

Gentle Introduction to Security Testing for Testers

Walter Kruse

2016-09-16
(updated 2017-05-23)

Introduction

- Currently technical testing at SARS
- 17 Years in software testing
- Made a career of technical testing
- Past author for trade publication, speaker, trainer



Agenda

- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources

Agenda

- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources

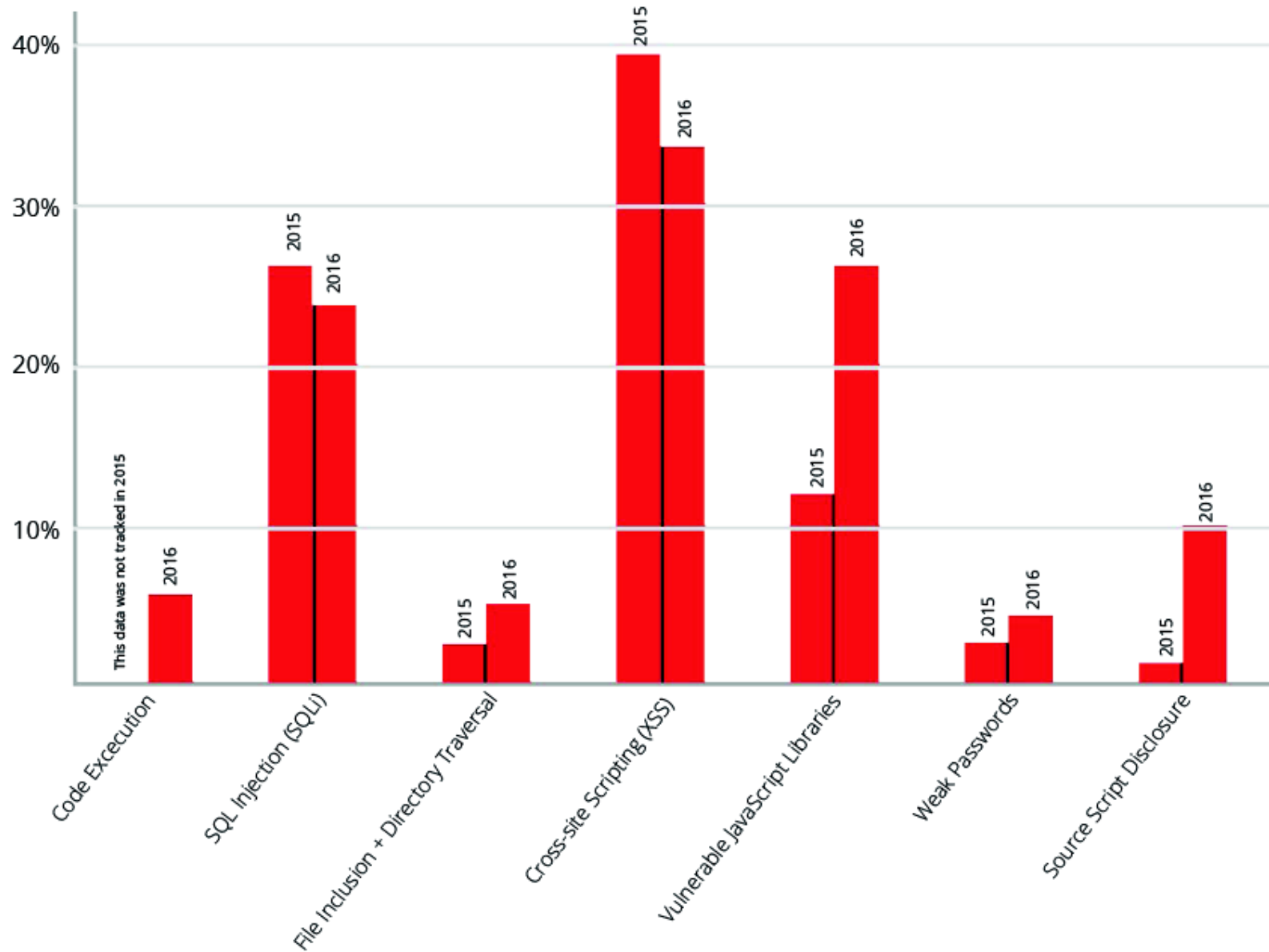
Positioning Security Testing

- Functional testing
- Non-functional testing
 - Performance testing
 - *Security testing*
 - Usability testing
- Security testing has manual and automated components
- Even manual security testing uses tools

Agenda

- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources

Vulnerabilities by Type - High Severity



Application security exposes businesses

By [Admire Moyo](#), ITWeb's senior news journalist.
Johannesburg, 18 May 2016

Businesses are falling victim to breaches mostly because they are neglecting application security.

