



OWASP – Beyond the Top 10

André Rochefort

TELUS Security Assessment Services

Sr. Consultant

andre.rochefort@telus.com

“All programmers are playwrights and all computers are lousy actors.” (unknown)

What is this about?

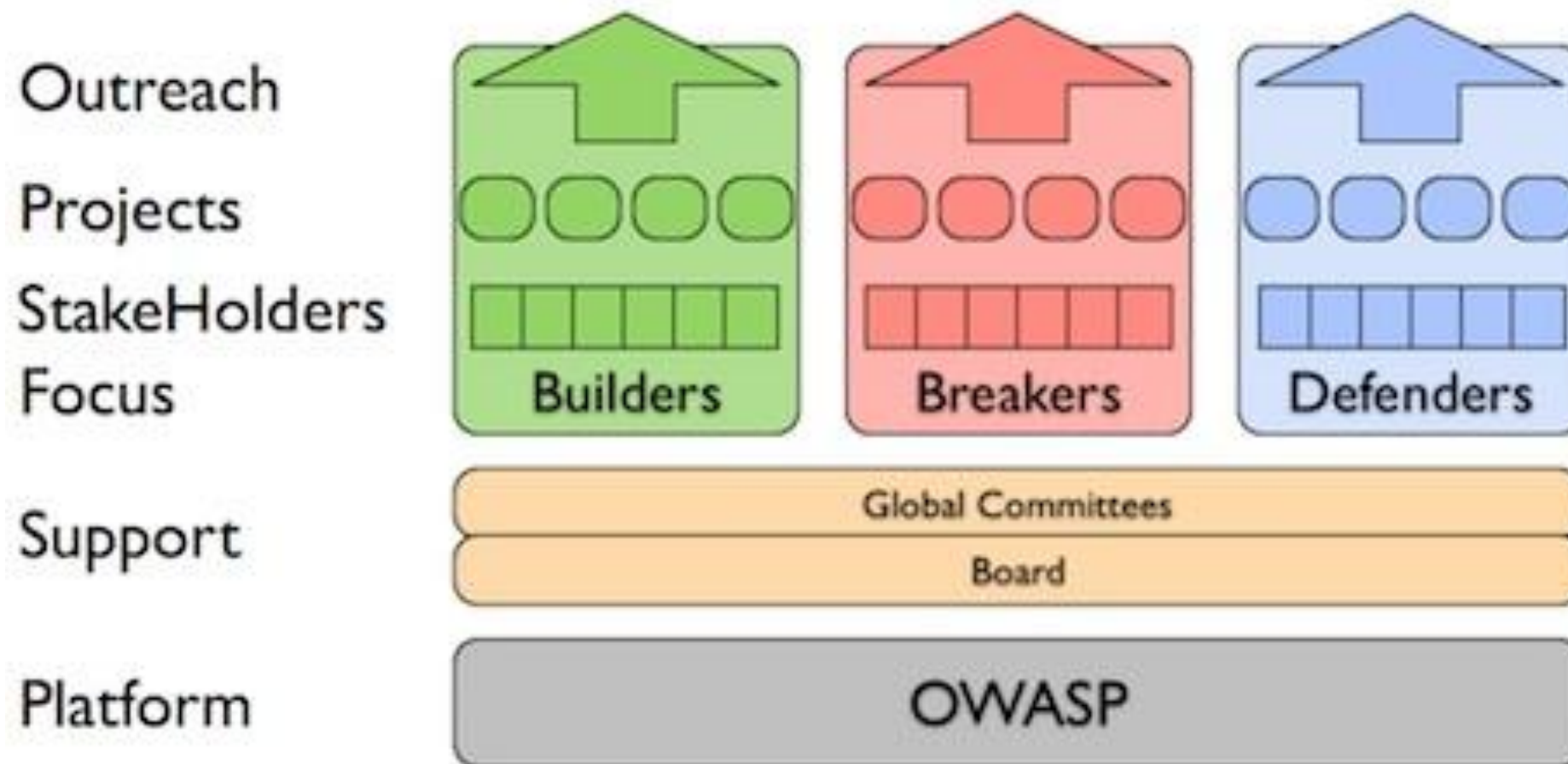
OWASP Present & Future Solutions:

- Flagship Projects
- Labs Projects
- Incubator Projects



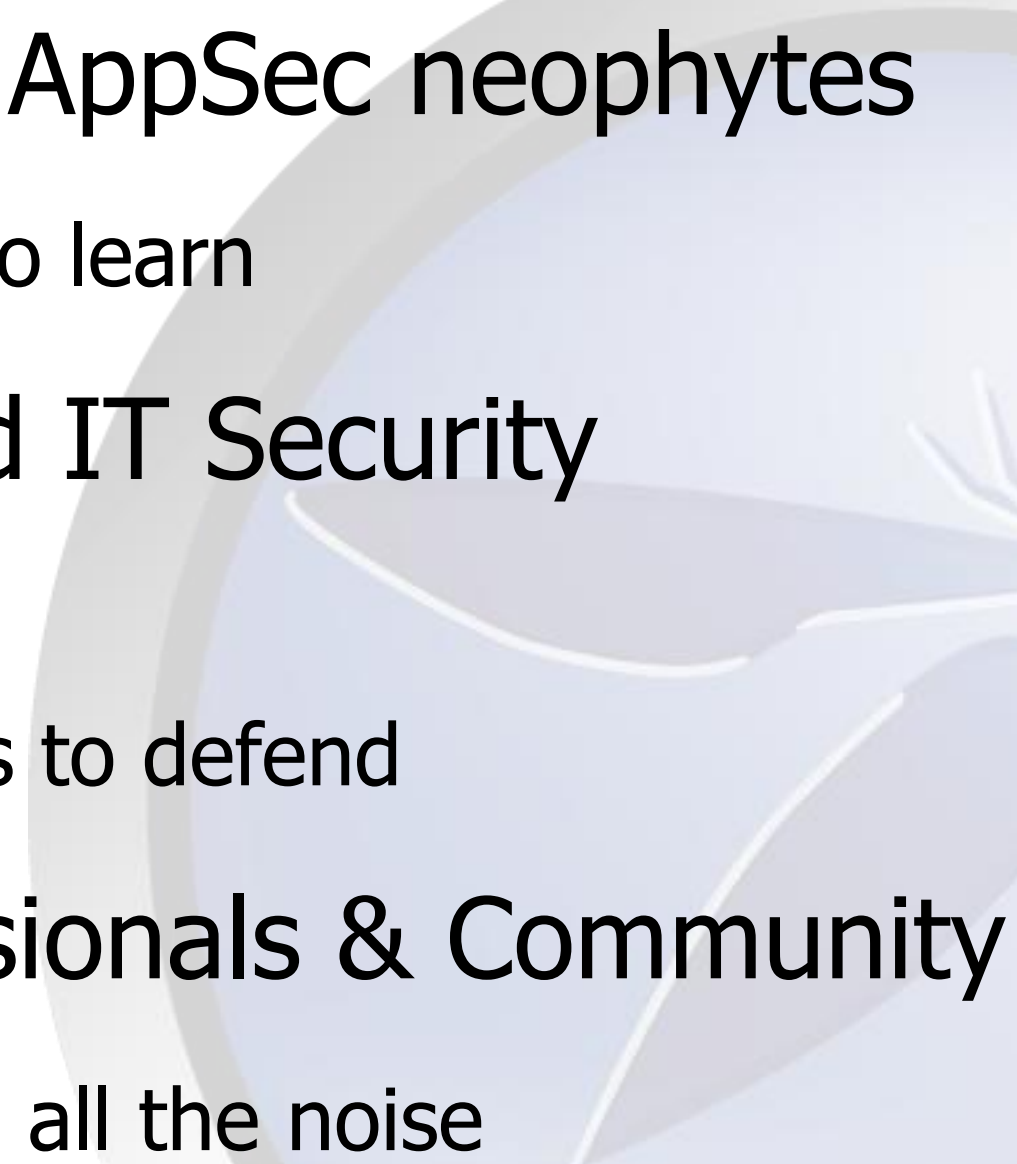
Communities

A Vision for OWASP





Target Audiences

- 1) Students* and AppSec neophytes
 - The ones eager to learn
 - 2) Developers and IT Security Administrators
 - The ones anxious to defend
 - 3) AppSec Professionals & Community
 - The ones making all the noise
- 



Why?

