Disclaimer!

No physical touching during presentation will be demonstrated!
I promise!

Can I touch you there?

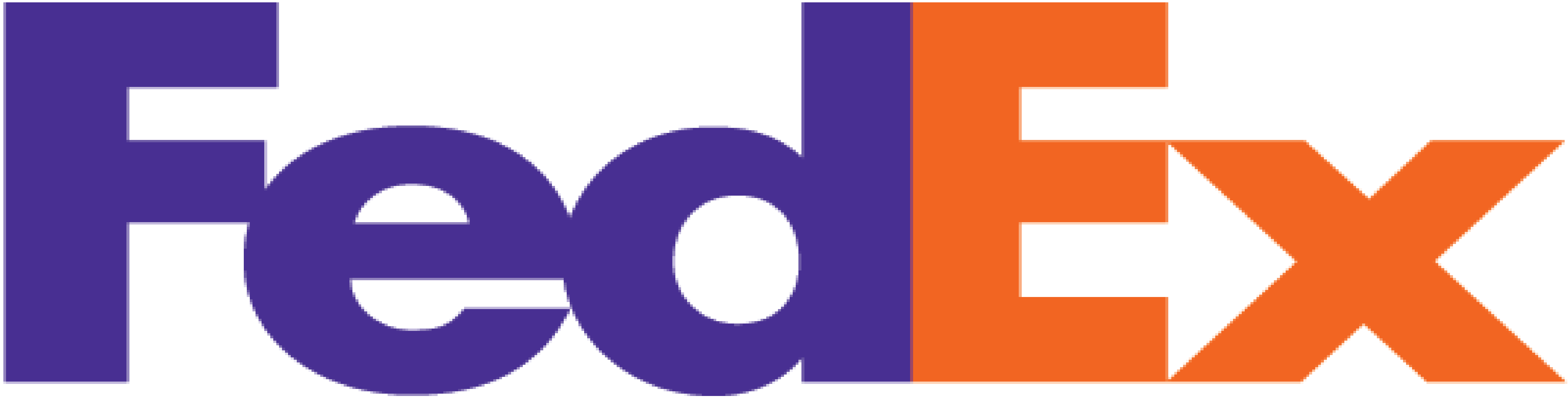
(Tools and Techniques for Security Testing)

Milan Gabor

/me

- Developer once
- Pen(tester) now
- Ethical Hacker
- Trainer
- Breaker
- BSidesLjubljana founder

https://medium.com/that-conference/test-until-fear-turns-to-boredom-fac0793b847d


FedEx

WE HAVE
SO MUCH IN
COMMON

Our job is to tell you

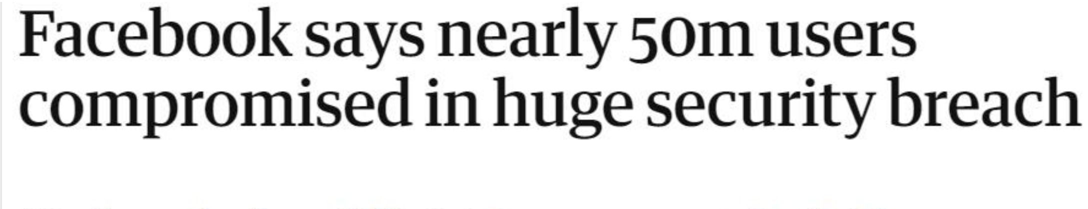
your baby is ugly!

-Software Testers- / pentesters

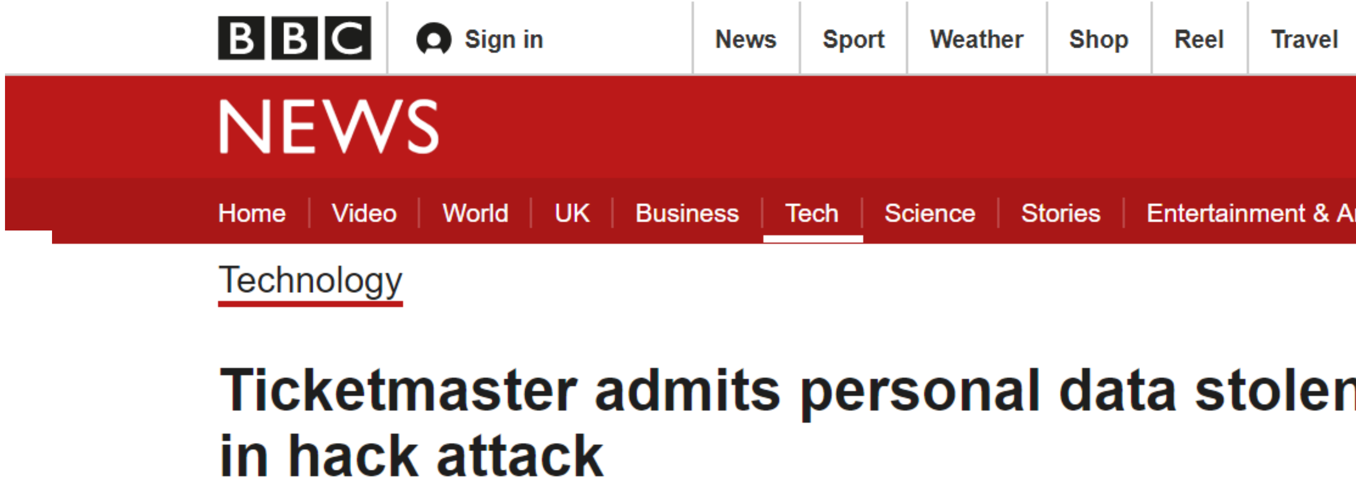
CURRENT STATUS:

standing on a line between giving up and seeing how much more I can take.

Don’t they do testing?

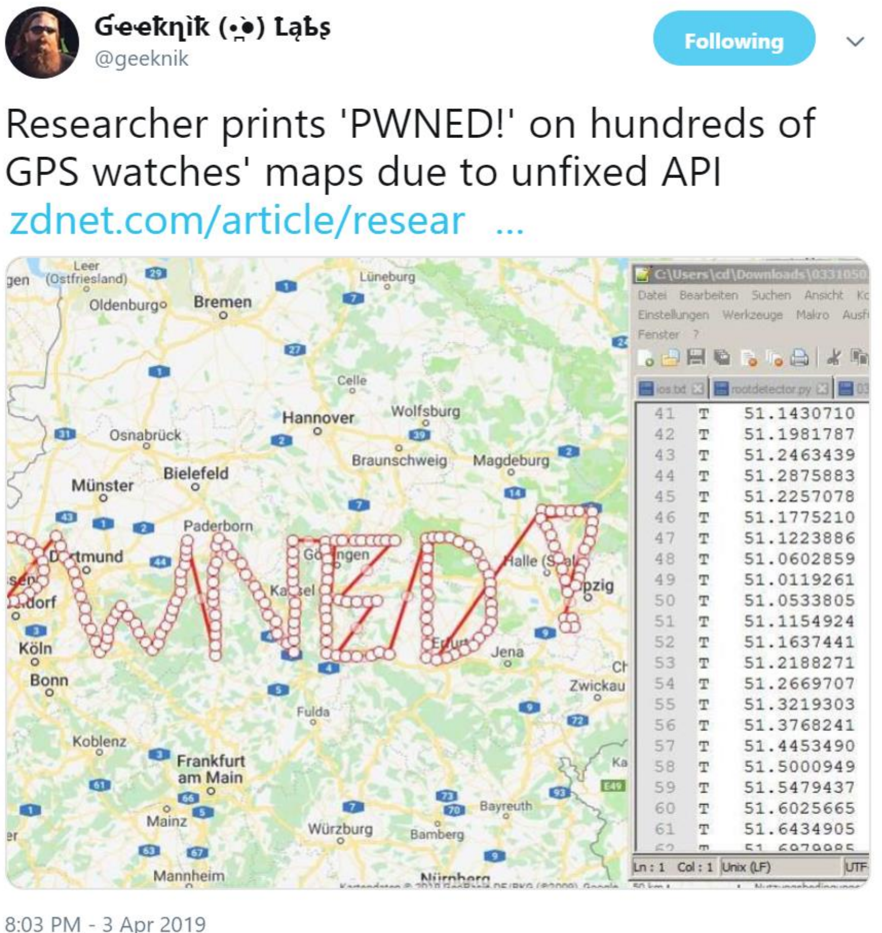


Facebook says nearly 50m users compromised in huge security breach



Technology

Ticketmaster admits personal data stolen in hack attack

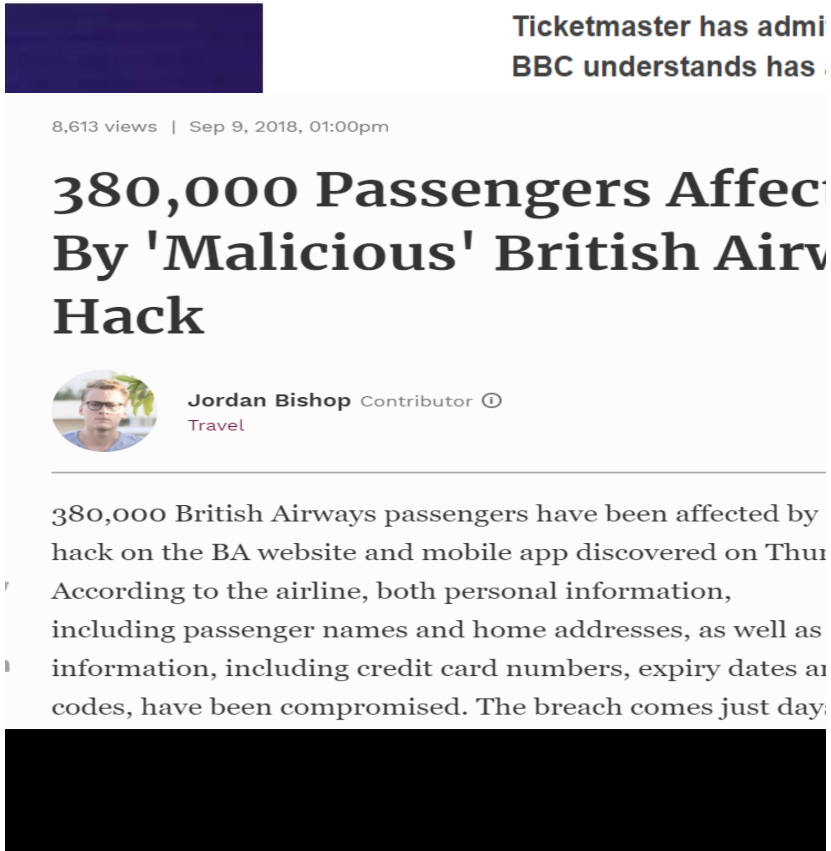


Geeknik (•̀ᴗ•́) Labs
@geeknik

Researcher prints 'PWNED!' on hundreds of GPS watches' maps due to unfixed API
zdnet.com/article/resear …

```
T   51.1430710
T   51.1981787
T   51.2463439
T   51.2875883
T   51.2257078
T   51.1775210
T   51.1223886
T   51.0602859
T   51.0119261
T   51.0533805
T   51.1154924
T   51.1637441
T   51.2188271
T   51.2669707
T   51.3219303
T   51.3768241
T   51.4453490
T   51.5000949
T   51.5479437
T   51.6025665
T   51.6434905
```

8:03 PM - 3 Apr 2019



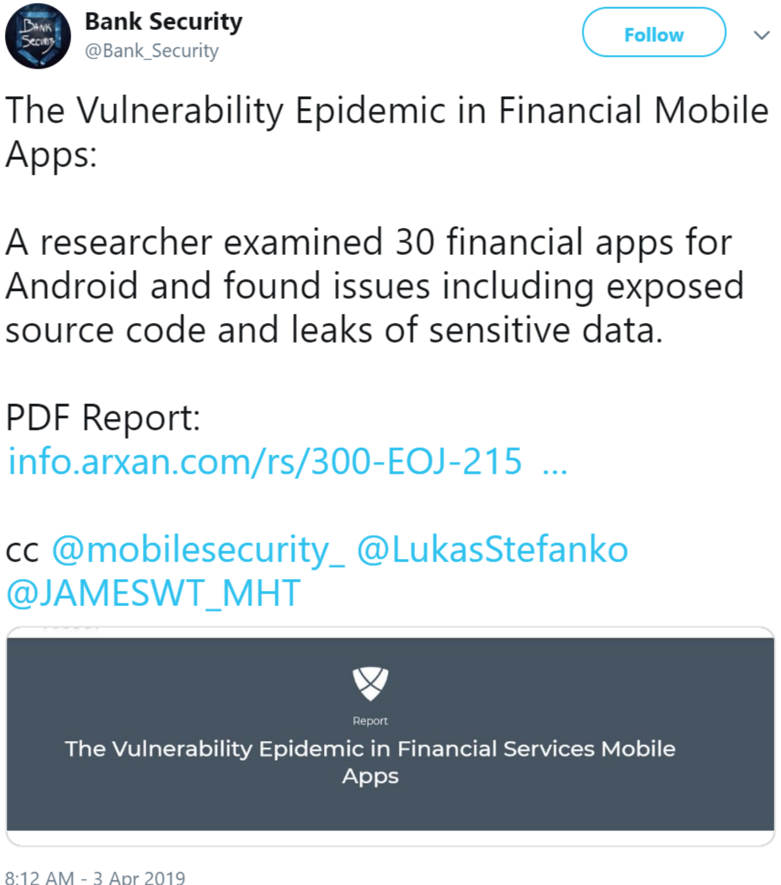
Ticketmaster has admi
BBC understands has

8,613 views | Sep 9, 2018, 01:00pm

380,000 Passengers Affec By 'Malicious' British Airv Hack

Jordan Bishop Contributor ⓘ
Travel

380,000 British Airways passengers have been affected by hack on the BA website and mobile app discovered on Thur According to the airline, both personal information, including passenger names and home addresses, as well as information, including credit card numbers, expiry dates ar codes, have been compromised. The breach comes just day



Bank Security
@Bank_Security

The Vulnerability Epidemic in Financial Mobile Apps:

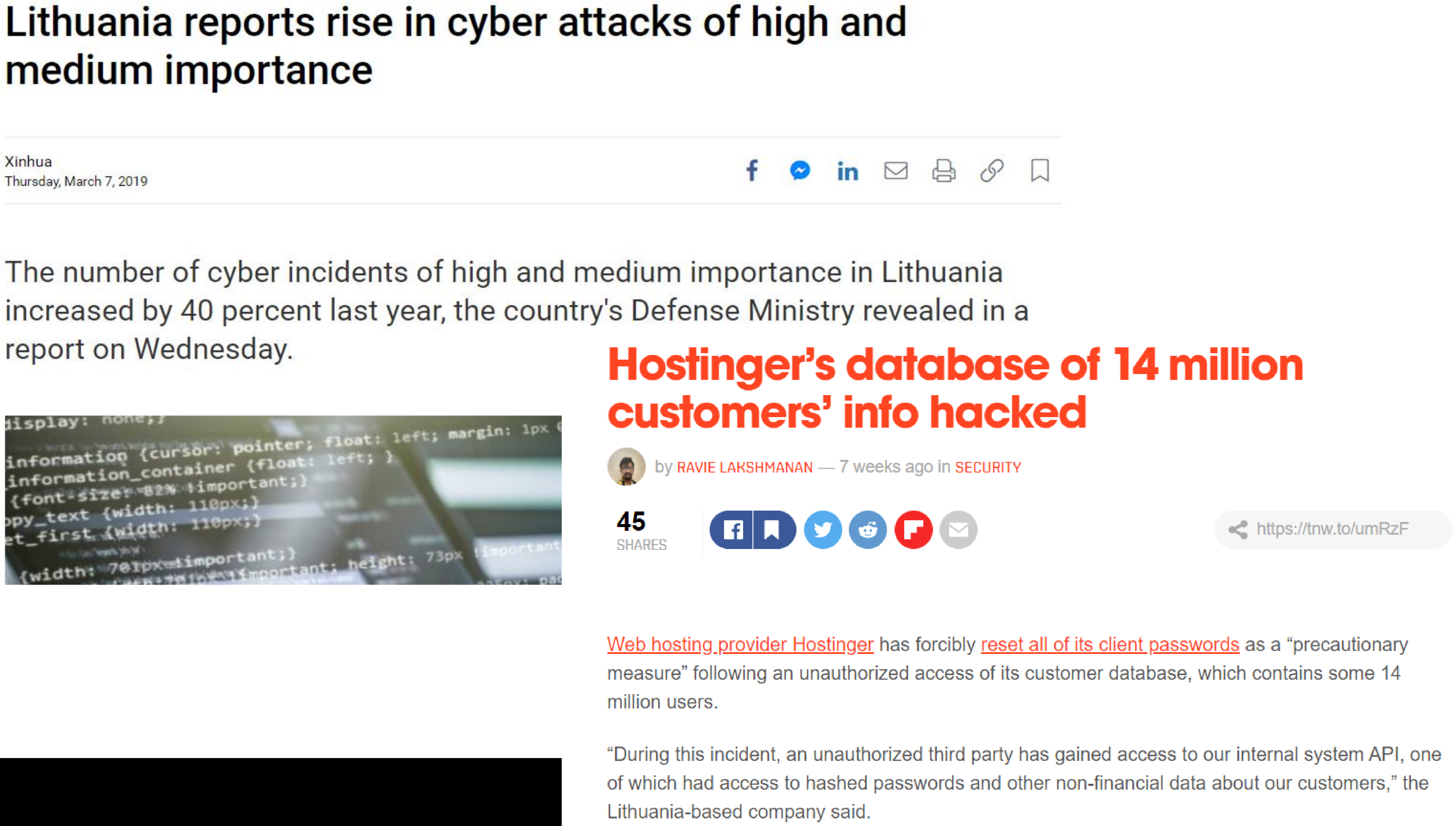
A researcher examined 30 financial apps for Android and found issues including exposed source code and leaks of sensitive data.

