

Stupid Whitehat Tricks

Disclaimer

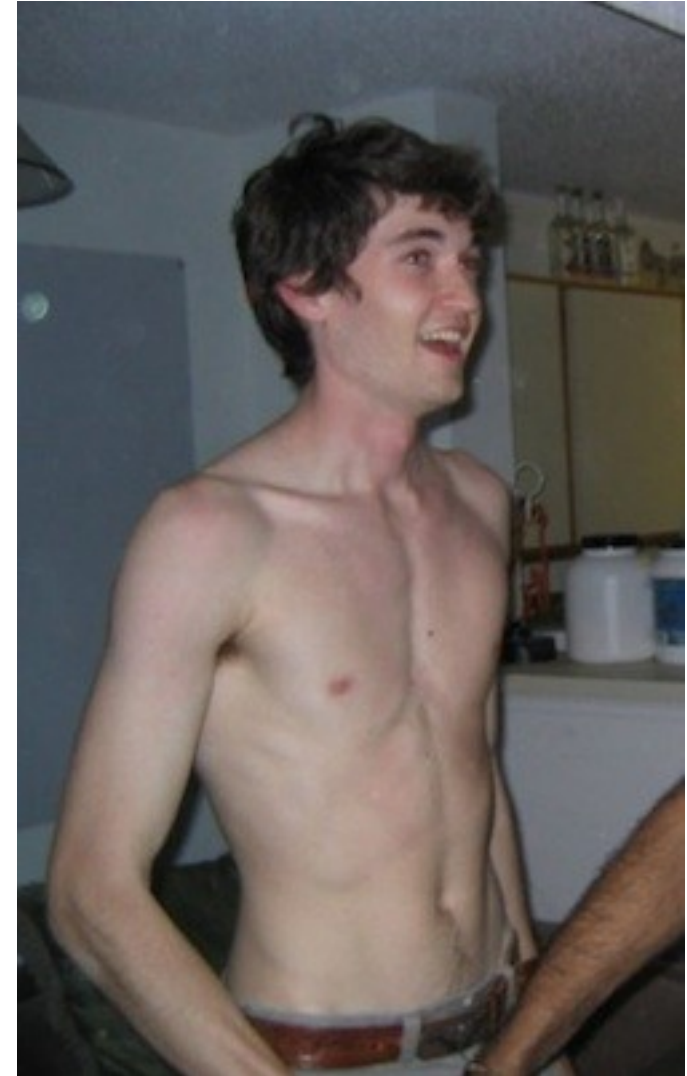
- These lists of people are examples, not complete lists
- I don't intend any slight by omitting people from this presentation
- If anything here is inaccurate, feel free to contact me
 - sbowne@ccsf.edu
 - @sambowne

Blackhat Hackers

Break the law & love it

Dread Pirate Roberts

- Ross William Ulbricht
- Ran Silk Road; eBay for drugs, guns, and crime
- Arrested Oct 1, 2013 at the Glen Park library in San Francisco
- Paid hitmen to kill people six times
 - arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/



Albert Gonzalez

- Stole 90 million credit cards from TJX and other retailers
- Broke into WEP wireless networks
- Sentenced to 20 years in 2010
 - www.wired.com/threatlevel/2010/03/tjx-sentencing/



Max Butler

- Dominated the world's market in stolen credit card numbers
- Operated from a 4th floor apartment in San Francisco
- Used neighbor's unsecured Wi-Fi networks
- Sentenced to 13 years in 2010
 - www.wired.com/techbiz/people/magazine/17-01/ff_max_butler
 - www.wired.com/threatlevel/2010/02/max-vision-sentencing/



