

Whitehat Vigilante

BayThreat

Dec. 10, 2011

Executive Summary

- This talk has no
 - Demos
 - Exploits
 - 1337ness
- It's just a sermon about social skills
 - Ethics
 - Legality
 - Attitude

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](#)



BERT AND ERNIE

America's most socially accepted gay couple

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

PBS Hacked



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

Attitudes

Blend In: Hide

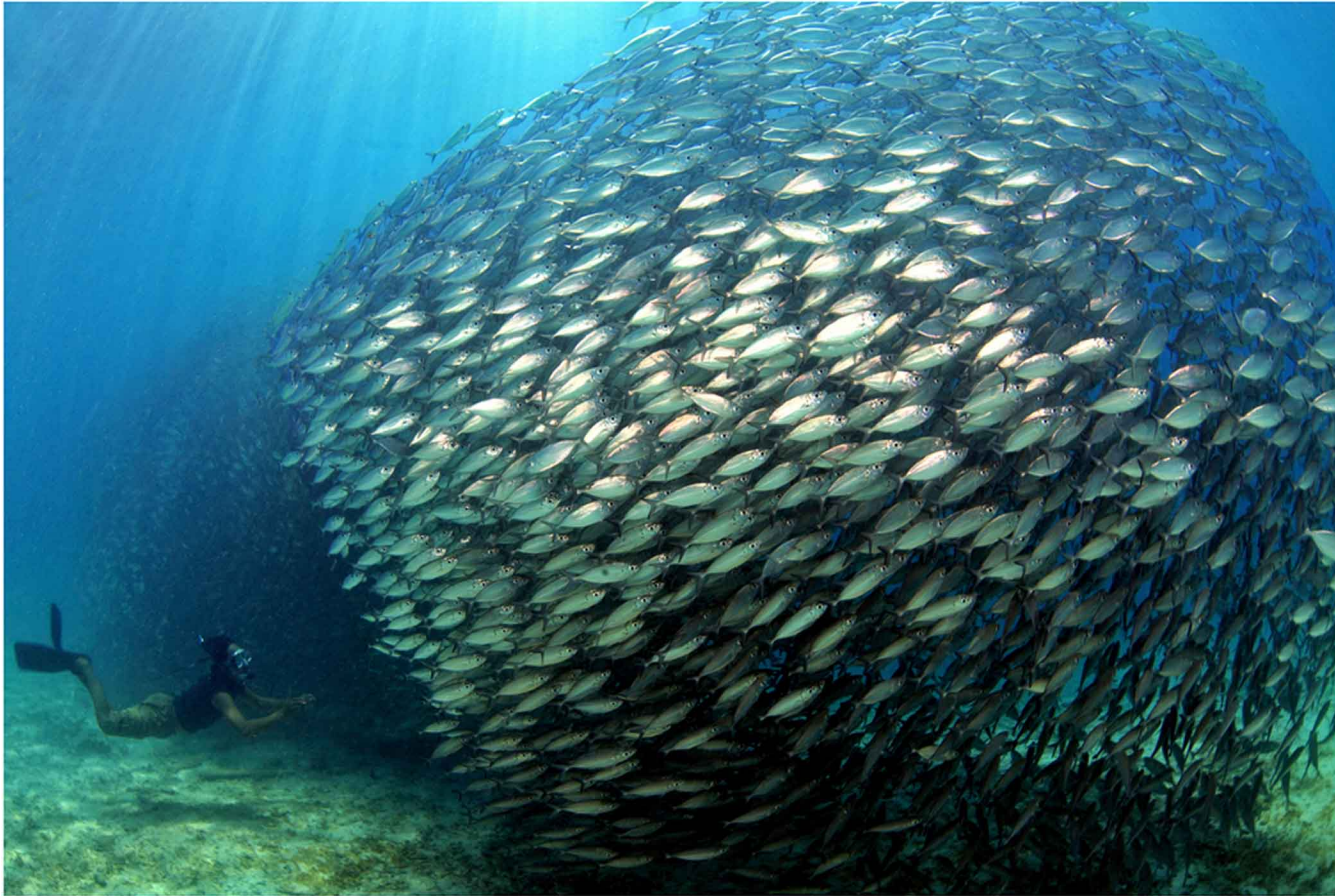


Image from presenceinbusiness.com

Make Your Own Rules



Images from listentoleon.net & anpop.com

Cyber-Terrorists Masked Mobs

- Create fear
- Cause paranoia
- Intimidate critics into silence

A screenshot of a TeamPoison announcement post. The title "TEAMP0ISON" is written in large, green, block letters. Below the title, the text "Hacked By TriCk aka Saywhat? & iN^SaNe - TeaMp0isoN" is written in a smaller, green font. The main body of the post is in white text on a black background, starting with "BREAKING NEWS: TEH LULZBOAT HAS OFFICALY SANK WITH 100S OF ANON MEMBERS ON BOARD!". The post contains a long paragraph of text, including a list of names and a closing statement.

Lone Vigilantes



Boondock Saint

@th3j35t3r Behind you.

