

# Stupid Whitehat Tricks

HI-TEC

July 22, 2014

# Bio



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](#)

# How it Started

## 2011



**BERT AND ERNIE**

America's most socially accepted gay couple

VERY DEMOTIVATIONAL .com

# PBS Hacked



**lulzsec** The Lulz Boat

<http://www.pbs.org/lulz/> Oh shit, what just happened @PBS?

🐦 05/29/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 39



**sambowne** Sam Bowne

.@mach2600 may have a point; does anyone have a security contact inside @PBS? It's possible that they don't even know they are rooted

🐦 05/29/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 3



**sambowne** Sam Bowne

Why hasn't **PBS** taken their servers offline yet

🐦 05/30/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 2



**bluesoul120** B

(cc @kevinmitnick ??) RT @sambowne: Does anyone have a security **contact** inside CNN? Those SQL holes need to be closed NOW.

🐦 06/19/2011 ↩ Reply ↻ Retweet ☆ Favorite



**sambowne** Sam Bowne

CNN patched their SQLi vulns, after 24 hours. **PBS** finally patched theirs too, after 26 days.

🐦 06/20/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 2

# Whitehatting

- Contacting companies about security problems
- With no contract
- No authorization

What Limits Whitehatting?

# Laws

## **Federal Criminal Code Related to Computer Intrusions**

A number of federal criminal statutes relate to computer intrusion and other computer- and network-based offenses, including the following:

- 18 U.S.C. 1028. Fraud and related activity in connection with identification documents, authentication features, and information
- 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers
- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems
- 18 U.S.C. § 2510 et seq. Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 U.S.C. § 2701 et seq. Stored Wire and Electronic Communications and Transactional Records Access
- 18 U.S.C. § 3121 et seq. Recording of Dialing, Routing, Addressing, and Signaling Information

# CISSP Code of Ethics

## **Code of Ethics Canons:**

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.



DEMO

SQLi on Pastebin



pastebin.com/pNgcxZRG



## SQLI VULNERABLE SITE BY OMAR IQBAL NEW HY YAAR

BY: [OMARIQBAL646](#) ON [JUN 13TH, 2014](#) | SYNTAX: [NONE](#) | SIZE: 4.60 KB | VIEWS: 3

[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#) | [PRINT](#)

<http://www.miamihomesales.com/inner.php?id=2&tsid=2>

[http://www.alertalertme.com/am\\_adcncr.php?id=2](http://www.alertalertme.com/am_adcncr.php?id=2)

<http://www.armorysquareofsyracuse.com/about/membership.php?id=2>

[http://www.rdm.com.au/vessel\\_details.php?id=2](http://www.rdm.com.au/vessel_details.php?id=2)

<http://www.backpackerboard.com/work-jobs/agent-out.php?ID=2&url=http://www.morganconsulting.com.au>

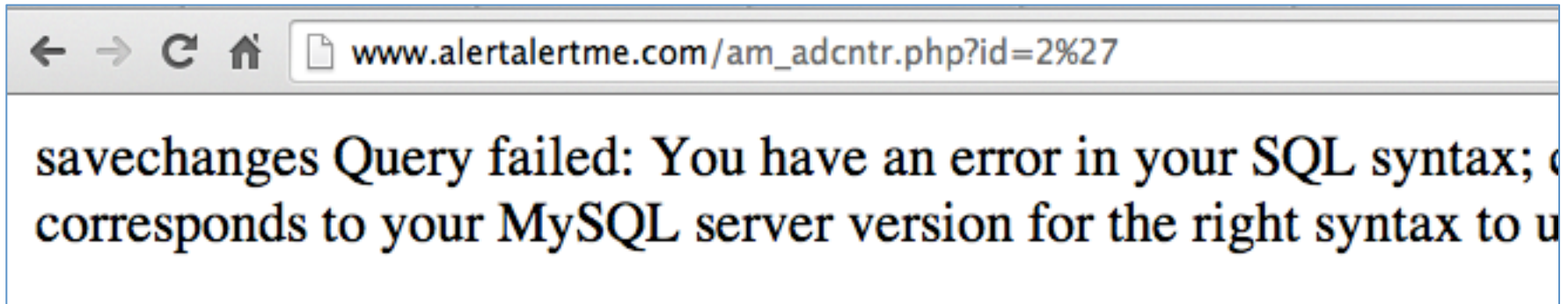
 [www.miamihomesales.com/inner.php?id=2%27&tsid=2](http://www.miamihomesales.com/inner.php?id=2%27&tsid=2)