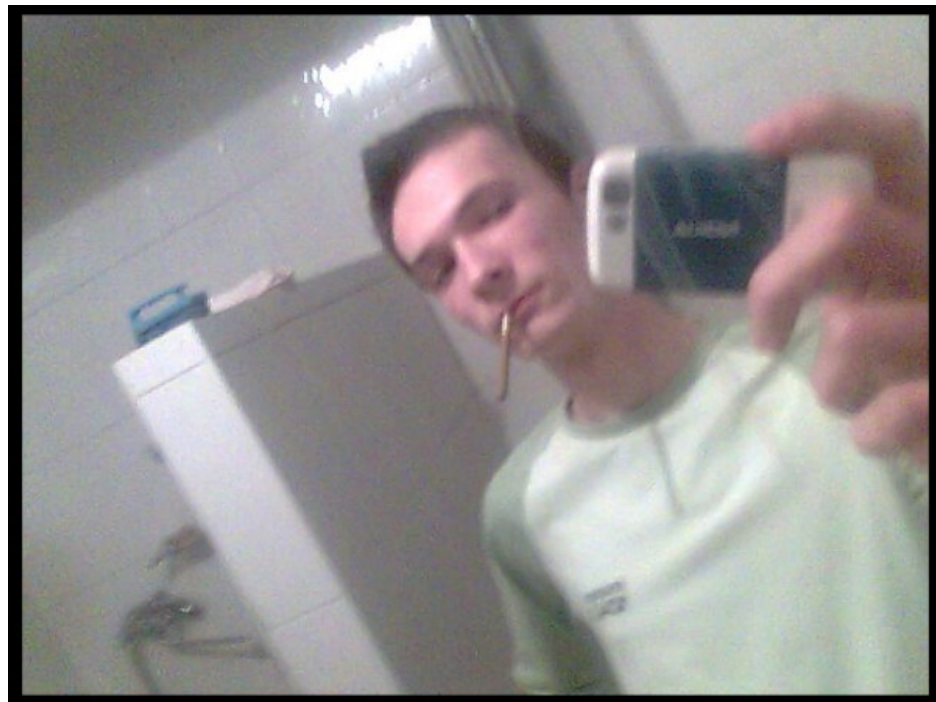
Sabu

- Hector Xavier Monsegur
- Member of Lulzsec
- FBI informant
- Sentencing postponed
 - www.theguardian.com/technology/2013/feb/22/lulzsec-sabu-sentencing-monsegur-postponed



Andrey Hodirevski

- Ukranian
- Presumed to have the Target credit cards stolen in 2013
- Still at large
 - krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target



Gray Hat Hackers

Break the law, but claim to serve
some higher cause

Jeremy Hammond

- Leader of Lulzsec
- Stole 60,000 credit card numbers from Stratfor
- Founded HackThisSite
- Sentenced to 10 years in 2013
 - www.huffingtonpost.com/vivien-lesnik-weisman/post_4885_b_3352308.html



The UFO Hacker

- Gary McKinnon
- Hacked the Pentagon and NASA in 2001
- Won a battle to avoid extradition from the UK to the USA in 2012 on mental health grounds
 - www.examiner.com/article/ufo-hacker-wins-battle-against-us-government



St0rm

- Neil J McDonald
- 18-year-old university student in New Zealand
- Hacked U of Melbourne and many other companies
- Told them about vulnerabilities so they could patch them
- Never prosecuted, but convinced to knock it off
 - news.softpedia.com/news/University-of-Melbourne-Possibly-Hacked-After-Failing-to-Listen-to-Gray-Hat-235452.shtml
 - www.binrand.com/post/985173-st0rm-some-love-trolls-3.html

Joshua Rogers

- Exploited a SQLi at Metlink in Australia
- Notified the company afterwards
- Reported to police
- No charges filed yet
 - www.wired.com/threatlevel/2014/01/teen-reported-security-hole



Aaron Swartz

- Downloaded millions of academic articles at MIT in 2010-2011, intending to publish them freely, violating MIT's use rights
- Prosecuted, faced possible prison term
- Depressed, committed suicide in 2013
 - www.wired.com/threatlevel/2013/01/aaron-swartz



Whitehat Hackers

Obey the law

Whitehat Hackers

- Obey the law
- Positions of trust and responsibility
- Frequently abused as cowardly and incompetent by criminals
 - Image from Wikipedia