Hactivist for good. Obstructing lines of communication for terrorists, sympathizers, fixers, facilitators. No botnets here. I'll do my own dirty.

<http://th3j35t3r.wordpress.com>

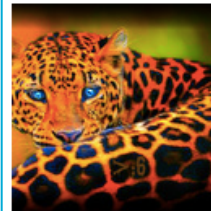


Lone Gunman

@th3Jasper Somewhere

I Fight The Future #FTF, You Better Expect Me. Stay Frosty My Friends

<http://jaspersec.wordpress.com>



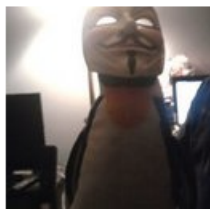
'Ονειροι

@On3iroi

#Hactivist #ProSec #OccupyTheArcana

<http://pastebin.com/7H33cVuM> #FollowTheWhiteRabbit

<http://pastebin.com/u/On3iroi>



pr0f

@pr0f_srs International Waters

A guy the DHS says is Probably Not Great! I do stuff and like embedded. Bitcoins go here:

1PTVF69KGjth7ZhA3gcNsb3XG6AnpJVNgu

<http://info.publicintelligence.net/NCCIC-AnonymousICS.pdf>



Storm

@_St0rm In the clouds

Ex hacker, Ex vigilante, Used to support CyberSecurity infrastructures. Used to attack Scamming websites to keep them slowly at bay. I'll always be watching.

<http://stormsecurity.org>

Nobody's Right if Everybody's Wrong



Buffalo Springfield image from freewebs.com

The Middle Way

Laws

Federal Criminal Code Related to Computer Intrusions

-top-

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

From cybercrime.gov



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.

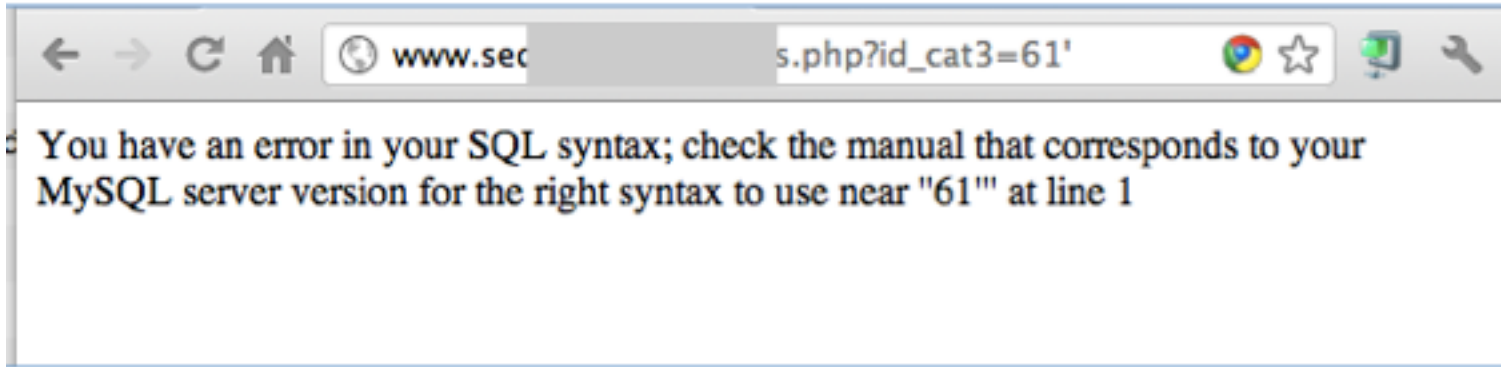
Cold Calls

Find Vulnerable Sites Dumped on Pastebin

```
Fresh SQLi Scan by AnonHex x
pastebin.com/Kfdrj5kD

1.
2. /$$$$$ /$$ /$$
3. /$$_ $$ | $$ | $$
4. | $$ \ $$ /$$$$$$ /$$$$$$ /$$$$$$ | $$ | $$ /$$$$$$ /$$ /$$
5. | $$$$$$$| $$_ $$ /$$_ $$| $$_ $$| $$$$$$$ /$$_ $$| $$ /$$/
6. | $$_ $$| $$ \ $$| $$ \ $$| $$ \ $$| $$_ $$| $$$$$$$ \ $$$$/
7. | $$ | $$| $$ | $$| $$ | $$| $$ | $$| $$ | $$| $$$$/ gt;$$
8. | $$ | $$| $$ | $$| $$$$$$/| $$ | $$| $$ | $$| $$$$$$$ /$$/\ $$
9. |_/ |_/|_/ |_/ \___/ |_/ |_/|_/ |_/ \___/|_/ \_/
10. //Screwing your security since 2011
11.
12.
13.
14.
15.
16. Website Vulnerability
17.
18. Research by @AnonHex //// Sign up at www.HackSociety.net
19. =====
20.
21.
22. http://www.regi [REDACTED] vent.php?id=1191'
23. http://www.sedi [REDACTED] hp?id_cat3=61'
24. http://www.adae [REDACTED] php?id=2'
25. http://www.actf [REDACTED] s_full.php?id=111'
26. http://www.ezsk [REDACTED] php?id=1'
```

Verify the Vulnerability



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

Find a Contact Address

Contacts

The quickest way to contact us and an immediate answer is to fill the following form with the fields needed to complete the most of your request. Fields marked with * are required. If the request requires a response from us you will receive it within a few minutes. **IMPORTANT:** Please respond to our response as indicated in any email you receive, or click on the email link at the head, and simply not replying to the email with the key 'Reply' in Outlook or other email programs.