- Raise awareness
- Call to Arms / Engage
- Sharpen those soft skills

“No man is exempt from saying silly things; the mischief is to say them deliberately.” - Michel de Montaigne

WebAppSec Resources vs. Backlog



Assumptions

	Number
Number of websites on the public Internet	672,985,183
Number of hours a webappsec pen-tester takes to assess the average website	16
Number of work hours in the average year	2,000
Number of people working as webappsec pen-testers today	300,000
Number of scans required per year	4

Results

Number of web application testers needed to test the entire Internet manually:	21,535,526
Number we will have to hire to get full global coverage:	21,235,526
Number of sites that won't get assessed by hand due to shortage:	663,610,183
Percent of all Sites Covered by Manual Assessments:	1.4%












The Top 10

(and other news)

Recent OWASP News

- The 2013 WebAppSec Top 10 Launched
 - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Source Code Analyzer Coverity joins OWASP
 - <http://www.coverity.com/company/press-releases/read/coverity-joins-open-web-application-security-project-owasp>
- State of the Community

OWASP Top 10 2013

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection 
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management 
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS) 
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References 
A6 – Security Misconfiguration	A5 – Security Misconfiguration 
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure 
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control 
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF) 
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards 
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

OWASP Top 10 2013

Additional Risks to Consider

The Top 10 cover a lot of ground, but there are many other risks you should consider and evaluate in your organization. Some of these have appeared in previous versions of the Top 10, and others have not, including new attack techniques that are being identified all the time. Other important application security risks (in alphabetical order) that you should also consider include:

- Clickjacking
- Concurrency Flaws
- Denial of Service (Was 2004 Top 10 – Entry 2004-A6)
- Expression Language Injection (CWE-917)
- Information Leakage and Improper Error Handling (Was part of 2007 Top 10 – Entry 2007-A6)
- Insufficient Anti-automation (CWE-799)
- Insufficient Logging and Accountability (Related to 2007 Top 10 – Entry 2007-A6)
- Lack of Intrusion Detection and Response
- Malicious File Execution (Was 2007 Top 10 – Entry 2007-A3)
- Mass Assignment (CWE-915)
- User Privacy

e.g. WS Amplification

e.g. Facebook
Shadow
Profiles

e.g. PRISM

Other Top 10s

OWASP Mobile Top 10 Risks

- Top 10 Mobile Risks (refresh: 2013)

M1 – Insecure Data Storage

M2 – Weak Server-Side Controls

M3 - Insufficient Transport Layer Protection

M4 - Client Side Injection

- Top 10 Mobile Security Controls

M5 - Poor Authorization and Authentication

M6 - Improper Session Handling

M7 - Security Decisions Via Untrusted Inputs

M8 - Client Side Data Leakage

- Top 10 Source Code Flaws (2010)

- Top 10 Defenses

M9 - Broken Cryptography

M10 - Sensitive Information Disclosure

- Top 10 Cloud Risks

Also:

- Alternative classification schemes, e.g. The Seven Pernicious Kingdoms

Gartner Magic Quadrant



State of the Community

- Mark Curphey on OWASP; Seconauts, and Security Tools for Developers
- OWASP Top 10 – 9 Too Many?
- Dini Cruz and OWASP in 2014
 - <http://blog.diniscruz.com/2012/11/i-wish-that-owasp-in-2014.html>
- Pushing for more activity in T.O.

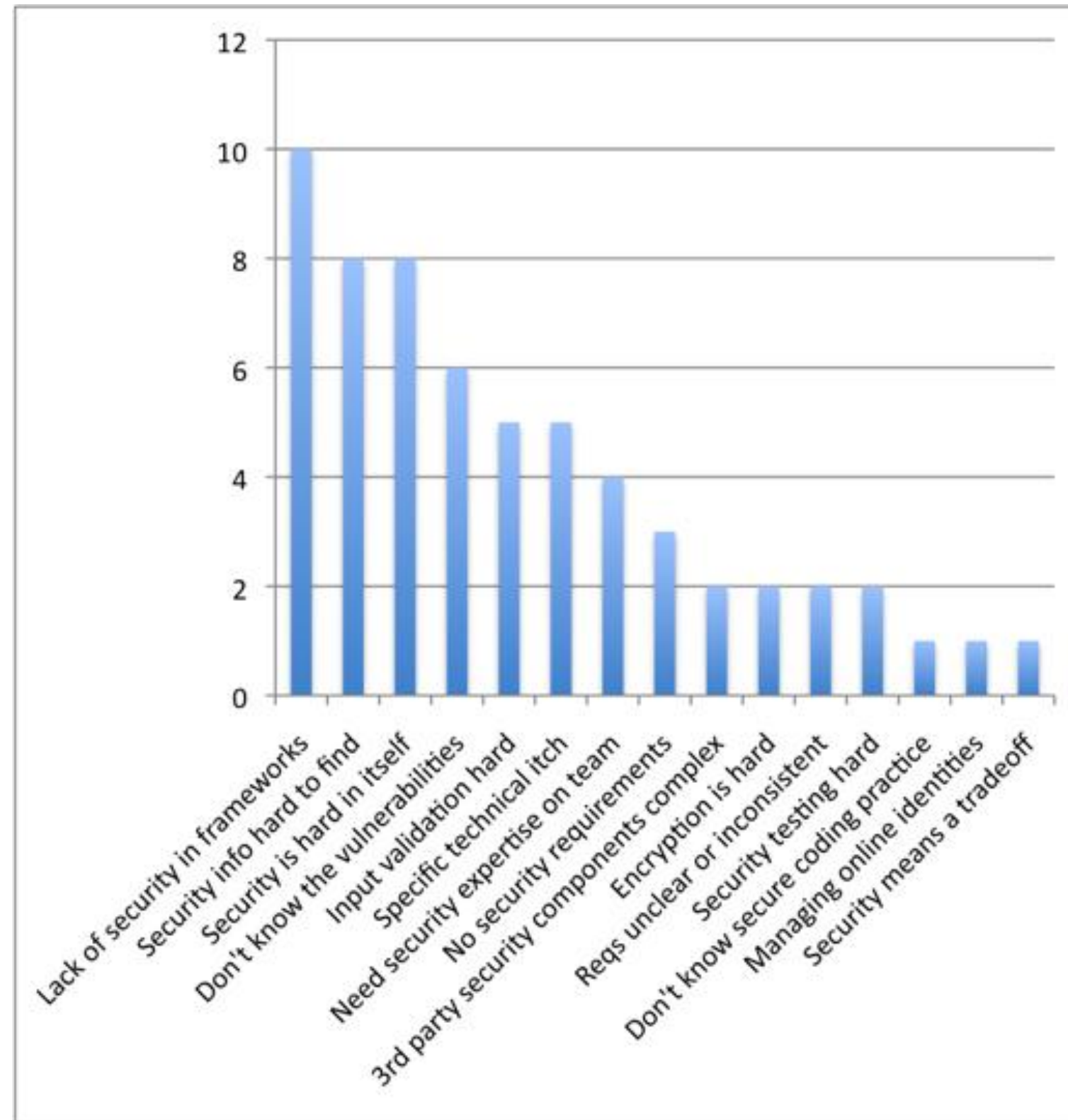


SECONAUTS

Top 5 Developer Fears

(from: Itworld/StackOverflow)

1. Screwing up*
2. Losing their jobs
3. No longer liking the job
4. Learning new technologies
5. Incompetent Management/Coworkers





Beyond the Top 10



The Inventory*

- Resources for WebAppSec Training
- Secure Coding Materials, APIs, SCAs
- Tools for Vulnerability Mitigation, Discovery
- Miscellany in between

The Learning Curve

OWASP Tools for WAS Education:

- Tutorials / Exercised-based Training
- Vulnerable Web Applications
- Books!

Download the PDFs free or buy hardcopies and support OWASP

OWASP WebGoat

Choose another language: English ▾ Logout ?



OWASP WebGoat v5.4 [Show Params](#) [Show Cookies](#) [Lesson Plan](#)

LAB: Cross Site Scripting

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)

[Phishing with XSS](#)

[LAB: Cross Site Scripting](#)

[Stage 1: Stored XSS](#)

[Stage 2: Block Stored XSS
using Input Validation](#)

[Stage 3: Stored XSS
Revisited](#)

[Stage 4: Block Stored XSS
using Output Encoding](#)

[Stage 5: Reflected XSS](#)

[Stage 6: Block Reflected XSS](#)

[Stored XSS Attacks](#)

[Reflected XSS Attacks](#)

[Cross Site Request Forgery
\(CSRF\)](#)

[CSRF Prompt By-Pass](#)

[CSRF Token By-Pass](#)

Solution Videos

[Restart this Lesson](#)

Stage 4

Stage 4: Block Stored XSS using Output Encoding.

THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT

Implement a fix to block XSS after it is read from the database. Repeat stage 3. Verify that 'David' is not affected by Bruce's profile attack.



