Thinking Like A Hacker

- Application Security Tester (Professional Hacker)
- OWASP Melbourne chapter lead
- Web developer in a previous life
- Climber of rocks

Contact

- meetup.com/Application-Security-OWASP-Melbourne/
- @JulianBerton (Twitter - not very active)
- au.linkedin.com/in/julianberton
- bertonjulian.github.io (also not very active)

Meetup Find a Meetup Group Start a Meetup Group

OWASP Melbourne - Application Security

Home Members Sponsors Photos Pages Discussions More Group tools My profile

OWASP

Melbourne, Australia

Founded Nov 11, 2013

About us...

Invite friends

Members	496
Group reviews	7
Upcoming Meetups	1
Past Meetups	14

Welcome!

+ SCHEDULE A NEW MEETUP

Upcoming Past Calendar

There are no upcoming Meetups

You can schedule one!

Schedule a Meetup

Recent Meetups

What's new

MORE

NEW MEMBER
Moss Ebeling

Todays Agenda

- What hackers are up to?
- What motivates them to hack?
- The Hacker Mindset
- Why the current security model fails?
- Securing applications in a modern world
- How to start improving your security tomorrow?

Training

Hacker Mindset

Time

Tools

Secure SDLC

Cyber Security Trends

What are the hackers up to?


Trustwave
Smart security on demand
2015
TRUSTWAVE GLOBAL
SECURITY REPORT

574

Compromised Businesses

15

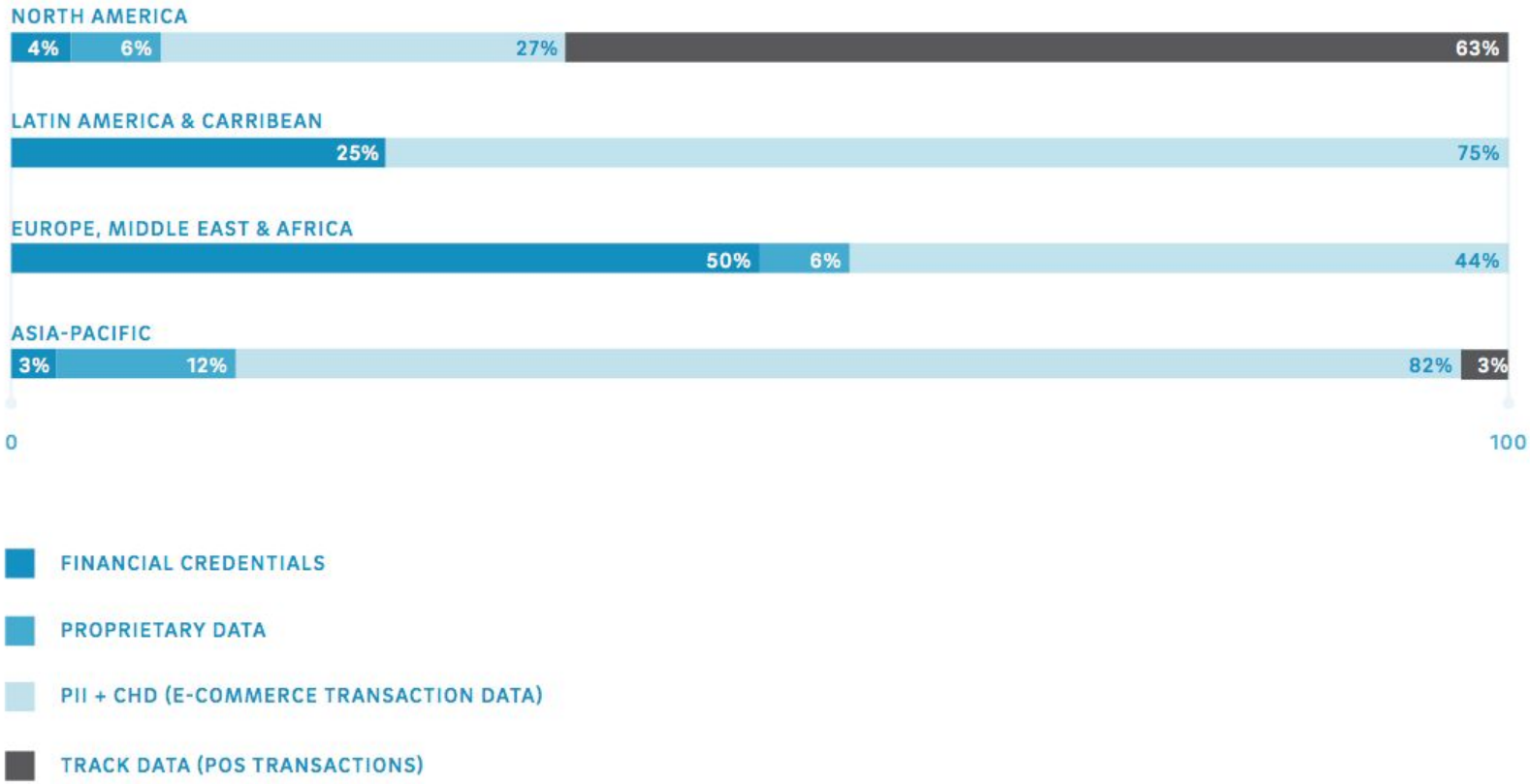
Different Countries

24%

Within Australia in 2014

13% increase in attacks from 2013 - 2014

Data Targeted



No credit card data or passwords stolen… But still made the ABC news

David Jones computer system hacked and customers' private details stolen

PM By Will Ockenden

Updated 2 Oct 2015, 11:52pm

Australian fashion retailer David Jones says its computer system has been hacked and the private details of some of its customers have been stolen by criminals.

The retailer said no credit card information or passwords were stolen, and once it discovered the issue it moved quickly to prevent any further incident.

It came a day after retailer Kmart said it had suffered from a privacy breach in which customer data was stolen.

PHOTO: Department store David Jones has suffered a privacy breach. (David Gray: Reuters)

No credit card data or passwords stolen… But still made the ABC news

Kmart online customers' information hacked in security breach

October 1, 2015

Comments 3 Read later

Marc Moncrief

Data Editor, The Age

View more articles from Marc Moncrief

Follow Marc on Twitter Follow Marc on Google+ Email Marc

Hackers stole data not to sell but to extort!

Aussie Farmers Direct customers' data hacked

November 6, 2015

Be the first to comment

Read later

Helen Velissaris

Tweet Pin it submit

Email article Print

Hack attack: Aussie Farmers Direct home grocery delivery service chief Keith Louie. *Photo: Pat Scala*

Thousands of Aussie Farmers Direct customers have had their private information posted online in a hacking attack, the latest in a string of consumer data breaches in recent months.

The food delivery company was the target of an extortion attempt by international hackers, who demanded a six-figure sum of cash before posting the information of more than 5000 customers on October 30.

Again, not going after data but after the money directly!

Home › Cybercrime

Austrian Firm Fires CEO After $56-million Cyber Scam

By AFP on May 25, 2016

Tweet RSS

Austrian aircraft parts maker FACC said Wednesday that it has fired its chief executive of 17 years after cyber criminals stole some 50 million euros ($55.7 million) in a so-called "fake president" scam.

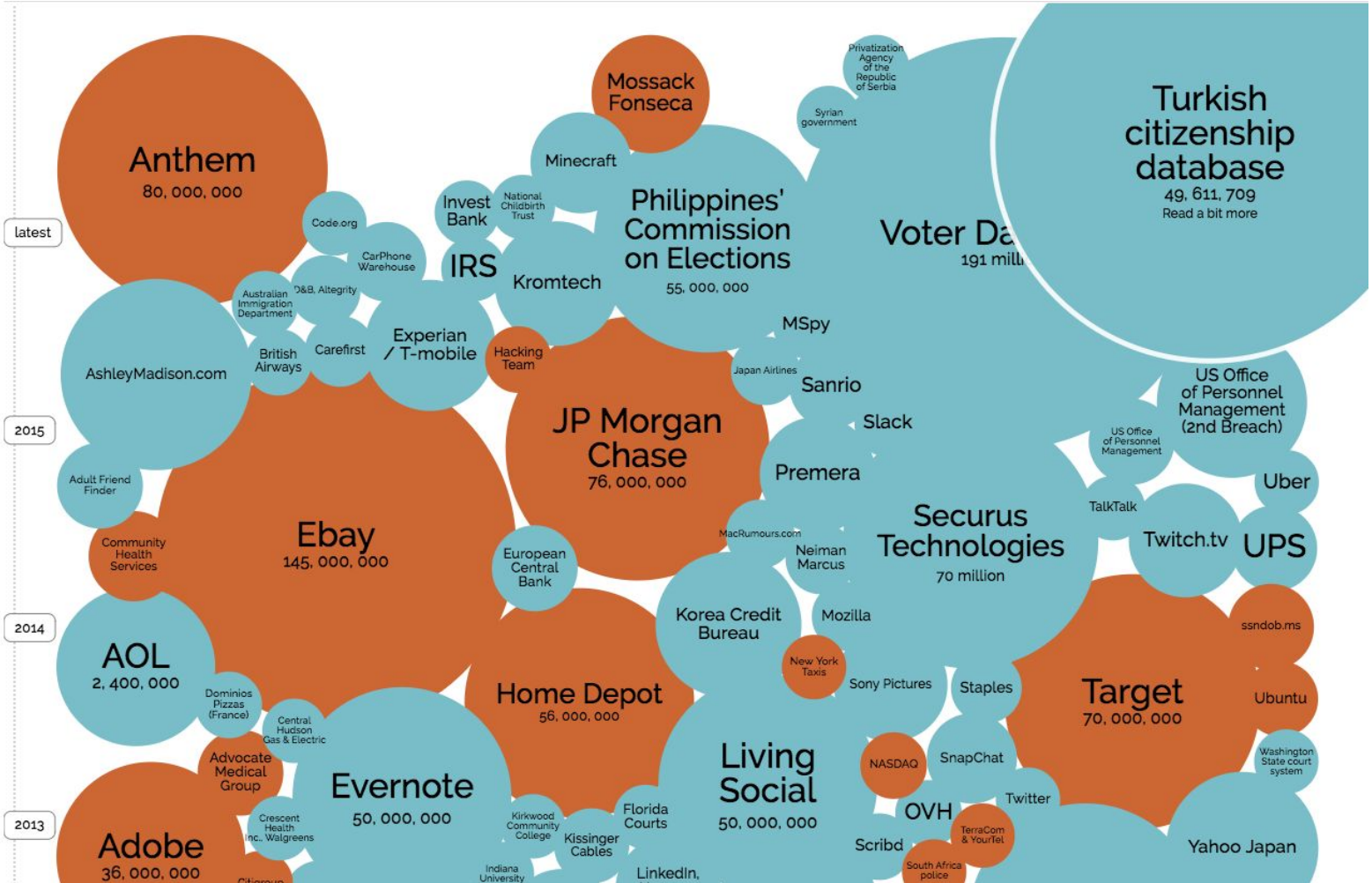
FACC, whose customers include Airbus, Boeing and Rolls-Royce, said that the its supervisory board sacked Walter Stephan with immediate effect after he "severely violated his duties".

Press reports said that in January a FACC employee wired around 50 million euros, equivalent to almost 10 percent of annual revenues, after receiving emailed instructions from someone posing as Stephan.

By the time the firm, which began life making skis before expanding into aeronautics, realized the mistake, it was too late. The money had disappeared in Slovakia and Asia, the Standard daily reported.

The company said Wednesday that the scam, also known as "bogus boss" or "CEO fraud" and increasingly popular with sophisticated organized criminals, cost it 41.9 million euros in its 2015/16 business year.

