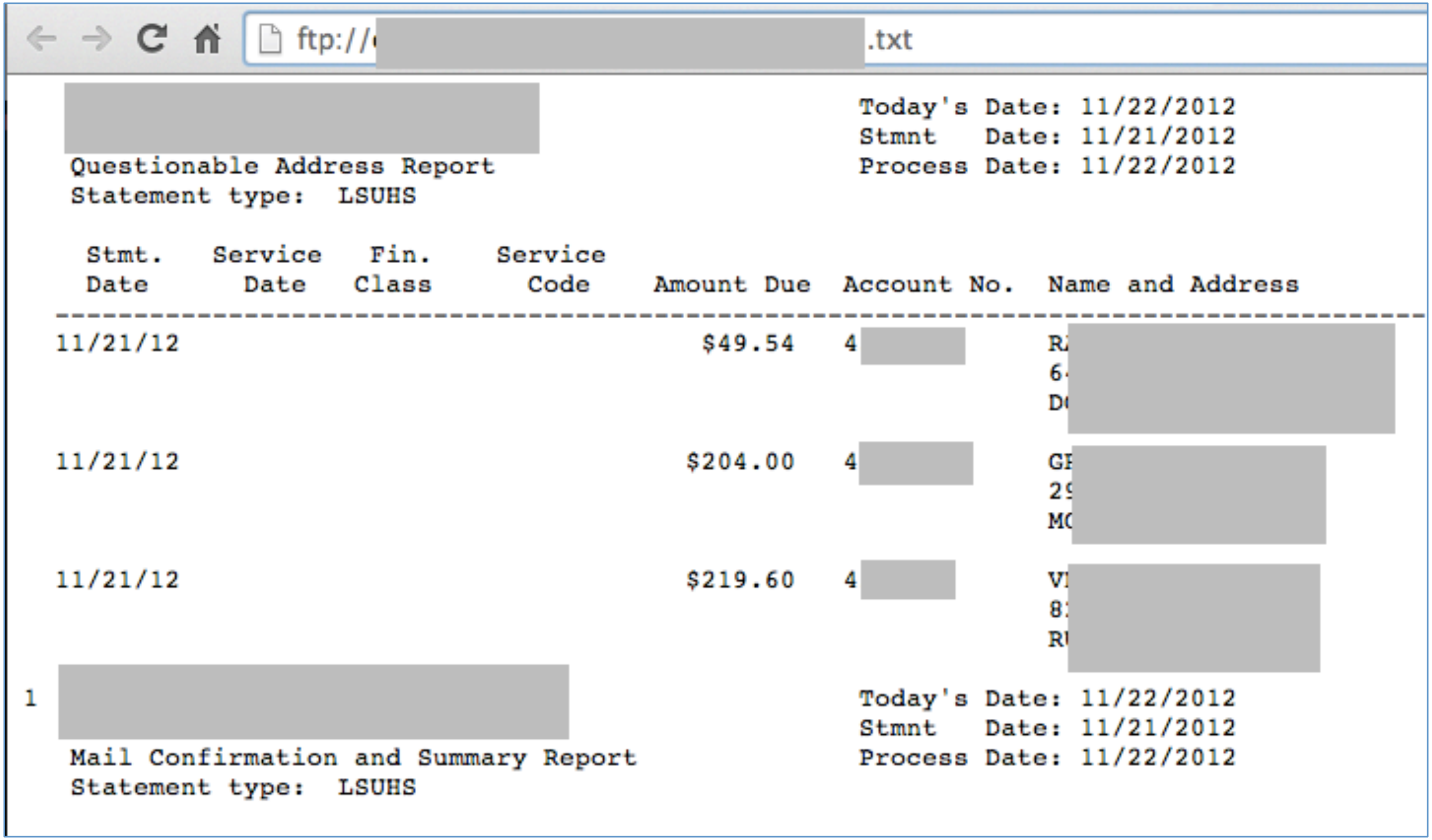
All materials posted at samsclass.info and free to use