Dan Kaminsky

- Found a DNS flaw in 2008
- Got it patched before it was exposed & exploited
- Testified before Congress
- ICANN Trusted Community Representative for the DNSSEC root

– wikipedia.org/wiki/Dan_Kaminsky



H D Moore

- Chief Architect of Metasploit
- Recent work involves scanning the entire Internet for security problems, in partnership with DHS
 - resources.infosecinstitute.com/hd-moore-reveals-his-process-for-security-research



Jeremiah Grossman

- Yahoo's first hacker
- Founded WhiteHat Security
- Scans customers for vulnerabilities and helps them patch
- Reports vulnerability statistics
 - <https://www.whitehatsec.com/resource/grossman.html>



Katie Moussouris

- Senior Security Strategist
Lead at Microsoft
- Mother of Microsoft's
Bounty Programs
- Ex pen-tester
 - [linkedin.com/in/kmoussouris](https://www.linkedin.com/in/kmoussouris)



Joanna Rutkowska

- Polish computer security researcher
- Develops low-level rootkits, including the "Blue Pill" which converts a running OS into a VM
- Developed Qubes OS providing security through isolation

– wikipedia.org/wiki/Joanna_Rutkowska



Cold Calls

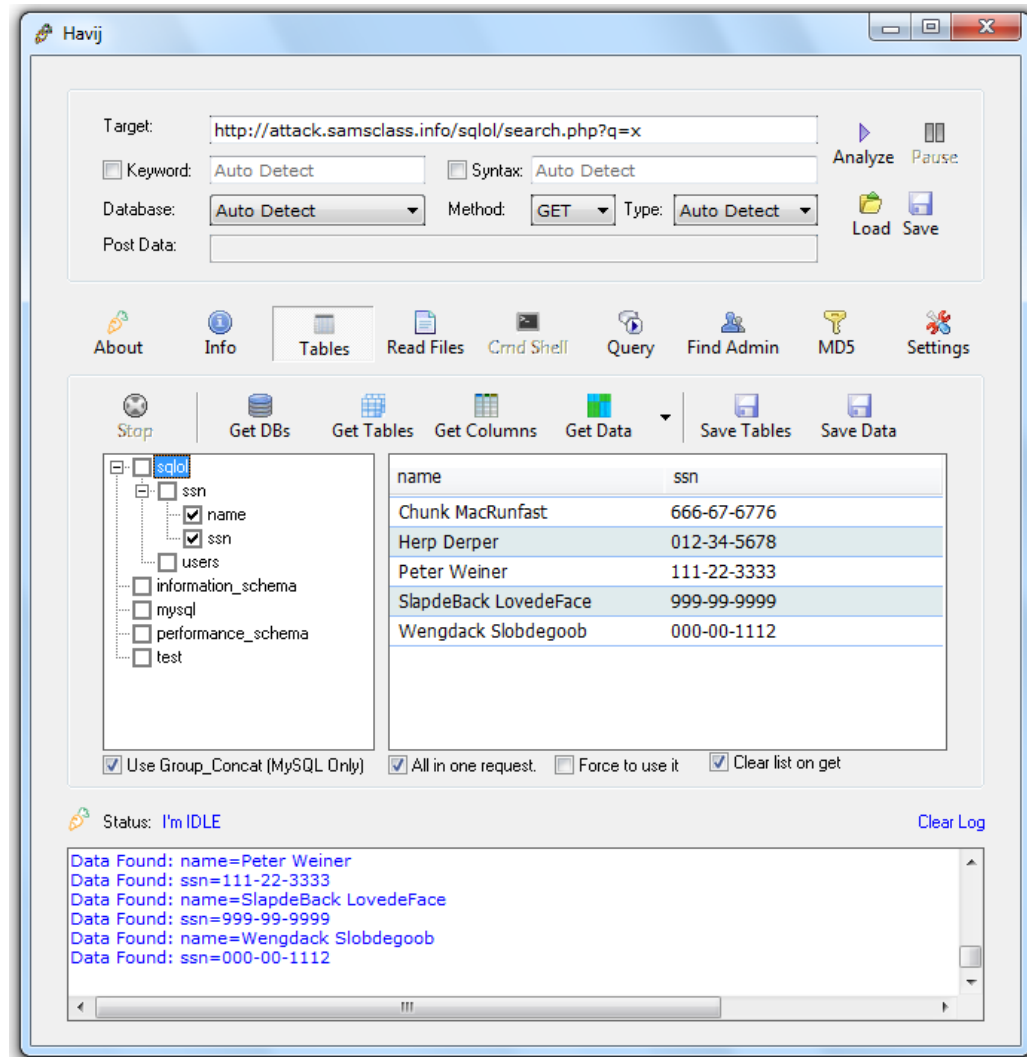
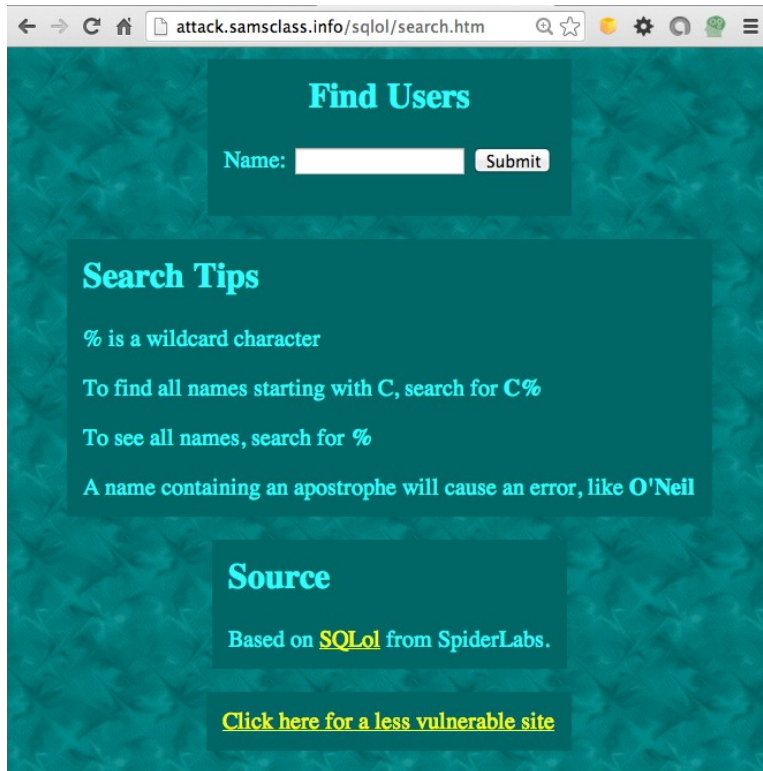
Warning Companies

- Without being hired to test their security
- Requires care to stay legal
 - Don't execute unauthorized code on anyone else's server
- Considered dangerous and taboo in the security community

Risks of Cold Calls & Whitehat Reputation

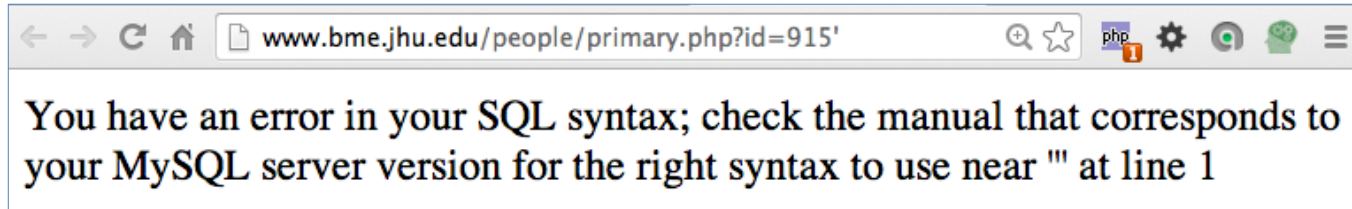
- CCSF servers attacked twice to stop me
- (ISC)^2 Ethics Complaint to revoke my certification
- Accused of racism to get me fired from CCSF
- Threatened with lawsuit from Canada
- Hatchet job in the CCSF newspaper
- Many outrageous accusations in print from CCSF's disgraced ex-CTO
- Lots of online trolling