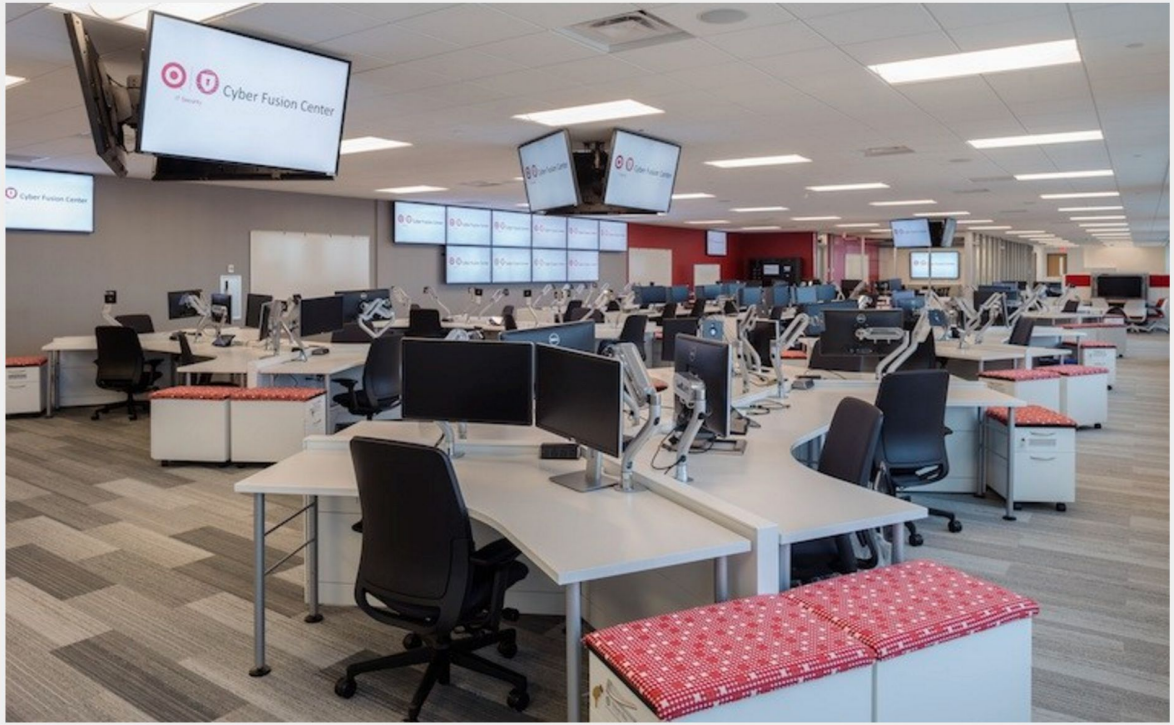
We seem to be losing the battle… But why?



Is Awareness To Blame?

A BULLSEYE VIEW

company careers corporate responsibility news & features



Inside Target's Cyber Fusion Center

JAN 30, 2016 @ 09:02 AM 8,918 VIEWS

Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity

Steve Morgan
CONTRIBUTOR
I write about the business of cybersecurity.
FULL BIO ›
Opinions expressed by Forbes Contributors are their own.

(Photo by Spencer Platt/Getty Images)

Or is it that our approach to security is outdated?

More on that later!

Hacker Motivations

What do hackers want?

Like any business, cybercriminals do what they do to generate revenue. And like businesses, they prefer to make that money as quickly and efficiently as possible.

Hacker Motivations

Money

To make money and lots of it!

Politics/Government

The Syrian Electronic Army (SEA) is a group of computer hackers aimed at supporting the government of Syria.

Religion

Some terrorist and hacktivist groups hack due to certain religious beliefs.

Fun/Fame

More prevalent in the early days of the internet.

World Domination

Well maybe just in the movies...

War/Protection

State sponsored hackers with the aim of gathering intelligence on other countries.

Types of attackers

- For fun
- Board
- Fame
- Money

- To make a statement
- People’s voice
- Revenge

- Money
- Power
- Did i mention money?

- Intelligence
- Tracking
- Terrorism
- War

What type of threats have i missed?

24 AUG 15 Leaked AshleyMadison Emails Suggest Execs Hacked Competitors

Hacked online cheating service **AshleyMadison.com** is portraying itself as a victim of malicious cybercriminals, but leaked emails from the company's CEO suggest that AshleyMadison's top leadership hacked into a competing dating service in 2012.

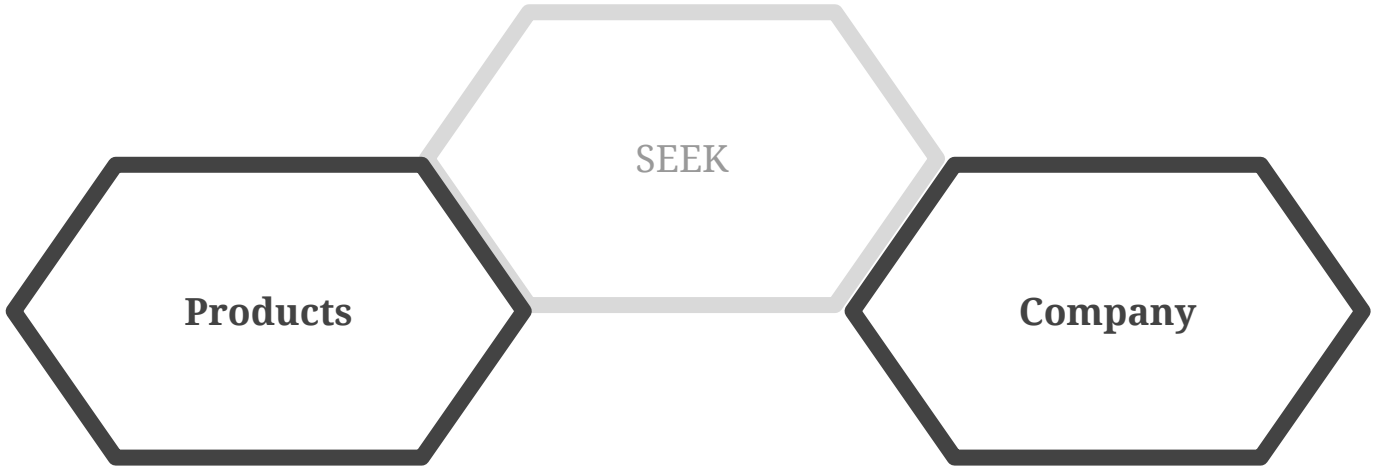
Late last week, the **Impact Team** — the hacking group that has claimed responsibility for leaking personal data on more than 30 million AshleyMadison users — released a 30-gigabyte archive that it said were emails lifted from AshleyMadison **CEO Noel Biderman**.

AshleyMadison CEO Noel Biderman. Source: Twitter.

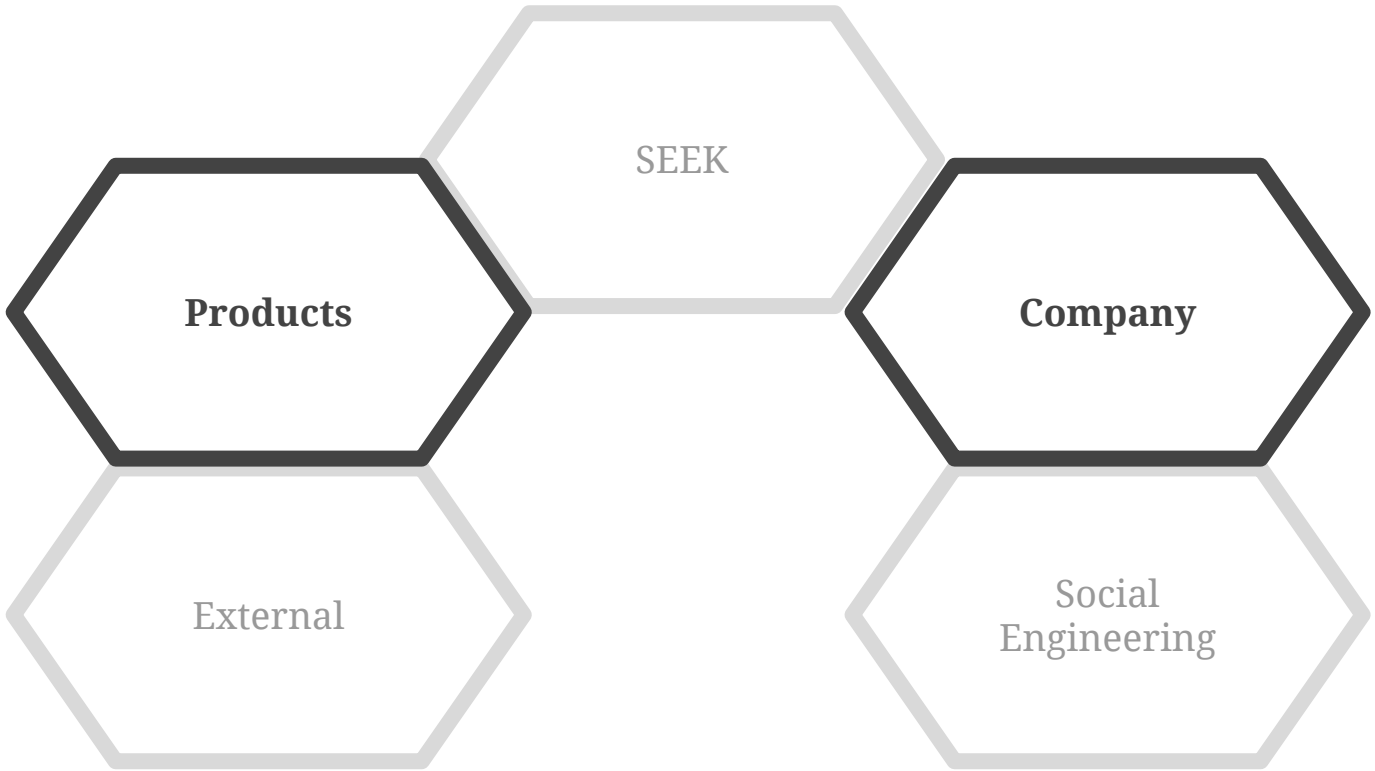
A review of those missives shows that on at least one occasion, a former company executive hacked another dating website, exfiltrating their entire user database. On Nov. 30, 2012, **Raja Bhatia**, the founding chief technology officer of AshleyMadison.com, sent a message to Biderman notifying his boss of a security hole discovered in **nerve.com**, an American online magazine dedicated to sexual topics, relationships and culture.

Edward Snowden and the NSA: A Lesson About Insider Threats

July 4, 2013 – 6:12 AM AEST


SEEK
Products
Company

The Weakest Link



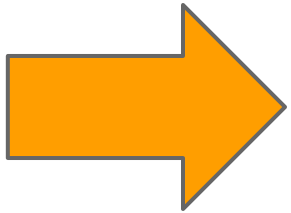
What Most Companies Care About

Brand Damage

Loss of customer or investor trust usually due to bad media coverage.

Loss of Revenue

Suffers a loss of revenue either directly or indirectly.



Strategic/Operational

Achieving goals and objectives are impacted.

Making A Profit Attacking Your Employer?

How would you attack your employer?

Making a Profit

Extortion

Steal data and blackmail company into giving you money or you will dump the data publically (**Brand damage**).

Threaten to take down the website or products for long periods of time, think distributed denial of service(DDOS) or deleting data / servers (**Loss of Revenue**).

Steal data

Steal customer credit cards and either sell on the dark markets or drain accounts (**Brand damage**).

Steal customer personally identifiable information (PII) and sell it on the dark markets for profit (**Brand damage**).

Social Engineering

Stealing customer PII and using this to steal money from them personally. Think, opening a new credit card in there name (**Brand damage**).

CEO Fraud - Tricking employees into transferring money to an attacker's account (**Loss of Revenue**)

What happens to the breached data?