That was the word from Helen Bravo, head of product management at Israeli-based cyber security firm Checkmarx, speaking yesterday at ITWeb Security Summit 2016.

Citing a Gartner report, Bravo said 80% of successful cyber security attacks target the application layer. She added that according to the Web Application Security Consortium, 86% of the organisations surveyed were found to have medium or higher severity **vulnerabilities** on their application layer.

"In a recent survey of chief information security officers, when asked about what are the main areas of **risks** in their organisations, 51% pointed to application security, followed by 36% who said **infrastructure** security," said Bravo.

She noted that the main reason why the application layer is left so vulnerable in most organisations is because most of these companies lack secure coding knowledge.



Most organisations lack secure coding knowledge, says Helen Bravo, head of product management at Checkmarx.


ARMSCOR

Armaments Corporation of South Africa SOC Ltd

Gateway to defence solutions

ARMSCOR SYSTEM

INFORMATION

ALLOWANCES

Invoices

Per Order

Per Supplier

Individual Invoices

Outstanding Balances

Payments

Last RCB Date

Specific RCB Date

Current Month

Last Two Months

Last Three Months

ORDER NUMBER
INVOICE NUMBER
INVOICE AMOUNT
INVOICE BALANCE
INVOICE DATE
DATE RECEIVED
CHEQUE NUMBER
CHEQUE DATE

12345678

INV001234

R 100,000.00

R 0.00

15/01/2014

20/01/2014

0

Not Paid

12345678

INV001234

R 300,000.00

R 0.00

15/01/2014

20/01/2014

0

Not Paid

12345678

INV001234

R 1,500,000.00

R 0.00

15/01/2014

20/01/2014

0

Not Paid

Page 2 of 2

PREV

PRINT ALL



Agenda

- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources

Threats

- Identity theft and fraud
 - Social engineering: Phishing, SpearPhishing, Whaling, Pharming, Shmising, Vishing
- Insecure infrastructure
 - Every node that is accessible from the internet
 - IoT !
- Insecure applications
 - OWASP Top 10
 - SANS Top 20

Agenda

- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources

Significance of threats

- Law: POPI Act
 - Lawful processing of personal information
 - If any information is compromised, the liability remains with the organization
- Compliance: King III (code of corporate governance)
 - Key principle: The requirement for effective auditing
- Standard: ISO/IEC 27002
 - Section 12 discusses software development
- Standard: Payment Card Industry Data Security Standard (PCI-DSS)

What do we do about it ?