Goat Hills Financial
Human Resources

Please Login

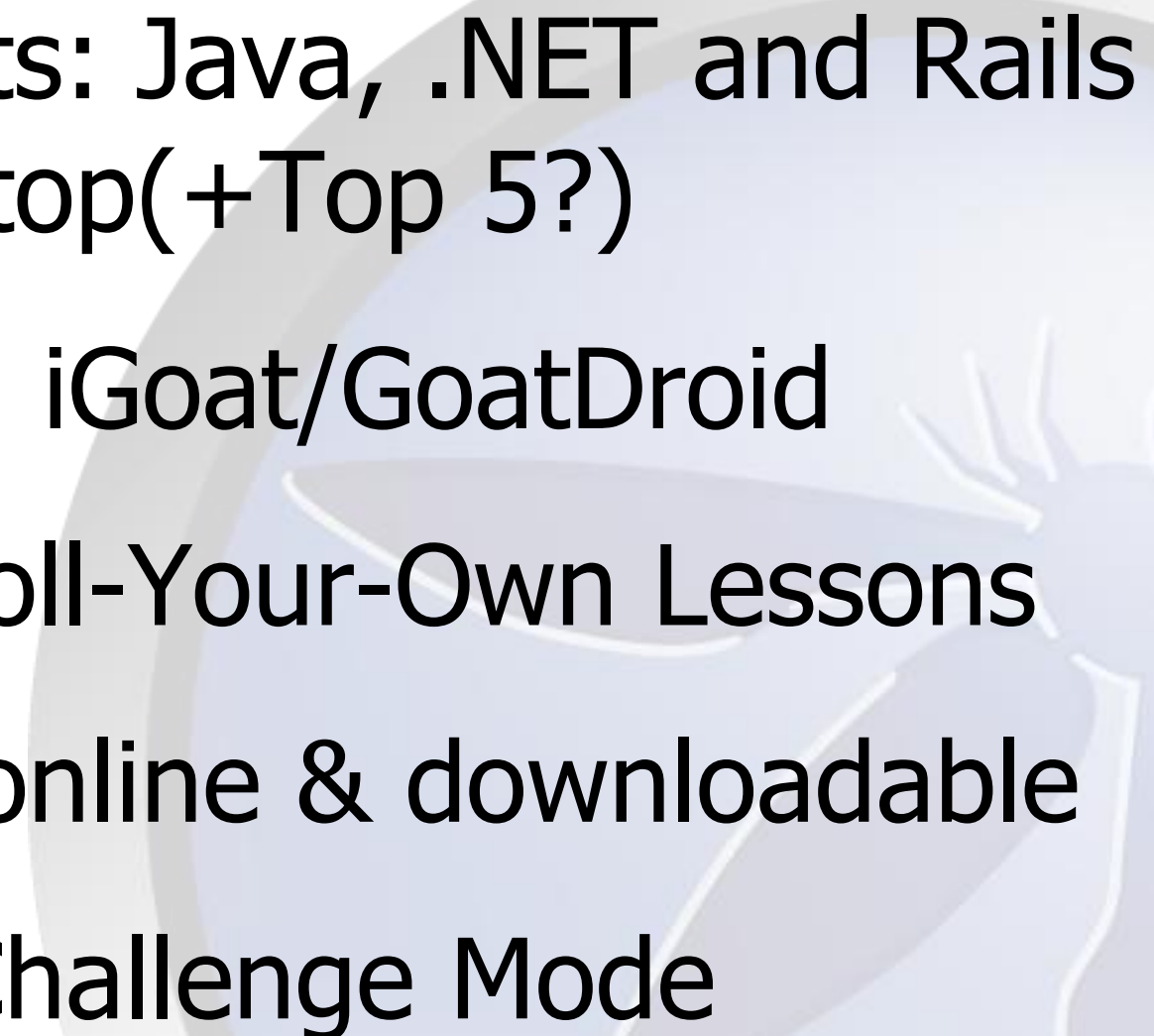
Larry Stooze (employee) ▾

Password

Login



OWASP WebGoat

- Platform variants: Java, .NET and Rails (coming), Desktop(+Top 5?)
 - Mobile variants: iGoat/GoatDroid
 - Content-rich; Roll-Your-Own Lessons
 - Video tutorials online & downloadable
 - Report Cards, Challenge Mode
- 

OWASP Mutillidae 2



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.5.11

Security Level: 0 (Hosed)

Hints: Enabled (1 - 5cr1pt K1dd1e)

Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Toggle Security](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#) | [Hide Popup Hints](#) | [Enforce SSL](#)

OWASP Top 10

A1 - SQL Injection

Web Services

A1 - Other Injection

HTML 5

A2 - Cross Site Scripting (XSS)

Others

A3 - Broken Authentication and Session Management

Documentation

A4 - Insecure Direct Object References

Resources

A5 - Cross Site Request Forgery (CSRF)

A6 - Security Misconfiguration

A7 - Insecure Cryptographic Storage

A8 - Failure to Restrict URL Access

A9 - Insufficient Transport Layer Protection

A10 - Unvalidated Redirects and Forwards

HTML Injection (HTMLi)

HTMLi via HTTP Headers

HTMLi Via DOM Injection

HTMLi Via Cookie Injection

Frame Source Injection

Command Injection

JavaScript Injection

HTTP Parameter Pollution

Cascading Style Injection

JavaScript Object Notation (JSON) Injection

Buffer Overflow

Parameter Addition

XML External Entity Injection

Deliberately Vulnerable Web Pen-Testing Application

Browser Info

Site Footer

HTTP Response Splitting (Hint: Difficult)

of vulnerabilities

ort Email Address

Announcements

Site hacked...err...quality tested with Firefox, Burp-Suite and thes Mozilla Add-ons



[PHP MyAdmin Console](#)



[Feature Requests](#)

OWASP Mutillidae 2

- Includes HTML5-oriented lessons
- Plenty of content (lessons, tutorials)
- Video guides available (YouTube)
- Gamified! Keeps track of your score
- PHP, requires (L|W|M)AMP stack

OWASP Bricks

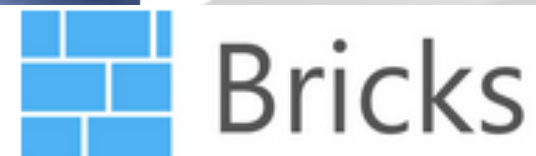
[Home](#)[Bricks](#)[Setup](#)[About](#)

Welcome to Bricks!

Bricks is a web application security learning platform built on [PHP](#) and [MySQL](#). The project focuses on variations of commonly application security issues. Each 'Brick' has some sort of security issue which can be leveraged manually or using automated s. The mission is to '[Break the Bricks](#)' and thus learn the various aspects of web application security.

Bricks is a completely free and open source project brought to you by [OWASP](#). The [complete documentation](#) and [instruction v](#) be accessed or downloaded for free. Bricks are classified into three different sections: [login pages](#), [file upload pages](#) and [cont](#)

OWASP Bricks



File Upload pages

Each file upload page has its own security mechanisms. Some pages break them, upload shell scripts, execute them and gain access.

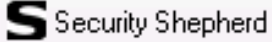



Upload #1
[Simple file upload.](#)



Upload #2
[Challenge #6](#)

OWASP Security Shepherd

 Security Shepherd



Security Shepherd

Welcome admin

Logout

Submit Result Key:

Submit

Show Module Cheat Sheet...

Admin

Next Challenge

Insecure Direct Object References

What are Insecure Direct Object References?

Imagine a web page that allows you to view your personal information. The web page that shows the user their information is generated based on a user ID. If this page was vulnerable to **Insecure Direct Object References** an attack would be able to modify the user identifier to reference any user object in the system. Insecure Direct Object References occur when an application references an object by its actual ID or name. This object that is referenced directly is used to generate a web page. If the application does not verify that the user is allowed to reference this object, then the object is **insecurely referenced**.

Attackers can use insecure object references to compromise any information that can be referenced by the parameter in question. In the above example, the attacker can access any user's personal information.

The severity of insecure direct object references varies depending on the data that is been compromised. If the

Guided Lessons

e-Learning Project (CBT)

OWASP **HACK**ademic

(live version: <http://hackademic1.teilar.gr/>)

<http://vicnum.ciphertechs.com/> (Games!)

<http://google-gruyere.appspot.com/>

<http://www.hackertest.net/>

Advanced: <https://www.hacking-lab.com/about/> (english language issues)

*Vulnerable Web Apps

(*intentionally!)

- OWASP Broken Web Apps (VM)
- Damn Vulnerable Web Application
- KILL ALL THE VENDOR'S SITES! (live)
- OWASP SiteGenerator (RIP)
- Build your own, then break it!