Leaked in

Stories About Data Leaks and Related Stuff

Shellcode

Posted by PasteMon on October 18th, 2015

86 voted **vote**

Detected 2 occurrence(s) of '\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}\\x[0-9a-f]{2}':

```
from pwn import *

gets = 0x08048350
pop3ret = 0x804855a
leak = 0x080498dc
size_t = pack(0x00000050)
return_address = pack(0x8049914)
dest = return_address
```

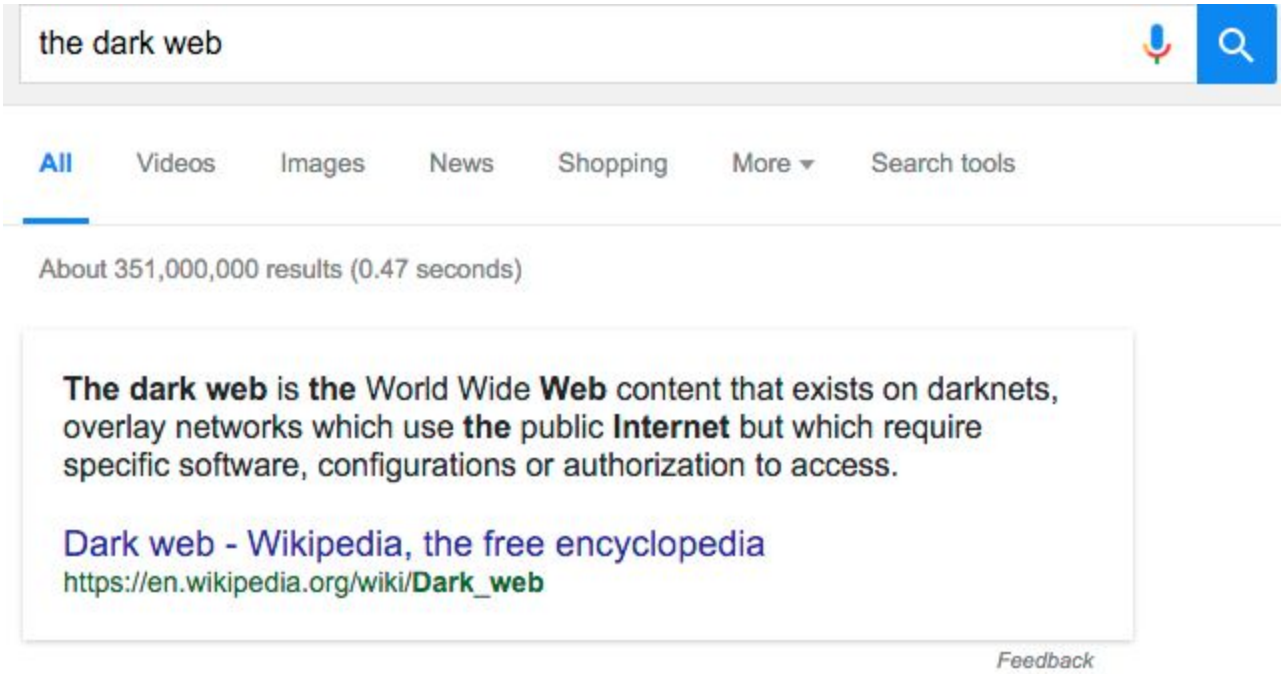

TOP-5 LEAKS

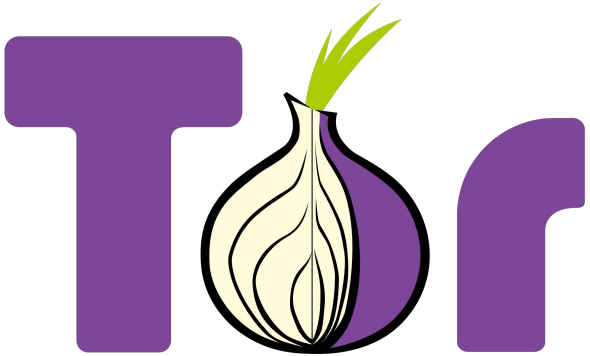
Potential leak of data: VISA Credit Card (1157)

Potential leak of data: VISA Credit Card (497)

Potential leak of data: MasterCard Credit Card (428)

MasterCard Credit Card (423)


the dark web
All
Videos
Images
News
Shopping
More
Search tools
About 351,000,000 results (0.47 seconds)
The dark web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but which require specific software, configurations or authorization to access.
Dark web - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Dark_web
Feedback


Tor

+

=


?

Well maybe not so anonymous...

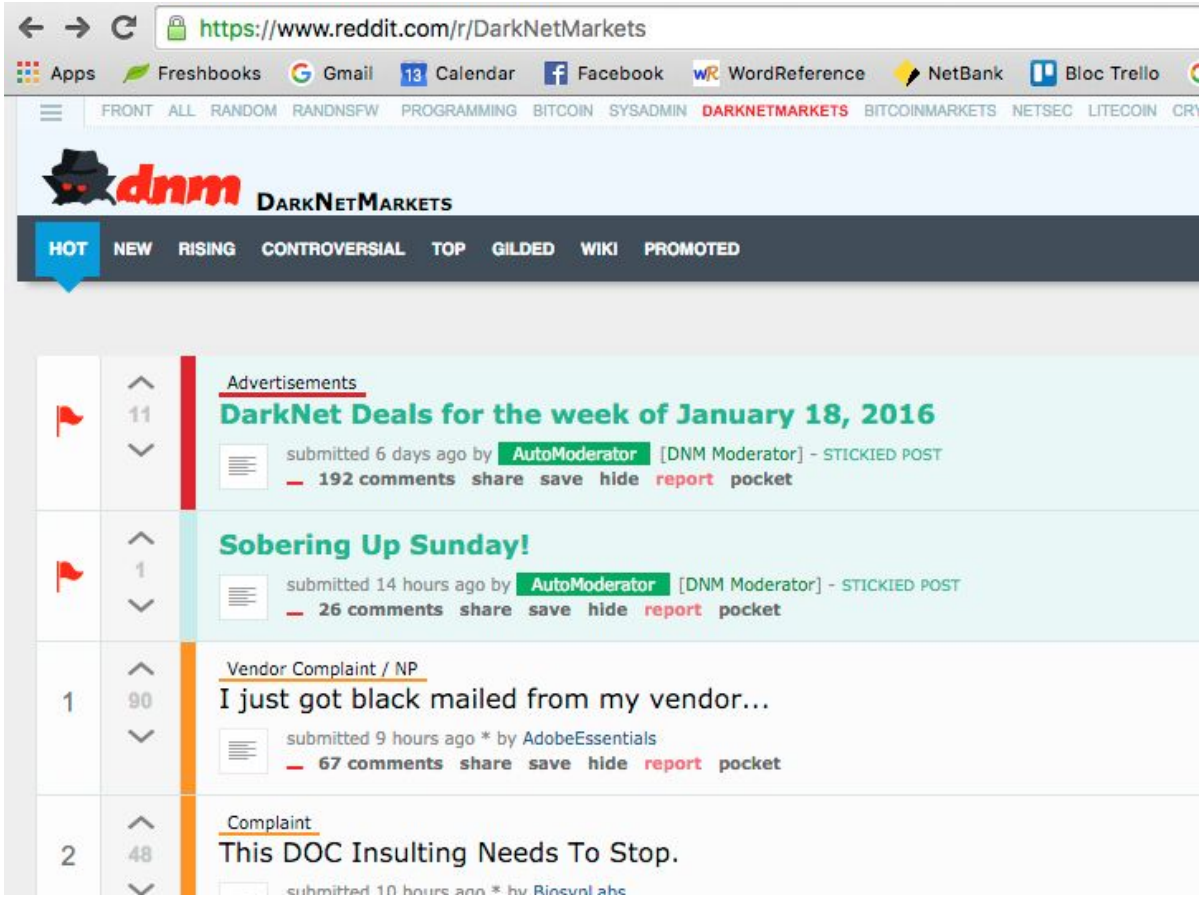
Forbes / Security

Top 20 Stocks for 2016

OCT 2, 2013 @ 12:35 PM 221,734 VIEWS

End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market

Sold on the Dark Web



The Superlist

This is a list of all currently known, operating markets and tumblers. If you feel a market is missing or should be removed, please message us here explaining why. All markets listed should not be taken as endorsements or confirmation by the moderators that a market is trusted. Always confirm links before you use them.

Requirements for this list

1. Market has to been up for at least a week after announcing their self on /r/DarkNetMarkets
2. Market has to have at least 20 listings from active vendors
3. Service must have at least 50% uptime over the span of a week, under moderator discretion.
4. Users must be able to withdraw their coins.

Referral links can be found in the respective market subreddit

Superlist - Removed Listings

Markets

A.C.A.S MARKET

Address: http://lpwiqq7bjenhkucm.onion
Multisig: Yes
Subreddit: /r/ACASMarket
Forums: http://lpwiqq7bjenhkucm.onion/forum/
Reddit accounts: /u/ACASadmin
PGP key: ACAS Market

The Superlist
- Markets
  - A.C.A.S Market
  - Acropolis
  - AlphaBay
  - Crypto Market
  - DarkNet Heroes League
  - Dream Market
  - East India Company Warning: Was down for 7 days - Unknown status - Use caution
  - German-Plaza
  - Hansa Market
  - Nucleus Marketplace
  - Oasis
  - Outlaw Marketplace
  - Python Market
  - The Real Deal Market
  - Tochka
  - Silkkitie / Valhalla
- Forum Based Markets
  - French Marketplace
  - The Majestic Garden
- Popular Coin Tumblers
  - Bitcoin Blender / BitBlender
  - Bitcoin Fog / BitcoinFog / BTCFog

Sold on the Dark Web

Home • Sales • Messages • Listings • Balance • Orders • Feedback • Forums • Cont

336.05 ▼AUD 512.69 ▼GBP 239.69

Cards / *AU*SUPREME FULLZ*(Australia) FULLZ*(DOB/MMN/BILL)

*AU*SUPREME FULLZ*(Australia) FULLZ*(DOB/MMN/BILL)

Ultimate Freshness guarantee at all times! This listing is for x1 AU (Australia) Fullz. *If you need some custom request, kindly dont forget to choose from the Drop Down list on the Add On's, so it will be able to get those request guaranteed. If none of the Add-On's are taken, the order will be Issued by Randoms Fullz.* **TIP: Also have in mind, when ordering, please write in the...

Sold by Kingsup - *224* sold since *Mar 19, 2015* **Level 7**

	Features		Features
Product class	Digital goods	**Origin country**	Australia
Quantity left	12 items	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

No additional extras/options - 1 days - USD +0.00 / item

Purchase price: USD 25.00

Qty: 1 Buy Now Queue

0.0693 BTC

Sold on the Dark Web

Product Description

Ultimate Freshness guarantee at all times!

This listing is for x1 AU (Australia) Fullz.

If you need some custom request, kindly dont forget to choose from the Drop Down list on the Add On's, so it will be able to get those request guaranteed. If none of the Add-On's are taken, the order will be Issued by Randoms Fullz.

TIP: Also have in mind, when ordering, please write in the buyer notes what to do in case your request is not available at that very moment, like if you have another choices for complete your order or if you rather me to decline in that case; so inform me everytime how to proceed and it will shorter the shipping time.

**********Considered the Best Fullz Ever **********
You can rely on the Best Quality. State of the Art techniques on accessing them guarantees the authenticity of the product itself, and combined with a Friendly Customer service every time.

The fullz format

| Known e-mail(s):
| Known password(s):
| Full Name:
| DOB: Age:
| Address:
| Billing Telephone:
| Mothers Maiden Name:
+ Billing Information
| Card BIN:
| Card Bank: | Card Type:
| Cardholders Name:
| Card Number:
| Valid
| Expiration date:
| CVV:
+ Social Media Information
| Details:
| IP Address:
| Location:
| UserAgent:

“With a friendly customer service every time”

“All of the information is accurate and confirmed. Clients are from an insurance company database with GOOD to EXCELLENT credit rating!”

I, myself was able to apply for credit cards valued from $2,000 – $10,000 with my fullz. Info can be used to apply for loans, credit cards, lines of credit, bank withdrawal, assume identity, account takeover.”

Kingsup | User Profile

Kingsup(7842) **Level 7**

Positive feedback (last 12 months): 96%
[How is the feedback score calculated?]

Member since: March 19, 2015
Contracts: 0 in progress, 0 complete

View Store
Send Message
Favorite
Blacklist

Seller Feedback Ratings (last 12 months) ?

	1 month	6 months	12 months
Positive	185	1500	364
Neutral	3	35	8
Negative	12	59	11

Buyer Statistics (since join date) ?

	Since join
Total disputes / orders	0 / 1
Total spendings	---
Feedback left	0 (100.0% positive)
Last online	Nov 9, 2015

	Stealth	Quality	Value for price
Detailed seller ratings:	★★★★★	★★★★★	★★★★★

Sold on the Dark Web

Search or enter address

Search

Welcome back, 0 0 0 BTC 0.0000 Home My RealDeal Support Logout

TheRealDeal

All I want to order ... Go

Home / Information and Fraud / Databases / LinkedIn 167M

LinkedIn 167M

By peace_of_mind (100.0%) Level 1 (14)

0 2.0000 / BTC 2.0000

In stock.

Qty: 0

Buy It Now

Postage Option

Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide

Favorite Question

Details | Feedback | Return Policy

	Feedback	From	Date
+	Great transaction. As advertised.	G***e	May 26, 2016 00:57
+	Got what I paid for. Good vendor. Follows up with your questions and delivers promptly.	B***r	May 24, 2016 00:09
+	As described	y***Z	May 20, 2016 04:43

The Hacker Mindset

Stepping into the mind of a criminal

“The best possible way to focus on security, as a developer, is to begin to think like a hacker. Examine the very methods hackers use to break into and attack Web sites, and use those same practices to prevent attacks.”