PDF Report:
info.arxan.com/rs/300-EOJ-215 …

cc @mobilesecurity_ @LukasStefanko @JAMESWT_MHT

Report
The Vulnerability Epidemic in Financial Services Mobile Apps

8:12 AM - 3 Apr 2019



Lithuania reports rise in cyber attacks of high and medium importance

Xinhua
Thursday, March 7, 2019

The number of cyber incidents of high and medium importance in Lithuania increased by 40 percent last year, the country's Defense Ministry revealed in a report on Wednesday.

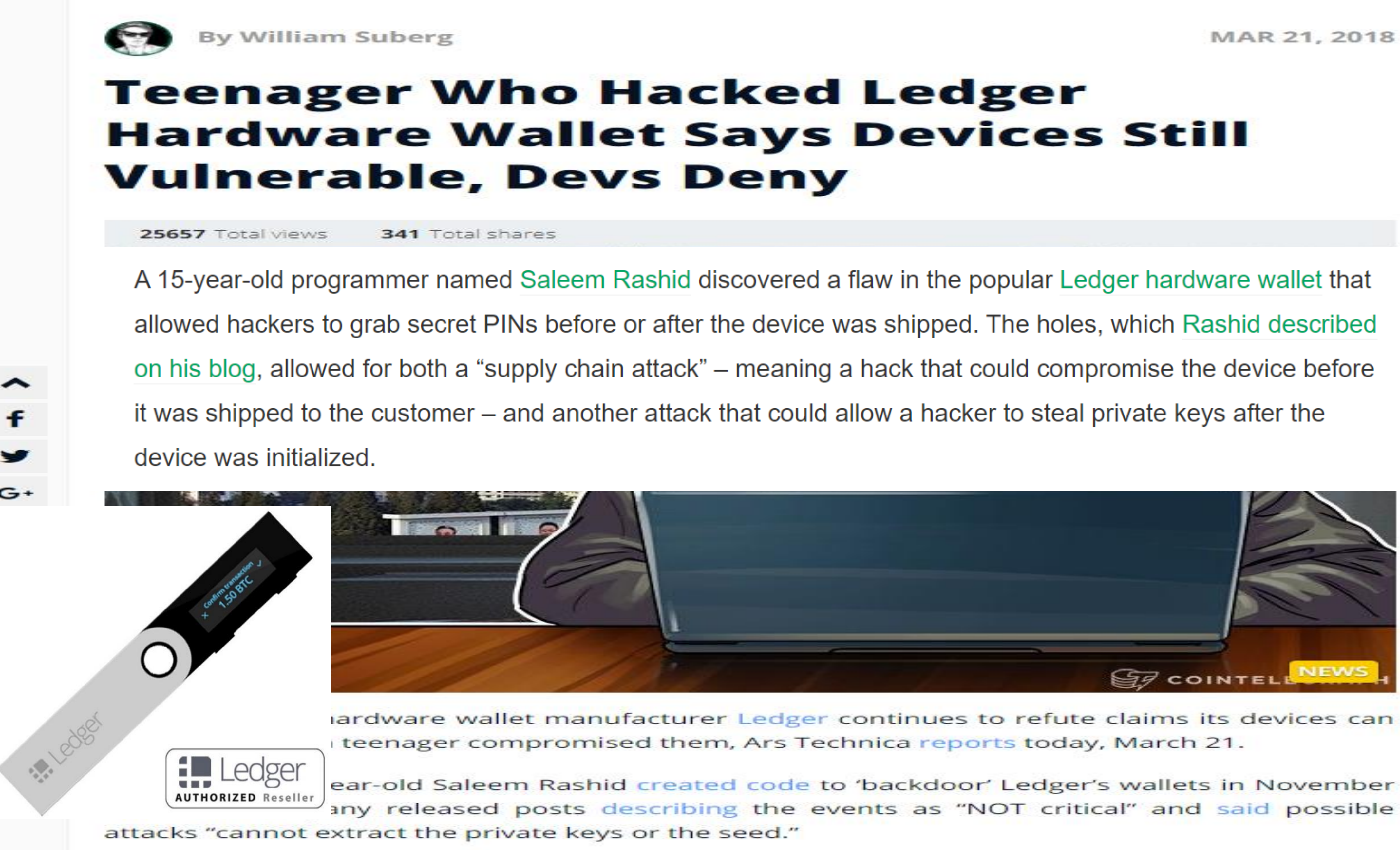
display: none;}
information {cursor: pointer; float: left; margin: 1px
information_container {float: left; }
{font-size: 82% !important;}
py_text {width: 110px;}
et_first {width: 110px;}
{width: 70px !important;}
!important; height: 73px !important

Hostinger's database of 14 million customers' info hacked

by RAVIE LAKSHMANAN — 7 weeks ago in SECURITY

Web hosting provider Hostinger has forcibly reset all of its client passwords as a “precautionary measure” following an unauthorized access of its customer database, which contains some 14 million users.

“During this incident, an unauthorized third party has gained access to our internal system API, one of which had access to hashed passwords and other non-financial data about our customers,” the Lithuania-based company said.



By William Suberg

MAR 21, 2018

Teenager Who Hacked Ledger Hardware Wallet Says Devices Still Vulnerable, Devs Deny

25657 Total views 341 Total shares

A 15-year-old programmer named Saleem Rashid discovered a flaw in the popular Ledger hardware wallet that allowed hackers to grab secret PINs before or after the device was shipped. The holes, which Rashid described on his blog, allowed for both a “supply chain attack” – meaning a hack that could compromise the device before it was shipped to the customer – and another attack that could allow a hacker to steal private keys after the device was initialized.

ıardware wallet manufacturer Ledger continues to refute claims its devices can ı teenager compromised them, Ars Technica reports today, March 21.

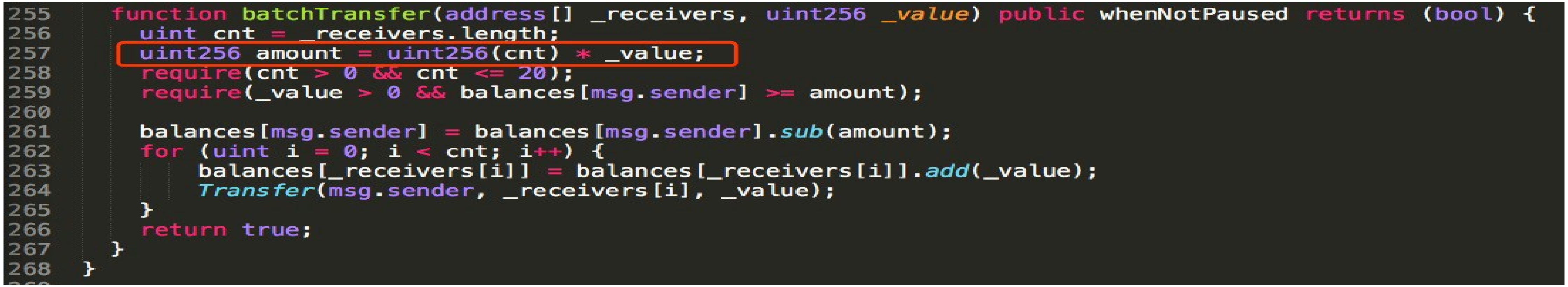
ear-old Saleem Rashid created code to ‘backdoor’ Ledger’s wallets in November ıny released posts describing the events as “NOT critical” and said possible attacks “cannot extract the private keys or the seed.”

Overflow error shuts down token trading

John Biggs @johnbiggs / Yesterday

Comment

A recently discovered programming error can make some crypto tokens susceptible to hackers. The exploit allows a hacker to pass an unusually high value to the exchange and get a ridiculous number of tokens in exchange, a problem that has caused the Okex exchange to shut down all token trading, including one called BeautyChain (BEC).



```
  function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {
    uint cnt = _receivers.length;
    uint256 amount = uint256(cnt) * _value;
    require(cnt > 0 && cnt <= 20);
    require(_value > 0 && balances[msg.sender] >= amount);

    balances[msg.sender] = balances[msg.sender].sub(amount);
    for (uint i = 0; i < cnt; i++) {
        balances[_receivers[i]] = balances[_receivers[i]].add(_value);
        Transfer(msg.sender, _receivers[i], _value);
    }
    return true;
  }
}
```

What's really interesting is how the hack worked. As you can see above, a line in the smart contract creates another value — amount — by multiplying cnt and _value. The hackers made a transfer and set the value to eight vigintillion — an eight with 63 zeroes. When this value is passed, the code overflows, allowing the hacker to gain a massive number of tokens. Thanks to the smart contract's "code-is-law" principal, each of these transfers are technically legitimate.

"There is no traditional well-known security response mechanism in place to remedy these vulnerable contracts!" wrote one researcher on Medium. "With that, we further run our system to scan and analyze other contracts. Our results show that more than a dozen of ERC20 contracts are also vulnerable to batchOverflow."

drive dream desire goals
goals inspiration dreams drive
success $ drive incentive
dream innovation motivation ambition dreams
success desire drive goals success action success
hunt incentive
incentive inspiration dreams action dream dream
motivation success
$ success action dreams wish innovation goals hunt goals drive
dreams
drive success wish innovation goals success desire innovation incentive motivation wish hunt
action MOTIVATION action
goals success
inspiration drive goals
desire
success dream innovation hunt wish motivation drive innovation incentive success
innovation goals drive action desire dreams ambition
innovation
success motivation ambition action drive innovation wish innovation
action desire drive inspiration drive goals dream goals
success innovation
drive incentive dreams dream incentive
ambition success innovation inspiration
goals innovation ambition action drive
dreams motivation desire success drive
wish
drive
hunt
action
goal
wish
dream
$

Results from our little research

- Analyzed web pentest results from last two years
- Compared those results with knowledge of juniors/newcomers
- Results
  - ~ 20% of issues can be easily detected by different tools
  - ~ 15% issues can be tested with no special tools, just browser
  - Majority severity issues are LOW, some MEDIUM

Security testing???

- It’s like **almost** any other testing except with security and data integrity in primary focus
- You shouldn't be **afraid** and **have your mind open** for **new** things
- Think about **common** vulnerabilities and scenarios
- Use **tools** to help you! (you are used to use tools) ;)
- **Enjoy**!

Challenges of Security Testing

- Application Security testing
  - Identifying all **unintended** functions in the code
  - Testing using data that application is **not expecting**
  - Try to get **unintended responses** from the application
  - Identify some **unplanned workflows** in the application

- Not always **trivial** and **simple** task!
  - Sometimes ‘ character gives really crazy results

Software testers

Characteristics

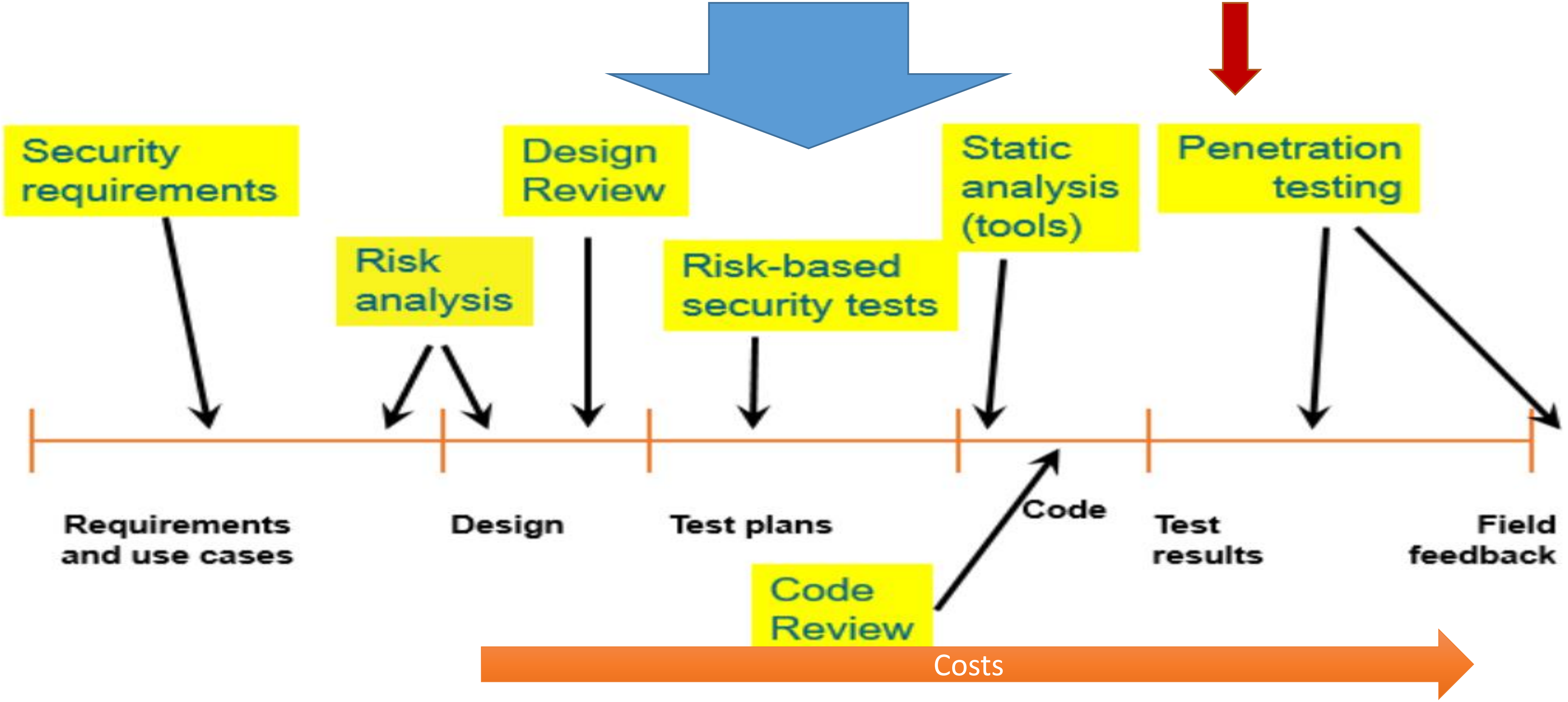
- Motivations
  - Validation of correct execution
  - Repeatable and predictable evidence
- Skills
  - Deep understanding of actual usage
- Advantages
  - Can reach every function/action
  - Have test data for all cases
- Weaknesses
  - Focused on “happy path”
  - Little or no security expertise

Contribution to security

- Can exercise much more than any pentester
- Can provide logs, test data, test environment
- Can repeat security tests long after pentester are gone

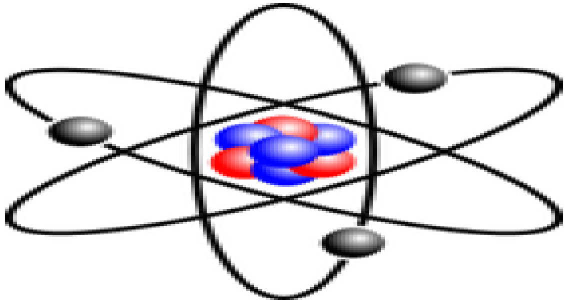
https://conference.eurostarsoftwaretesting.com/wp-content/uploads/K6-Paco-Hope-Wild-West-EuroSTAR-2015-Final-Slides.pdf

Testers vs pentesters



Myth or truth?

Everyone who has something to do with SOFTWARE has something to do with SOFTWARE SECURITY!



KEEP CALM AND TEST MY HYPOTHESIS

My hypothesis!