**TRY TO HACK THEM
ALL!**

More from OWASP

- Book: WebGoat and WebScarab
- The AppSec Tutorial Series (Videos):
 - https://www.owasp.org/index.php/OWASP_Appsec_Tutorial_Series
- Cheat Sheets
- Book: Securing WebGoat with ModSecurity

Tangent: Visualization

- Tilt (DEMO!)
- Logstalgia (DEMO!)
- glTail (video!)
- Kinectaploit (video!)
- <http://secviz.org/>

psDoom



Defending the Code

- Guides, Guides and More Guides
- Enterprise Security API
- AntiSAMY
- Source Code Analyzers
- Java Dependency Checker

Guides! (ick, PDFs)

- Web Application Secure Development Guide
- Code Review Guide (2.0 underway)
- Testing Guide
- Software Assurance Maturity Model (SAMM)
- Periodic Table of Vulnerabilities
- Application Security Verification Standard

Security Requirements

Network security includes the system of computers, routers, cables, switches and wireless access points. It is the entire system of transport and storage technologies.

7.1 Are networks segregated physically and/or logically to separate systems containing personal information from public networks such as the Internet? ☐ YES ☐ NO

7.2 Where a local area network containing personal information is connected to a public network, does the organization use perimeter defence safeguards (e.g. firewalls, routers, intrusion detection or prevention systems, anti-virus/anti-spyware software, etc.) to mediate all traffic and to protect systems that are accessible from the Internet? ☐ YES ☐ NO

7.3 Are systems and their software "hardened" (e.g. applications, operating systems, etc.) to protect against security threats?

Policy Source	Security Category	Policy Statement
DEP 390	Password Control	Strong passwords will be used. Passwords shall have these minimum characteristics:

7.4 Are ports closed and services are not running on unnecessary ports?

7.5 Are these safe?

V2 - Authentication Verification Requirements

The Authentication Verification Requirements define a set of requirements for generating and handling account credentials safely. The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 2 - OWASP ASVS Authentication Requirements (V2)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V2.1 Verify that all pages and resources require authentication except those specifically intended to be public.	✓	✓	✓	✓	✓	✓
V2.2 Verify that all password fields do not echo the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.	✓	✓	✓	✓	✓	✓
V2.3 Verify that if a maximum number of authentication attempts is exceeded, the account is locked for a period of time long enough to deter brute force attacks.	✓		✓	✓	✓	✓
V2.4 Verify that all authentication controls are enforced on the server side.			✓	✓	✓	✓

DEP 390	Password Control	Strong passwords will be used. Passwords shall have these minimum characteristics:				
		Have a length of 7 or more alphanumeric characters for Windows based systems, 8 or more for Unix based system				
		Contain both upper and low characters (e.g. a-z, A-Z)				
		Have digits and punctuation characters as well as letters (e.g. 0-9, !@#\$%^&*(){}[]:;';<>?.,/)				
		Are not words in any language, slang, dialect, or jargon				
DEP 390	Password Control	All user-level passwords (e.g., email, desktop computer, etc.) must be changed at least every 90	*may only apply at user level, not application level.	Does the application expire passwords within 90 days or uses a system whereby users		

OWASP ASVS

Flagship Project

At higher levels in ASVS, the use of tools is encouraged. But to be effective, the tools must be heavily tailored and configured to the application and framework in use

A standard to verify a
web app's security

Application- and lifecycle- independent

Manual
Design and
Code Review

Manual Design
Review

Manual Test
and Review

Tools

OWASP ASVS Levels

1

2

3

4

OWASP Cornucopia



Microsoft



elevation of
privilege

Microsoft.com/security/sdl/eop

Q

Spoofing

An attacker could go after the way credentials are updated or recovered (account recovery doesn't require disclosing the old password)

Q

Tampering

An attacker can change parameters over a trust boundary and after validation (for example, important parameters in a hidden field in HTML, or passing a pointer to critical memory)

Q

Information Disclosure

An attacker can read the entire channel because the channel (say, HTTP or SMTP) isn't encrypted

Don't tell anyone, but...



a network security game

[ab0ut]

[n3ws]

36



Game includes:

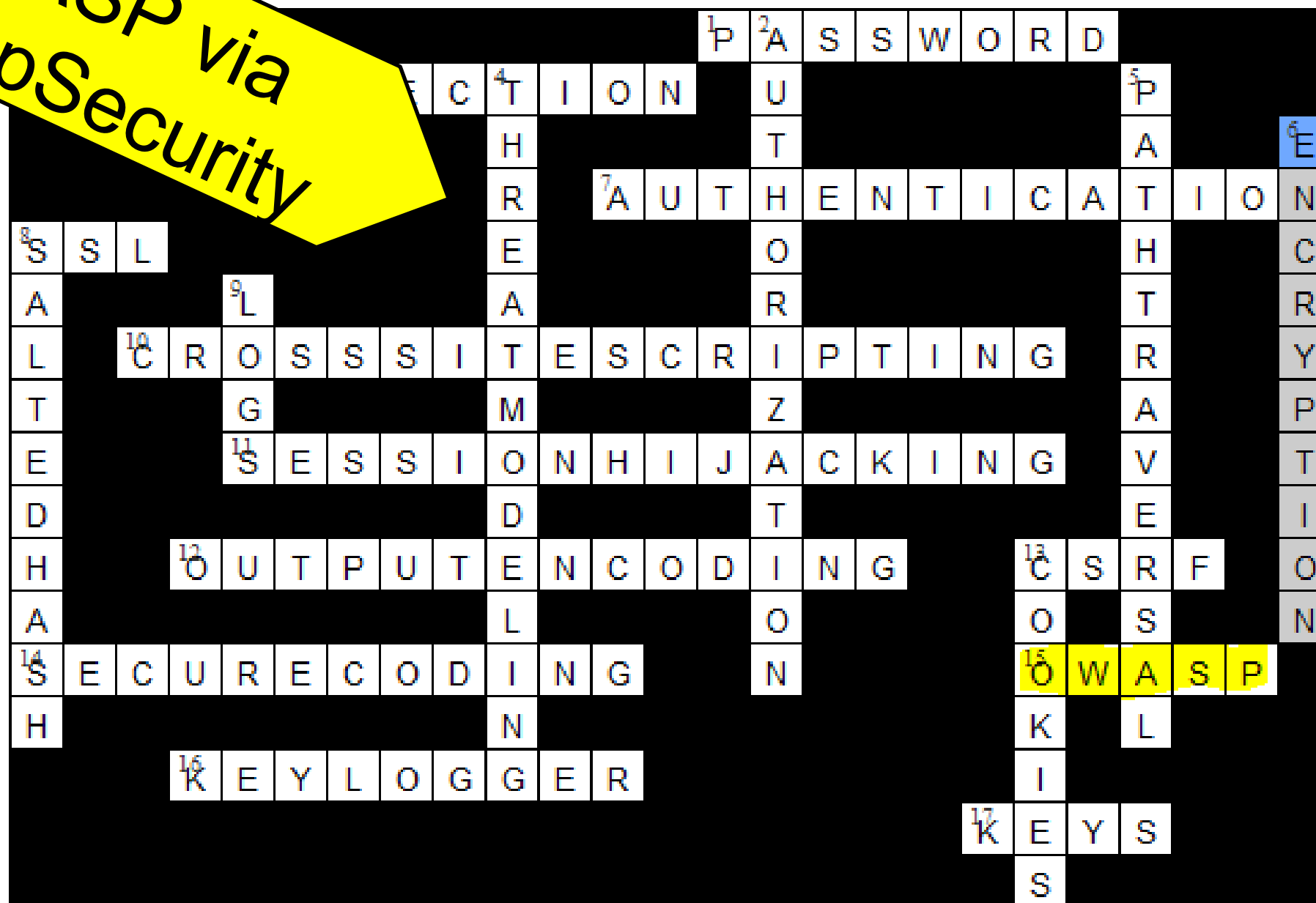
- 1 rulebook
- 3 dice
- 156 game cards
 - 16 Hacker cards
 - 56 Mission cards
 - 72 Entropy cards
 - 12 Attendance cards
- 58 Hacker Cred tokens
- 42 Money tokens



Daily Crossword

Web Application Security

OWASP via
MyAppSecurity



Not hard enough?

RegEx
Crossword
FTOMGWTF

OWASP ESAPI

- FREE Security Control Library
- Reference implementations included
- Extensible, customizable, mature*
- Support includes Java, .NET, PHP, ...
- AppSensor integration

“Good artists copy; great artists steal”

OWASP AntiSAMY

- Policy-based HTML/CSS input validator
- Support includes Java and .NET
- Sample policies available
- PHP: use HTMLPurifier instead
- Sadly, dormant.

OWASP YASCA

The screenshot displays the OWASP YASCA v2.2 report interface within a Microsoft Internet Explorer browser window. The browser's address bar shows the report file path: `C:\Documents and Settings\Andre\Desktop\Yasca\Yasca-Report-20130709110546.html`. The report header includes the Yasca logo, version 2.2, the report generation date (2013-07-09), and a link to change options. Below the header is a table of detected vulnerabilities.