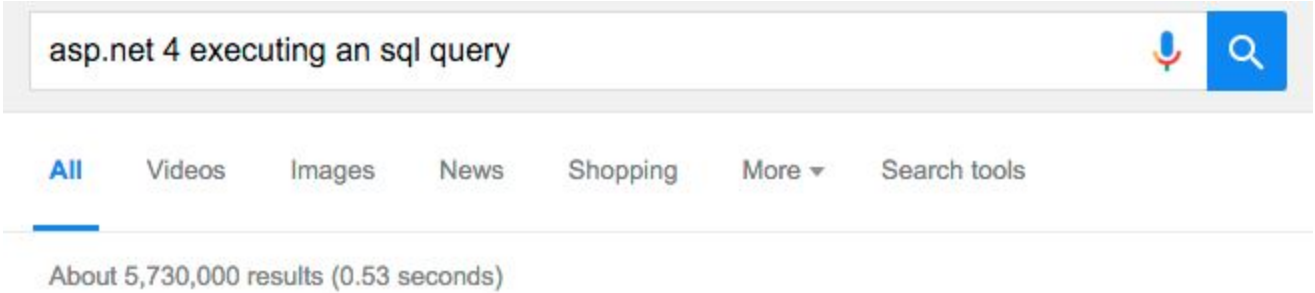
Developer’s Guide to Web Application Security, Michael Cross, 2007

Why do security bugs exist in software?

- The “just trying to get it released” attitude. Not given time to look at the app from a security POV.
- Most developers have never been taught about security.
- “I assume my framework is protecting me”. Modern frameworks are doing more so the developer assumes it's got security covered.
- Never stepping back and thinking about the app from a hackers POV.

Let's take an example:

I’m building a .NET web app and I need to make a database query to fetch some user data… To Google you say!



https://msdn.microsoft.com/en-us/library/fksx3b4f.aspx
https://stackoverflow.com/questions/11821907/executing-query-in-c-sharp-asp-net

How to: Create and Execute an SQL Statement that Returns Rows

Other Versions

To execute an SQL statement that returns rows, you can run a TableAdapter query that is configured to run an SQL statement (for example, `CustomersTableAdapter.Fill(CustomersDataTable)`).

If your application does not use TableAdapters, call the `ExecuteReader` method on a command object, setting its `CommandType` property to Text. ("Command object" refers to the specific command for the .NET Framework Data Provider your application is using. For example, if your application is using the .NET Framework Data Provider for SQL Server, the command object would be SqlCommand.)

The following examples show how to execute SQL statements that return rows from a database using either TableAdapters or command objects. For more information on querying with TableAdapters and commands, see Filling Datasets with Data.

Executing SQL Statements that Return Rows Using a TableAdapter

This example shows how to create a TableAdapter query using the TableAdapter Query Configuration Wizard, and then it provides information on how to declare an instance of the TableAdapter and execute the query.

Note

Your computer might show different names or locations for some of the Visual Studio user interface elements in the following instructions. The Visual Studio edition that you have and the settings that you use determine these elements. For more information, see Customizing Development Settings in Visual Studio.

Just show me an example!

To execute an SQL statement returning rows programmatically using a command object

- Add the following code to a method that you want to execute the code from. You return rows by calling the ExecuteReader method of the command (for example, ExecuteReader). The data is returned in a SqlDataReader. For more information on accessing the data in a SqlDataReader, see Retrieving Data Using a DataReader.

C# | VB

```
SqlConnection sqlConnection1 = new SqlConnection("Your Connection String");
SqlCommand cmd = new SqlCommand();
SqlDataReader reader;

cmd.CommandText = "SELECT * FROM Customers";
cmd.CommandType = CommandType.Text;
cmd.Connection = sqlConnection1;

sqlConnection1.Open();

reader = cmd.ExecuteReader();
// Data is accessible through the DataReader object here.

sqlConnection1.Close();
```

```
4  SqlConnection sqlConnection1 = new SqlConnection("Your Connection String");
5  SqlCommand cmd = new SqlCommand();
6  SqlDataReader reader;
7
8  cmd.CommandText = "SELECT * FROM Customers where username = " + username_from_client;
9  cmd.CommandType = CommandType.Text;
10 cmd.Connection = sqlConnection1;
11
12 sqlConnection1.Open();
13
14 reader = cmd.ExecuteReader();
15 // Data is accessible through the DataReader object here.
16
17 sqlConnection1.Close();
```

WOOT! I'm done! That was easy...

Executing SQL Statements that Return Rows Using a Command Object

The following example shows how to create a command and execute an SQL statement that returns rows. For information on setting and getting parameter values for a command, see How to: Set and Get Parameters for Command Objects.

Setting Parameter Values

Before you execute a command, you must set a value for every parameter in the command.

To set a parameter value

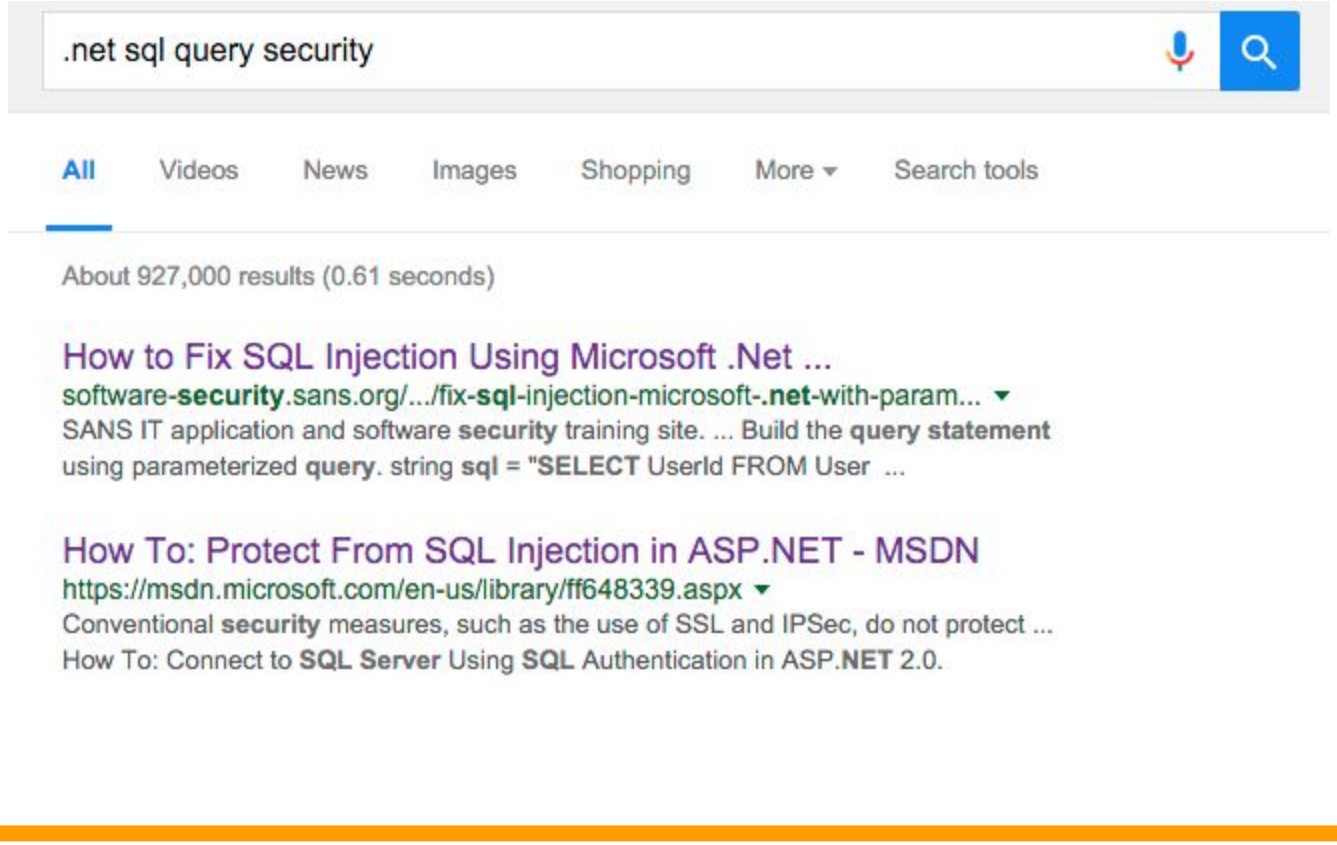
- For each parameter in the command's parameters collection, set its `Value` property.

  The following example shows how to set parameters before executing a command that references a stored procedure. The sample assumes that you have already configured the parameters collection with three parameters named `au_id`, `au_lname`, and `au_fname`. The individual parameters are set by name to make it clear which parameter is being set.

C# | VB

```
oleDbCommand1.CommandText = "UpdateAuthor";
oleDbCommand1.CommandType = System.Data.CommandType.StoredProcedure;

oleDbCommand1.Parameters["au_id"].Value = "172-32-1176";
oleDbCommand1.Parameters["au_lname"].Value = "White";
oleDbCommand1.Parameters["au_fname"].Value = "Johnson";
```


.net sql query security
All
Videos
News
Images
Shopping
More
Search tools
About 927,000 results (0.61 seconds)
How to Fix SQL Injection Using Microsoft .Net ...
software-security.sans.org/.../fix-sql-injection-microsoft-.net-with-param...
SANS IT application and software security training site. ... Build the query statement using parameterized query. string sql = "SELECT UserId FROM User ...
How To: Protect From SQL Injection in ASP.NET - MSDN
https://msdn.microsoft.com/en-us/library/ff648339.aspx
Conventional security measures, such as the use of SSL and IPSec, do not protect ...
How To: Connect to SQL Server Using SQL Authentication in ASP.NET 2.0.

How to Fix SQL Injection Using Microsoft .Net Parameterized Queries

Paramaterized Query

The purpose of a parameterized query is to allow the data source to be able to distinguish executable statements from untrusted data.

Secure Usage

```
1  // Build the query statement using parameterized query.
2  string sql = "SELECT UserId FROM User WHERE " +
3                "UserName = @UserName AND Password = @Password";
4
5  using (SqlCommand cmd = new SqlCommand(sql))
6
7  {
8      // Create the parameter objects as specific as possible.
9      cmd.Parameters.Add("@UserName", System.Data.SqlDbType.NVarChar, 50);
10     cmd.Parameters.Add("@Password", System.Data.SqlDbType.NVarChar, 25);
11
12     // Add the parameter values.  Validation should have already happened.
13     cmd.Parameters["@UserName"].Value = UserName;
14     cmd.Parameters["@Password"].Value = Password;
15     cmd.Connection = connnection;
```

https://software-security.sans.org/developer-how-to/fix-sql-injection-microsoft-.net-with-parameterized-queries

The Solution?

Can we make software 100% secure?

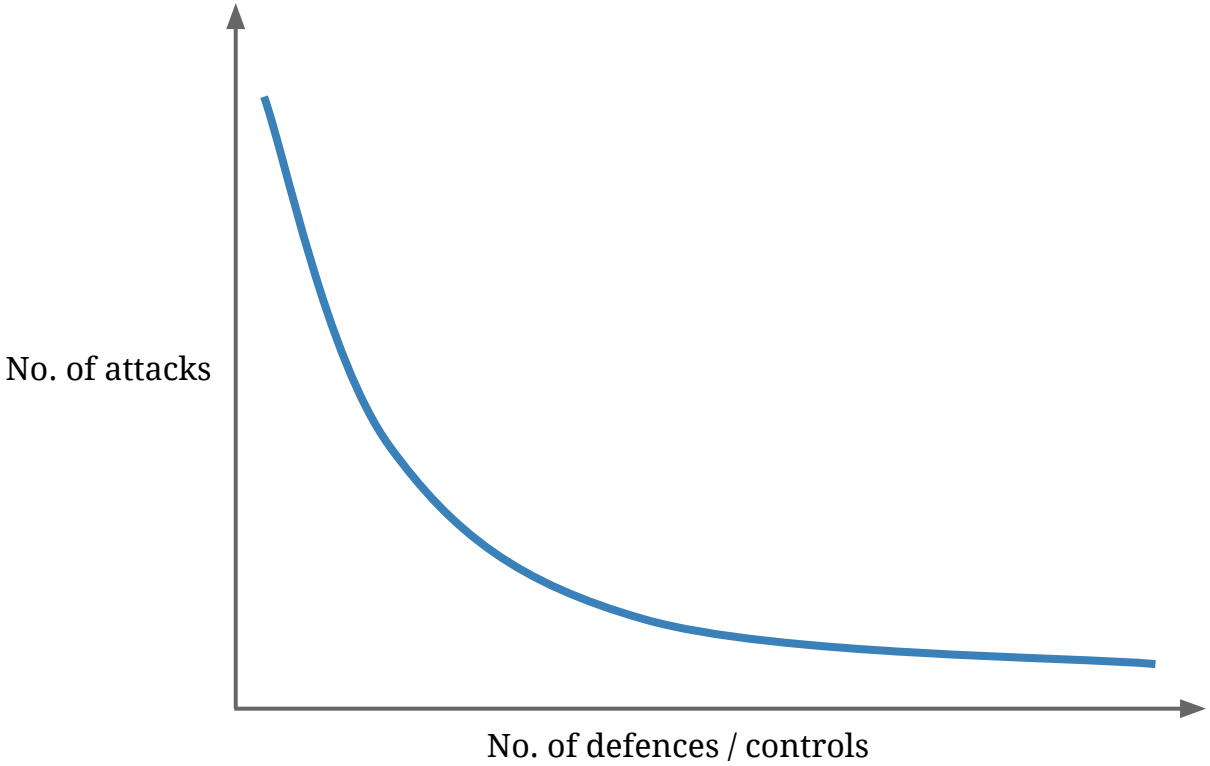
Yes there is a way!