Every software/hardware tester should have small/tiny positive

“**criminal**”

mindset!

Think like a hacker!

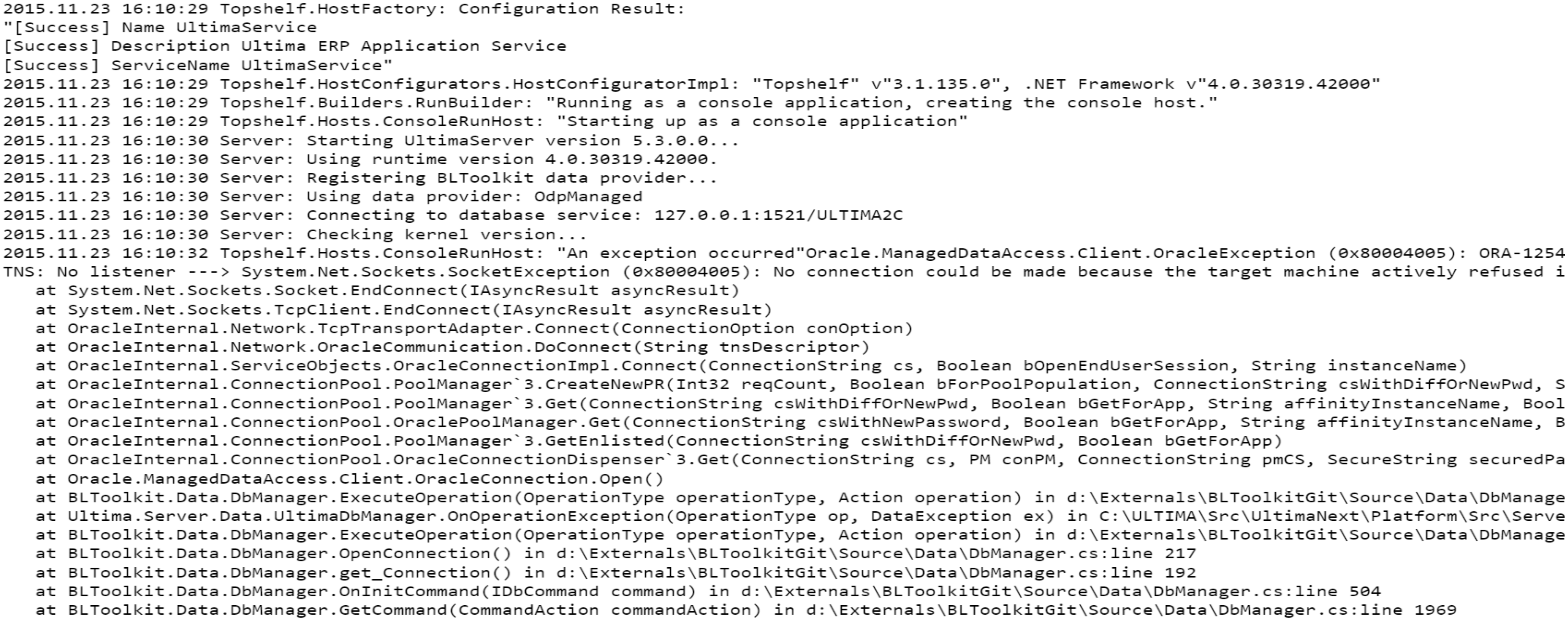
- **Terminology**
  - Defects known as vulnerabilities or vulns
- **Mindset**
  - Program deviations, corner cases
- **Method**
  - How to bypass or destroy things
- **Tools**
  - Well known or private arsenal
- **Goal**
  - Abuse, break, manipulate

Issues! Our own experience

- HTTP, secure cookies
- Password policies allowing to set password as “a”
- In local storage **admin=false** or other values
- User with **USER privilege** can create another user
- Insufficient validation and session issues (expiration)
- Old or even vulnerable libraries used
- Improper error handling
- Negative amounts!

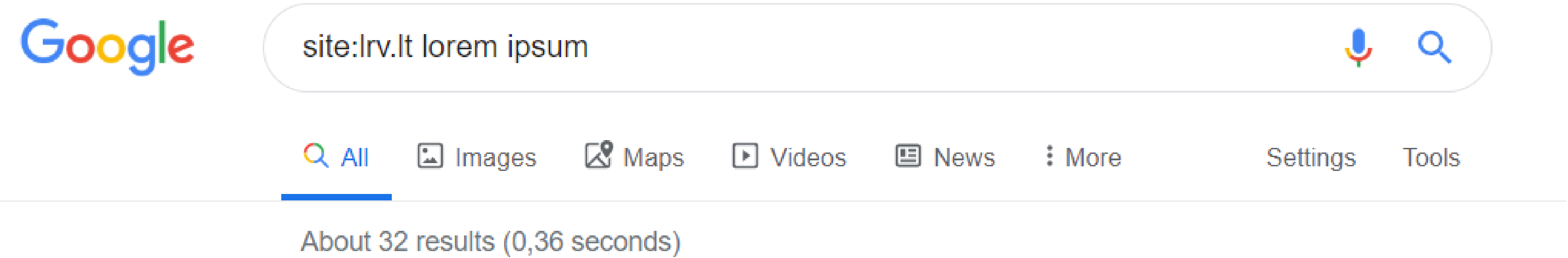
GET
INSPIRED
BY THESE
EXAMPLES

Errors, strange disclosures. Easy to spot and find!



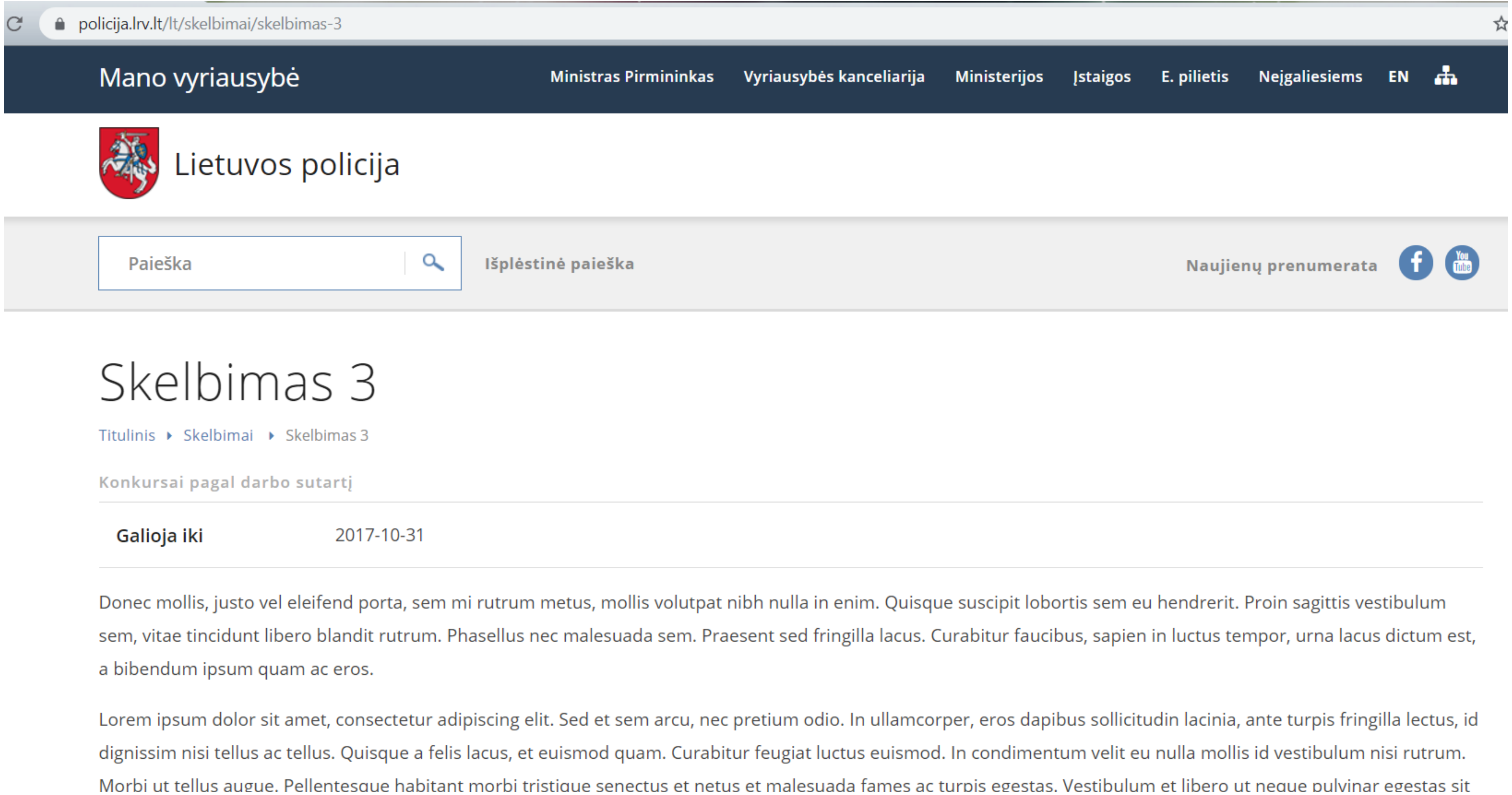
```
2015.11.23 16:10:29 Topshelf.HostFactory: Configuration Result:
"[Success] Name UltimaService
[Success] Description Ultima ERP Application Service
[Success] ServiceName UltimaService"
2015.11.23 16:10:29 Topshelf.HostConfigurators.HostConfiguratorImpl: "Topshelf" v"3.1.135.0", .NET Framework v"4.0.30319.42000"
2015.11.23 16:10:29 Topshelf.Builders.RunBuilder: "Running as a console application, creating the console host."
2015.11.23 16:10:29 Topshelf.Hosts.ConsoleRunHost: "Starting up as a console application"
2015.11.23 16:10:30 Server: Starting UltimaServer version 5.3.0.0...
2015.11.23 16:10:30 Server: Using runtime version 4.0.30319.42000.
2015.11.23 16:10:30 Server: Registering BLToolkit data provider...
2015.11.23 16:10:30 Server: Using data provider: OdpManaged
2015.11.23 16:10:30 Server: Connecting to database service: 127.0.0.1:1521/ULTIMA2C
2015.11.23 16:10:30 Server: Checking kernel version...
2015.11.23 16:10:32 Topshelf.Hosts.ConsoleRunHost: "An exception occurred"Oracle.ManagedDataAccess.Client.OracleException (0x80004005): ORA-1254
TNS: No listener ---> System.Net.Sockets.SocketException (0x80004005): No connection could be made because the target machine actively refused i
   at System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult)
   at System.Net.Sockets.TcpClient.EndConnect(IAsyncResult asyncResult)
   at OracleInternal.Network.TcpTransportAdapter.Connect(ConnectionOption conOption)
   at OracleInternal.Network.OracleCommunication.DoConnect(String tnsDescriptor)
   at OracleInternal.ServiceObjects.OracleConnectionImpl.Connect(ConnectionString cs, Boolean bOpenEndUserSession, String instanceName)
   at OracleInternal.ConnectionPool.PoolManager`3.CreateNewPR(Int32 reqCount, Boolean bForPoolPopulation, ConnectionString csWithDiffOrNewPwd, S
   at OracleInternal.ConnectionPool.PoolManager`3.Get(ConnectionString csWithDiffOrNewPwd, Boolean bGetForApp, String affinityInstanceName, Bool
   at OracleInternal.ConnectionPool.OraclePoolManager.Get(ConnectionString csWithNewPassword, Boolean bGetForApp, String affinityInstanceName, B
   at OracleInternal.ConnectionPool.PoolManager`3.GetEnlisted(ConnectionString csWithDiffOrNewPwd, Boolean bGetForApp)
   at OracleInternal.ConnectionPool.OracleConnectionDispenser`3.Get(ConnectionString cs, PM conPM, ConnectionString pmCS, SecureString securedPa
   at Oracle.ManagedDataAccess.Client.OracleConnection.Open()
   at BLToolkit.Data.DbManager.ExecuteOperation(OperationType operationType, Action operation) in d:\Externals\BLToolkitGit\Source\Data\DbManage
   at Ultima.Server.Data.UltimaDbManager.OnOperationException(OperationType op, DataException ex) in C:\ULTIMA\Src\UltimaNext\Platform\Src\Serve
   at BLToolkit.Data.DbManager.ExecuteOperation(OperationType operationType, Action operation) in d:\Externals\BLToolkitGit\Source\Data\DbManage
   at BLToolkit.Data.DbManager.OpenConnection() in d:\Externals\BLToolkitGit\Source\Data\DbManager.cs:line 217
   at BLToolkit.Data.DbManager.get_Connection() in d:\Externals\BLToolkitGit\Source\Data\DbManager.cs:line 192
   at BLToolkit.Data.DbManager.OnInitCommand(IDbCommand command) in d:\Externals\BLToolkitGit\Source\Data\DbManager.cs:line 504
   at BLToolkit.Data.DbManager.GetCommand(CommandAction commandAction) in d:\Externals\BLToolkitGit\Source\Data\DbManager.cs:line 1969
```

Google!



site:lrv.lt lorem ipsum

About 32 results (0,36 seconds)



policija.lrv.lt/lt/skelbimai/skelbimas-3

Skelbimas 3

Titulinis ‣ Skelbimai ‣ Skelbimas 3

Konkursai pagal darbo sutartį

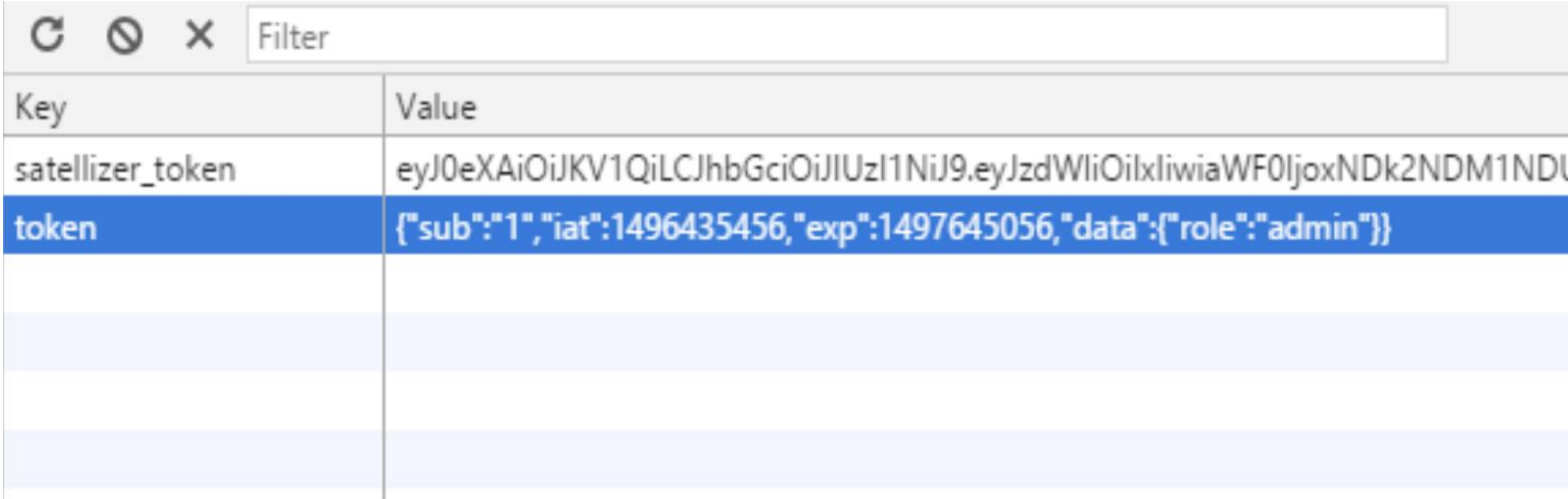
Galioja iki	2017-10-31

Donec mollis, justo vel eleifend porta, sem mi rutrum metus, mollis volutpat nibh nulla in enim. Quisque suscipit lobortis sem eu hendrerit. Proin sagittis vestibulum sem, vitae tincidunt libero blandit rutrum. Phasellus nec malesuada sem. Praesent sed fringilla lacus. Curabitur faucibus, sapien in luctus tempor, urna lacus dictum est, a bibendum ipsum quam ac eros.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed et sem arcu, nec pretium odio. In ullamcorper, eros dapibus sollicitudin lacinia, ante turpis fringilla lectus, id dignissim nisi tellus ac tellus. Quisque a felis lacus, et euismod quam. Curabitur feugiat luctus euismod. In condimentum velit eu nulla mollis id vestibulum nisi rutrum. Morbi ut tellus augue. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Vestibulum et libero ut neque pulvinar egestas sit