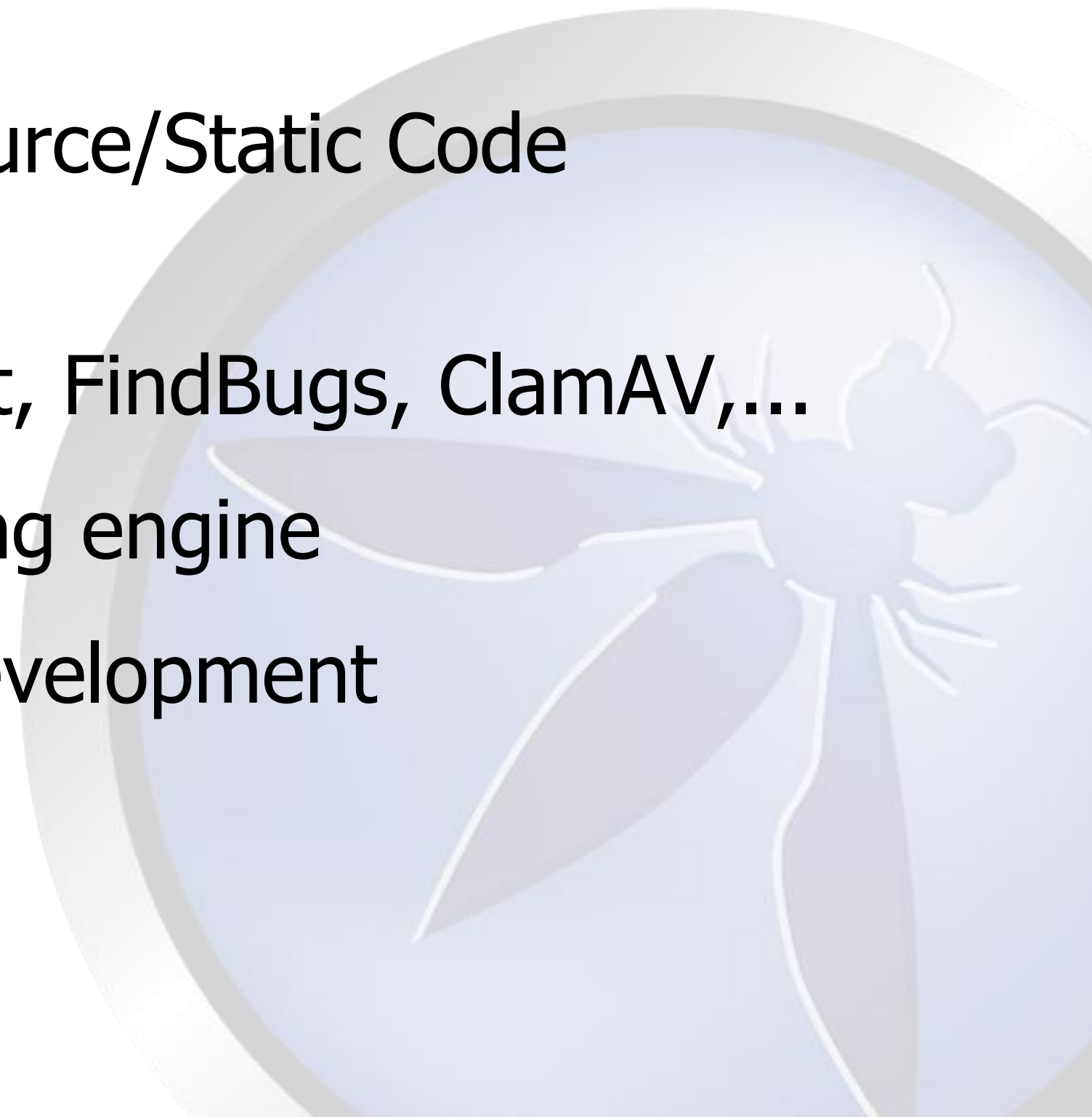
#	Location
W3 Core <i>hide</i>	
0001	tbl_gis_visualization.js:2
0002	server_synchronize.js:3
0003	server_synchronize.js:6
0004	OpenLayers.js:21
0005	OpenLayers.js:54
0006	OpenLayers.js:140
0007	OpenLayers.js:142
0008	OpenLayers.js:152

Overlaid on the right side of the browser window is a Windows Command Prompt window. It shows the execution of the Yasca tool, displaying various warning messages about missing plugins and the final report location.

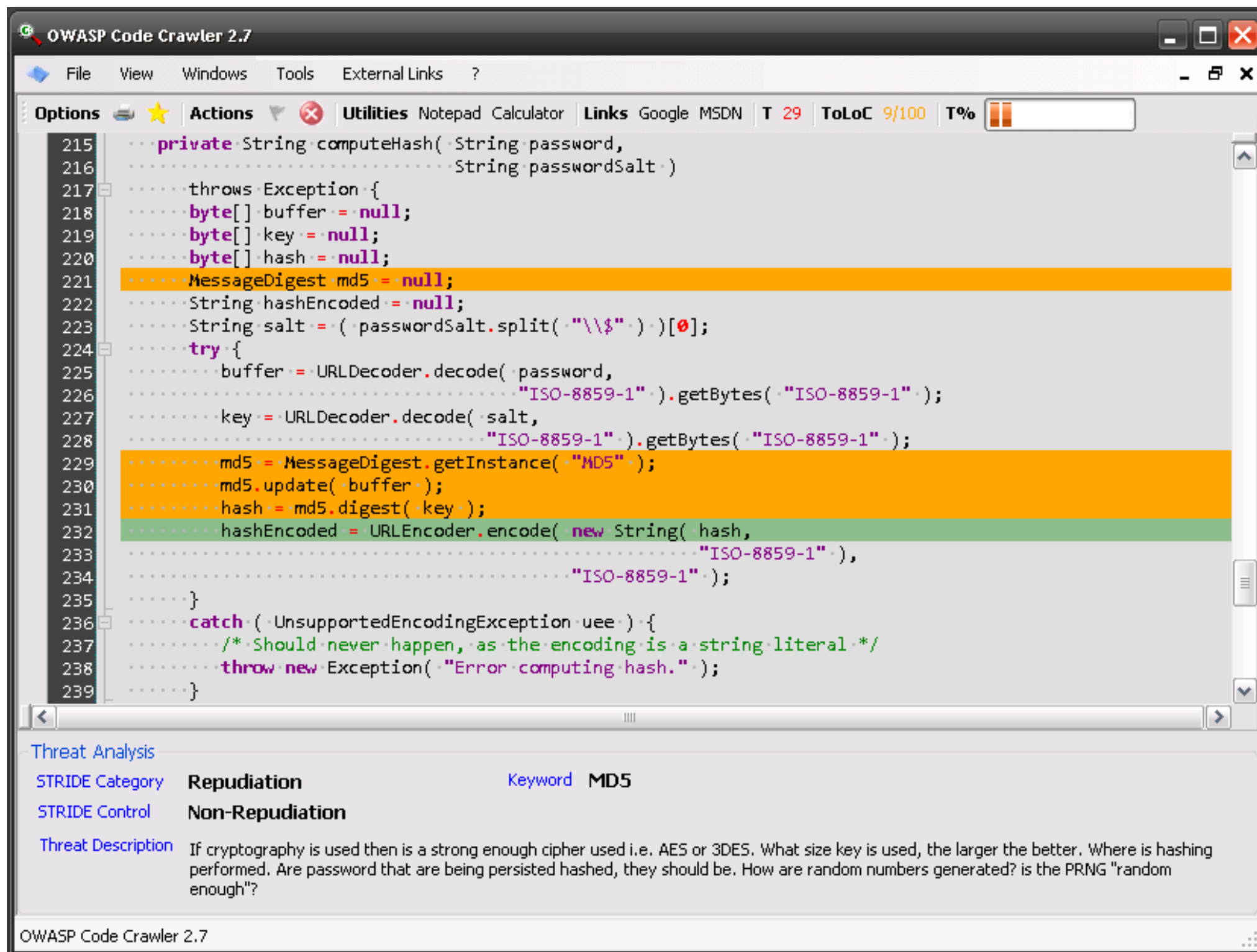
```
WARN Commercial support is now available for Yasca. Contact scovetta@users.sourceforge.net for more information.
WARN Initializing components...
WARN Using Static Analyzers located at [.]
WARN Starting scan. This may take a few minutes to complete...
WARN Plugin "jlint" not installed. Download it at yasca.org.
WARN Plugin "ClamAV" not installed. Download it at yasca.org.
WARN Plugin "cppcheck" not installed. Download it at yasca.org.
WARN Plugin "findbugs" not installed. Download it at yasca.org.
WARN Unable to find FxCop despite the installation marker.
WARN IntegrityCheck not initialized. Run with "-d "IntegrityCheck_Initialize=true"" to create baseline.
WARN Plugin "javascriptlint" not installed. Download it at yasca.org.
WARN Plugin "pmd" not installed. Download it at yasca.org.
WARN Plugin "rats" not installed. Download it at yasca.org.
WARN Plugin "fxcop" not installed. Download it at yasca.org.
WARN Plugin "phplint" not installed. Download it at yasca.org.
WARN Plugin "pixy" not installed. Download it at yasca.org.
WARN Creating report...
WARN Results have been written to C:\Documents and Settings\Andre\Desktop\Yasca\Yasca-Report-20130709110546.html
C:\Tools\yasca>
```