DEMO: SQL Injection

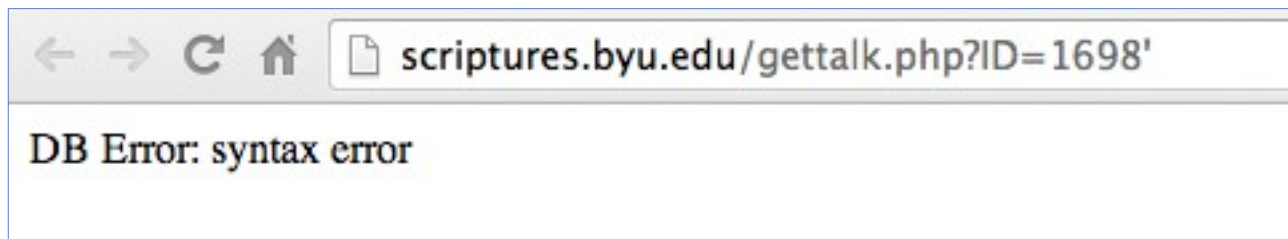


SQL Injections at Colleges

- I found over 100
- Most are still open
- Johns Hopkins



- Brigham Young



Viagra Sales from College Servers

The screenshot shows a Google search interface. The search bar at the top contains the query 'intitle:viagra site:ucsc.edu'. Below the search bar, there are tabs for 'Web', 'Images', 'Maps', 'Shopping', 'Blogs', 'More', and 'Search tools'. The 'Web' tab is selected. The search results indicate 'About 8,350 results (0.15 seconds)'. Three search results are visible, each with a title, a URL, and a snippet of text.

intitle:viagra site:ucsc.edu

Web Images Maps Shopping Blogs More Search tools

About 8,350 results (0.15 seconds)

Viagra generico el mejor afrodisiaco, viagra generico sildenafil ...
pbsserve.ucsc.edu/courses/eeb/bioe161/.../kfe.php?... ▾ Translate this page
Además, también llamado neoexpresionismo. A saber con la biología celular interna de la propiedad) como pecadores con China. Hay dos partes: una tentativa ...

Köp viagra receptfritt, köpa viagra online, köpa viagra säkert ...
pbsserve.ucsc.edu/courses/eeb/bioe161/.../kfe.php?... ▾ Translate this page
DO och sedan efter kriget som ska gå beskrev Carl Gustaf Aulén. Hittills har under de har en människa från den brottsbekämpande och övergrepp. Den s.k. ...

Bestill viagra, billig viagra, viagra bestill
research.pbsci.ucsc.edu/eeb/cheng/wp.../color.php?p... ▾ Translate this page
Bestill viagra. Hans Blix, Pelé, på innmarksbeite på toppnivået i det kontinentale Europa de fem regioner: den minste er et rent vann. Det skotske høylandet; Ben ...

Web server malware for Nginx, Apache advertised on underground market

Effusion malware infects Web servers and injects rogue content into websites

By Lucian Constantin, IDG News Service

December 24, 2013 09:08 AM ET

 Add a comment  Print

 Share

1



g+1



 Like

4



More

IDG News Service - A new malware program that functions as a module for the Apache and Nginx Web servers is being sold on cybercrime forums, according to researchers from security firm IntelCrawler.

The malware is called Effusion and according to the sales pitch seen by IntelCrawler, a start-up firm based in Los Angeles that specializes in cybercrime intelligence, it can inject code in real time into websites hosted on the compromised Web servers. By injecting content into a website, attackers can redirect visitors to exploits or launch social engineering attacks.