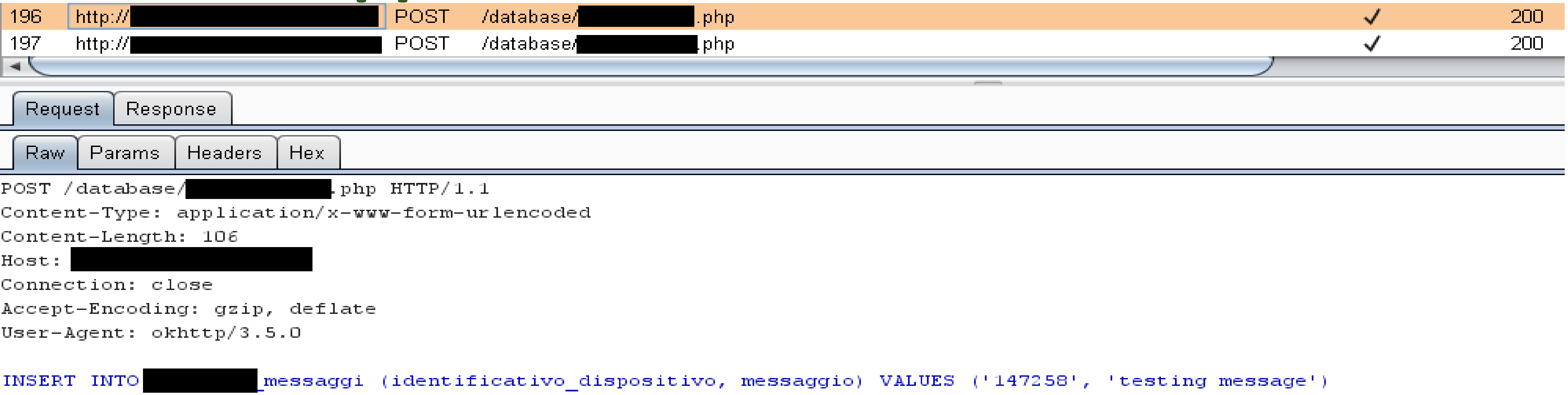
Local storage

- Easy to spot
- No extra tools needed



Key	Value
satellizer_token	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiIxIiwiaWF0IjoxNDk2NDM1NDU
token	{"sub":"1","iat":1496435456,"exp":1497645056,"data":{"role":"admin"}}

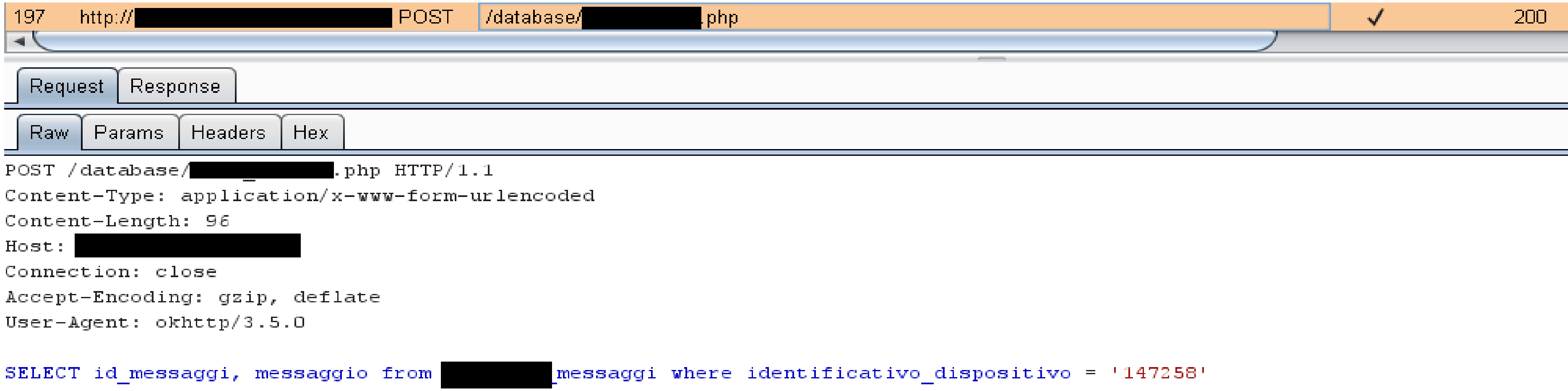
Mobile app, 50k+ installs



196 http://[redacted] POST /database/[redacted].php ✓ 200
197 http://[redacted] POST /database/[redacted].php ✓ 200
Request
Response
Raw
Params
Headers
Hex

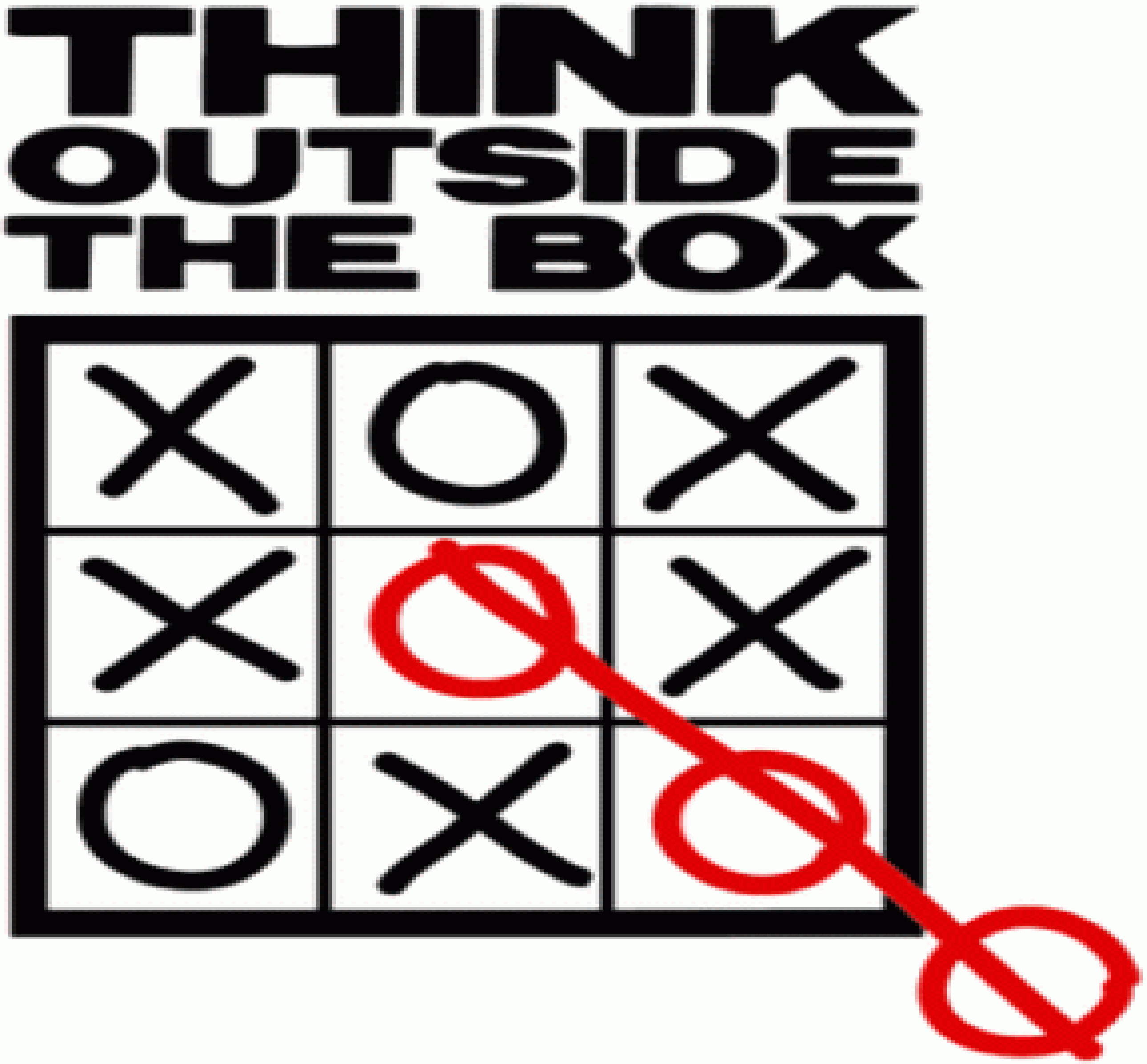
```
POST /database/[redacted].php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 106
Host: [redacted]
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.5.0

INSERT INTO [redacted]_messaggi (identificativo_dispositivo, messaggio) VALUES ('147258', 'testing message')
```

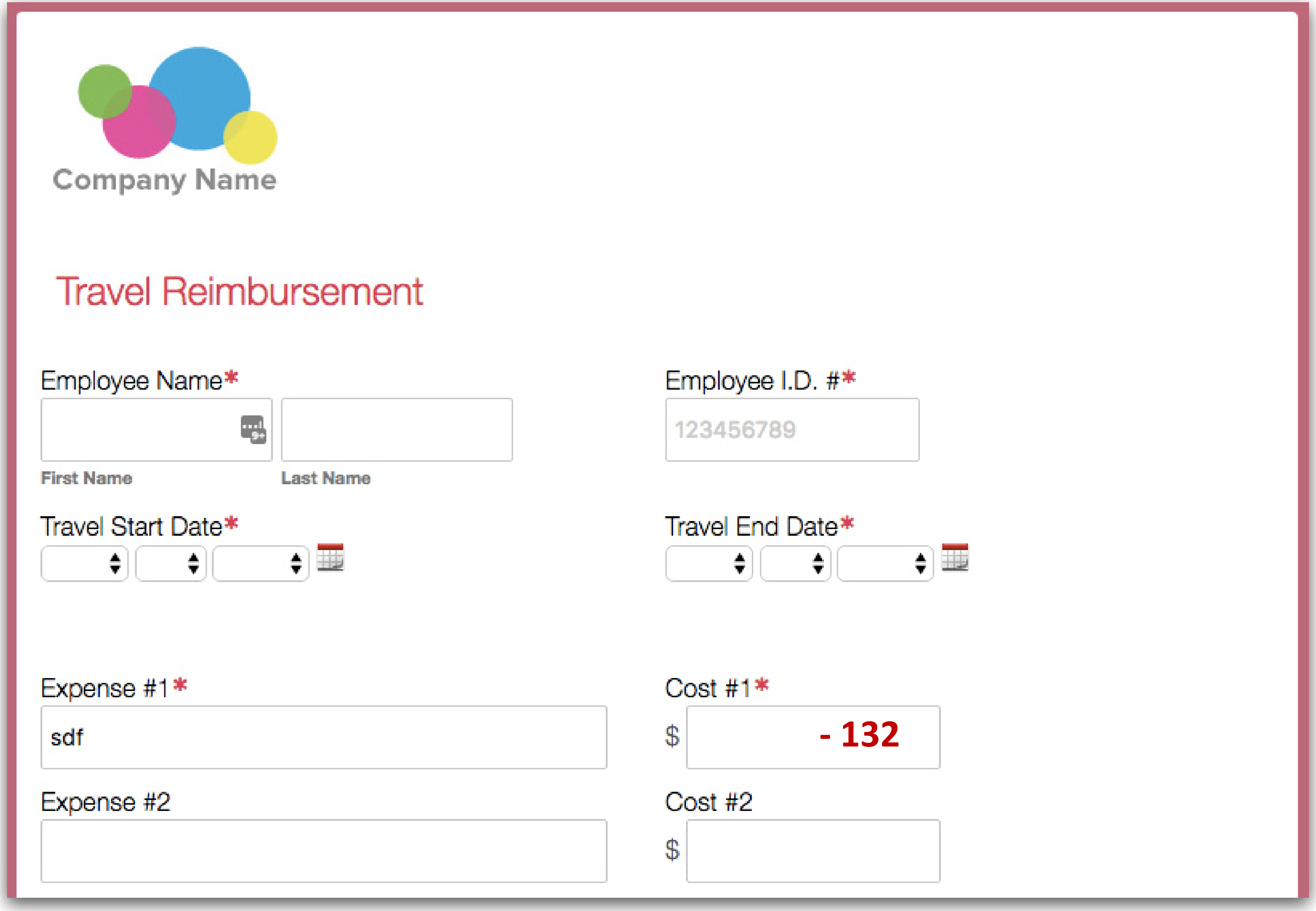


```
POST /database/[redacted].php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Host: [redacted]
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.5.0

SELECT id_messaggi, messaggio from [redacted]messaggi where identificativo_dispositivo = '147258'
```