Defence In Depth

- Safety Features List
  - Auto Emergency Braking (AEB)
  - Forward Collision Warning
  - Higher Speed AEB
  - Low Speed Auto Emergency Braking
  - Pedestrian Auto Emergency Braking
  - Curtain Airbags
  - Electronic Stability Control
  - Active Braking Systems
  - Intelligent Speed Assist ISA
  - Active Cruise Control
  - Thorax Airbags With Head

- Protection
  - Traction Control
  - Brake Assist System
  - Adjustable Steering Column
  - Blindspot Warning System
  - Daytime Running Lights
  - Drivers Knee Airbag
  - Fog Lamps
  - Front Airbags Driver
  - Front Airbags Passenger
  - Head Restraints All
  - Headup Display
  - Lanekeeping Assist
  - Passenger Knee Airbag
  - Precrash Safety System
  - Reversing Camera
  - Seatbelt Pretensioner Driver
  - Seatbelt Pretensioner Passenger
  - Seatbelt Rear 3 Point
  - Tyre Pressure Monitor

Defence In Depth



Stepping back in time (Hopefully)...

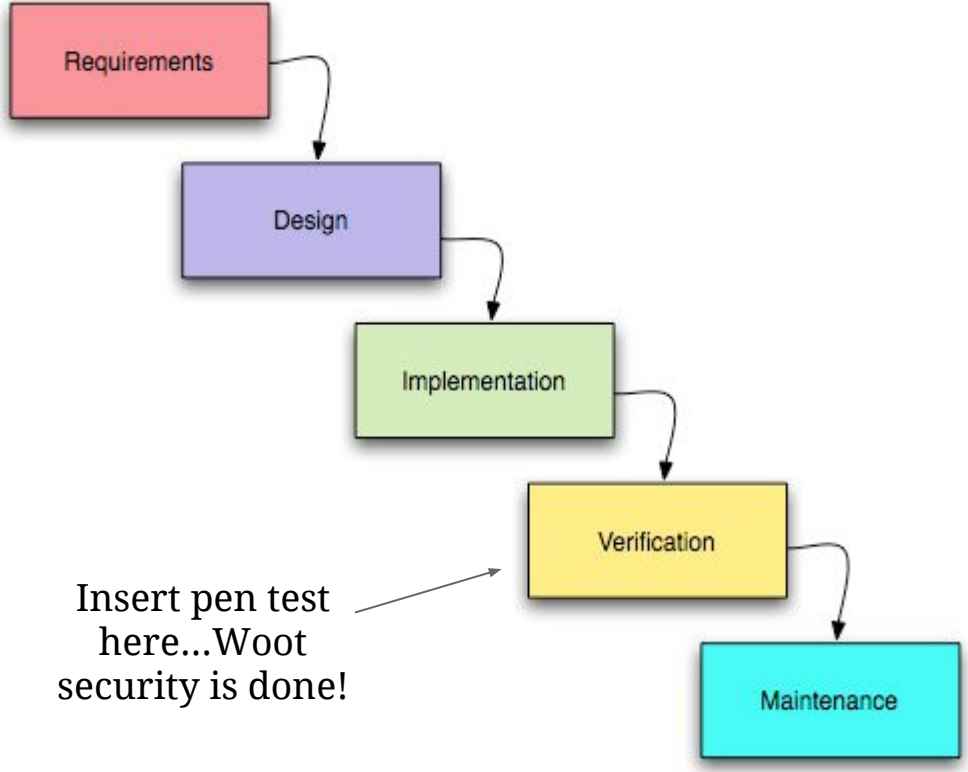
Whats wrong with the current app sec model?

The current application security model was designed when:

- There were 3-6 month deploy to prod cycles (think waterfall).
- One software stack per company (for example, only allowed to use C#, .NET, SQL Server and IIS).
- Ratio of security people to devs… Well that's always been skewed :)

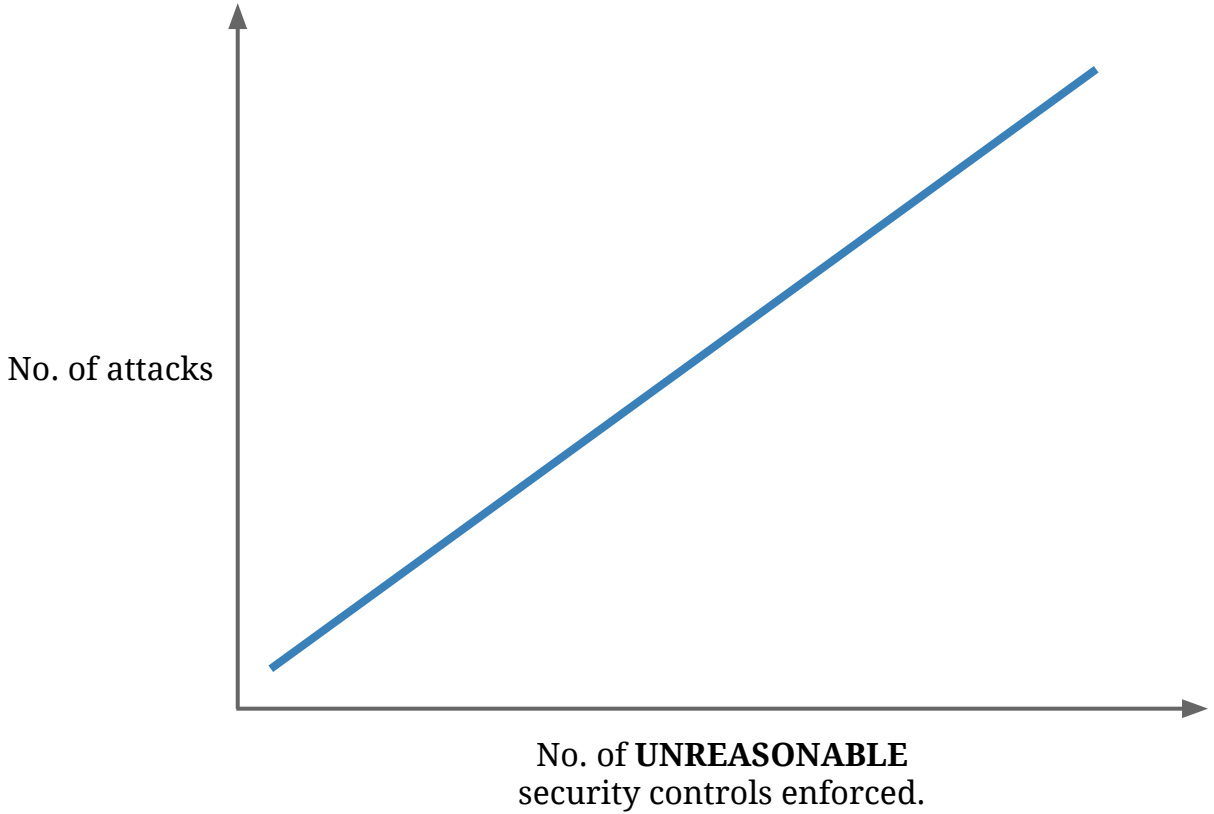
So how was app sec approached?

The Current Security Model



Insert pen test here…Woot security is done!

Security Need To Compromise



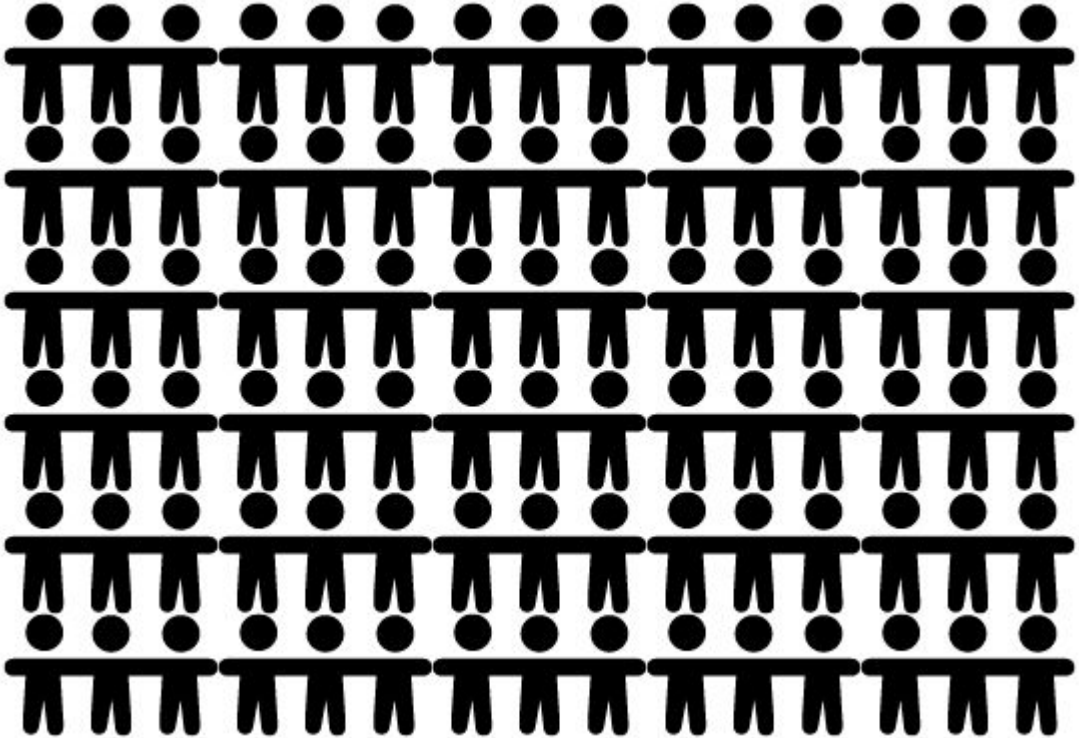
Why would this be the case?

Why The Security Model Has To Change...

- Small teams (Max 5-10)
- Agile development methodologies (move faster)
- Teams can choose what stack to use...But they have to support it (devops).
- CD / CI , deploy to prod daily (move even faster)

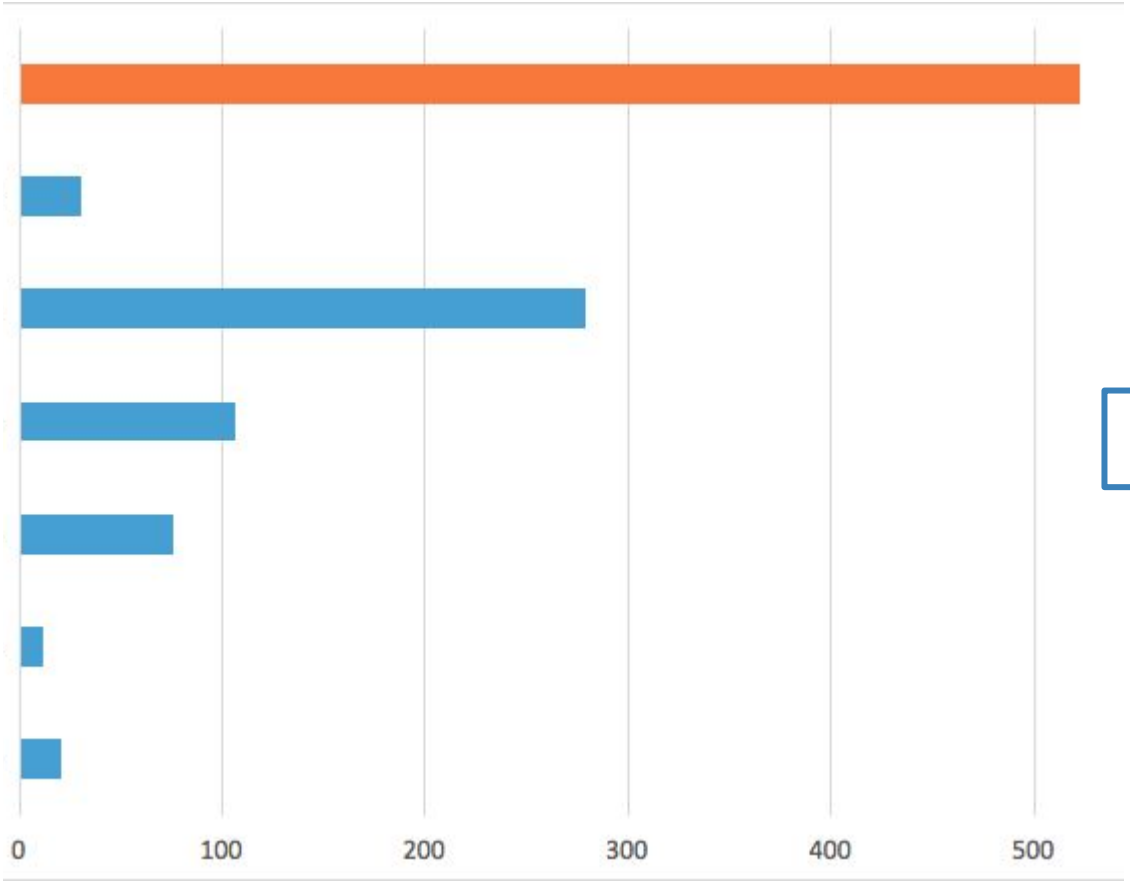
Security Talent Shortage

~140 Tech Team



1-2 App Sec Team

Deploys To Prod Per Month



~30 times a day!