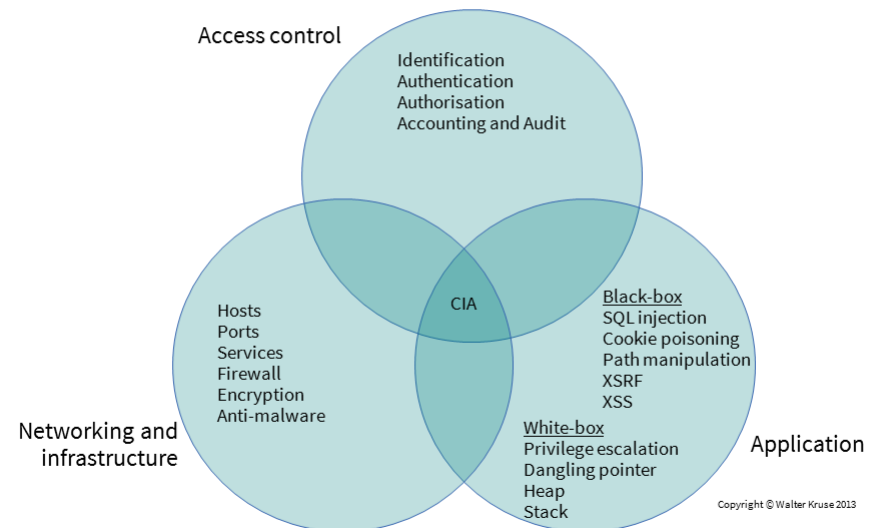


Agenda

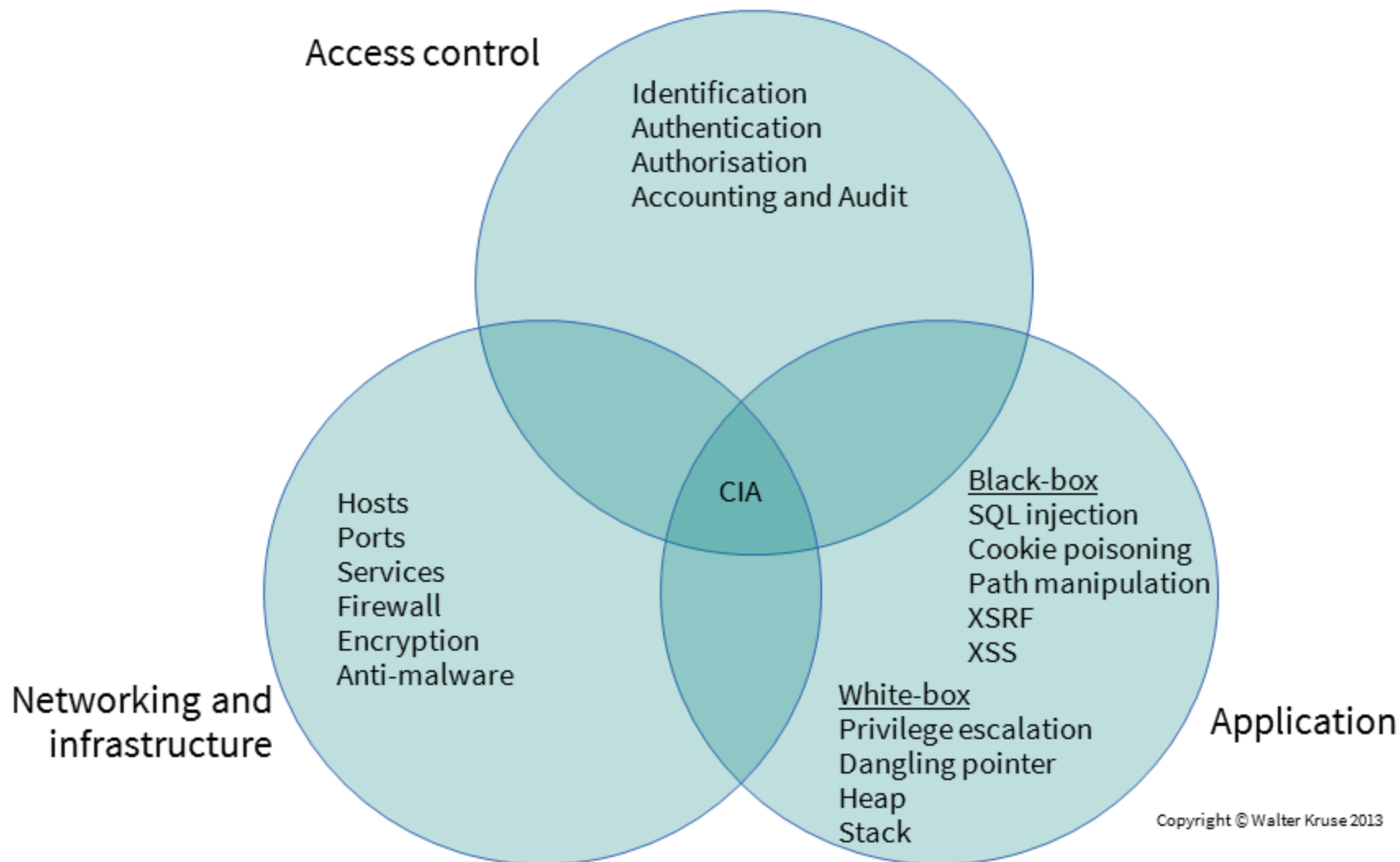
- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources

Security Testing Overview

- CIA Triad
 - Confidentiality
 - Integrity
 - Availability
- Security is:
 - Protection
 - Detection
 - Response