OWASP YASCA

- Yet Another Source/Static Code Analyzer
 - Frontend to Lint, FindBugs, ClamAV,...
 - Pattern-matching engine
 - Still in active development
- 

OWASP Code Crawler



The screenshot displays the OWASP Code Crawler 2.7 application window. The main pane shows a C# code snippet for a `computeHash` method. The code is analyzed for security issues, with several lines highlighted in orange and green. The orange highlights indicate potential issues with MD5 usage and string encoding. The green highlight indicates a successful encoding operation.


```
215 private String computeHash(String password,
216                             String passwordSalt)
217     throws Exception {
218     byte[] buffer = null;
219     byte[] key = null;
220     byte[] hash = null;
221     MessageDigest md5 = null;
222     String hashEncoded = null;
223     String salt = (passwordSalt.split("\\$"))[0];
224     try {
225         buffer = URLDecoder.decode(password,
226                                     "ISO-8859-1").getBytes("ISO-8859-1");
227         key = URLDecoder.decode(salt,
228                                "ISO-8859-1").getBytes("ISO-8859-1");
229         md5 = MessageDigest.getInstance("MD5");
230         md5.update(buffer);
231         hash = md5.digest(key);
232         hashEncoded = URLEncoder.encode(new String(hash,
233                                                    "ISO-8859-1"),
234                                         "ISO-8859-1");
235     }
236     catch (UnsupportedEncodingException uee) {
237         /* Should never happen, as the encoding is a string literal */
238         throw new Exception("Error computing hash.");
239     }
```

Threat Analysis

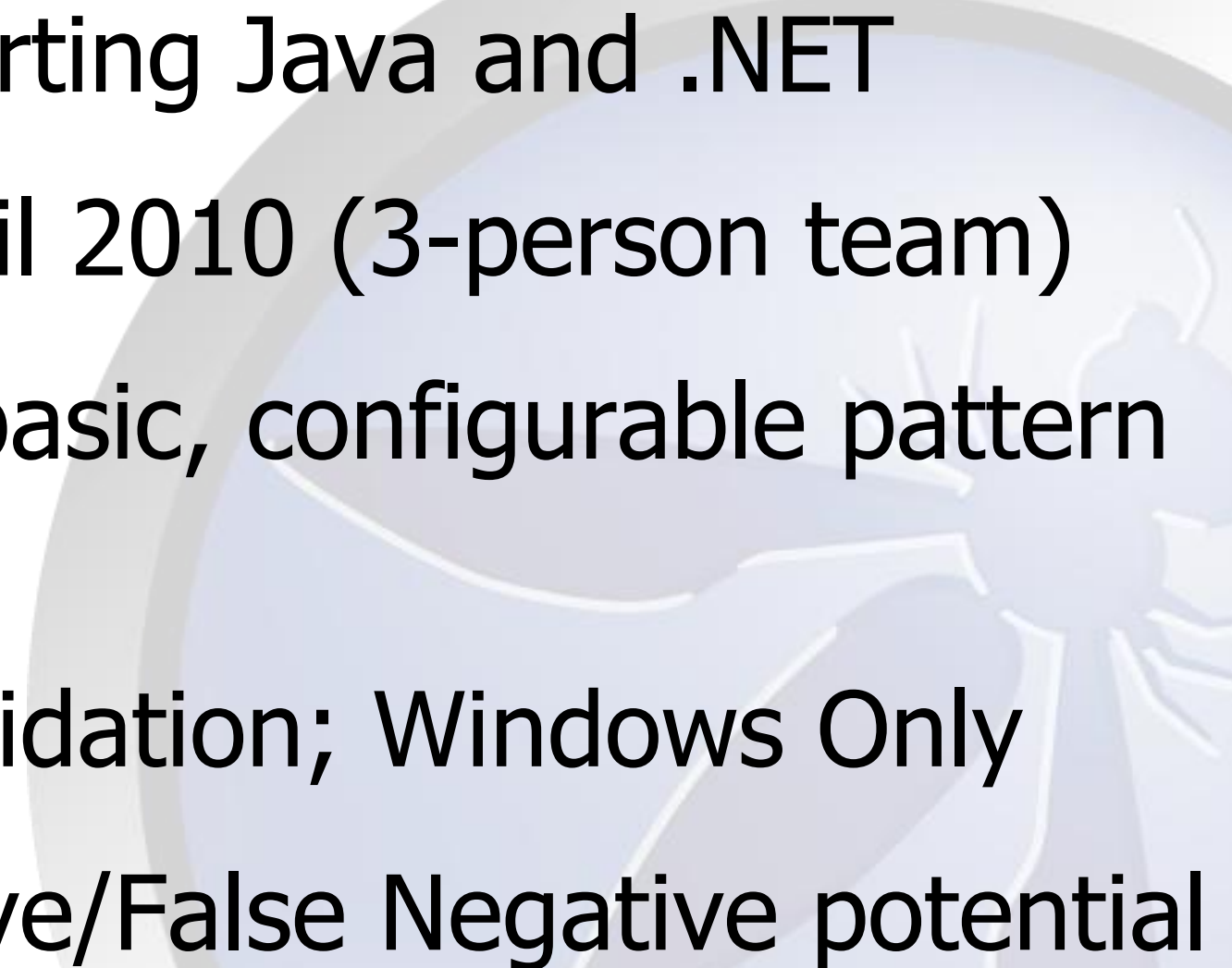
STRIDE Category	Repudiation	Keyword
STRIDE Control	Non-Repudiation	MD5

Threat Description If cryptography is used then is a strong enough cipher used i.e. AES or 3DES. What size key is used, the larger the better. Where is hashing performed. Are password that are being persisted hashed, they should be. How are random numbers generated? is the PRNG "random enough"?

OWASP Code Crawler 2.7



OWASP CodeCrawler

- Static SCA supporting Java and .NET
 - Last Update: April 2010 (3-person team)
 - RegEx filtering; basic, configurable pattern matching
 - No Data Flow validation; Windows Only
 - High False Positive/False Negative potential
- 



Defending the Web App

ModSecurity Core Rule Set (new release
July 2)

AppSensor (App-based IDS)

More WAF projects on the horizon



Hunting for Vulnerability

- WebScarab
- Zed Attack Proxy
- JoomScan and CMS Scan
- WebSlayer with
- O2 platform

इरानदा

OWASP WebScarab

WebScarab

File View Tools Help

XSS/CRLF SessionID Analysis Scripted Fragments **Fuzzer** Compare Search

Summary Messages Proxy Manual Request Spider Extensions

Method URL Version

GET http://localhost:8080/test HTTP/1.0

Header	Value
--------	-------

Add
Delete

Parameters

Location	Name	Type	Value	Priority	Fuzz Source
----------	------	------	-------	----------	-------------

Add
Delete

Classic!

Total Requests : 0
Current Request : 0

Sources Start Stop

ID	Date	Method	Host	Path	Parameters	Status	Origin	Tag	Size
----	------	--------	------	------	------------	--------	--------	-----	------

Started

Used 10.53 of 247.5MB

OWASP Zed Attack Proxy

Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Online Help

Standard mode

Sites

- admin
- bank
- GET:feedback.aspx
- GET:default.aspx(content)
- GET:cgi.exe
- GET:survey_questions.aspx
- GET:style.css
- POST:comment.aspx(cfile,comments)
- GET:disclaimer.htm(url)
- GET:high_yield_investments.htm
- GET:default.aspx(content,job)
- images
- GET:search.aspx(txtSearch)
- GET:inside_points_of_interest.htm
- GET:notfound.aspx(asperrorpath)

Quick Start Request Response Break

Header: Text Body: Text

HTTP/1.1 200 OK
Date: Wed, 10 Jul 2013 00:06:23 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=knffesfulpanvk55megqql45; path=/; HttpOnly
Set-Cookie: amSessionId=1962312505; path=/
Cache-Control: private

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >

<head id="_ctl0_ctl0_head"><title>

Altoro Mutual: Survey

Forced Browse Fuzzer Params Http Sessions WebSockets AJAX Spider Output

History Search Break Points Alerts Active Scan Spider

Site: demo.testfire.net:80 100% Current Scans: 0 | URIs Found: 109

Processed	Method	URI
●	GET	http://demo.testfire.net/
●	GET	http://demo.testfire.net/
●	GET	http://www.ibm.com/
●	GET	http://demo.testfire.net/
●	GET	http://demo.testfire.net/
●	GET	http://demo.testfire.net/
●	GET	http://demo.testfire.net/
●	GET	http://demo.testfire.net/
●	GET	http://demo.testfire.net/

Alerts 1 0 4 1



OWASP Mantra

[Tools](#)[Bookmarks ▾](#)[Download ▾](#)[Support ▾](#)

Tools

Information Gathering

Flagfox Displays a flag icon indicating the current webserver's physical location with many additional features.