THE RADAR

TECHNIQUES

ADOPT
1 Capturing client-side JavaScript errors
2 Continuous delivery for mobile devices
3 Mobile testing on mobile networks
4 Segregated DOM plus node for JS Testing
5 Windows infrastructure automation

TRIAL
6 Capture domain events explicitly
7 Client and server rendering with same code
8 HTML5 storage instead of cookies
9 Instrument all the things
10 Masterless Chef/Puppet
11 Micro-services
12 Perimeterless enterprise
13 Provisioning testing
14 Structured Logging

ASSESS
15 Bridging physical and digital worlds with simple hardware
16 Collaborative analytics and data science
17 Datensparsamkeit
18 Development environments in the cloud
19 Focus on mean time to recovery
20 Machine image as a build artifact
21 Tangible interaction

HOLD
22 Cloud lift and shift
23 Ignoring OWASP Top 10
24 Siloed metrics
25 Velocity as productivity

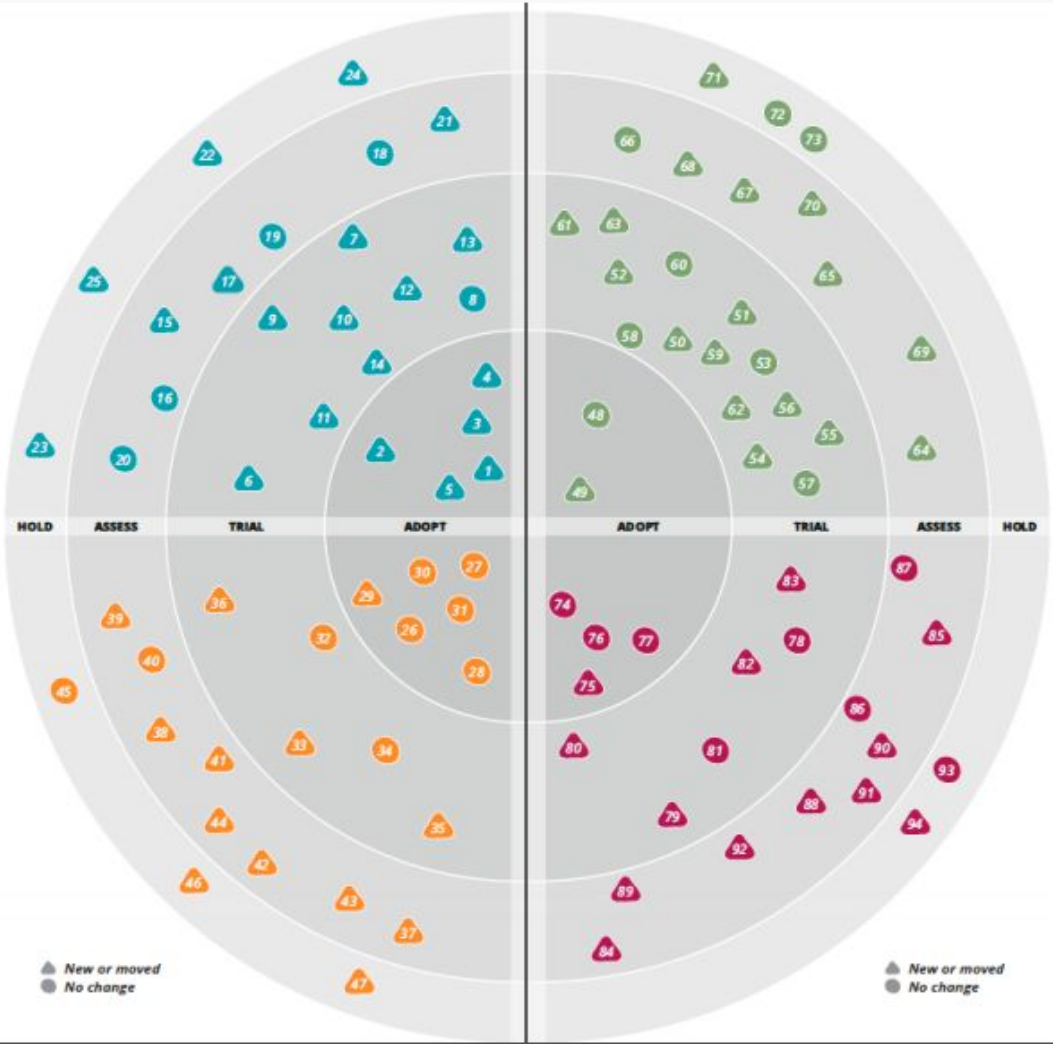
PLATFORMS

ADOPT
26 Elastic Search
27 MongoDB
28 Neo4J
29 Node.js
30 Redis
31 SMS and USSD as a UI

TRIAL
32 Hadoop 2.0
33 Hadoop as a service
34 OpenStack
35 PostgreSQL for NoSQL
36 Vumi

ASSESS
37 Akka
38 Backend as a service
39 Low-cost robotics
40 PhoneGap/Apache Cordova
41 Private Clouds
42 SPDY
43 Storm
44 Web Components standard

HOLD
45 Big enterprise solutions
46 CMS as a platform
47 Enterprise Data Warehouse



THE RADAR

TOOLS

ADOPT
48 D3
49 Dependency management for JavaScript

TRIAL
50 Ansible
51 Calabash
52 Chaos Monkey
53 Gatling
54 Grunt.js
55 Hystrix
56 Icon fonts
57 Librarian-puppet and Librarian-Chef
58 Logstash & Graylog2
59 Moco
60 PhantomJS
61 Prototype On Paper
62 SnapCI
63 Snowplow Analytics & Piwik

ASSESS
64 Cloud-Init
65 Docker
66 Octopus
67 Sensu
68 Travis for OSX/iOS
69 Visual regression testing tools
70 Xamarin

HOLD
71 Ant
72 Heavyweight test tools
73 TFS

LANGUAGES & FRAMEWORKS

ADOPT
74 Clojure
75 Dropwizard
76 Scala, the good parts
77 Sinatra

TRIAL
78 CoffeeScript
79 Go language
80 Hive
81 Play Framework 2
82 Reactive Extensions across languages
83 Web API

ASSESS
84 Elixir
85 Julia
86 Nancy
87 OWIN
88 Pester
89 Pointer Events
90 Python 3
91 TypeScript
92 Yeoman

HOLD
93 Handwritten CSS
94 JSF

Tools/Platforms/Frameworks

~150 different tools, languages, platforms, frameworks and techniques

6501

My friend's office has been in a post-it war with the neighbors...and yesterday, the neighbors won. (i.imgur.com)

submitted 1 day ago by FUNKYDISCO x2

2712 comments share save hide give gold report pocket

Secure Development Lifecycle.

How can we add security into an SDLC?

It all starts with….

Training	Inception	Development	Deployment	Monitoring
Train the tech team about web application security concepts	Review the system design to make sure there are no inherent security weaknesses	Security specific tests are added into the test suite	Automated security scanning tools implemented into the build pipeline	Targeted security testing for complex or high value components
Security awareness throughout the whole product department I.e Brownbags, etc.	Develop realistic attack scenarios and identify high risk areas of projects.	Adoption of security standards, security architecture guidance and security release plans	Deploy static source code security analysis tools into deployment pipeline	Implement ongoing bug bounty program

“Adding security at each phase of a project's lifecycle will ensure the ongoing security of our products.”

OWASP AppSec Pipeline

Main | Pipeline Tools | Pipeline Design Patterns | Presentations | Metrics | FAQs | Acknowledgements | Getting Involved

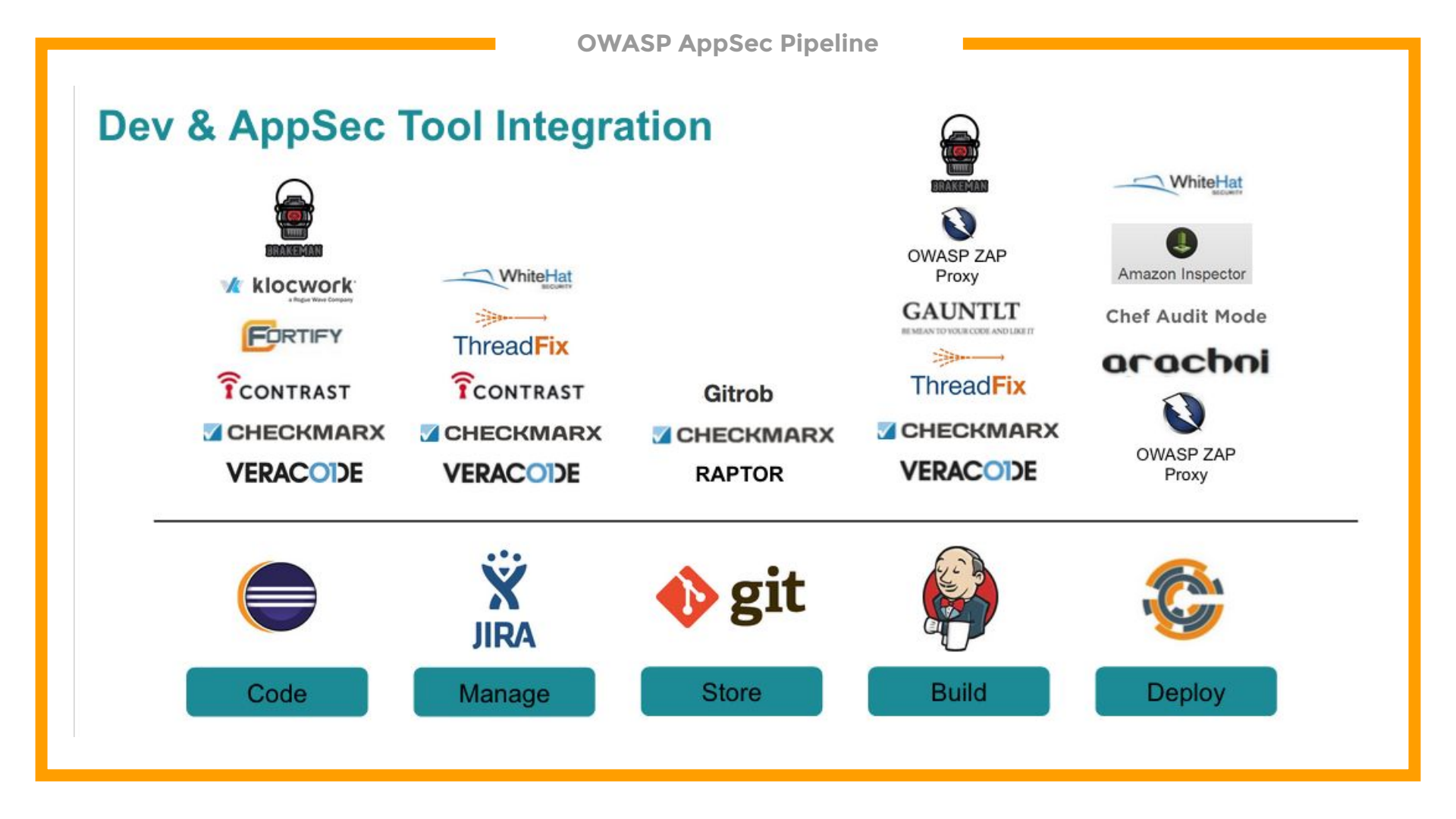
The OWASP AppSec Rugged DevOps Pipeline Project

The OWASP AppSec Rugged DevOps Pipeline Project is the place to find the information you need to increase the speed and automation of your AppSec program. Using the documentation and references of this project will allow you to setup your own AppSec Pipeline.