THINK
OUTSIDE
THE BOX



Company Name

Travel Reimbursement

Employee Name*

First Name

Last Name

Employee I.D. #*

123456789

Travel Start Date*

Travel End Date*

Expense #1*

sdf

Cost #1*

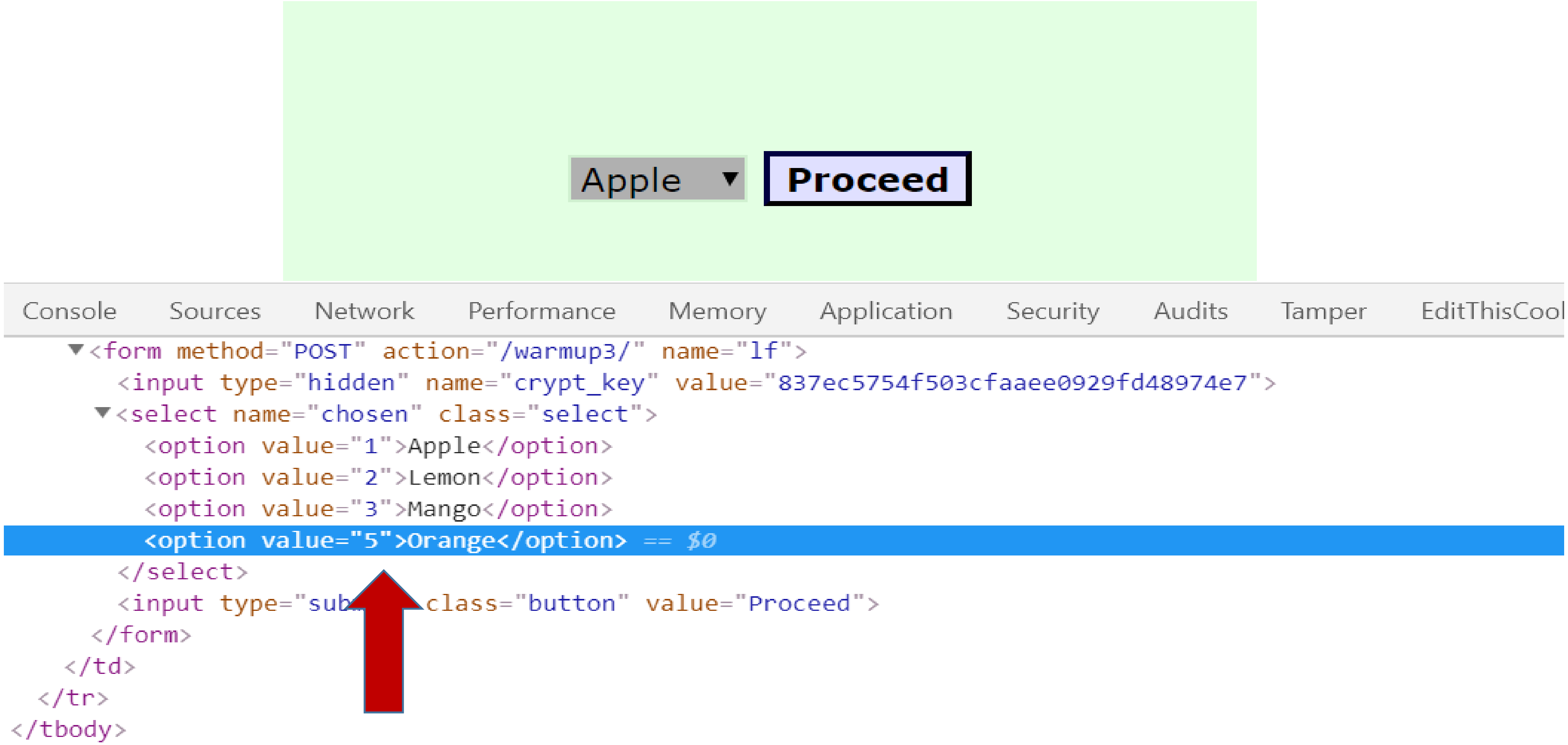
$ - 132

Expense #2

Cost #2

$

Demo – manipulate app logic



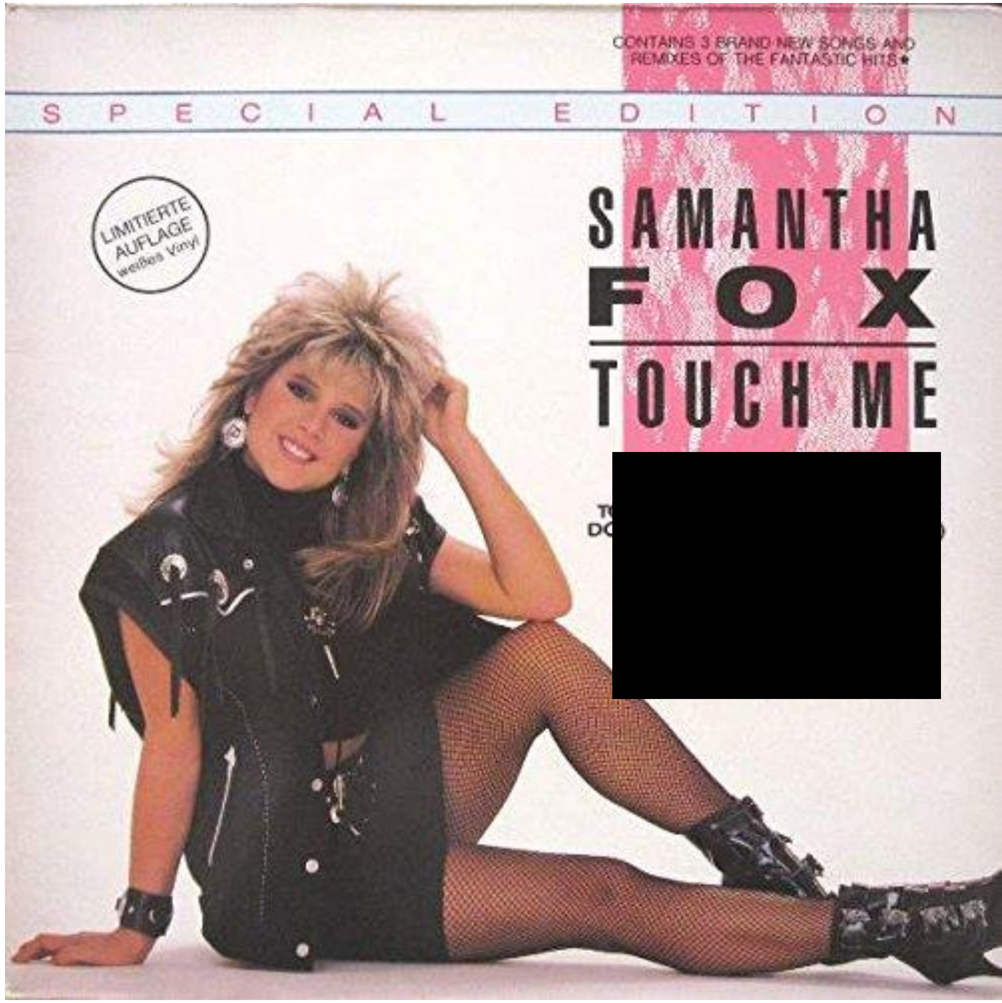
```
  ▼<form method="POST" action="/warmup3/" name="lf">
     <input type="hidden" name="crypt_key" value="837ec5754f503cfaaee0929fd48974e7">
   ▼<select name="chosen" class="select">
       <option value="1">Apple</option>
       <option value="2">Lemon</option>
       <option value="3">Mango</option>
       <option value="5">Orange</option> == $0
     </select>
     <input type="sub      class="button" value="Proceed">
   </form>
  </td>
 </tr>
</tbody>
```

TOUCH ME!

- So what your title has to do with testing and testers???
- You need to start **touching** things **outside** of you **comfort/knowledge** zone!

Why?

  - To make our (pentester) life **easier**, so we can **focus** on **real** issues!



CONTAINS 3 BRAND NEW SONGS AND REMIXES OF THE FANTASTIC HITS
SPECIAL EDITION
LIMITIERTE AUFLAGE weißes Vinyl
SAMANTHA FOX
TOUCH ME

[redacted]

Ask yourself a question!

AppSec Testing 101

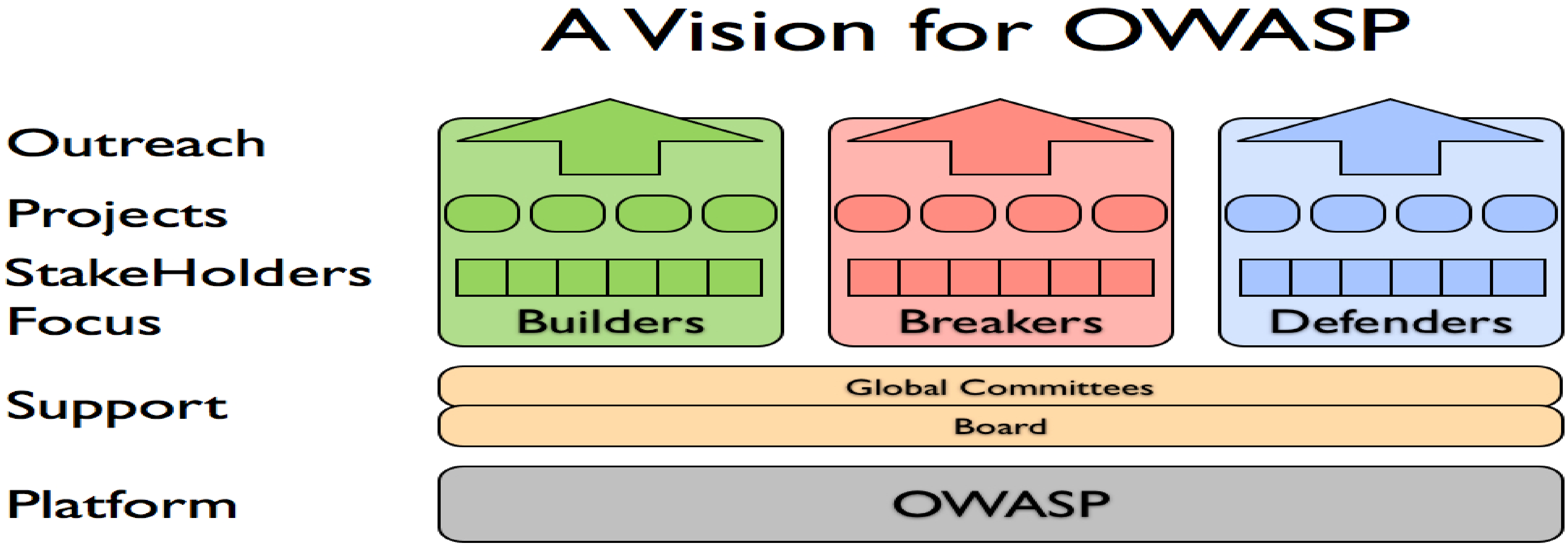
- Know at least some security **basics**
- There are plenty **resources** possible to find using Google
  - OWASP (web, mobile, IoT)
  - CWE (Common Weakness Enumeration) Classified application weaknesses
  - WASC (Web Application Security Consortium) – Threat classifications
- Get familiar with **Offensive** and **Defensive** Techniques
  - Mailing lists
  - Conferences – talk to people – **sharing** is **caring**

Really good start for web, mobile, IoT, …

OWASP

Open Web Application
Security Project

OWASP cont’d



A Vision for OWASP

Outreach

Projects

StakeHolders

Focus

Builders

Breakers

Defenders

Support

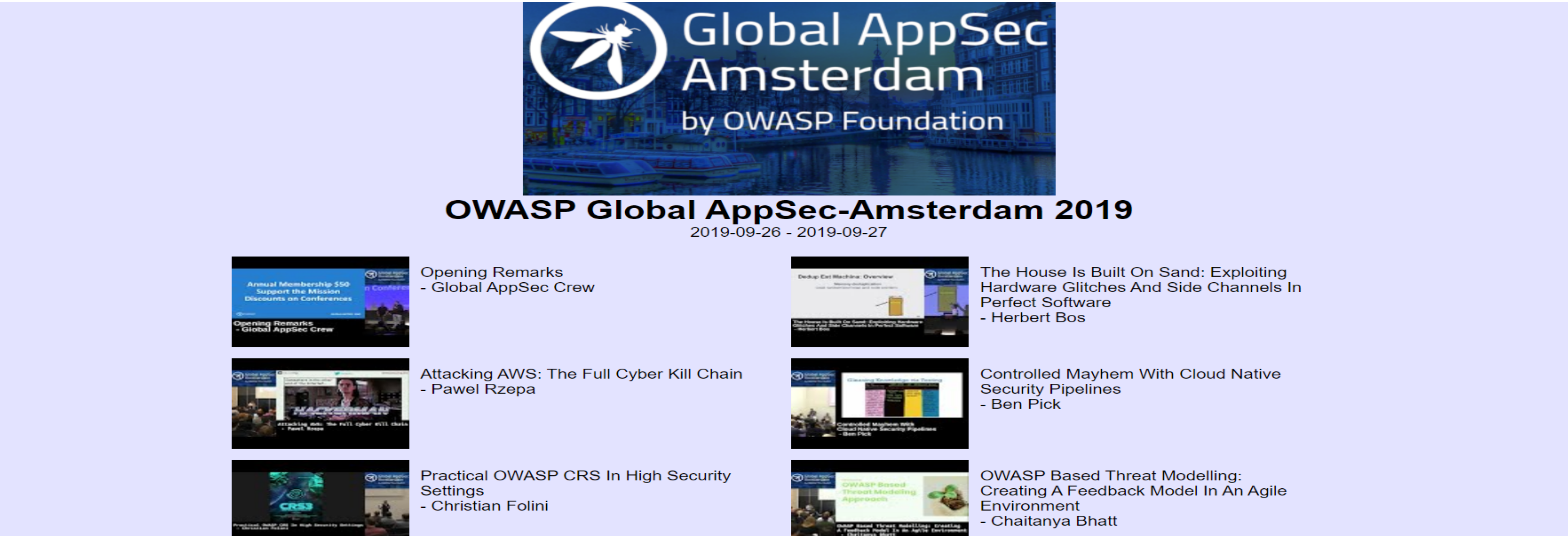
Global Committees

Board

Platform

OWASP

Fresh from the oven!



Global AppSec Amsterdam

by OWASP Foundation

OWASP Global AppSec-Amsterdam 2019

2019-09-26 - 2019-09-27

Opening Remarks
- Global AppSec Crew

The House Is Built On Sand: Exploiting Hardware Glitches And Side Channels In Perfect Software
- Herbert Bos

Attacking AWS: The Full Cyber Kill Chain
- Pawel Rzepa

Controlled Mayhem With Cloud Native Security Pipelines
- Ben Pick

Practical OWASP CRS In High Security Settings
- Christian Folini

OWASP Based Threat Modelling: Creating A Feedback Model In An Agile Environment
- Chaitanya Bhatt

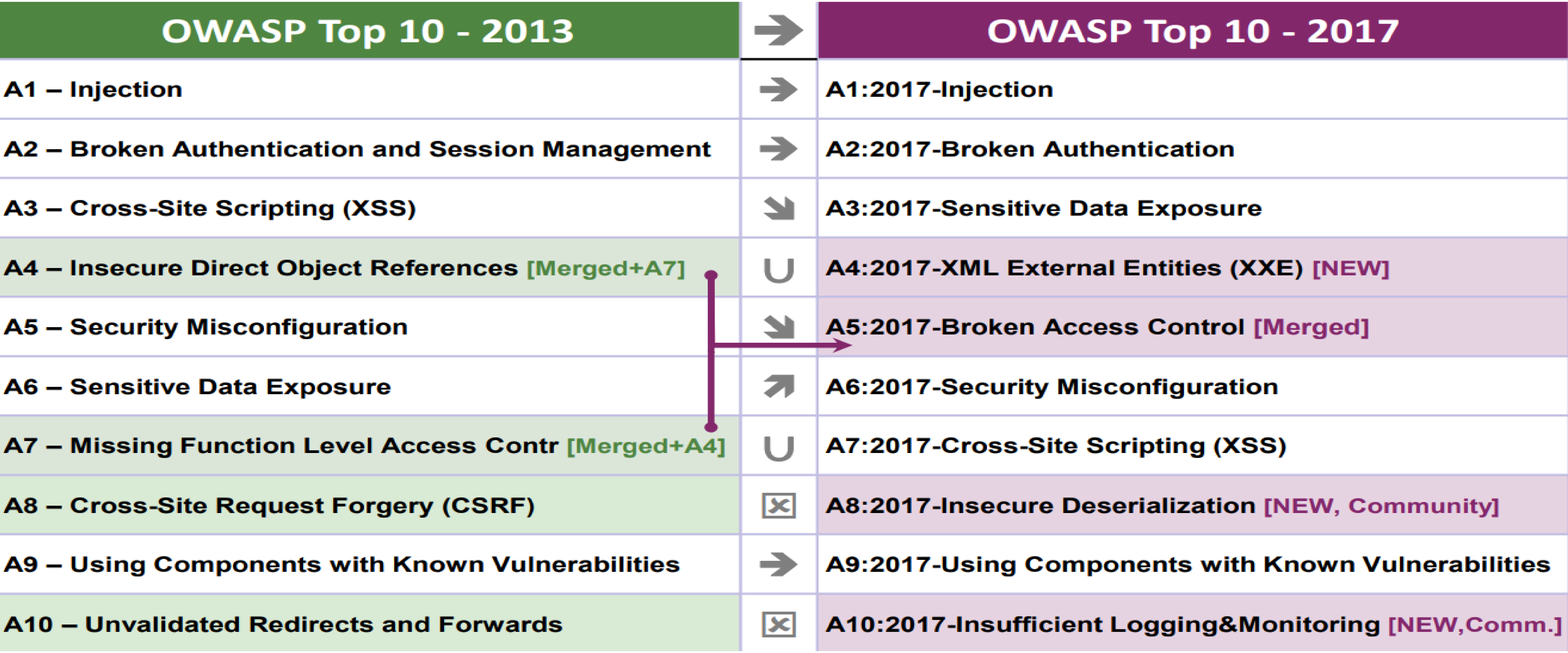
https://administraitor.video/edition/OWASP%20Global%20AppSec-Amsterdam/2019

OWASP Testing Framework/guide

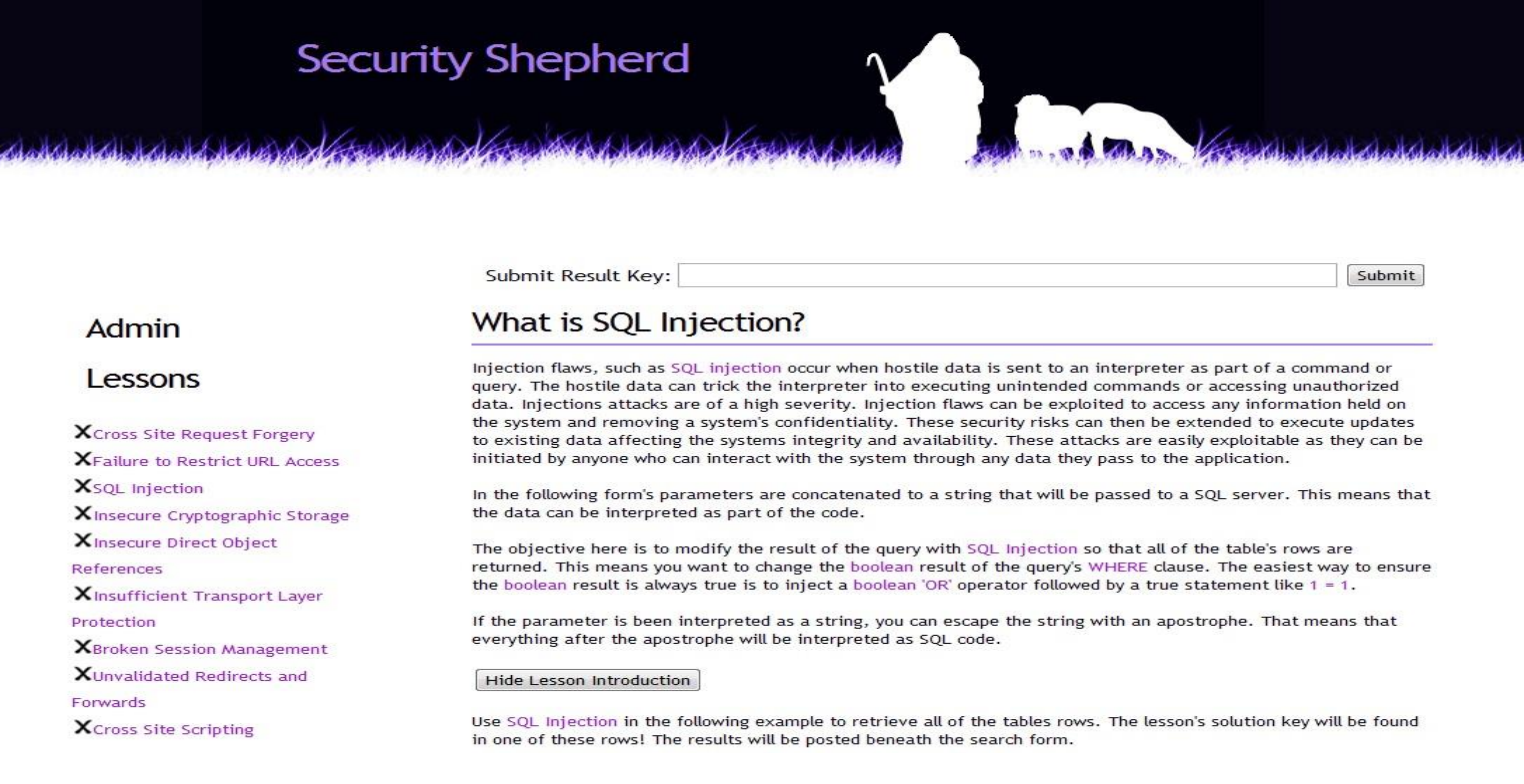
Every tester **should/must** be familiar with this! (only **224 pages**)

- 4.2 Information Gathering
- 4.3 Configuration Management Testing
- 4.4 Business logic testing
- 4.5 Authentication Testing
- 4.6 Authorization Testing
- 4.7 Session Management Testing
- 4.8 Data Validation Testing
- 4.9 Testing for Denial of Service
- 4.10 Web Services Testing

OWASP TOP 10



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.]