JSView Get straight access to scripts and stylesheets included in the current web page.

PassiveRecon Perform passive discovery of target resources utilizing publicly available information.

Wappalyzer Uncovers underlying technologies used on websites like CMS, e-commerce systems, JavaScript frameworks, analytics tools etc..

View Dependencies Shows you all the files which were loaded to show the current page.

Link Sidebar View, search and test hyperlinks in a web page.

Application Auditing

Hackbar Simple security audit / Penetration test tool.

Editors

JSView Get straight access to scripts and stylesheets included in the current web page. View the source code external stylesheets and javascripts.

Firebug Edit, debug, and monitor CSS, HTML, and JavaScript live in any web page.

Proxy

HTTP Fox A built in local proxy for analyzing traffic.

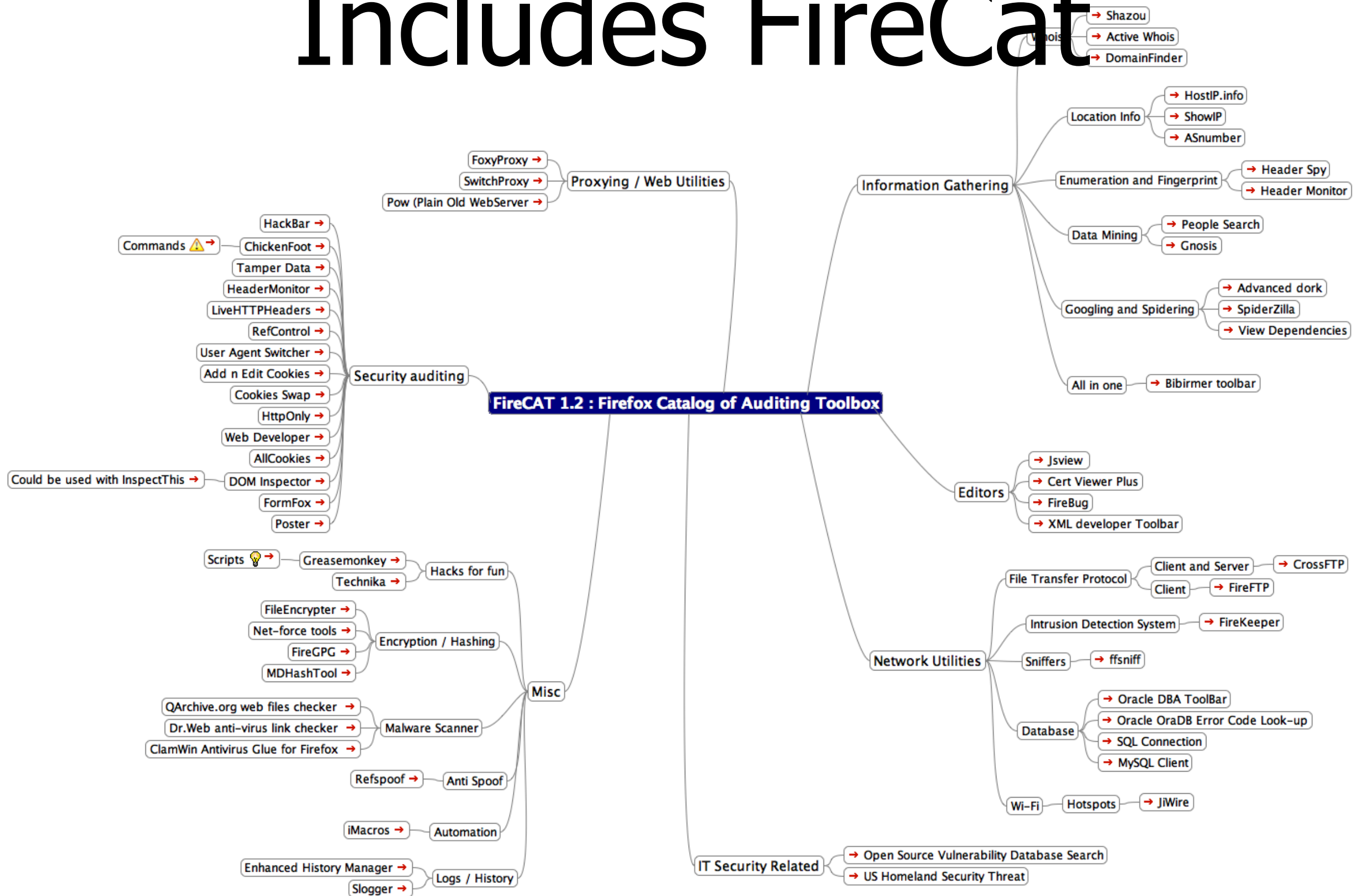
FoxyProxy A proxy management tool with ability to switch between multiple proxies with few clicks.

Proxy Tool A proxy management tool with lots of additional features to enhance the privacy.

Network Utilities

FireFTP FTP/SFTP Client which provides intuitive access to FTP/SFTP servers.

Includes FireCat





OWASP Mantra Start Pag...

06:37:05 PM

Mantra Browser

OWASP Mantra Start Page - OWASP Mantra

File Edit View Tools Help

OWASP Mantra Start Page

about:home

Google

Security Compass Access Me

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

sidebar spoofmark spoof: url=ref

Google Search

Fast. Smart. Safe. Get the mobile browser that's got your back.

Downloads

Bookmarks

History

Add-ons

Sync

Settings

DNS Flusher

Cache

Not in Hosts

mozilla

Many toolbars behave like malware

Remove unwanted toolbars with avast! Browser Cleanup

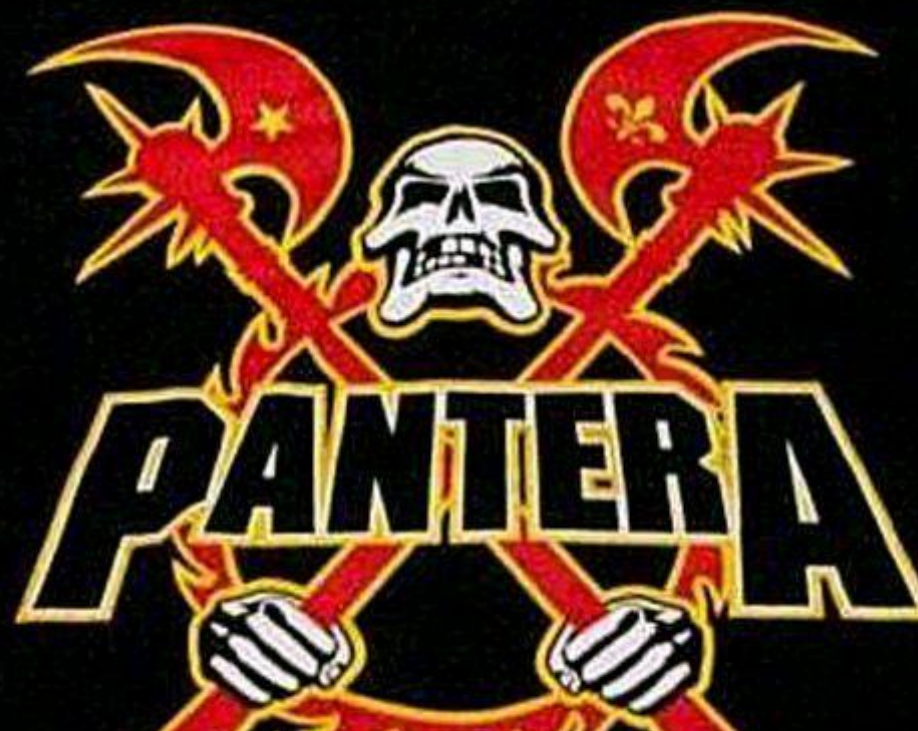


OWASP OWTF

Offensive Web Testing Framework

GASP! VIDEO BREAK!

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



Pantera Web Assessment Studio (WAS) Project: OWASP ASSESSMENT

File

Tools

Modules

Help



Last 7 Requests

>> GET http://www.owasp.org/index.php?title=MediaWiki:Common.css&action=raw&ctype=te...