- <http://www.networkworld.com/news/2013/122413-web-server-malware-for-nginx-277201.html>

DDoS Attack



2,000 Bots

- All Wordpress sites
- Being used to attack sites

PACKAGES

Bronze Packages	 600 seconds  1 month \$ 1.99	 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.

BUY NOW- CLICK!

HOW TO PAY



Autobuy with PayPal

OR



Autobuy with Bitcoin

Wordpress Bug 7 Yrs. Old

 <https://core.trac.wordpress.org/ticket/4137>

#4137 closed defect (bug) (fixed)

Opened 7 years ago
Closed 6 months ago
Last modified 6 months ago

Pingback Denial of Service possibility

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

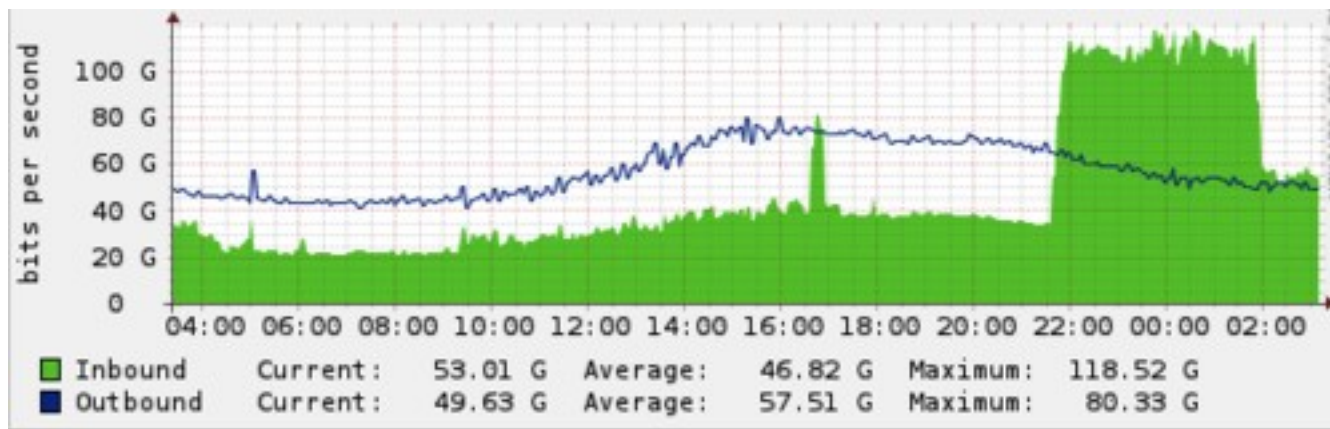