Security Shepherd

Submit Result Key: Submit

Admin

Lessons

- ✗Cross Site Request Forgery
- ✗Failure to Restrict URL Access
- ✗SQL Injection
- ✗Insecure Cryptographic Storage
- ✗Insecure Direct Object References
- ✗Insufficient Transport Layer Protection
- ✗Broken Session Management
- ✗Unvalidated Redirects and Forwards
- ✗Cross Site Scripting

What is SQL Injection?

Injection flaws, such as SQL injection occur when hostile data is sent to an interpreter as part of a command or query. The hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. Injections attacks are of a high severity. Injection flaws can be exploited to access any information held on the system and removing a system's confidentiality. These security risks can then be extended to execute updates to existing data affecting the systems integrity and availability. These attacks are easily exploitable as they can be initiated by anyone who can interact with the system through any data they pass to the application.

In the following form's parameters are concatenated to a string that will be passed to a SQL server. This means that the data can be interpreted as part of the code.

The objective here is to modify the result of the query with SQL Injection so that all of the table's rows are returned. This means you want to change the boolean result of the query's WHERE clause. The easiest way to ensure the boolean result is always true is to inject a boolean 'OR' operator followed by a true statement like 1 = 1.

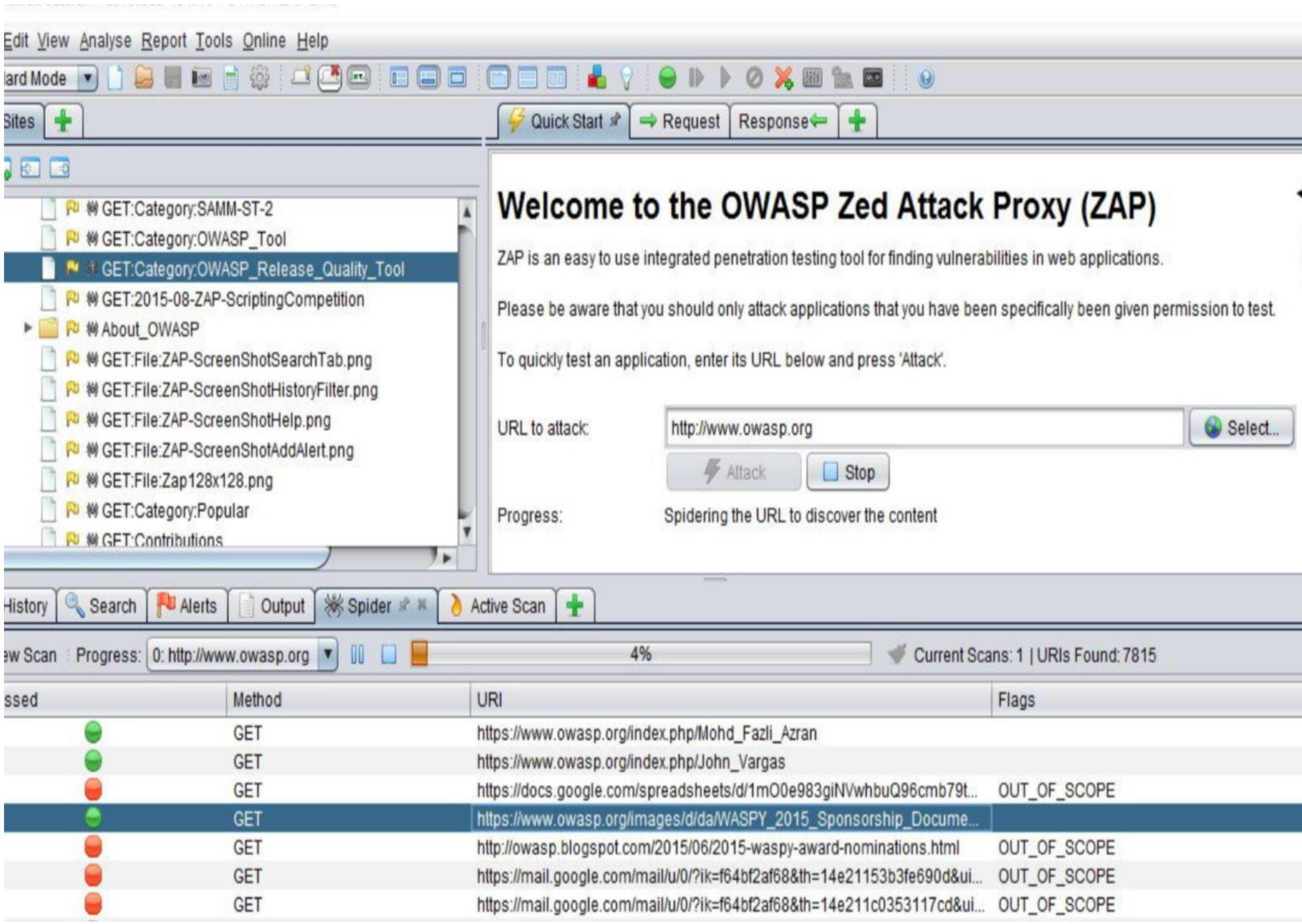
If the parameter is been interpreted as a string, you can escape the string with an apostrophe. That means that everything after the apostrophe will be interpreted as SQL code.

Hide Lesson Introduction

Use SQL Injection in the following example to retrieve all of the tables rows. The lesson's solution key will be found in one of these rows! The results will be posted beneath the search form.

OWASP ZAP

- Free proxy
- Portable – Java
- Simple to use
- Flagship product
- Point and shoot
- CI/CD ready headless mode



GET:Category:SAMM-ST-2
GET:Category:OWASP_Tool
GET:Category:OWASP_Release_Quality_Tool
GET:2015-08-ZAP-ScriptingCompetition
About_OWASP
GET:File:ZAP-ScreenShotSearchTab.png
GET:File:ZAP-ScreenShotHistoryFilter.png
GET:File:ZAP-ScreenShotHelp.png
GET:File:ZAP-ScreenShotAddAlert.png
GET:File:Zap128x128.png
GET:Category:Popular
GET:Contributions

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.owasp.org Select...

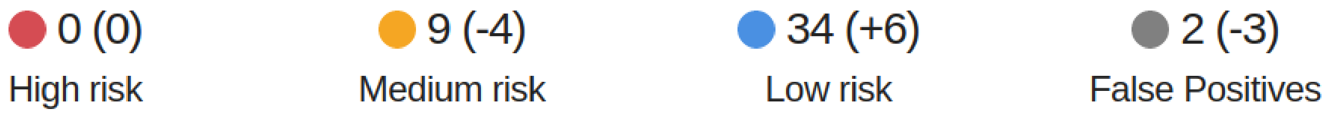
Attack Stop

Progress: Spidering the URL to discover the content

ew Scan Progress: 0: http://www.owasp.org 4% Current Scans: 1 | URIs Found: 7815

ssed	Method	URI	Flags
●	GET	https://www.owasp.org/index.php/Mohd_Fazli_Azran	
●	GET	https://www.owasp.org/index.php/John_Vargas	
●	GET	https://docs.google.com/spreadsheets/d/1mO0e983giNVwhbuQ96cmb79t...	OUT_OF_SCOPE
●	GET	https://www.owasp.org/images/d/da/WASPY_2015_Sponsorship_Docume...	
●	GET	http://owasp.blogspot.com/2015/06/2015-waspy-award-nominations.html	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e21153b3fe690d&ui...	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e211c0353117cd&ui...	OUT_OF_SCOPE

ZAP with Jenkins

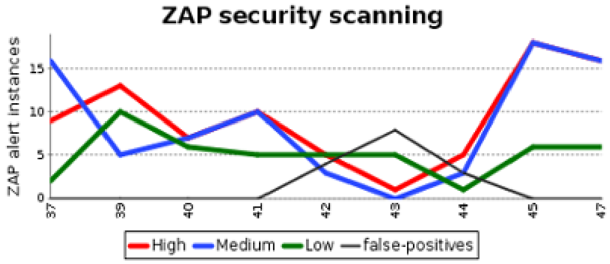


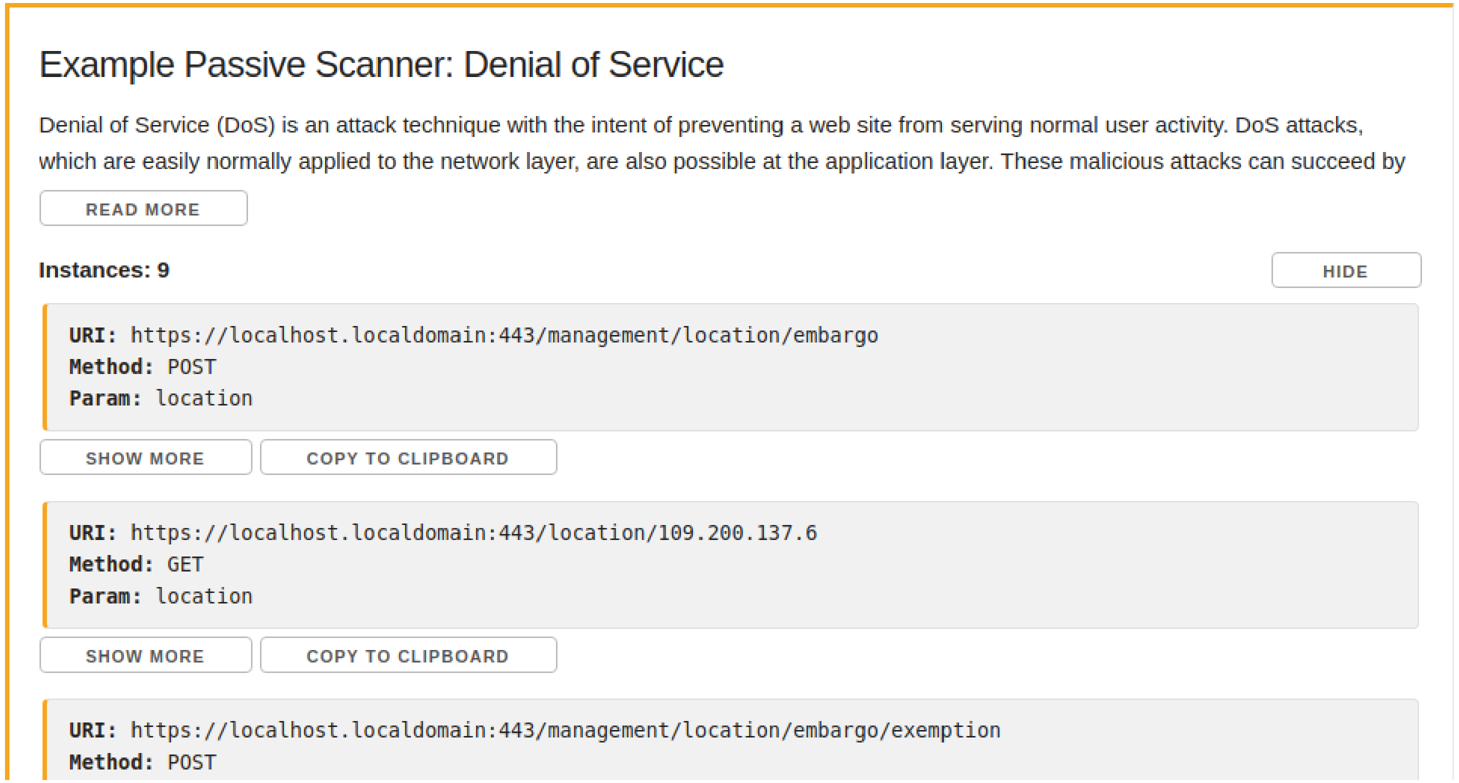
● 0 (0) High risk

● 9 (-4) Medium risk

● 34 (+6) Low risk

● 2 (-3) False Positives





Example Passive Scanner: Denial of Service

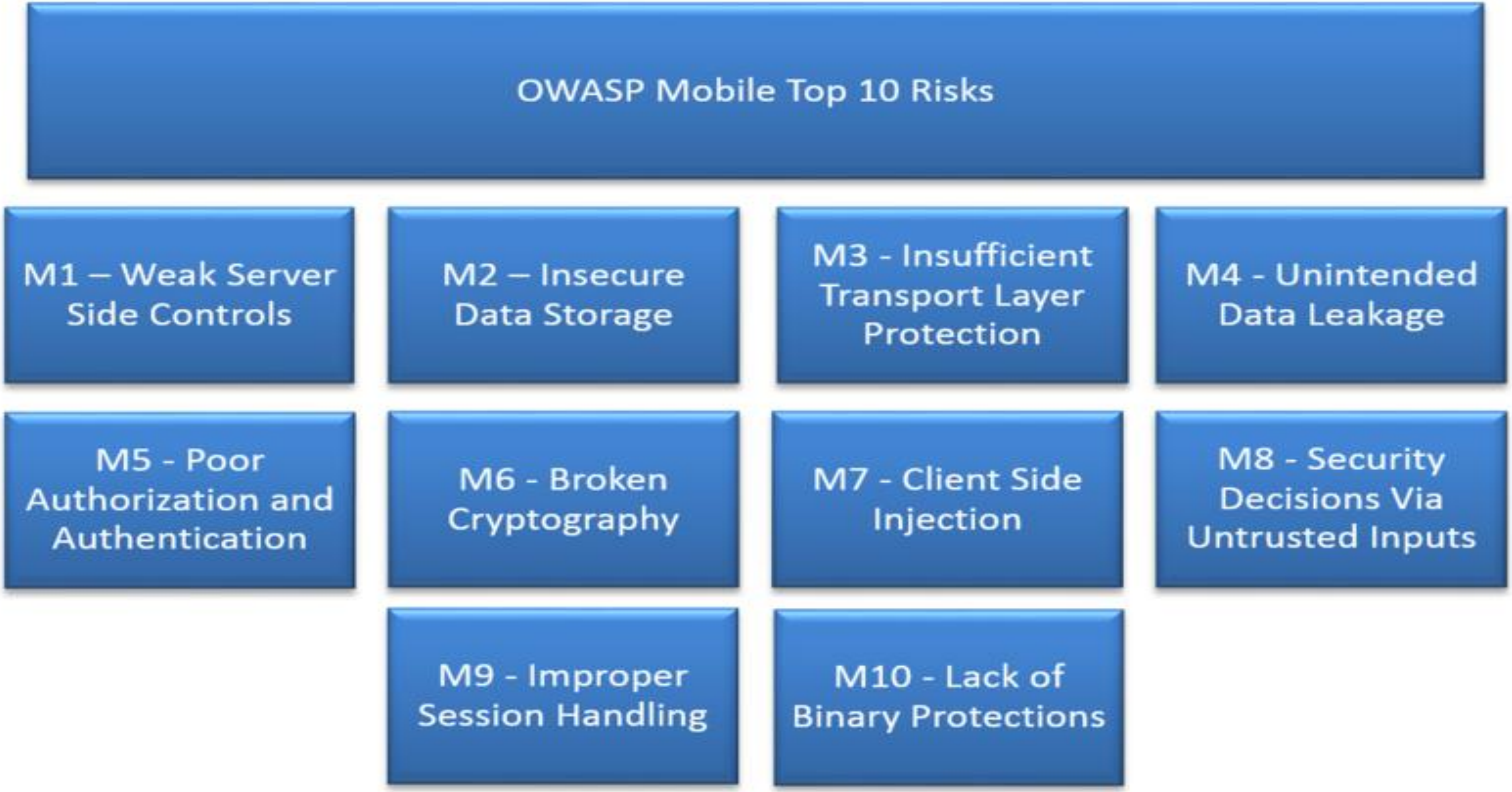
Denial of Service (DoS) is an attack technique with the intent of preventing a web site from serving normal user activity. DoS attacks, which are easily normally applied to the network layer, are also possible at the application layer. These malicious attacks can succeed by