Your data	
Name and Surname:	<input type="text" value="Sam Bowne"/> *
Email:	<input type="text" value="sbowne@ccsf.edu"/> *
Communicate your message	
Subject:	<input type="text" value="Your site is at risk"/> *
Message, problem, request:	<p>You have a serious security problem on your Website. It has been published on a list here:</p> <p>http://pastebin.com/Kfdri5kD</p> <p>This is the vulnerable URL:</p>

My Letter

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
- Don't demand anything
- Don't make any threats

Pilot Study

- 3 days after notification

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

- 7/23 Fixed (30%)
 - <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

- FBI (many times)
- UK Supreme Court
- Chinese Government
- Police departments (many of them)
- Other Courts
- CNN, PBS
- Apple
- Schools (many of them)

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

CERT

← → ↻ 🏠 🔒 <https://forms.cert.org/VulReport/> 🌐 ☆ 🖨️ 🔧

  **Software Engineering Institute**
Carnegie Mellon

search  [Publications Catalog](#)

[HOME](#) | [Software Assurance](#) | [Secure Systems](#) | [Organizational Security](#) | [Coordinated Response](#) | [Training](#)

Vulnerability Reporting Form

We accept reports of security vulnerabilities and serve as a coordinating body that works with affected vendors to resolve vulnerabilities. If you believe you have found a [security vulnerability](#) that has not been resolved, please complete the following form. As our [vulnerability disclosure policy](#) explains, we send information submitted in vulnerability reports to affected vendors. By default, we will share your name with vendors and publicly acknowledge you in documents we publish. If you do not want us to share your name or publicly acknowledge you, select the appropriate responses below.

For additional information about the fields in this form, refer to the [instructions](#). If you have any problems or want to use another format for submitting this report, [contact us](#).

Please provide as much information as you can. When you are finished, submit your report using the [button](#) at the end of the form.

Your Contact Information

Provide [contact information](#) about yourself in case we have additional questions regarding this vulnerability report. This information is not required to report a vulnerability, but without it we will be unable to contact you.

Name

Organization

Email

Telephone

May we [provide your name](#) to the vendor? Yes No

Do you want to be [publicly acknowledged](#)? Yes No

Positive Results

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

Negative Results

- A few of my 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
- All 100% false & baseless

Ethics Complaint



(ISC)²

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)² is in receipt of a formal ethics complaint that has been filed against you.

Pursuant to (ISC)² Policy governing ethics complaints, as posted on the (ISC)² 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

Fortuitous Timing

Sat 9-17	No Quiz LOCKDOWN	Ch 2: Access controls
Sat 9-24	Quiz on Ch 1 & 2	Ch 3: Application Security
Sat 10-1	Quiz on Ch 3	Ch 4: Business Continuity and Disaster Recovery Planning
Sat 10-8	Quiz on Ch 4	Ch 5: Cryptography
<i>Fri 10-21</i>	<i>Mid-Term Grades Due</i>	
Sat 10-15	Quiz on Ch 5	Ch 6: Legal, Regulations, Compliance and Investigations
Sat 10-22	Quiz on Ch 6	Ch 7: Operations Security
Sat 10-29	Quiz on Ch 7	Ch 8: Physical and Environmental Security
Sat 11-5	No Quiz	Ch 8 Continued

Recommendations for Cold Calls

Be Respectful

- No abuse or criticism
- Sincere desire to help
- Accept being ignored without protest
- Demand nothing
- Respect their right to leave their servers unpatched

Be Right

- Report clear-cut vulnerabilities, widely understood and important, like SQL Injection
- Do nothing illegal or suspicious
 - No vulnerability scans
 - No intrusion or exploits
 - Report only vulnerabilities that are already published by others

Clarity of Purpose

- Genuine desire to help the people you are contacting
- No hidden agenda
 - Desire to sell a product
 - Desire to belittle or mock
 - Dominate and control others
 - Plans to attack sites yourself
 - Revenge

Expect Abuse

- If you become visible in the hacking community, you are a target
- It doesn't matter what you say or do
- Many hackers are arrogant, insecure, and emotionally immature

Be Fearless

- Understand the importance of the sites you are helping
- Are they worth more than your
 - Inconvenience
 - Time expended
 - Exposure to criticism and humiliation

Acknowledgements

- I am very grateful for the support of CNIT, MPICT, and CCSF
- Especially
 - Carmen Lamha
 - Maura Devlin-Clancy
 - Pierre Thiry
 - James Jones
 - Tim Ryan
- It would be much simpler to just fire me than to support my mad actions