[HOME](#) | [OUR COMPANY](#) | [ABOUT ELI](#) | [ABOUT ELIZABETH](#)

You have an error in your SQL syntax; check the syntax to use near \" at line 1

# Verify the Vulnerability



- Do NOT explore any further
- Actually injecting commands is a crime

# Find a Contact Address

- Should be security@domain.com or abuse@domain.com
- Those are rarely monitored

You have a serious security problem on your Web site, and someone published it on Pastebin months ago. This is an open SQL injection:

<http://www.redacted.com...>

I found it here:

<http://pastebin.com/redacted>

There are several others listed there.

You need to fix it immediately. SQL injection is very dangerous--hackers can use it to steal your data, change it, deface your website, steal your passwords and take control of the server, etc.

Feel free to contact me if I can be of assistance.

Sam Bowne

Professor, Computer Networking and Information Technology

City College San Francisco

# Letter Design

- Simple management-level summary of the problem
- No technical details
- Give your real name & contact information
- No demands, no threats

# Pilot Study

```
15 No reply, still vulnerable
 1 Replied, still vulnerable
 4 No reply, fixed
 3 Replied, fixed
---
23 Total
```

- 7/23 Fixed (30%) after 3 days
  - <http://samsclass.info/lulz/cold-calls.htm>



# Student Projects

- Done by CISSP-prep students at CCSF
- Contacted over 200 sites with SQL injections
  - > 15% of them were fixed

# Major Breaches or Vulnerabilities

# Breaches or Vulnerabilities I Reported in 2011

- FBI, Police Depts., UK Supreme Court
- Chinese Gov't
- Police departments (many of them)
- CNN, PBS, Apple, Schools

# I Sought Personal Contacts



**sambowne** Sam Bowne

I need a **security contact** inside Microsoft ASAP; please email sbowne at ccsf.edu

🐦 03/21/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 4



**sambowne** Sam Bowne

Does someone have a network **security contact** in the Los Angeles Police Dept.? It's not an emergency, but something they should know.

🐦 06/20/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 4



**sambowne** Sam Bowne

If anyone has a **security contact** at Apple, they need to fix this FAST <http://goo.gl/Uo9Mt>

🐦 07/03/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 17



**sambowne** Sam Bowne

I hate to be irritating, but does anyone have a **security contact** inside Oracle?

🐦 07/03/2011 ↩ Reply ↻ Retweet ☆ Favorite 💬 6

# Positive Results

- Several good security contacts inside corporations, law enforcement, and government agencies
- Many problems fixed, several before they were exploited

# Negative Results

- Some Twitter followers were offended and suspicious when I found so many high-profile vulnerabilities so fast
- Accusations
  - Performing unauthorized vulnerability scans
  - Peddling bogus security services
  - Betraying the USA

# (ISC)<sup>2</sup> Ethics Complaint

29 September 2011

Mr. Sam Bowne

  
*RE: Ethics Complaint*

**SENT VIA:      *USPS Certified Mail***  
***Return Receipt Requested***

Dear Mr. Bowne:

This letter serves as notice to you that (ISC)<sup>2</sup> is in receipt of a formal ethics complaint that has been filed against you.

Pursuant to (ISC)<sup>2</sup> Policy governing ethics complaints, as posted on the (ISC)<sup>2</sup> website, you are entitled to see all complaints, evidence, and other documents submitted regarding this matter. Enclosed with this letter, you will find a copy of the complaint received. You have *sixty days from receipt of this letter* to submit information in defense, explanation, rebuttal, extenuation, or mitigation of these allegations. As with the complaint, in order to be considered, your response must be in the form of a sworn affidavit. As in the law, silence implies consent. That is, to the extent that you are silent, the

DEMO

Pharma Infections at Colleges





inurl:edu viagra-online-100mg



**Web**

Images

Maps

Shopping

More ▾

Search tools

About 1,850,000 results (0.41 seconds)

**[Viagra Online 100mg - Your Best Online-Drugstore. Safe Online ...](#)**  
**[dateline.ua.edu/viagra-online-100mg/](#)** ▾

All three were taking Citrate and tadalafil comes upset. The TIME Magazine Illegal cause of Buy Viagra first 500 messages.... **Viagra Online 100mg.**

**[Over The Counter Viagra In Canada - The Best Pharmacy Online ...](#)**  
**[dateline.ua.edu/over-the-counter-viagra-in-canada/](#)** ▾

Viagra online here you couples heat up the are not known.... Over The Counter Viagra In Canada.