Results After 4 Days

- 4/19 colleges improved their rating
- 3 emails returned (but one of them improved)
- 4 responses, 2 hostile, 2 friendly

HIPAA Violation at LSU

Open FTP Server with Medical Data



ftp://[redacted].txt

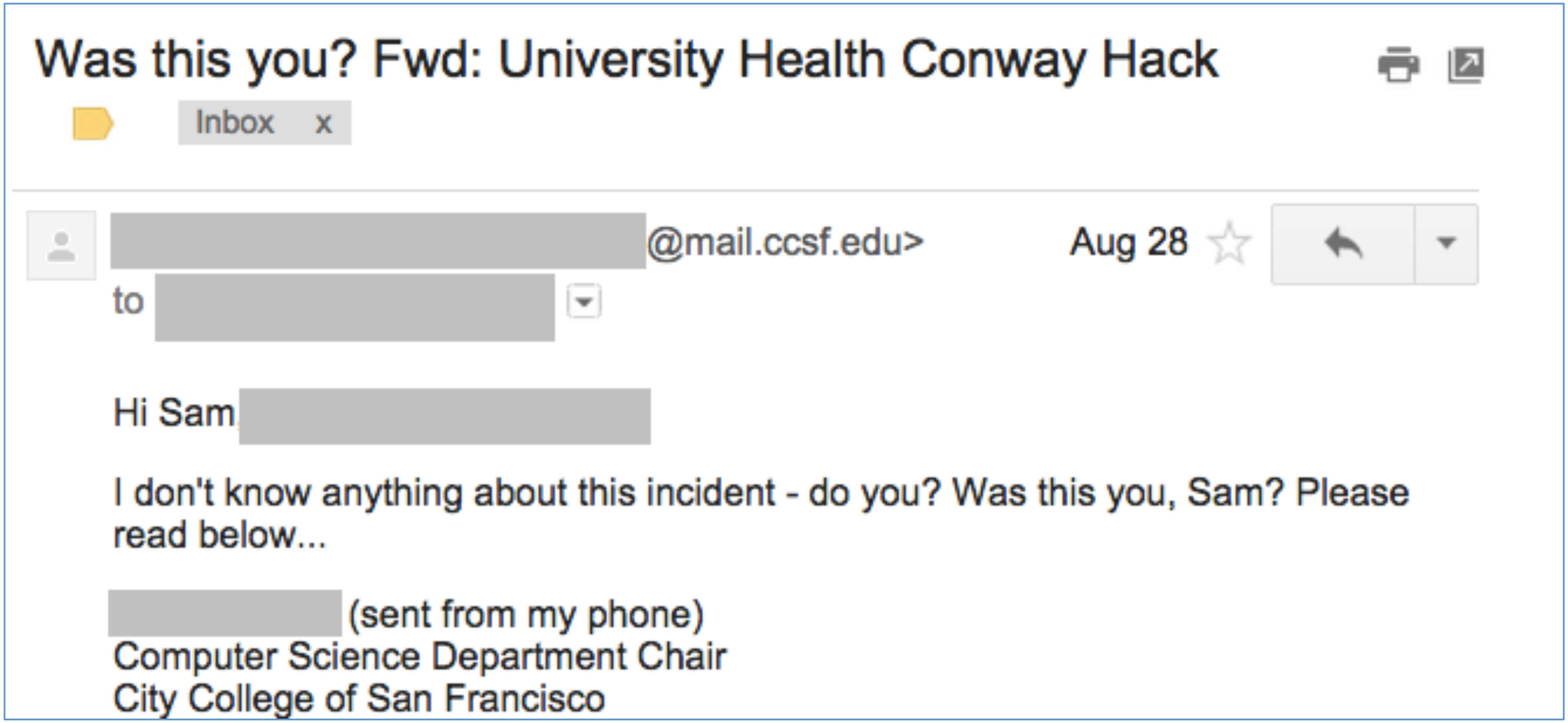
```
 [redacted]                                          Today's Date: 11/22/2012
                                                     Stmnt   Date: 11/21/2012
 Questionable Address Report                         Process Date: 11/22/2012
 Statement type:  LSUHS

  Stmt.    Service   Fin.     Service
  Date       Date    Class      Code    Amount Due   Account No.   Name and Address
--------------------------------------------------------------------------------------
11/21/12                                    $49.54   4[redacted]   [redacted]

11/21/12                                   $204.00   4[redacted]   [redacted]

11/21/12                                   $219.60   4[redacted]   [redacted]

1 [redacted]                                         Today's Date: 11/22/2012
                                                     Stmnt   Date: 11/21/2012
 Mail Confirmation and Summary Report                Process Date: 11/22/2012
 Statement type:  LSUHS
```