Description

The AppSec pipeline project is a place to gather together information, techniques and tools to create your own AppSec Pipeline. AppSec Pipelines takes the principles of DevOps and Lean and applies that to an application security program. The project will gather references, cheat sheets, and specific guidance for tools/software which would compose an AppSec Pipeline.

Dev & AppSec Tool Integration



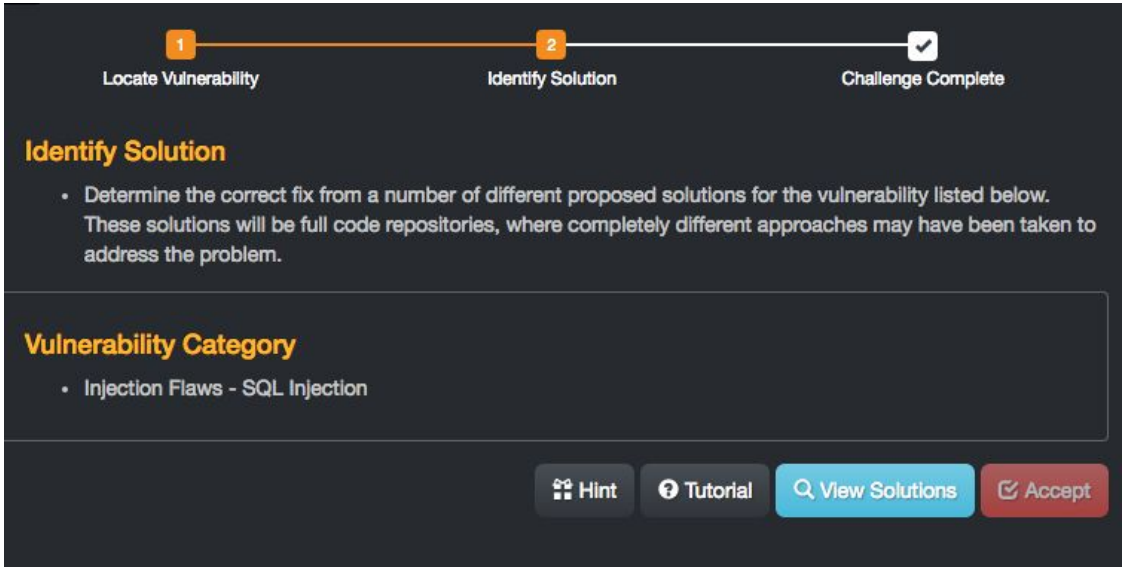
- Cyber security trends.
- Hacker motivations.
- Dark Markets.
- Thinking like a hacker.
- Secure Development Lifecycle.
- Web hackers toolkit.

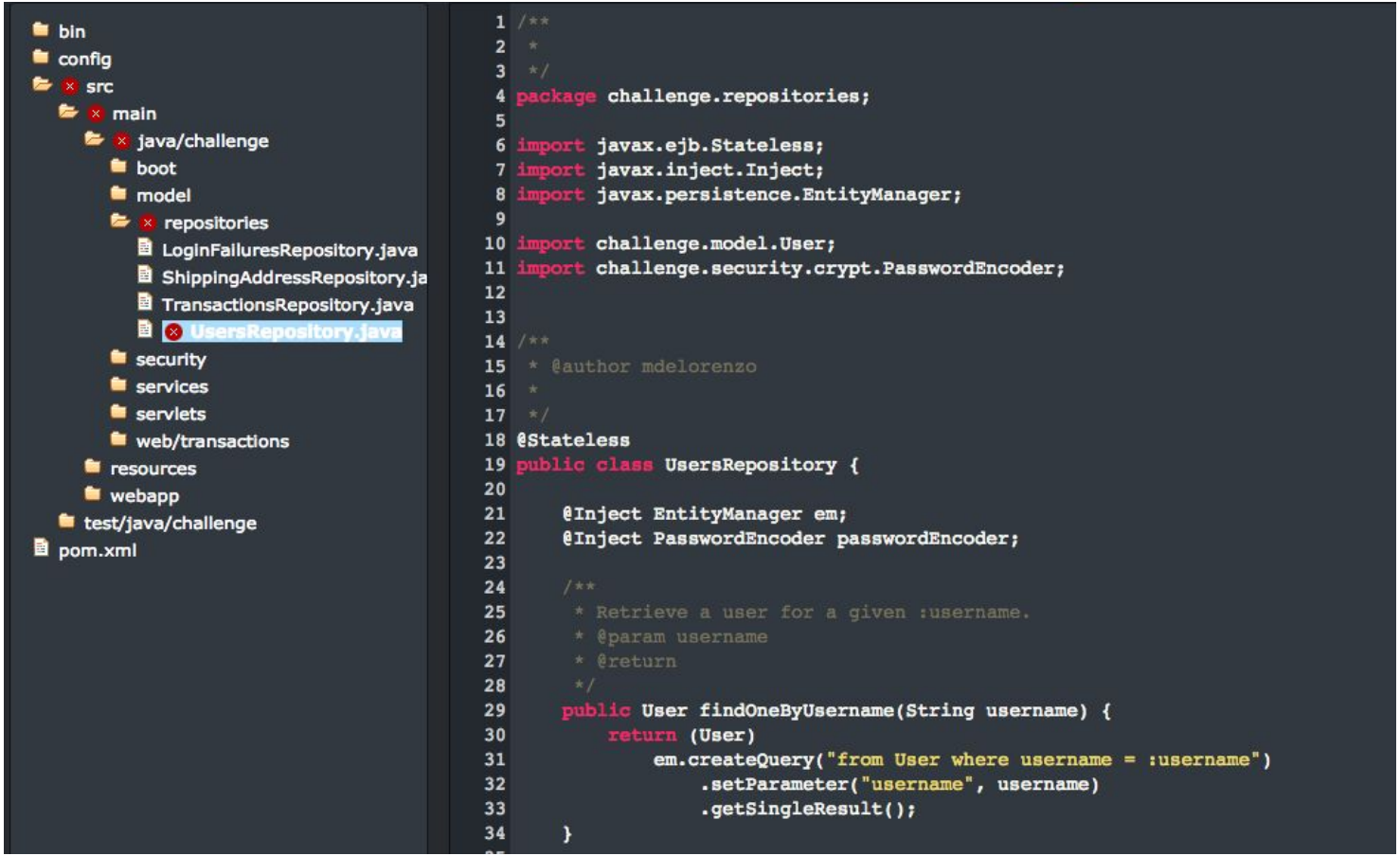
- Application security overview
- HTTP
- SSL/TLS
- Cookies
- Untrusted Data
- Cross-site scripting
- SQL Injection

- More common vulnerabilities.
- CORS
- Security Headers

- Compete against each other to solve several web security challenges.


Hone Your Skills
Practice finding, identifying and fixing real-world software security vulnerabilities.
Defend Your Code
Defeat the attackers targeting your client's systems and code to gain points. Rise through the levels to tackle more difficult security vulnerabilities in critical systems.
Demonstrate Your Expertise
Compete against other developers and see how you rate compared with other developers in your industry or region.


1
Locate Vulnerability
2
Identify Solution
Challenge Complete
Identify Solution
Determine the correct fix from a number of different proposed solutions for the vulnerability listed below. These solutions will be full code repositories, where completely different approaches may have been taken to address the problem.
Vulnerability Category
Injection Flaws - SQL Injection
Hint
Tutorial
View Solutions
Accept




```java
/**
 *
 */
package challenge.repositories;

import javax.ejb.Stateless;
import javax.inject.Inject;
import javax.persistence.EntityManager;

import challenge.model.User;
import challenge.security.crypt.PasswordEncoder;


/**
 * @author mdelorenzo
 *
 */
@Stateless
public class UsersRepository {

    @Inject EntityManager em;
    @Inject PasswordEncoder passwordEncoder;

    /**
     * Retrieve a user for a given :username.
     * @param username
     * @return
     */
    public User findOneByUsername(String username) {
        return (User)
            em.createQuery("from User where username = :username")
                .setParameter("username", username)
                .getSingleResult();
    }
```

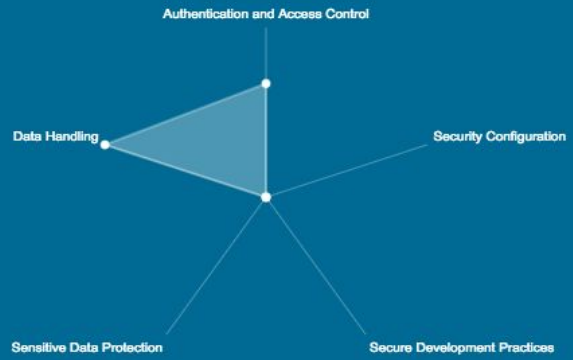
Julian Berton Security Skill Scorecard

Security Maturity

Beginner

Points Scored	Rank
2646 points	#1 New

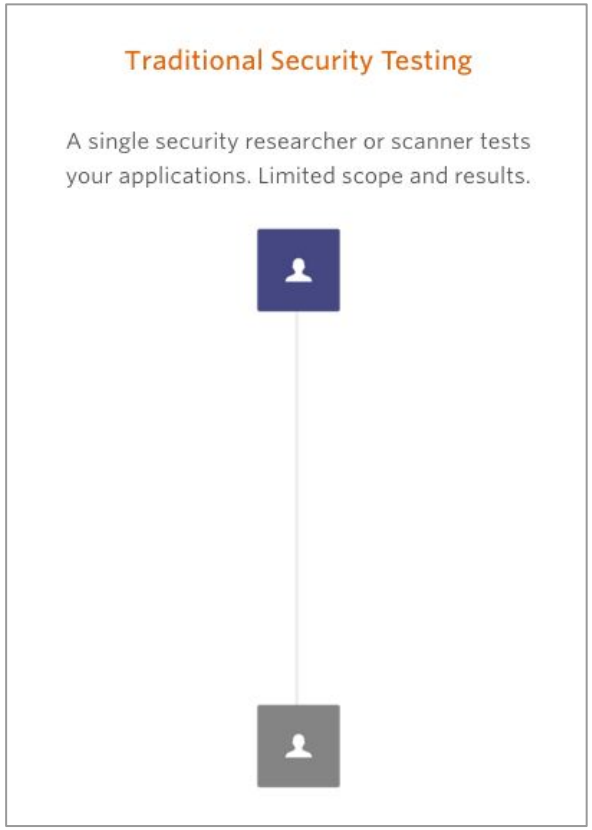
Average Strengths and Weaknesses



Authentication and Access Control	Data Handling	Security Configuration	Sensitive Data Protection	Secure Dev Practices

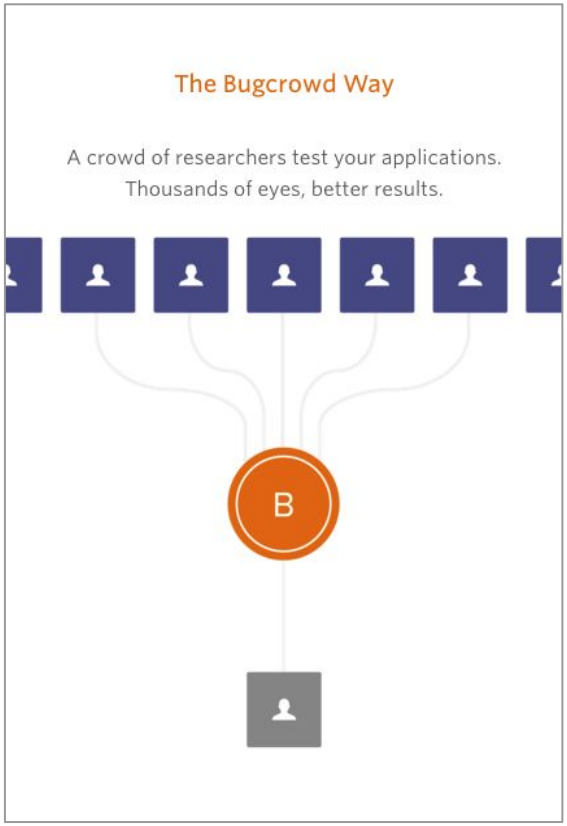
Challenge Accuracy
13 attempts / 12 correct / 1 incorrect