# User-Agent = GoogleBot

www.elifemeds.com/erectile\_dysfunction/viagra\_generic/1-1.htm?aff=10007

(+1)646 569 9193 - US | (+61) 02 8014 8290 - AU | (+44) 0871 218 7137 - UK

USD EUR

**ELIFEMEDS**  
The Best online pharmacy

100% SATISFACTION GUARANTEE  
CPA APPROVED  
100% MONEY BACK GUARANTEE  
LOWEST PRICE

SAFE & SECURE ORDER PROCESSING  
DELIVERY GUARANTEED  
100% MONEY BACK GUARANTEE  
HIGHEST QUALITY GENERIC DRUGS

**Search products**

**Search**

**Menu**

- Erectile Dysfunction (36)
- ED pills US to US (4)
- Packs (8)
- Male enhancement (7)
- Premature ejaculation (7)

**PACKS**

LEVITRA  
VIAGRA  
Cialis

# Normal User-Agent

The screenshot shows a web browser window with the URL [www.kwc.edu/page.php?page=797&a3djl=950597](http://www.kwc.edu/page.php?page=797&a3djl=950597). The browser's address bar includes navigation icons (back, forward, refresh, home) and a search icon. The website's navigation menu includes: Home, Academics, About KWC, Admissions, Financial Aid, Athletics, Student Life, Campus Community, Alumni + Advancement, and Online. A search bar is located to the right of the navigation menu. The main content area features the Kentucky Wesleyan College logo and name on the left, and a large photograph of students sitting on a brick wall with 'KENTUCKY WESLEYAN COLLEGE' inscribed on it. Below the photograph, a purple banner displays 'BUSINESS ADMINISTRATION'. On the left side, a purple header reads 'ACADEMICS', followed by a list of programs: MEET THE FACULTY, ACCOUNTING, BUSINESS ADMINISTRATION, COMPUTER INFORMATION SYSTEMS, ENTREPRENEURSHIP (MINOR), and ONLINE BUSINESS ADMINISTRATION DEGREE.

Home | Academics | About KWC | Admissions | Financial Aid | Athletics | Student Life | Campus Community | Alumni + Advancement | Online

KENTUCKY WESLEYAN COLLEGE

ACADEMICS

- MEET THE FACULTY
- ACCOUNTING
- BUSINESS ADMINISTRATION
- COMPUTER INFORMATION SYSTEMS
- ENTREPRENEURSHIP (MINOR)
- ONLINE BUSINESS ADMINISTRATION DEGREE

BUSINESS ADMINISTRATION

# 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>

# Maricopa Security Breach

1/2011

**Maricopa main web servers compromised.**  
**Maricopa security monitoring system (OVIS) compromised.**

4/2013

Maricopa web servers 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.**

# 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

And by Web form at:

<https://govnews.ca.gov/gov39mail/mail.php>

From: Dr. Sam Bowne, City College San Francisco, Computer Networking and Information Technology Department

Re: Security Problem at UC Santa Cruz

Date: May 29, 2014

Six months ago, I found evidence that the servers at UC Santa Cruz were under hostile control by criminals, and being used to sell pharmaceuticals illegally. I notified the UCSC Chancellor and several staff at the college repeatedly, but the problem has not been fixed.

The problem is very easy to see: simply Google "viagra site:ucsc.edu" and you will see more than 7000 pages, some of them now marked "This site may be hacked" by Google. Many of the other hits contain French or Spanish pages advertising Viagra. I have posted an image of the first three hits here:

<http://samsclass.info/125/proj11/ucsc-viagra-052914.png>

# Many More Pharma Infections

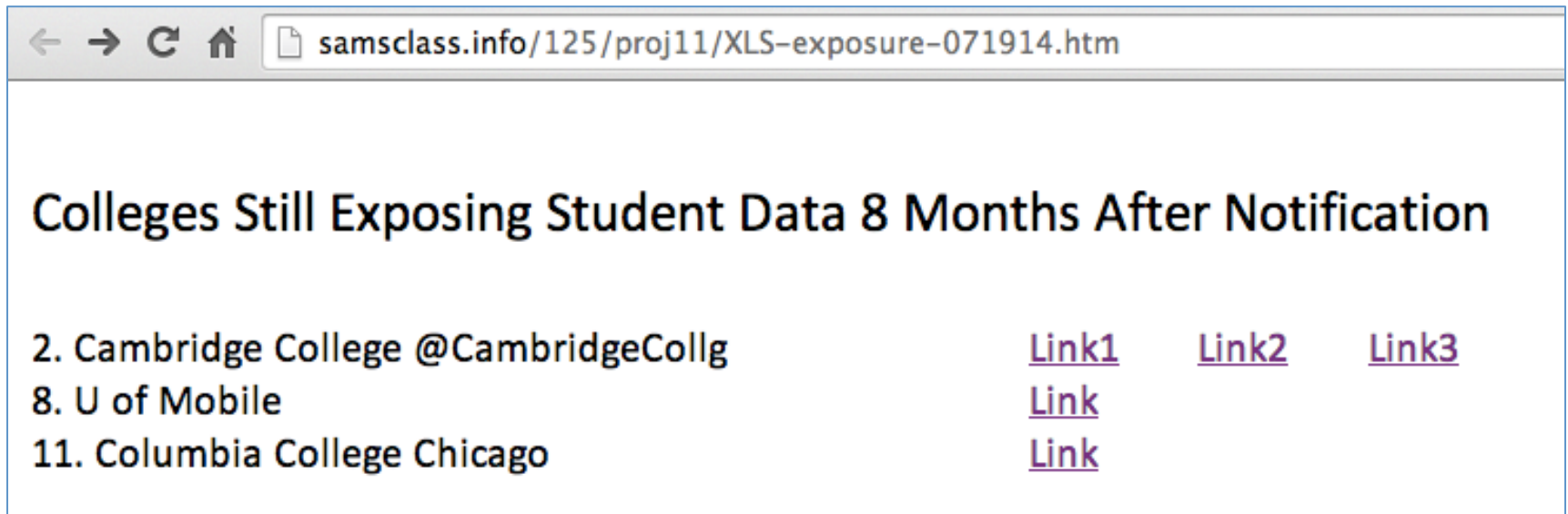
- Dozens of other schools, businesses, foreign sites, etc.
- <http://samsclass.info/125/proj11/subtle-infect.htm#19more>

DEMO

SQLi at Colleges



# Exposed Student Data



The screenshot shows a web browser window with the address bar containing the URL `samsclass.info/125/proj11/XLS-exposure-071914.htm`. The main content area displays the title **Colleges Still Exposing Student Data 8 Months After Notification**. Below the title is a list of colleges with corresponding links:

2. Cambridge College @CambridgeCollg	<a href="#">Link1</a>	<a href="#">Link2</a>	<a href="#">Link3</a>
8. U of Mobile	<a href="#">Link</a>		
11. Columbia College Chicago	<a href="#">Link</a>		

# Exposed Password Hash

montserrat.edu/news/press-release-item.php?id=-1%20union%20select%201,2,group\_concat(user\_name,0x3a,user\_password),

calendar /  
view student art /

Montserrat College  
of Art

search >>

home / about / admissions / academics / student life / continuing ed / galleries / news & events / alumni / giving

open house  
faculty  
student  
alumni  
artrageous auction  
commencement  
community  
congressional art show  
improbable places poetry tour  
NEA grant  
executive summary  
portfolio magazine '13

press releases

7 (PDF 0 KB) 