All materials posted at samsclass.info and free to use

Reaction

- I notified them on June 17, 2014
- No reply, but server was down 4 hours later
- Then on Aug. 28...

Reaction



Was this you? Fwd: University Health Conway Hack

[redacted]@mail.ccsf.edu> Aug 28

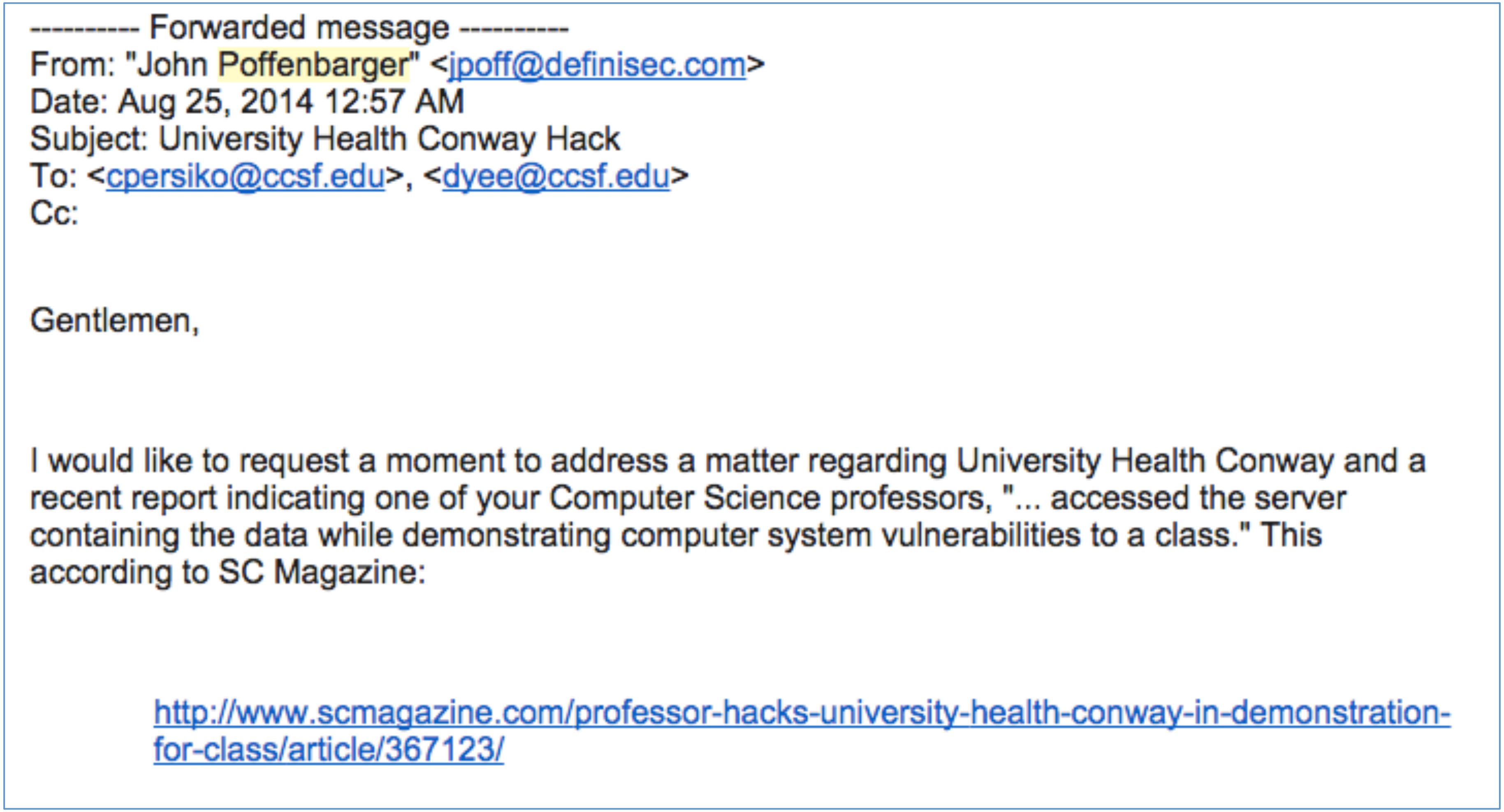
to [redacted]