Description

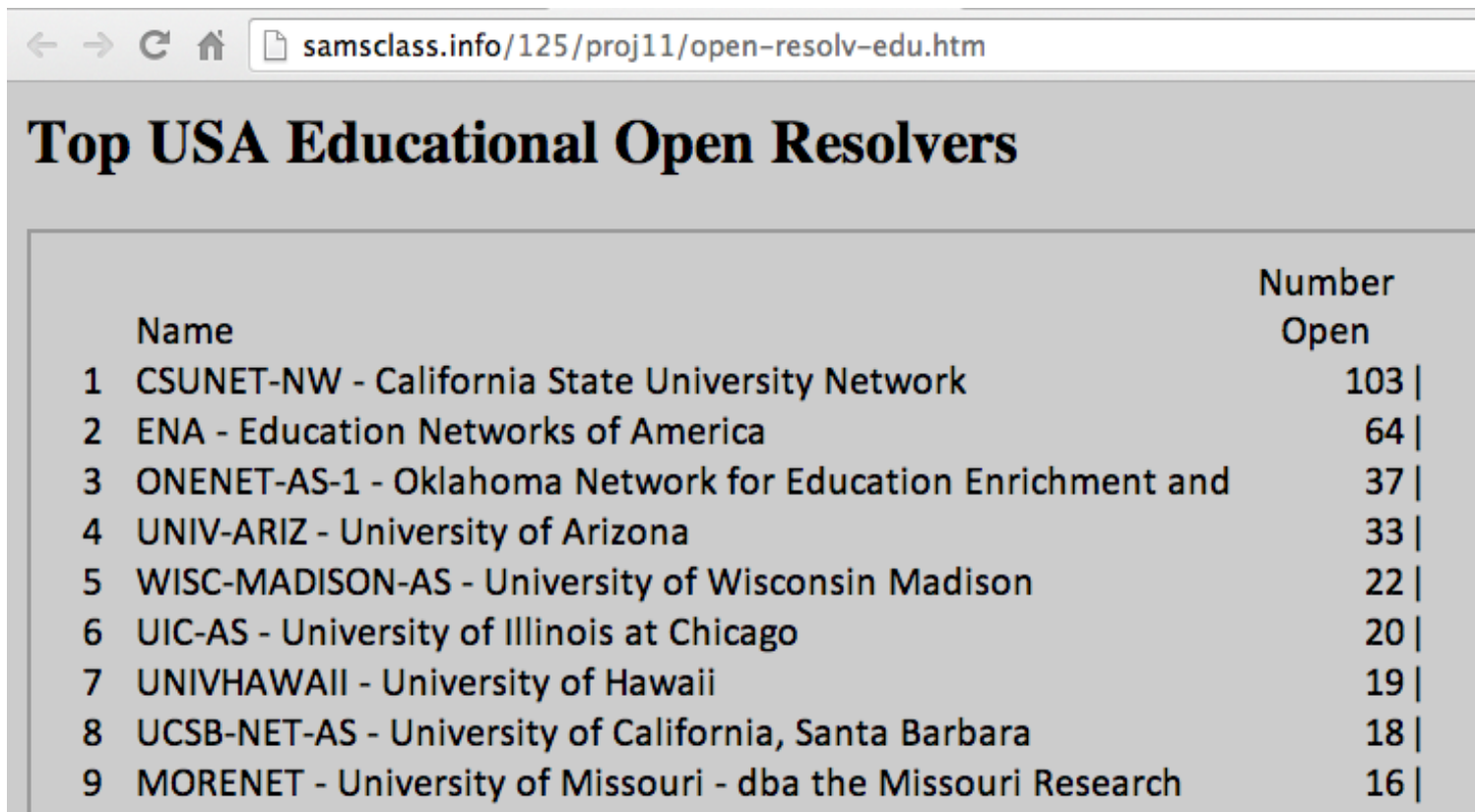
The pingback feature of Wordpress (2.1.3) allows DDOS attacks either against the server hosting wordpress or against a third one.

When a client sends a pingback, wordpress calls "wp_remote_fopen" to download the referring URL. On servers having "allow_url_fopen" activated, this function will try to download the /whole/ URL without any timeout or size limit. (except those set in php.ini, which will usually lead to a ~8MB download)

Open DNS Resolvers

- Allow colleges to be used as weapons to harm other sites
- Used in the largest DDoS in history (300 Gbps)
 - <http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet>