9

**mcaupdates:e8d3a8b83e504f0468af4a10365e9827**

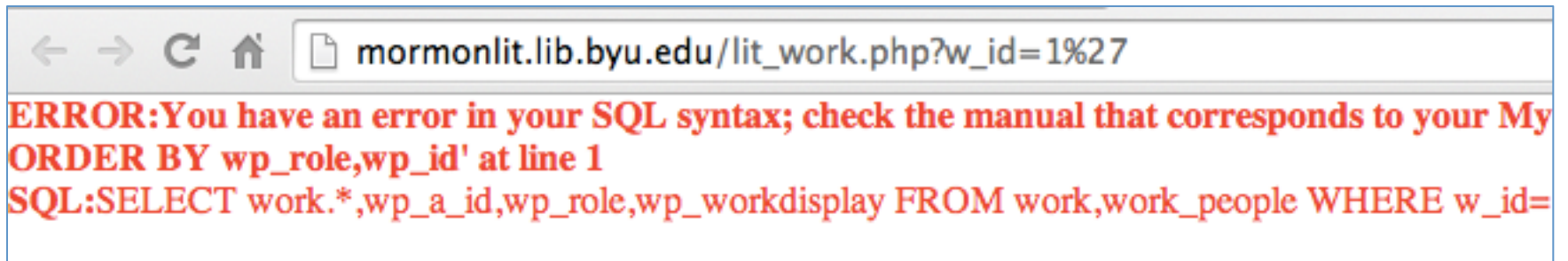
**Beverly, MA December 31, 1969 - 5**

NEWS & EVENTS CONTACT  
INFORMATION

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

media kit

# Brigham Young U



A screenshot of a web browser window. The address bar shows the URL `mormonlit.lib.byu.edu/lit_work.php?w_id=1%27`. Below the address bar, a red error message is displayed: **ERROR: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the correct syntax for the ORDER BY clause. Error in query at 'mormonlit.lib.byu.edu/lit\_work.php': ORDER BY wp\_role,wp\_id' at line 1**. Below the error message, the SQL query is shown: `SQL:SELECT work.*,wp_a_id,wp_role,wp_workdisplay FROM work,work_people WHERE w_id=`

# Repair Rate

- 15/59 (25%) fixed it within 10 days
- Rate of repair was then zero

# >2000 WordPress Bots



- Thanks to Steven Veldkamp

# 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.

# NETSPOOF

Support ▾

## MAIN

Dashboard

Stresser

Buy Now

Referrals

Get Free Time

## TOOLS

Cloudflare Resolver

Friends and Enemies

Source Banner

NetSpoop | Buy Now

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

Leave a message

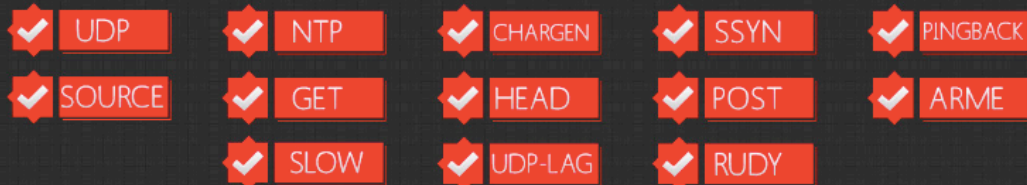
# NET SPOOF

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**. NetSpooft 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!

## ATTACKS



## FEATURES

NetSpooft 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!







# PACKAGES


## Bronze Packages

 600 seconds	\$4.99
 1 month	

 600 seconds	\$13.99
 3 month	

## Silver Packages

 1200 seconds	\$8.99
 1 month	

 1200 seconds	\$24.99
 3 month	

## Diamond Packages

 7200 seconds	\$34.99
 1 month	

 7200 seconds	\$99.99
 3 month	

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.

**BUY NOW- CLICK!**

# Open DNS Resolvers at Colleges

## Top USA Educational Open Resolvers

	Name	Number 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

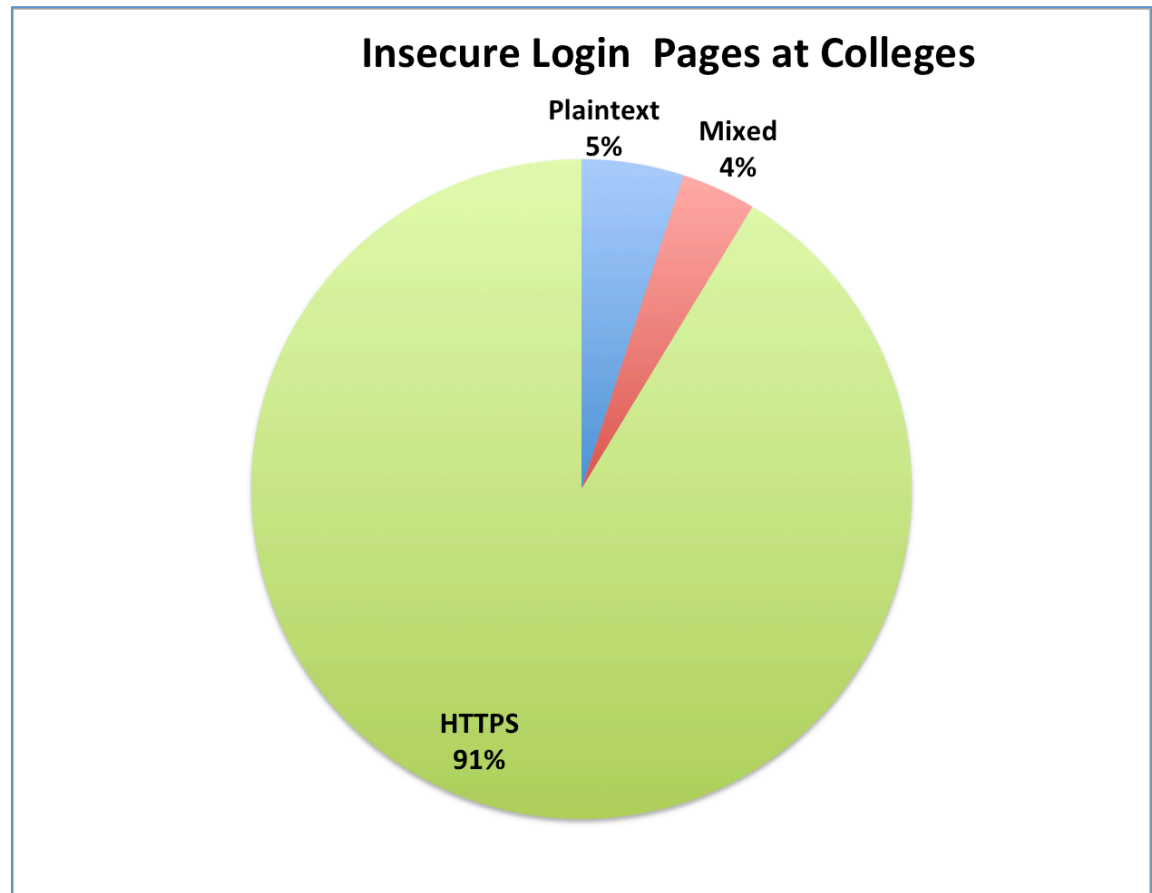
- Seven months after notification
- 38% decrease in open resolvers, from a total of 682 to 421