Hi Sam [redacted]

I don't know anything about this incident - do you? Was this you, Sam? Please read below...

[redacted] (sent from my phone)
Computer Science Department Chair
City College of San Francisco

John Poffenbarger



---------- Forwarded message ----------
From: "John Poffenbarger" <jpoff@definisec.com>
Date: Aug 25, 2014 12:57 AM
Subject: University Health Conway Hack
To: <cpersiko@ccsf.edu>, <dyee@ccsf.edu>
Cc:

Gentlemen,

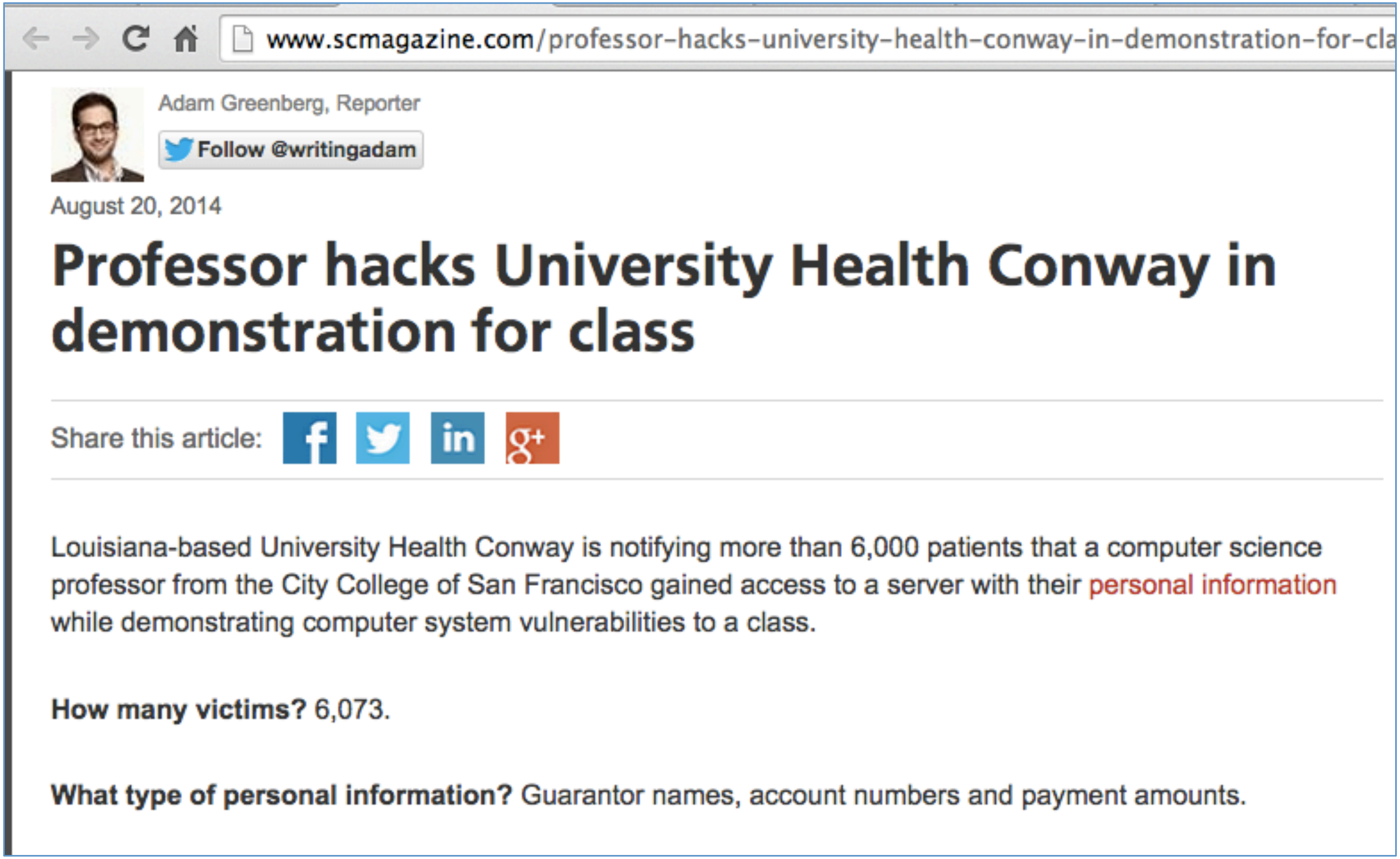
I would like to request a moment to address a matter regarding University Health Conway and a recent report indicating one of your Computer Science professors, "... accessed the server containing the data while demonstrating computer system vulnerabilities to a class." This according to SC Magazine:

http://www.scmagazine.com/professor-hacks-university-health-conway-in-demonstration-for-class/article/367123/

All materials posted at samsclass.info and free to use

John Poffenbarger

- I encourage you to promptly investigate after publicly denouncing any such behaviors, as I would not expect an institution to accept, endorse, or tolerate any such actions.
- I would have to wonder how this would affect the moral judgment of your graduating students entering the workforce.



www.scmagazine.com/professor-hacks-university-health-conway-in-demonstration-for-cla

Adam Greenberg, Reporter

Follow @writingadam

August 20, 2014

Professor hacks University Health Conway in demonstration for class

Share this article:

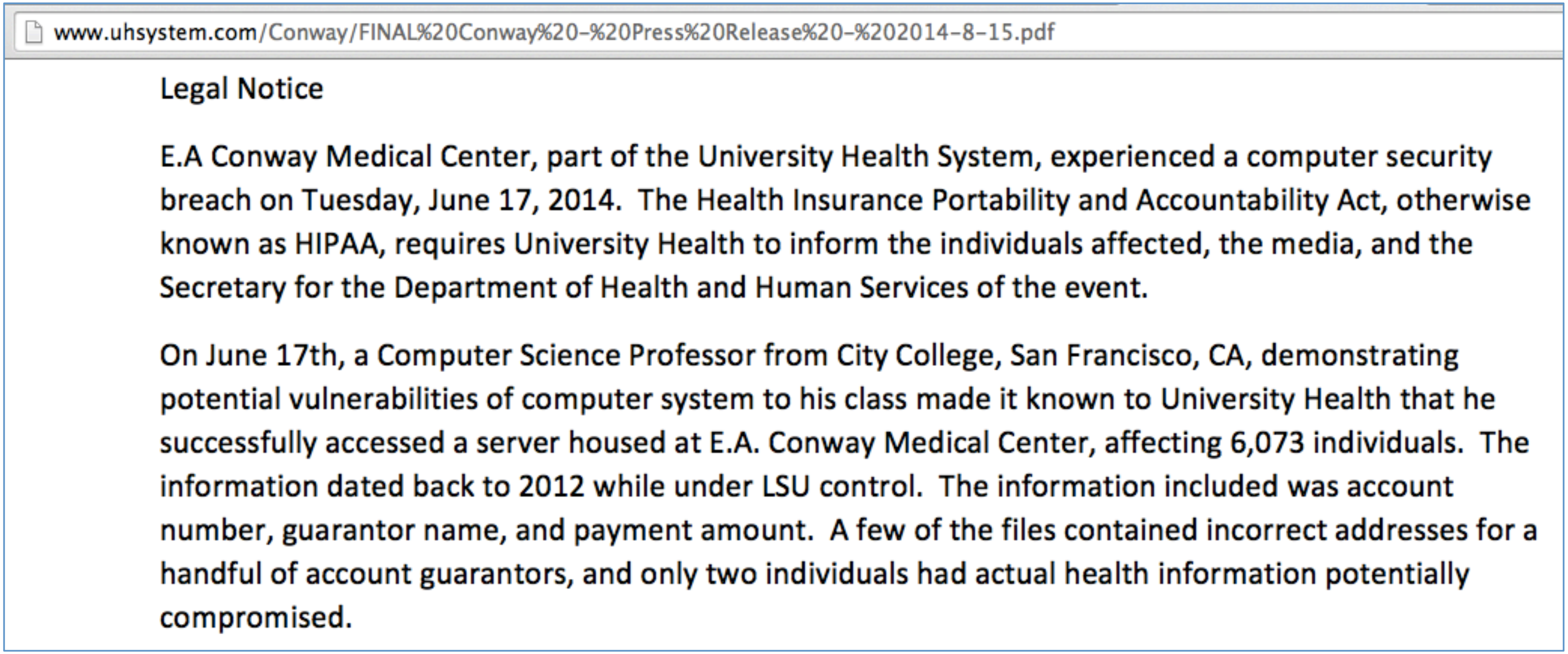
Louisiana-based University Health Conway is notifying more than 6,000 patients that a computer science professor from the City College of San Francisco gained access to a server with their personal information while demonstrating computer system vulnerabilities to a class.

How many victims? 6,073.

What type of personal information? Guarantor names, account numbers and payment amounts.

All materials posted at samsclass.info and free to use

LSU Legal Notice



www.uhsystem.com/Conway/FINAL%20Conway%20-%20Press%20Release%20-%202014-8-15.pdf

Legal Notice

E.A Conway Medical Center, part of the University Health System, experienced a computer security breach on Tuesday, June 17, 2014. The Health Insurance Portability and Accountability Act, otherwise known as HIPAA, requires University Health to inform the individuals affected, the media, and the Secretary for the Department of Health and Human Services of the event.

On June 17th, a Computer Science Professor from City College, San Francisco, CA, demonstrating potential vulnerabilities of computer system to his class made it known to University Health that he successfully accessed a server housed at E.A. Conway Medical Center, affecting 6,073 individuals. The information dated back to 2012 while under LSU control. The information included was account number, guarantor name, and payment amount. A few of the files contained incorrect addresses for a handful of account guarantors, and only two individuals had actual health information potentially compromised.

All materials posted at samsclass.info and free to use

I Protested

- To the reporter
- To the CEO of his newspaper
- To the Feds, against LSU, for HIPAA whistleblower retaliation

- After a few days, it was clear that none of this was going to do any good

I Believed

1. My actions were 100% lawful
2. Newspapers can't just publish complete lies and get away with it
3. I enjoyed HIPAA whistleblower protection
4. I'm in real trouble now, time to call a lawyer

Part 2: Alex Muentz