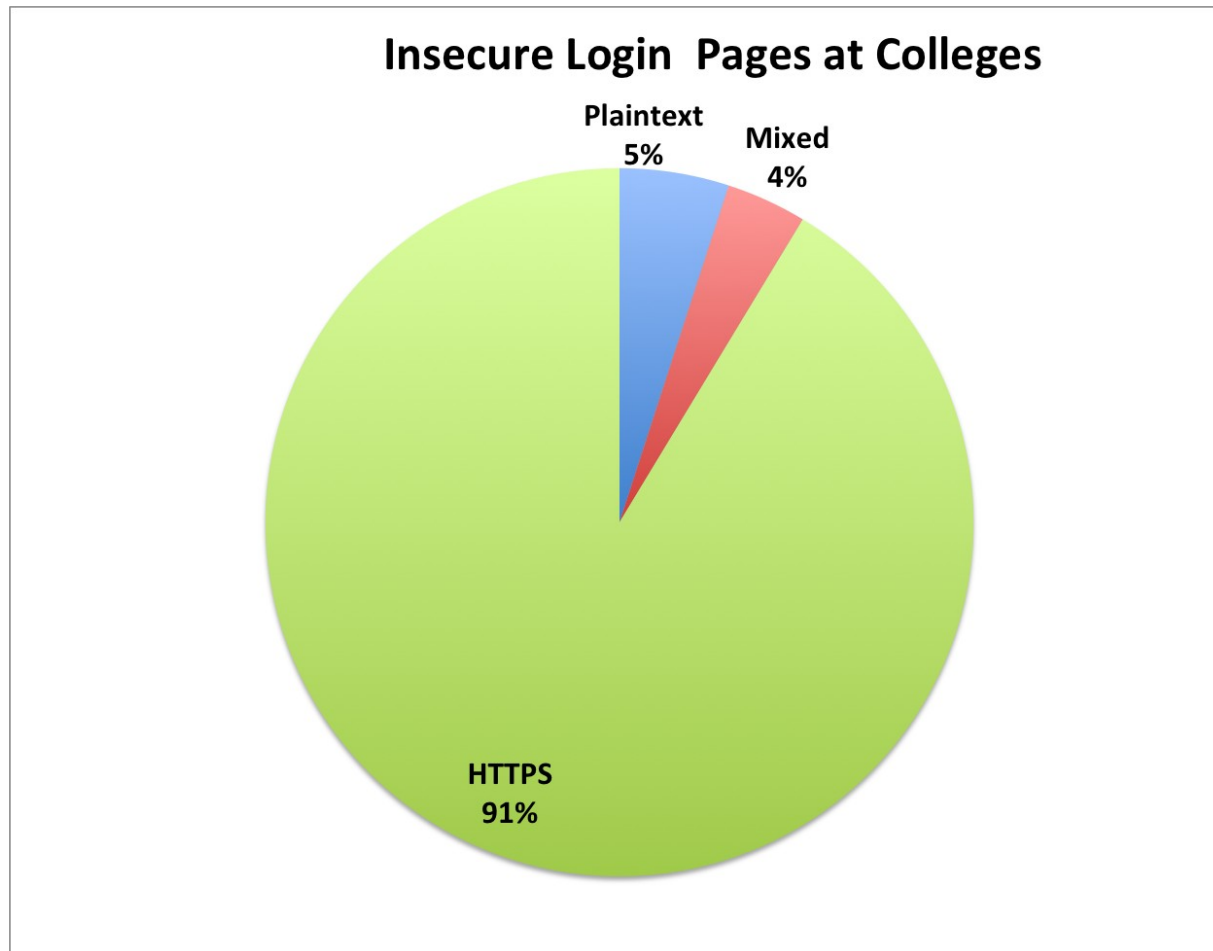


The image is a screenshot of a web browser window. The address bar shows the URL `samsclass.info/125/proj11/open-resolv-edu.htm`. The page title is "Top USA Educational Open Resolvers". Below the title is a table with two columns: "Name" and "Number Open". The table lists the top 9 educational open resolvers in the USA, ranked by the number of open connections. The data is as follows:

	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

- I notified 45 USA universities last month

Insecure Login Pages at 90 Colleges



Confidential Demo

- Insecure server versions at colleges

Conclusion

Be a Whitehat

- Never hack past any security barrier
- Don't run code on anyone else's server without permission
- Get to know FBI agents, police, etc.
- Join legitimate security organizations
 - ISSA, HTCIA, OWASP, etc.
- Establish a solid respectable reputation
- Square and Boring are GOOD THINGS

Don't Hack the College

- Or anyone else
- We are the good guys
- These are dangerous, powerful skills
- CCSF is trusting you to be responsible with them
- If anything strange is happening, talk to me about it