Bug Bounty Programs



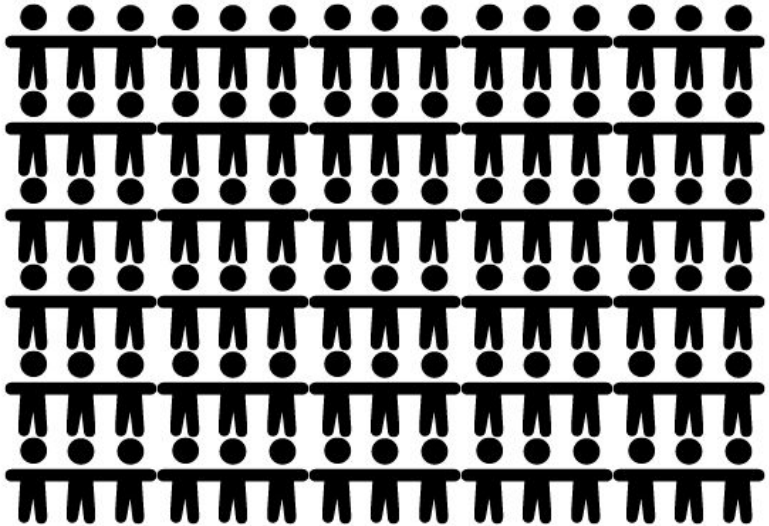
bugcrowd

hackerone

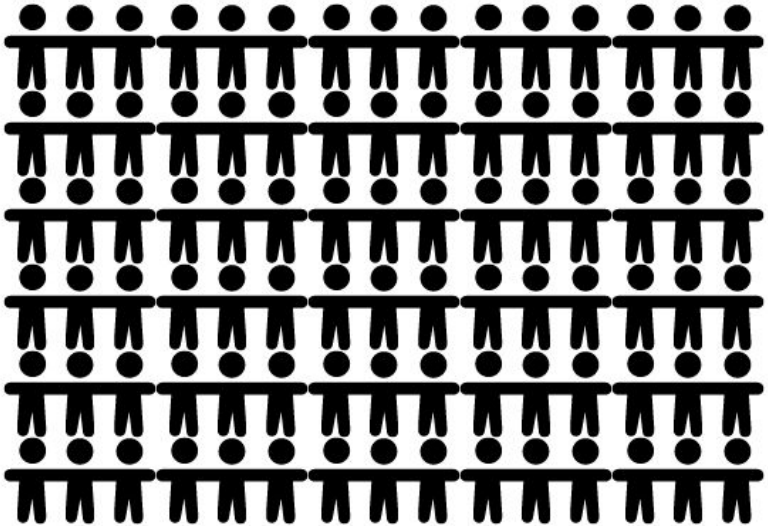


Bug Bounty Programs - Even the playing field

~100 Bounty Hunters



~100 Tech Team

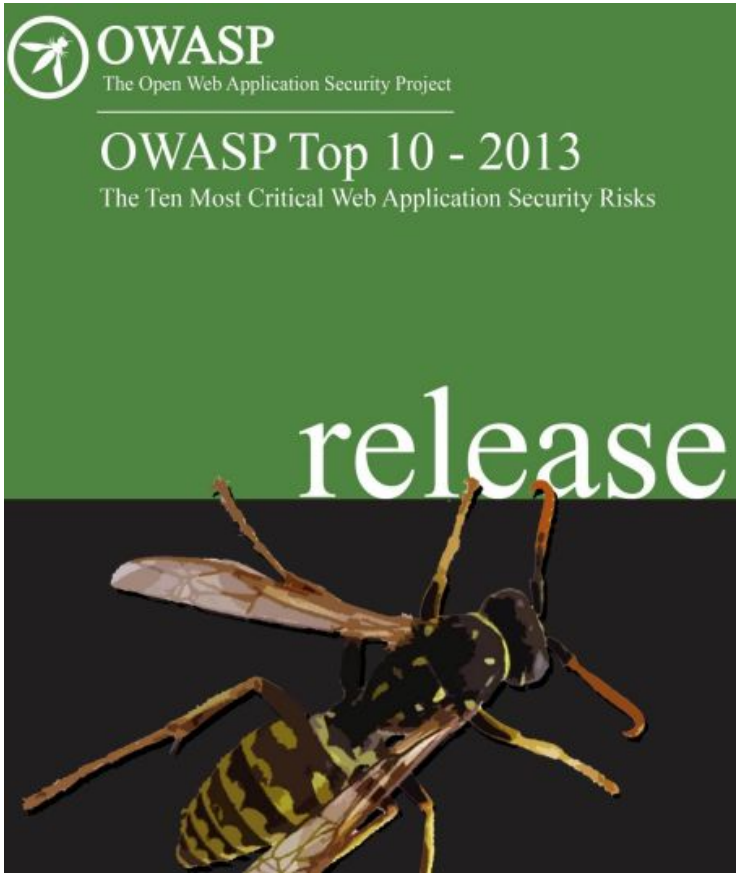


Bug Bounty Programs

Now	Then	Goal
Private Flex Program	Private Ongoing Program	Unmanaged Public Program

What can i start doing tomorrow to improve security?

- Awareness document for web application security.
- Updated every 3 years.
- Short descriptions and example scenarios.
- Broad consensus about what the most critical web application security flaws are.



OWASP Top 10 Application Security Risks – 2013

A1 – Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 – Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

A1 Injection

Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.	Attacker sends simple text-based attacks that exploit the syntax of the targeted interpreter. Almost any source of data can be an injection vector, including internal sources.	Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code. They are often found in SQL, LDAP, Xpath, or NoSQL queries; OS commands; XML parsers, SMTP Headers, program arguments, etc. Injection flaws are easy to discover when examining code, but frequently hard to discover via testing. Scanners and fuzzers can help attackers find injection flaws.		Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.	Consider the business value of the affected data and the platform running the interpreter. All data could be stolen, modified, or deleted. Could you reputation be harmed?

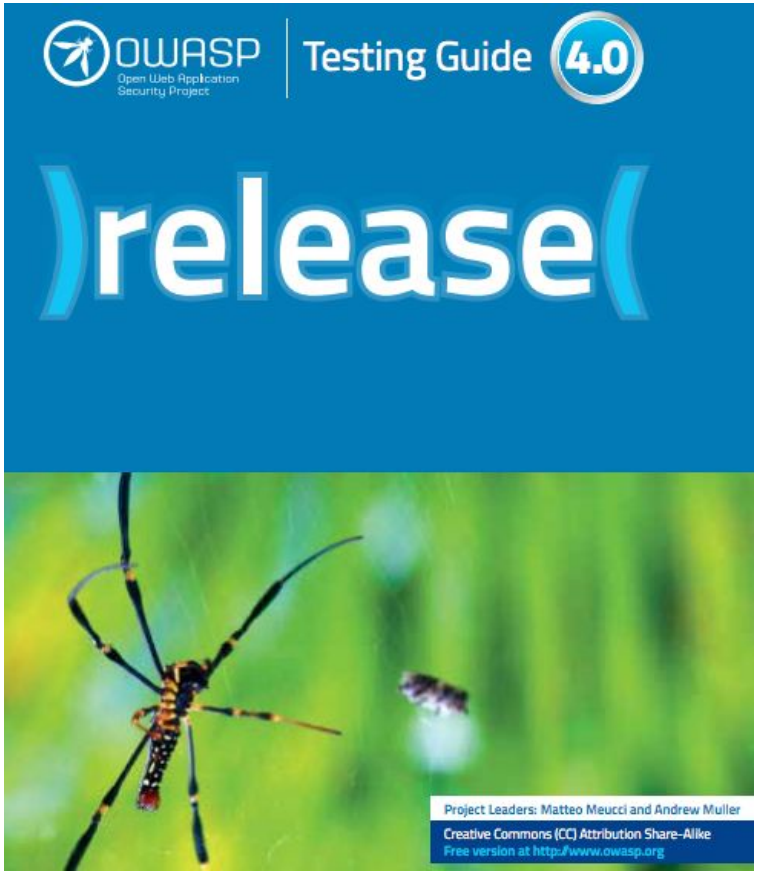
Am I Vulnerable To Injection?

The best way to find out if an application is vulnerable to injection is to verify that all use of interpreters clearly

How Do I Prevent Injection?

Preventing injection requires keeping untrusted data separate from commands and queries.

- Explains how to test different categories of security vulnerabilities.
- Gives an overview of how to integrate security into an SDLC.
- Just released (2015).
- Free to download!



owasp.org/index.php/OWASP_Testing_Project

Authentication Testing

Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)
Testing for default credentials (OTG-AUTHN-002)
Testing for Weak lock out mechanism (OTG-AUTHN-003)
Testing for bypassing authentication schema (OTG-AUTHN-004)
Test remember password functionality (OTG-AUTHN-005)
Testing for Browser cache weakness (OTG-AUTHN-006)
Testing for Weak password policy (OTG-AUTHN-007)
Testing for Weak security question/answer (OTG-AUTHN-008)
Testing for weak password change or reset functionalities (OTG-AUTHN-009)
Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)

Authorization Testing

Testing Directory traversal/file include (OTG-AUTHZ-001)
Testing for bypassing authorization schema (OTG-AUTHZ-002)
Testing for Privilege Escalation (OTG-AUTHZ-003)
Testing for Insecure Direct Object References (OTG-AUTHZ-004)

Session Management Testing

Testing for Bypassing Session Management Schema (OTG-SESS-001)
Testing for Cookies attributes (OTG-SESS-002)
Testing for Session Fixation (OTG-SESS-003)
Testing for Exposed Session Variables (OTG-SESS-004)
Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)
Testing for logout functionality (OTG-SESS-006)

Testing for Error Handling

Analysis of Error Codes (OTG-ERR-001)
Analysis of Stack Traces (OTG-ERR-002)

Testing for weak Cryptography

Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)
Testing for Padding Oracle (OTG-CRYPST-002)
Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

Business Logic Testing

Test Business Logic Data Validation (OTG-BUSLOGIC-001)
Test Ability to Forge Requests (OTG-BUSLOGIC-002)
Test Integrity Checks (OTG-BUSLOGIC-003)
Test for Process Timing (OTG-BUSLOGIC-004)
Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005)
Testing for the Circumvention of Work Flows (OTG-BUSLOGIC-006)
Test Defenses Against Application Mis-use (OTG-BUSLOGIC-007)
Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)
Test Upload of Malicious Files (OTG-BUSLOGIC-009)

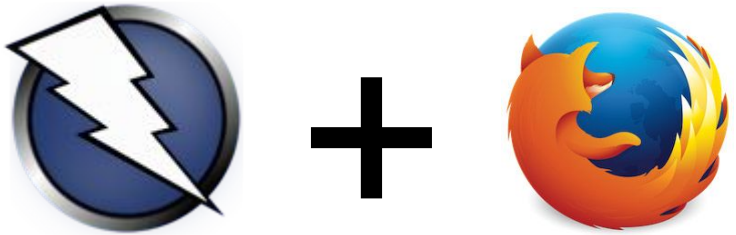
Client Side Testing

Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)
Testing for JavaScript Execution (OTG-CLIENT-002)
Testing for HTML Injection (OTG-CLIENT-003)
Testing for Client Side URL Redirect (OTG-CLIENT-004)
Testing for CSS Injection (OTG-CLIENT-005)
Testing for Client Side Resource Manipulation (OTG-CLIENT-006)

Who has used a proxy before?

ZAP

1. Open Source (and free!!).
2. Cross platform (Java).
3. Has security specific features (Fuzzer, auto scanner, etc).
4. Can be run in headless mode with API (think automation and build pipeline).



Firefox

1. Uses its own Proxy settings (not the OS's like Chrome, etc).
2. Has its own list of certificates so we do not have to add the ZAP cert to the OS list.

- Being aware of software security is half the battle.
- Hackers are here to stay.
- Implementing a Secure Development Lifecycle is a must.

References

- http://www.slidescarnival.com/
- https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf
- http://krebsonsecurity.com/tag/fullz/
- http://www.leakedin.com/
- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- http://www.securityweek.com/austrian-firm-fires-ceo-after-56-million-cyber-scam
- http://krebsonsecurity.com/2015/08/leaked-ashleymadison-emails-suggest-execs-hacked-competitors/
- http://www.bloomberg.com/news/articles/2013-07-03/edward-snowden-and-the-nsa-a-lesson-about-insider-threats
- https://www.thoughtworks.com/insights/blog/build-your-own-technology-radar
- https://twitter.com/pencilsareneat/status/724711158863790084
- https://www.owasp.org/index.php/OWASP_AppSec_Pipeline#tab=Pipeline_Tools
- http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/#349d9b6f347d
- http://securecodewarrior.com
- owasp.org/index.php/Category:OWASP_Top_Ten_Project
- http://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#3136733a2a7f