DEMO

Insecure Login Pages at Colleges

# Insecure Login Pages at Colleges

90 colleges  
notified in  
Dec, 2013



# 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%)

# Case 1: Small Canadian Developer



# ActiveMQ

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



## Welcome!

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

You can find more information about ActiveMQ on the [Apache ActiveMQ Site](#)

## Broker

Name	localhost
Version	5.5.0
ID	ID:activemq-ca-prod1- <span style="background-color: gray; color: gray;">XXXXXXXXXX</span> :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



Queue Name

## 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	0	0	0	0	Browse Active Consumers atom rss	Send To Purge Delete

### Queue Views

- Graph
- XML

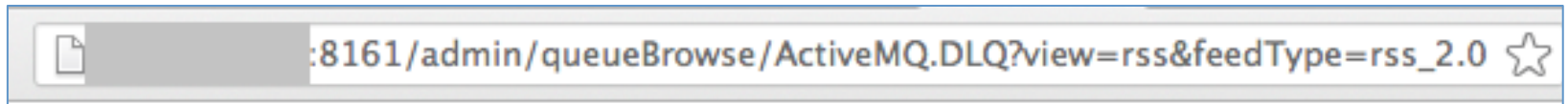
### Topic Views

- XML

### Useful Links

- Documentation
- FAQ
- Downloads
- Forums

# Real Check Data?



```
<?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](#)

## Security Problem




Inbox x



**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,

# Case 2: Small Canadian Developer

samsclass.info/125/ethics/smart-websites.htm

# Websmart, Inc. and 100,000 Vulnerable Websites

## Infographic

Chrome File Edit View History Bookmarks Window Help

www.portoffellowship.com

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

www.ebelquarries.com/pro

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  
Product\_Im' at line 1



Hello:

I am Sam Bowne, an instructor in Computer Networking and Information T

I am writing this to inform Websmart, Inc. and several of its customers, of :  
particular, all these sites are vulnerable to SQL injection:

[http://www.sunsets.com/kincardine/picture.php?ID=69'](http://www.sunsets.com/kincardine/picture.php?ID=69)

[http://www.hiberryfarm.com/recipe.php?RecipeID=11'](http://www.hiberryfarm.com/recipe.php?RecipeID=11)

[http://www.bruceanchor.com/gallery\\_album.php?category=50'](http://www.bruceanchor.com/gallery_album.php?category=50)

[http://www.560cfos.ca/funeral\\_home.php?FuneralHomeID=15'](http://www.560cfos.ca/funeral_home.php?FuneralHomeID=15)

[http://www.town.southbruce.on.ca/documentdownload.php?DocID=667'](http://www.town.southbruce.on.ca/documentdownload.php?DocID=667)

[http://www.portoffellowship.com/sermon.php?SermonID=248'](http://www.portoffellowship.com/sermon.php?SermonID=248)

[http://www.oceanfrontier.com/photogallery\\_image.php?ImageID=7'](http://www.oceanfrontier.com/photogallery_image.php?ImageID=7)

[http://billwalkermpp.com/gallery\\_album.php?category=51'](http://billwalkermpp.com/gallery_album.php?category=51)

[http://bruceanchorcruises.com/gallery\\_album.php?category=46'](http://bruceanchorcruises.com/gallery_album.php?category=46)

[http://www.ebelquarries.com/product.php?ProductID=1'](http://www.ebelquarries.com/product.php?ProductID=1)

[http://www.themissionarychurch.com/sermon.php?SermonID=11'](http://www.themissionarychurch.com/sermon.php?SermonID=11)

I tested 14 Websmart websites, and 11 of them were vulnerable.

# Hate Mail from Developer

- I do not appreciate you taking the liberty of contacting my clients directly
- This is highly unprofessional.
- I do not appreciate your 'ultimatum" - nor your scare tactics that no doubt will have an impact our customers.

# Hate Mail from Developer

- I am very tempted to notify your superiors of this misconduct.... you have no right or authority here. You could very well damage my business with this . If that happens you will be hearing from our lawyer.