<< HTTP/1.1 200 OK

[2006-08-18 | 17:46:07] ?

>> GET http://www.owasp.org/index.php?title=MediaWiki:Monobook.css&action=raw&ctype=...

<< HTTP/1.1 200 OK

[2006-08-18 | 17:46:07] ?

>> GET http://www.owasp.org/index.php?title=-&action=raw&gen=css&maxage=18000

<< HTTP/1.1 200 OK

[2006-08-18 | 17:46:07] ?

>> GET http://www.owasp.org/index.php?title=-&action=raw&gen=js

O2 Platform

The screenshot displays the OWASP O2 Platform v5.1.1.1 application window. The title bar indicates the CLR version (4.0) and the process ID (3592). The main menu includes Main, Debug, Compilation Cache(s), and Help. The O2 Platform logo is prominently displayed. On the right, there are configuration options for writing scripts, selecting O2 tools (currently 'Search Engine'), opening the O2 GUI for 'Security Consultants', and selecting 3rd party tools. A 'Find an O2 Script' link is also present.

The Log Viewer window on the left shows a series of log entries, including errors and debug messages. The Util - O2 Available scripts window on the right lists various scripts available for execution, such as Microsoft, MonoCecil, Nikto, NMap, NodeJS, NuGet, OWASP, PaintNet, Qualys, SecurityInnovation, Selenium, Snoop, SoSNet, TeamMentor, TightVNC, Veracode, and _Installers. A filter box is located at the bottom of the script list, and buttons for 'invoke selected script' and 'open log viewer' are visible.

Log Viewer

```
[2:08:23 PM] ERROR: in CSharp_FastCompiler.compileSourceCode, pr
[2:08:23 PM] DEBUG: [findFileOnLocalScriptFolder]in CompileEngine, c
[2:08:23 PM] INFO: Resource file already existed, so skipping it: C:\Tod
[2:08:23 PM] INFO: Resource file already existed, so skipping it: C:\Tod
[2:08:23 PM] INFO: in clearLocalScriptFileMappings
[2:08:23 PM] INFO: Setting CurrentScript to:: Search Engine Tool.h2
[2:08:23 PM] DEBUG: itemToExecute: Search Engine Tool.h2
[2:08:23 PM] INFO: in clearLocalScriptFileMappings
[2:08:23 PM] DEBUG: [findFileOnLocalScriptFolder]in CompileEngine, c
[2:08:23 PM] INFO: Resource file already existed, so skipping it: C:\Tod
[2:08:23 PM] INFO: Resource file already existed, so skipping it: C:\Tod
[2:08:23 PM] INFO: executing script mapped to 'Search Engine: Search
[2:07:55 PM] INFO: Trying to fetch assembly from O2's GitHub repositor
[2:07:55 PM] INFO: could not load/find assembly ('ICSharpCode.Avalon
[2:07:55 PM] ERROR: [tryToResolveReferencesForCompilation] failed t
[2:07:55 PM] INFO: could not load/find assembly ('Microsoft.Windows.S
[2:07:55 PM] DEBUG: We are currently offline, skipping the check
[2:07:29 PM] INFO: Trying to fetch assembly from O2's GitHub repositor
[2:07:29 PM] INFO: could not load/find assembly ('Microsoft.Windows.S
[2:07:29 PM] ERROR: [tryToResolveReferencesForCompilation] failed t
[2:07:29 PM] INFO: could not load/find assembly ('RibbonControlsLibrar
[2:07:29 PM] INFO: could not load/find assembly ('RibbonControlsLibrar
[2:07:29 PM] ERROR: [tryToResolveReferencesForCompilation] failed t
[2:07:29 PM] INFO: could not load/find assembly ('System.Web.dll')
[2:07:29 PM] INFO: could not load/find assembly ('System.Web.dll')
[2:07:29 PM] DEBUG: mapReferencesIncludedInSourceCode in 0s:27r
[2:07:29 PM] DEBUG: There are 27 referencedAssemblies used
```

Util - O2 Available scripts

- Microsoft
- MonoCecil
- Nikto
- NMap
- NodeJS
- NuGet
- OWASP
- PaintNet
- Qualys
- SecurityInnovation
- Selenium
 - API_Selenium.cs
 - PoC - Selenium - Gui with 3 Hijacked Browser Windows.h2
 - SeleniumWebDrivers_Setup.cs
 - Selenium_Installer.cs
- Snoop
- SoSNet
- TeamMentor
- TightVNC
- Veracode
- _Installers
- APIs
- Languages
- Utils

filter

[invoke selected script](#) [open log viewer](#)

☐ Run with no UAC) ☐ Start new Process

O2 Platform

NO
MORE



WITH
SECURITY FINDINGS



PLATFORM

PROBLEM:

BlackBox: Easily create XSS PoCs that are specific to the application and are much more than the ALERT pop-up box that nobody outside the WebAppSecurity space understands its implication

SOLUTION:

O2 :)

Warning:
Tangent

WARNING: TANGENT

- Jon McCoy @ SecTor 2012
- <video excerpt>





Swiss Army Knives

- OWASP Mantra OS (Mobile: MobiSec)
- Samurai Web Testing Framework

Alternatives:

- Kali (aka BackTrack)
 - Fedora Security Spin
- 

Incubators and More

- iSABEL Proxy Server, NAXSI, WAF Project
- Xenotix XSS Framework vs. XSSer, X5s
- Security Tools for Developers
- Java HTML Sanitizer (released)
- S.T.I.N.G. For Security Requirements?
- VaultDB vs Scytale (DBMS crypto-proxies)

Project Gaps?

- Lots of duplication; re-inventing the wheel
- Inconsistent Quality, no unity in delivery
- No visualization projects; forensics a stub
- Fragmentation; resources spread thin
- Over-promising; under-delivering
- Solutions?

Google Summer of Code 2013

Select program: GSoC 2013 (...

ACCEPTED PROJECTS

List of projects accepted into Google Summer of Code 2013

<input type="checkbox"/> RegExp Search <input type="button" value="CSV Export"/>		
Student	Title	Organization
		owasp
Abdelhadi	ZAP Proxy : CMS Scanner	OWASP
Alessandro Fano González	OWASP OWTF - Unit Test Framework	OWASP
Ankush Jindal	OWASP OWTF - Multiprocessing	OWASP
Assem Chelli	OWASP OWTF - Reporting	OWASP
Bharadwaj Machiraju	OWASP OWTF - INBOUND PROXY WITH MIT	OWASP
Cosmin Stefan	Enhanced HTTP Session Handling and users	OWASP
Daniel Kvist	Plugin api and plugin actions interface in C	OWASP
Mihai Pitu	OWASP ModSecurity CRS - Port to Java	OWASP
Pulasthi Mahawithana	OWASP ZAP - SAML 2.0 Support	OWASP
Rahul Chaudhary	OWASP PHP Security Project	OWASP
Rauf Butt	ZAP - Exploring Advanced reporting using	OWASP
<input type="button" value="Filter"/> <input type="button" value="Refresh"/> <input type="button" value="Columns"/> <input type="button" value="Page 1 of 1"/> <input type="button" value="View 1 - 11 of 11"/>		

Go, Toronto, Go!

Due to Seattle	\$2268.58
Due to Serbia	\$20
Due to Singapore	\$55
Due to Slovakia	\$20
Due to Slovenia	\$95.8
Due to South Africa	\$40
Due to South Dakota	\$20
Due to South Florida	\$180
Due to South Korea	\$364
Due to Spain	\$20
Due to Sri Lanka	\$28
Due to St. Louis	\$10
Due to Suncoast	\$126.5
Due to Sweden	\$10147.44
Due to Switzerland	\$6811.39
Due to Sydney	\$636
Due to Tampa	\$2260
Due to Thailand	\$76
Due to Tokyo	\$20
Due to Toronto	\$1090.93
Due to Tucson	\$40
Due to Turkey	\$185
Due to United Arab Emirates	\$60
Due to Uruguay	\$618.57
Due to Vancouver	\$200
Due to Venezuela	\$116
Due to Vermont	\$40
Due to Virginia	\$9077.19
Due to Washington DC	\$4905.08
Due to Ypisilanti	\$20
Total Due to Chapters:	\$222133.06

- Chapter participation appears to be on the rise
- Tremendous amount of infosec talent in the GTA and surrounding areas
- IRC? Reddit? Hackernews?
- Anyone need an opening act next time?



Q & A

Bookmark: <http://owasp.blogspot.ca/>



Thank you



THE PERFECT MARTINI

1. Pour gin, vermouth, and olives into the trash where they belong.
2. Drink whiskey

I always keep a supply of stimulant handy in case I see a snake--which I also keep handy.

W. C. Fields (1880 - 1946)

Toothpaste For Dinner.com