Instances: 9

```
URI: https://localhost.localdomain:443/management/location/embargo
Method: POST
Param: location
```

```
URI: https://localhost.localdomain:443/location/109.200.137.6
Method: GET
Param: location
```

```
URI: https://localhost.localdomain:443/management/location/embargo/exemption
Method: POST
```



OWASP Mobile Top 10 Risks

M1 – Weak Server Side Controls

M2 – Insecure Data Storage

M3 - Insufficient Transport Layer Protection

M4 - Unintended Data Leakage

M5 - Poor Authorization and Authentication

M6 - Broken Cryptography

M7 - Client Side Injection

M8 - Security Decisions Via Untrusted Inputs

M9 - Improper Session Handling

M10 - Lack of Binary Protections

OWASP TOP 10
INTERNET OF THINGS 2018

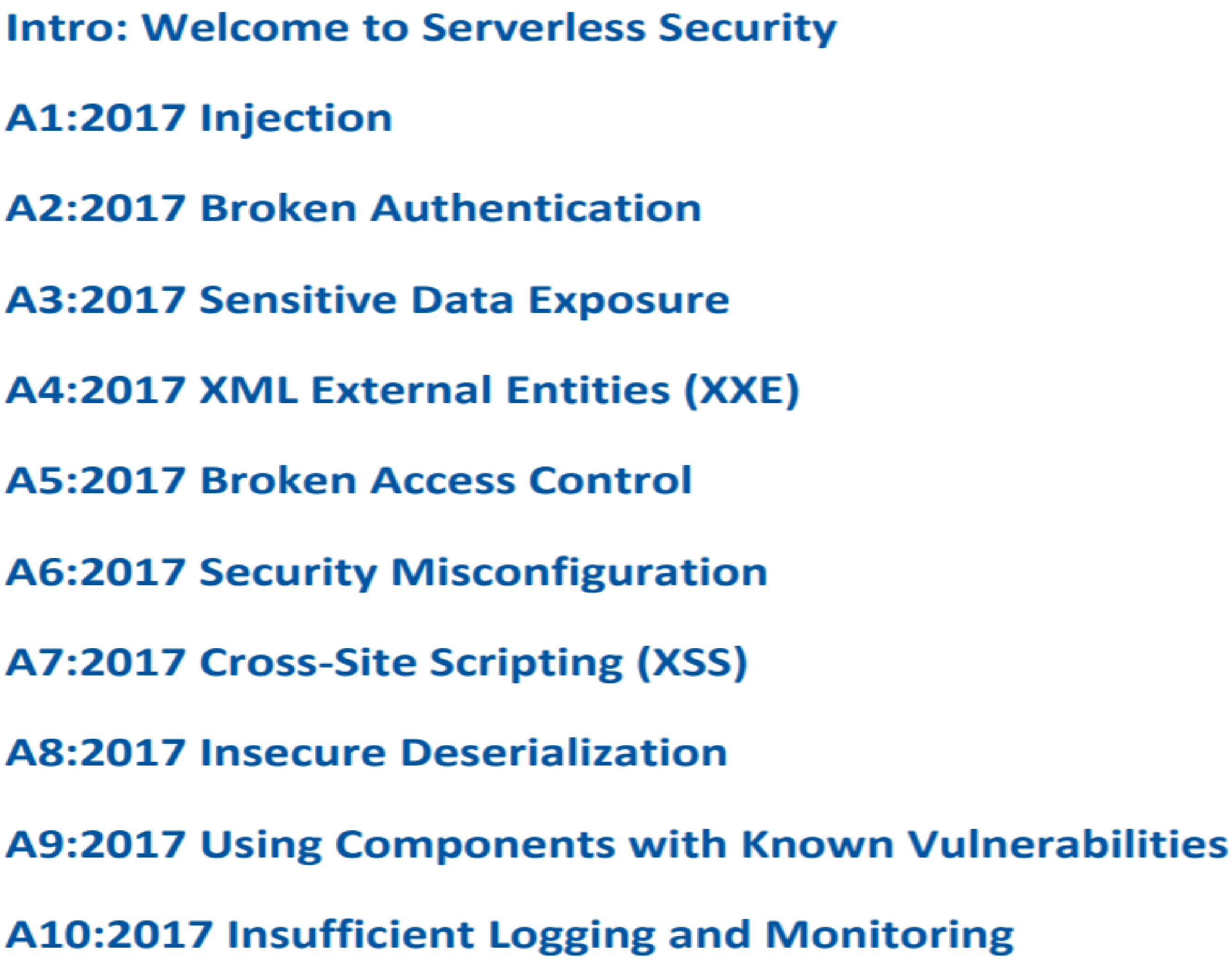
1 **Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 **Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 **Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 **Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

Serverless what?



Intro: Welcome to Serverless Security

A1:2017 Injection

A2:2017 Broken Authentication

A3:2017 Sensitive Data Exposure

A4:2017 XML External Entities (XXE)

A5:2017 Broken Access Control

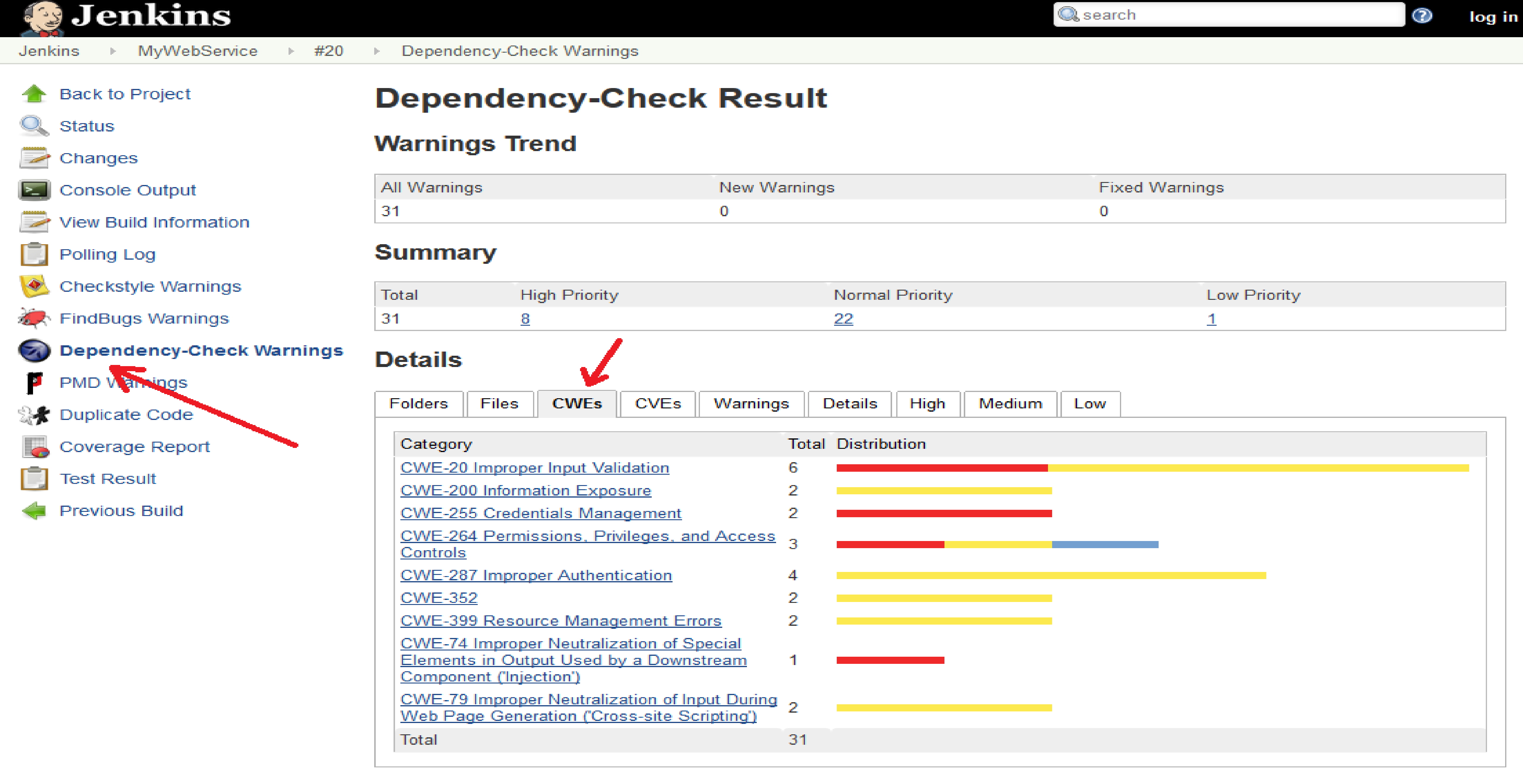
A6:2017 Security Misconfiguration

A7:2017 Cross-Site Scripting (XSS)

A8:2017 Insecure Deserialization

A9:2017 Using Components with Known Vulnerabilities

A10:2017 Insufficient Logging and Monitoring



Dependency-Check Result

Warnings Trend

All Warnings	New Warnings	Fixed Warnings
31	0	0

Summary

Total	High Priority	Normal Priority	Low Priority
31	8	22	1

Details

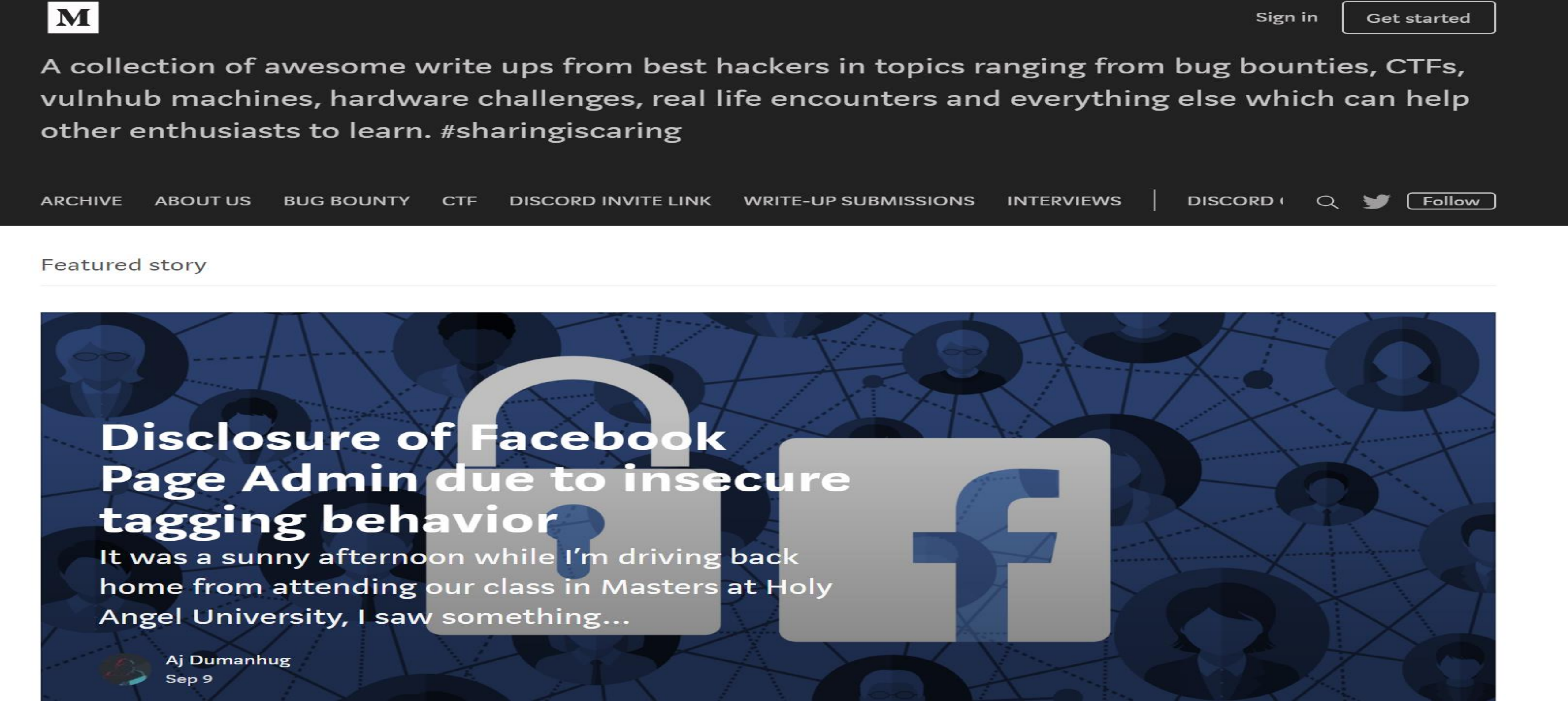
Category	Total	Distribution
CWE-20 Improper Input Validation	6	
CWE-200 Information Exposure	2	
CWE-255 Credentials Management	2	
CWE-264 Permissions, Privileges, and Access Controls	3	
CWE-287 Improper Authentication	4	
CWE-352	2	
CWE-399 Resource Management Errors	2	
CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1	
CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2	
Total	31	

Tools

- Browser – simple and effective, found on most OSes
  - Choose one that you like
  - Armor it with “hacking” add-ons
- Intercepting proxy is a must
  - OWASP ZAP
  - BurpSuite
  - Charles for Mac fans
- Mobile
  - Look into MobSF (Docker ready)
  - MOBEXLER (fresh VM from yesterday)

Some extra ideas!

- **Awake** that part of your **criminal** mind!
- Read through
  - Bug **bounties**
  - Hacking **walkthroughs** (Google IppSec on Youtube)
  - Check new **vulnerabilities** (ExploitDB)
- Get your **hands dirty**
  - Docker to the rescue



A collection of awesome write ups from best hackers in topics ranging from bug bounties, CTFs, vulnhub machines, hardware challenges, real life encounters and everything else which can help other enthusiasts to learn. #sharingiscaring

Featured story

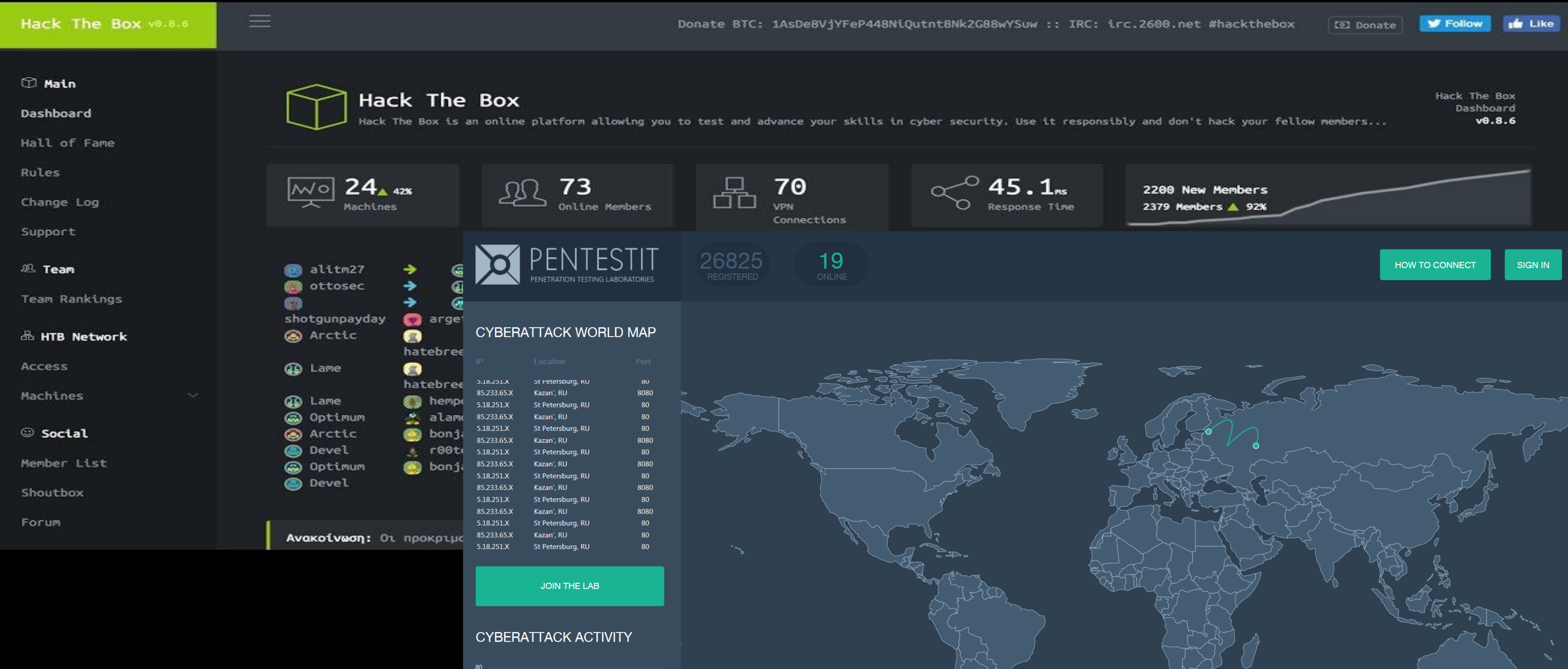
Disclosure of Facebook Page Admin due to insecure tagging behavior

It was a sunny afternoon while I’m driving back home from attending our class in Masters at Holy Angel University, I saw something…

Aj Dumanhug
Sep 9

https://medium.com/bugbountywriteup

Hack The Box platform



Hack The Box

Hack The Box is an online platform allowing you to test and advance your skills in cyber security. Use it responsibly and don't hack your fellow members...