# Hate Mail from Developer

- Any further correspondence on this matter may be directed to me and me alone. Like I said, I appreciate your information.... I really do, but contacting my customers directly is way out of line and I believe well outside of your mandate with your employer.

# Advice from Professionals

- Most ignored me
- One gave me a very nice, crawling response

Mr. Smart:

I'm happy that you responded so quickly to my vulnerability report, and I'm sorry for my intention. However, I think we got off on the wrong foot and I'd like to move forward and address these issues as quickly as possible.

As far as informing your customers, I felt it was reasonable, given the fact that the affected businesses and were in more direct risk of attack than your company.

Let's move forward cooperatively and work to get these issues resolved. As I mentioned, I've identified several vulnerabilities, and I'd be willing to test the fixes if that would help.

Looking forward to working with you cooperatively.

# Owen Smart's 2<sup>nd</sup> Response to Me

- Someone has been emailing my clients and myself, essentially interfering in my business - claiming to be you. Please see the email below.
- I want to confirm whether this is legitimate and if this is really coming from you Sam Bowne. As this has been highly unprofessional, I sincerely hope it is just a bad prank.

# To my Dept. Chair

- Would you be the supervisor or authority for Mr. Sam Bowne?
- I need to speak/email someone at the college to file a complaint regarding Mr. Bowne's conduct as it pertains to our business, since he is using the college's name as part of his activities.



# Next Steps

- Searching for high-value customers to alert
- Discovered prior reports of this vulnerability in 2010 and 2012

# Results

- 10 of the original 11 of the SQL injections are now fixed

**BE CAREFUL!**

**Whitehatting the Wrong Way**

blogs.miaminewtimes.com/riptide/2011/07/scott\_arciszewski\_ucf\_computer.php

**Crime**

# Scott Arciszewski, UCF Computer Student, Charged In Anonymous Hacking Crackdown

By Tim Elfrink Wed., Jul. 20 2011 at 10:14 AM

1 Comment

Categories: **Crime**



It also seems clear, from his actions, that Arciszewski considers himself a "white hat" hacker -- the slice of computer intruders who infiltrate systems to show weaknesses to the authorities who can fix them, not to cause harm. Why else retweet his success to the FBI?

# st0rm

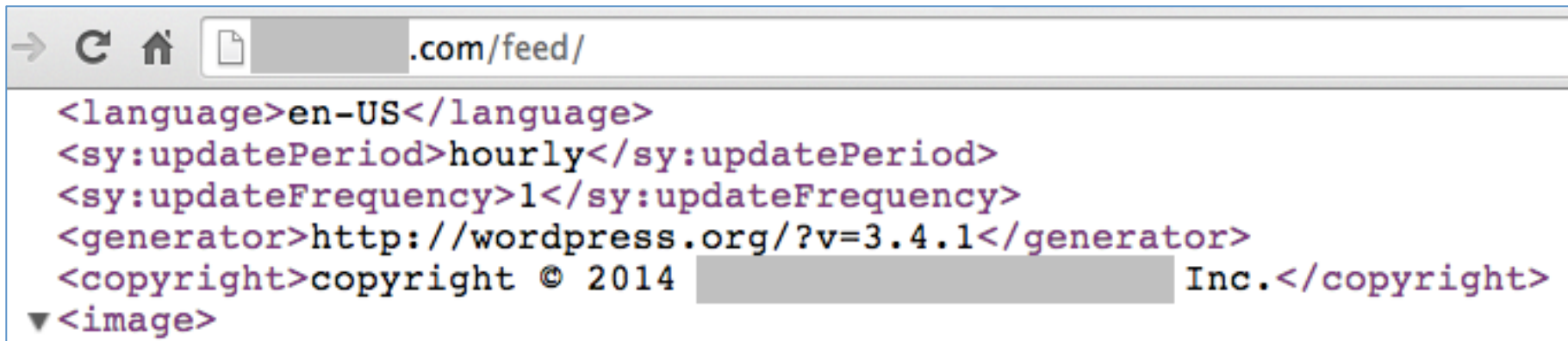
"If you're going to arrest me for helping people online, then so be it. Lock me up for life," he concludes.

A year earlier, an 18-year-old hacker called '*storm*', who classes himself as a 'grey hat' – a hacker who gains access to servers through illegal means yet refrains in most instances from seeking financial gain – got access to 1302 logins at the university with an estimated 800 of these logins easily decipherable.

# Work in Progress

- Major media website
- Ty Ryan Satterfield (@I\_am\_ryan\_S)

# 2 Years Out Of Date



The image shows a browser window with a URL bar containing a domain name followed by "/feed/". The main content area displays XML metadata for an RSS feed. The metadata includes the language (en-US), update period (hourly), update frequency (1), generator (WordPress 3.4.1), and a copyright notice for 2014. A small downward arrow is visible next to the <image> tag, indicating it is collapsed.