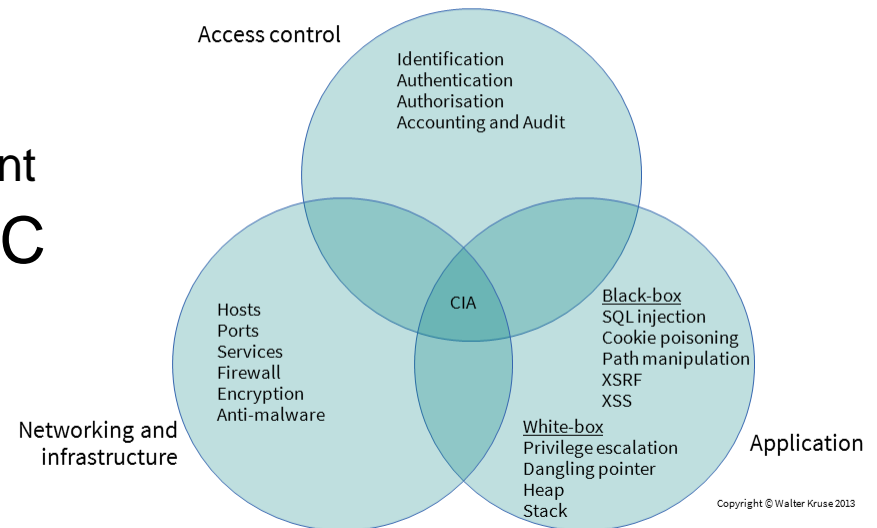


Security Testing Overview



Security Testing Overview

- Audit
 - Formal
- Vulnerability Assessment
 - Prep for audit
- Penetration testing
 - On-going in some orgs.
 - Questionable value:
 - Big report
 - Test if a hole is closed
 - Prep for vulnerability assessment
- Security testing in the SDLC
 - Should be standardised
 - Enterprise tools