Hack The Box Dashboard v0.8.6

24 42% Machines

73 Online Members

70 VPN Connections

45.1ms Response Time

2200 New Members

2379 Members 92%

alitm27 →
ottosec →
→
shotgunpayday arge
Arctic
hatebree
Lame
hatebree
Lame hemp
Optimum alam
Arctic bonj
Devel r00t
Optimum bonj
Devel

Ανακοίνωση: Οι προκριμ

CYBERATTACK WORLD MAP

IP	Location	Port
5.18.251.X	St Petersburg, RU	80
85.233.65.X	Kazan', RU	8080
5.18.251.X	St Petersburg, RU	80
85.233.65.X	Kazan', RU	80
5.18.251.X	St Petersburg, RU	80
85.233.65.X	Kazan', RU	8080
5.18.251.X	St Petersburg, RU	80
85.233.65.X	Kazan', RU	8080
5.18.251.X	St Petersburg, RU	80
85.233.65.X	Kazan', RU	8080
5.18.251.X	St Petersburg, RU	80
85.233.65.X	Kazan', RU	8080
5.18.251.X	St Petersburg, RU	80
85.233.65.X	Kazan', RU	80
5.18.251.X	St Petersburg, RU	80

CYBERATTACK ACTIVITY

Real skills necessary!

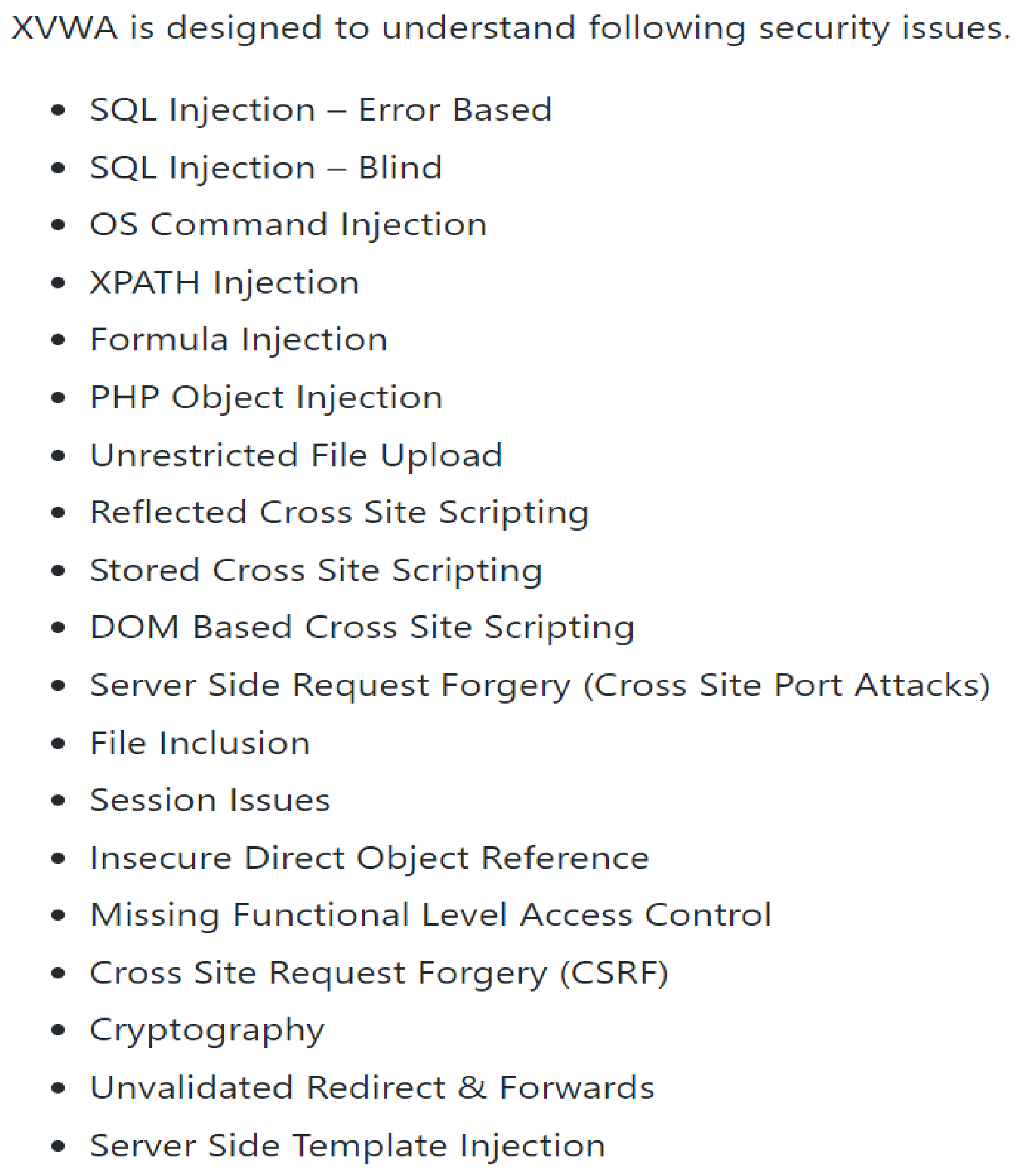
- **Damn vulnerable**
  - Web application
  - Fat application
  - DIVA – mobile application
  - Web services
  - Router
  - ARM router
  - Serverless Application
  - …

Start practicing and if you fail, remember:

Kartojimas yra mokymosi motina

Example - XVWA

- Real cases covered
- Easy start
- Easy setup
- One **Docker** instance for **multiple** hours of **fun**!



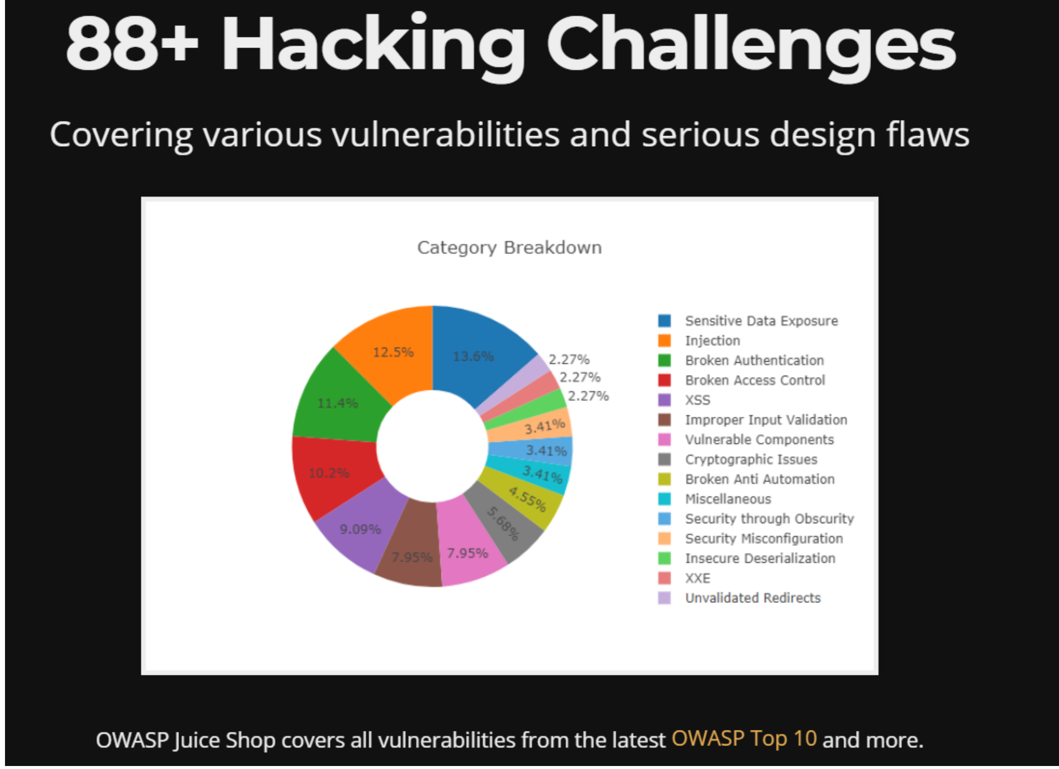
XVWA is designed to understand following security issues.

- SQL Injection – Error Based
- SQL Injection – Blind
- OS Command Injection
- XPATH Injection
- Formula Injection
- PHP Object Injection
- Unrestricted File Upload
- Reflected Cross Site Scripting
- Stored Cross Site Scripting
- DOM Based Cross Site Scripting
- Server Side Request Forgery (Cross Site Port Attacks)
- File Inclusion
- Session Issues
- Insecure Direct Object Reference
- Missing Functional Level Access Control
- Cross Site Request Forgery (CSRF)
- Cryptography
- Unvalidated Redirect & Forwards
- Server Side Template Injection

OWASP Juice Shop

Main Features Screenshots CTF News Sponsors Ecosystem

owasp flagship project | release v9.1.2 | GitHub ★ 2.5k | Follow 2.3k

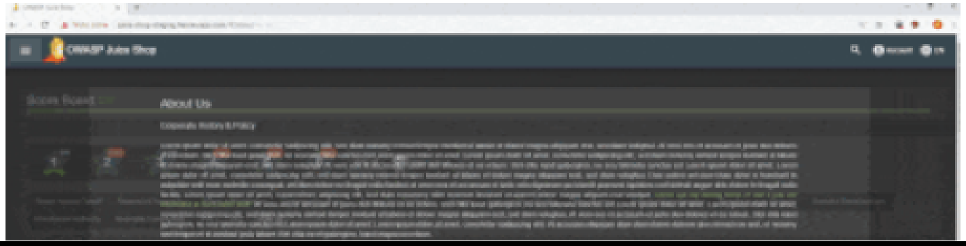


88+ Hacking Challenges

Covering various vulnerabilities and serious design flaws

OWASP Juice Shop covers all vulnerabilities from the latest OWASP Top 10 and more.

OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!



```
docker run --rm -p 3000:3000 bkimminich/juice-shop
```

More resources

- https://ctf101.org/
- https://hack.me/
- http://vulnhub.com/
- https://www.hackthebox.eu/
- https://lab.pentestit.ru/
- https://www.blackmoreops.com/2018/11/06/124-legal-hacking-websites-to-practice-and-learn/

- Google: free hacking training

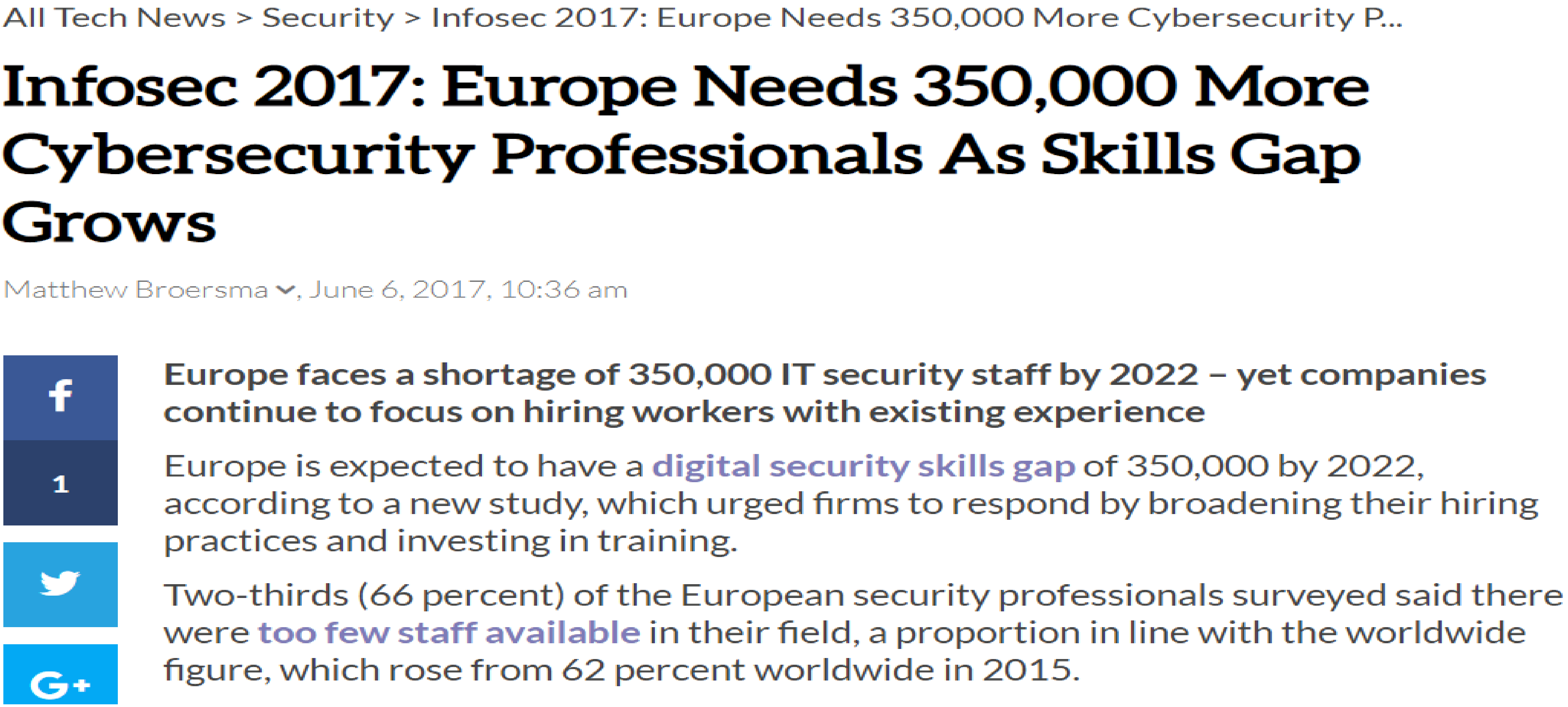
Educate whole ecosystem!

- **Developers** – Software security best practices
- **Testers** – Methods for identifying vulnerabilities ✓
- **Security Professionals** – Secure Software development (SSDLC), Software coding best practices
- **Executives, System owners, etc.** – Understanding the risk and why they should be concerned and invest $$$ to security testing too

KEEP CALM AND REPEAT TEST

FedEx

New opportunities!



All Tech News > Security > Infosec 2017: Europe Needs 350,000 More Cybersecurity P...

Infosec 2017: Europe Needs 350,000 More Cybersecurity Professionals As Skills Gap Grows

Matthew Broersma, June 6, 2017, 10:36 am

Europe faces a shortage of 350,000 IT security staff by 2022 – yet companies continue to focus on hiring workers with existing experience

Europe is expected to have a digital security skills gap of 350,000 by 2022, according to a new study, which urged firms to respond by broadening their hiring practices and investing in training.

Two-thirds (66 percent) of the European security professionals surveyed said there were too few staff available in their field, a proportion in line with the worldwide figure, which rose from 62 percent worldwide in 2015.

Conclusions

- **Security** is (getting) an **issue**!
- You need to **reach out** from your **comfort** zone!
- **Touch**, **explore** and **play** with new things!
- Remember: **sharing** is **caring**!
- Join **meetups** or even **start** some!
- Use the OWASP **tools**! From **pros** to **pros**!
- Develop your **potential**! You can do **more**!

Do it with

PASSION

or not at all

Ačiū!

@MilanGabor