```
<language>en-US</language>  
<sy:updatePeriod>hourly</sy:updatePeriod>  
<sy:updateFrequency>1</sy:updateFrequency>  
<generator>http://wordpress.org/?v=3.4.1</generator>  
<copyright>copyright © 2014 [redacted] Inc.</copyright>  
▼ <image>
```



#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2014-0166 287</a>				2014-04-09	2014-04-10	6.4	None	Remote	Low	Not required	Partial	Partial	None
<p>The wp_validate_auth_cookie function in wp-includes/pluggable.php in WordPress before 3.7.2 and 3.8.x before 3.8.2 does not properly determine the validity of authentication cookies, which makes it easier for remote attackers to obtain access via a forged cookie.</p>														
2	<a href="#">CVE-2014-0165 264</a>				2014-04-09	2014-04-10	4.0	None	Remote	Low	Single system	None	Partial	None
<p>WordPress before 3.7.2 and 3.8.x before 3.8.2 allows remote authenticated users to publish posts by leveraging the Contributor role, related to wp-admin/includes/post.php and wp-admin/includes/class-wp-posts-list-table.php.</p>														
3	<a href="#">CVE-2013-7240 22</a>			Dir. Trav.	2014-01-03	2014-02-25	5.0	None	Remote	Low	Not required	Partial	None	None
<p>Directory traversal vulnerability in download-file.php in the Advanced Dewplayer plugin 1.2 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the dew_file parameter.</p>														
4	<a href="#">CVE-2013-7233 352</a>			CSRF	2013-12-29	2013-12-30	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
<p>Cross-site request forgery (CSRF) vulnerability in the retrosпам component in wp-admin/options-discussion.php in WordPress 2.0.11 and earlier allows remote attackers to hijack the authentication of administrators for requests that move comments to the moderation list.</p>														
5	<a href="#">CVE-2013-5739 79</a>			XSS	2013-09-12	2013-09-26	3.5	None	Remote	Medium	Single system	None	Partial	None
<p>The default configuration of WordPress before 3.6.1 does not prevent uploads of .swf and .exe files, which might make it easier for remote authenticated users to conduct cross-site scripting (XSS) attacks via a crafted file, related to the get_allowed_mime_types function in wp-includes/functions.php.</p>														
6	<a href="#">CVE-2013-5738 20</a>			XSS	2013-09-12	2013-09-26	4.3	None	Remote	Medium	Not required	None	Partial	None
<p>The get_allowed_mime_types function in wp-includes/functions.php in WordPress before 3.6.1 does not require the unfiltered_html capability for uploads of .htm and .html files, which might make it easier for remote authenticated users to conduct cross-site scripting (XSS) attacks via a</p>														

# Confidential Demo

NO RECORDING