Access Control

Access control

Identification
Authentication
Authorisation
Accounting and Audit

CIA

Hosts
Ports
Services
Firewall
Encryption
Anti-malware

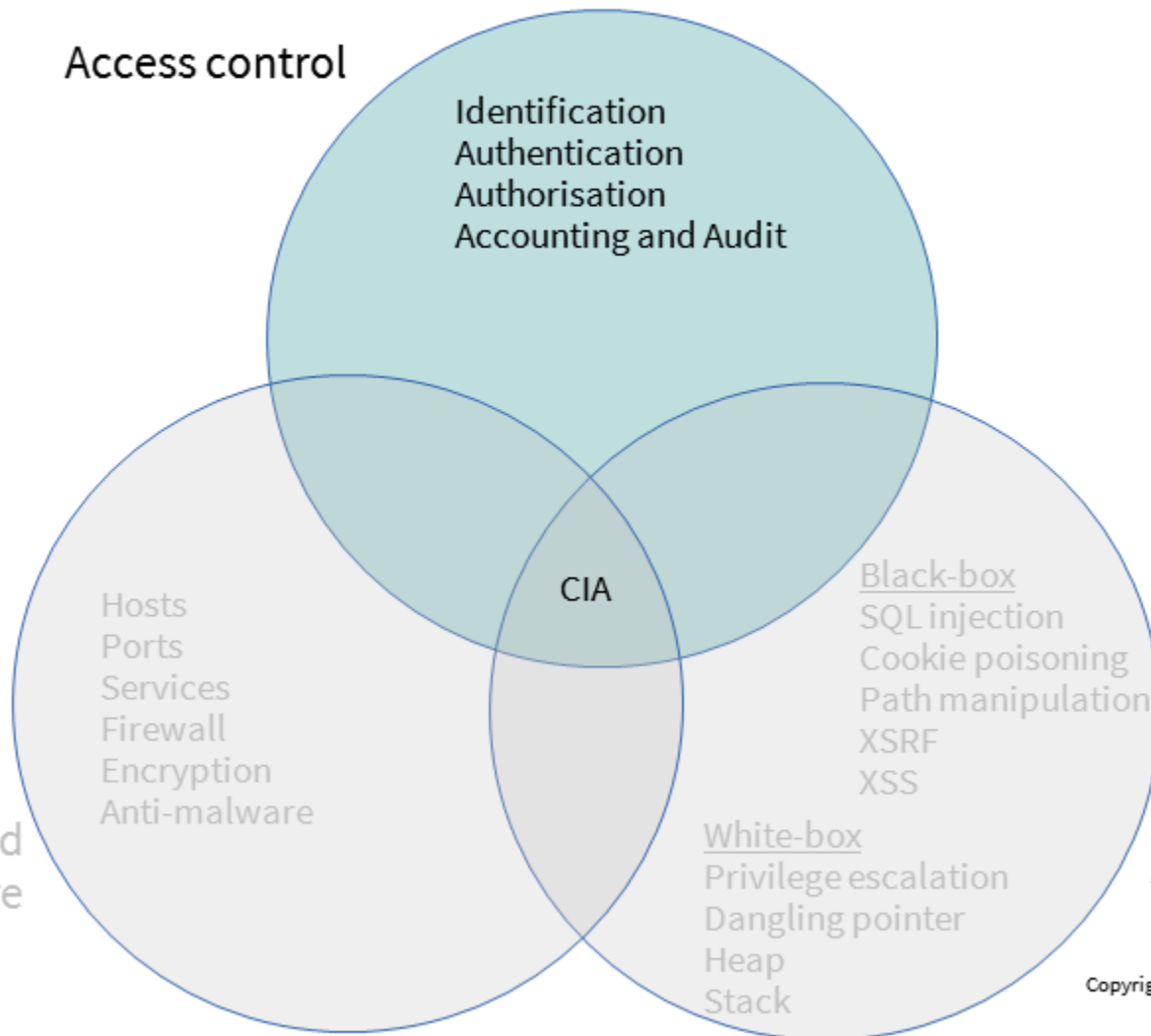
Networking and
infrastructure

Black-box
SQL injection
Cookie poisoning
Path manipulation
XSRF
XSS

White-box
Privilege escalation
Dangling pointer
Heap
Stack

Application

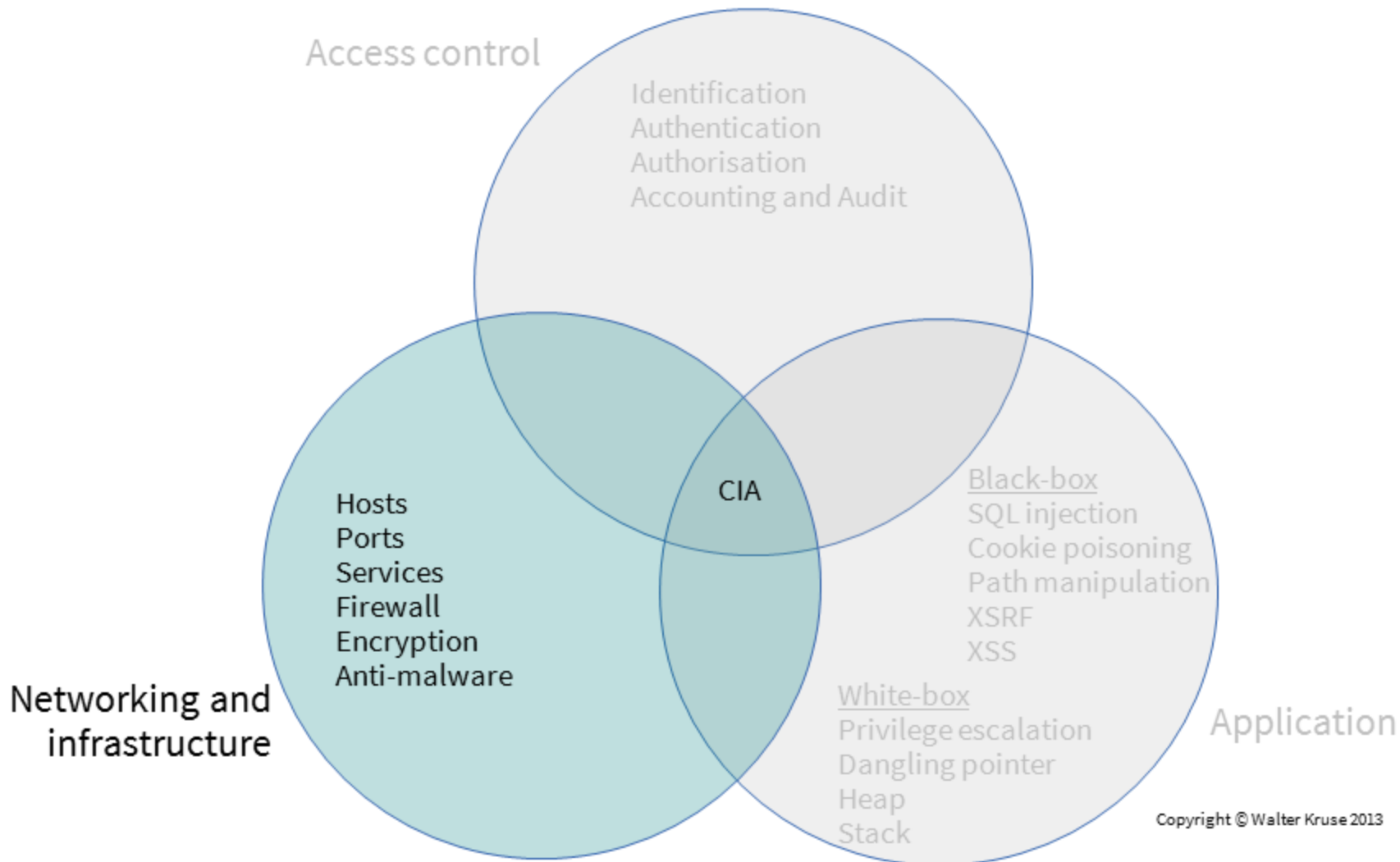
Copyright © Walter Kruse 2013



Agenda

- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources

Network Scanning Demo



Network Scanning Demo

- NMap: Fundamental port scanning
- OpenVAS: Open source network audit scanner
- Conceptual walkthrough of vulnerability finding
 - **Attacker's** perspective
 - **Defender's** perspective

Network Scanning Demo

- NMap: Fundamental port scanning
- OpenVAS: Open source network audit scanner
- Conceptual walkthrough of vulnerability finding
 - Attacker's perspective
 - Defender's perspective





Zenmap (as superuser)

ScanToolsProfileHelp

Target: 192.168.0.3Profile: Quick scan plusScanCancel

Command: nmap -sV -T4 -O -F --version-light 192.168.0.3

HostsServices

OS	Host
	tintin.ou-ryperd.net (192.168.0.190)
	snowy.ou-ryperd.net (192.168.0.191)
	blackbeard.ou-ryperd.net (192.168.0.192)
	192.168.0.190

Filter Hosts

Nmap OutputPorts / HostsTopologyHost DetailsScans

nmap -sV -T4 -O -F --version-light 192.168.0.190Details

Nmap scan report for **192.168.0.190**

Host is up (0.014s latency).

Not shown: 91 closed ports

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 3.9p1 (protocol 2.0)
80/tcp	open	http	Apache Advanced Extranet Server httpd 2.0.53 (mod_ssl/2.0.53 OpenSSL/0.9.7e PHP/4.3.10 mod_perl/1.999.21 Perl/v5.8.6)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: MDKGROUP)
443/tcp	open	ssl/http	Apache Advanced Extranet Server httpd 2.0.53 (mod_ssl/2.0.53 OpenSSL/0.9.7e PHP/4.3.10 mod_perl/1.999.21 Perl/v5.8.6)
445/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: MDKGROUP)
2049/tcp	open	nfs	2-4 (RPC #100003)
6000/tcp	open	X11	(access denied)
32768/tcp	open	nlockmgr	1-4 (RPC #100021)

MAC Address: E8:DE:27:A6:64:A6 (Tp-link Technologies Co.)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.8 - 2.6.12

Network Distance: 1 hop

Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 17.71 seconds





Network Scanning Demo

- NMap: Fundamental port scanning
- OpenVAS: Open source network audit scanner
- Conceptual walkthrough of vulnerability finding
 - Attacker's perspective
 - Defender's perspective

OpenVAS-Client

FileViewTaskScopeReportExtrasHelp

?

+

⊘

🔌

🔌

⚙️

Name	High	Medium
Global Settings	🔑	
▼ Task1		
▶ localhost	🔑	
▼ wlan	🔑	
Report 20160828-032122	11	20

Report for scope: wlan (Task: Task1)

CommentsOptionsReport

Host/Port/Severity

▶ 192.168.0.1

▼ 192.168.0.190

▶ microsoft-ds (445/tcp)

▼ http (80/tcp)

🚫 Security Hole

⚠️ Security Warning

💡 Security Note

🖋 Log Message

▶ ⚠️ ssh (22/tcp)

▶ ⚠️ netbios-ns (137/udp)

▶ 💡 x11 (6000/tcp)

▶ 💡 unknown (987/tcp)

▶ 💡 unknown (984/udp)

▶ 💡 unknown (796/udp)

▶ 💡 sunrpc (111/udp)

▶ 💡 sunrpc (111/tcp)

▶ 💡 nfs (2049/udp)

▶ 💡 nfs (2049/tcp)

▶ 💡 netbios-ssn (139/tcp)

▶ 💡 https (443/tcp)

▶ 💡 general/tcp

server.

Impact Level: Application

Affected Software/OS:
PHP version 4.4.4 and prior
PHP 5.1.x to 5.1.6
PHP 5.2.x to 5.2.5

Fix: No solution or patch is available as on 17th March, 2009. Information regarding this issue will be updated once the solution details are available. For updates refer, <http://www.php.net>

References:
<http://bugs.php.net/bug.php?id=27421>
https://bugzilla.redhat.com/show_bug.cgi?id=479272

CVSS Score:
CVSS Base Score : 2.1 (AV:L/AC:L/Au:NR/C:N/I:P/A:N)
CVSS Temporal Score : 1.9
Risk factor : Low
CVE : CVE-2009-0754
BID : 33542

=====

Reported by NVT "PHP < 5.2.13 Multiple Vulnerabilities" (1.3.6.1.4.1.256)

Overview:
The remote web server has installed a PHP Version which is prone to Multiple Vulnerabilities.

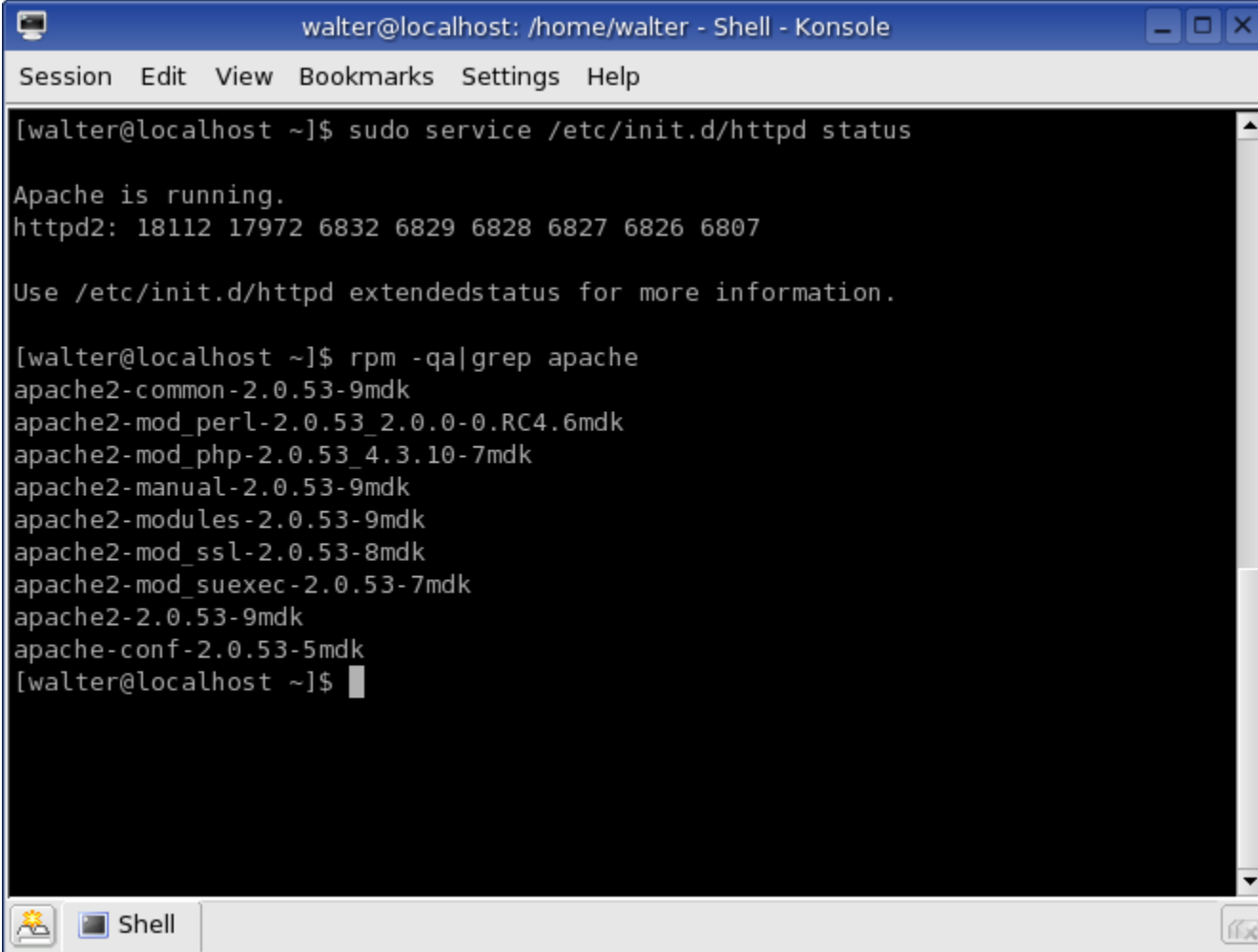
Scan took place from Sat Aug 27 22:36:44 2016 to Sun Aug 28 03:21:22 2016

not connected

Network Scanning Demo

- NMap: Fundamental port scanning
- OpenVAS: Open source network audit scanner
- Conceptual walkthrough of vulnerability finding
 - **Attacker's** perspective
 - **Defender's** perspective

1: An old version of apache



A terminal window titled "walter@localhost: /home/walter - Shell - Konsole" with a menu bar (Session, Edit, View, Bookmarks, Settings, Help). The terminal shows the following commands and output:

```
[walter@localhost ~]$ sudo service /etc/init.d/httpd status

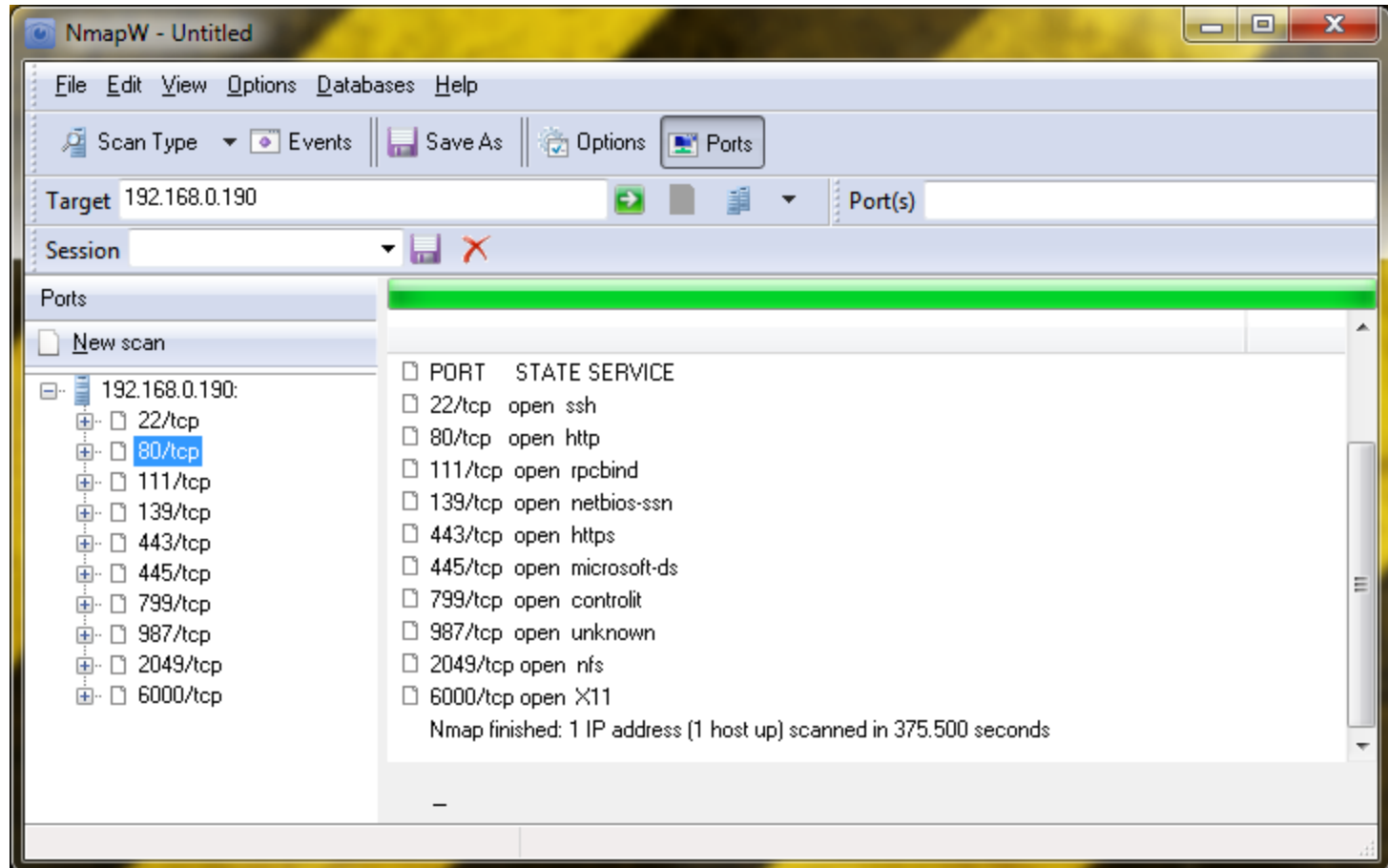
Apache is running.
httpd2: 18112 17972 6832 6829 6828 6827 6826 6807

Use /etc/init.d/httpd extendedstatus for more information.

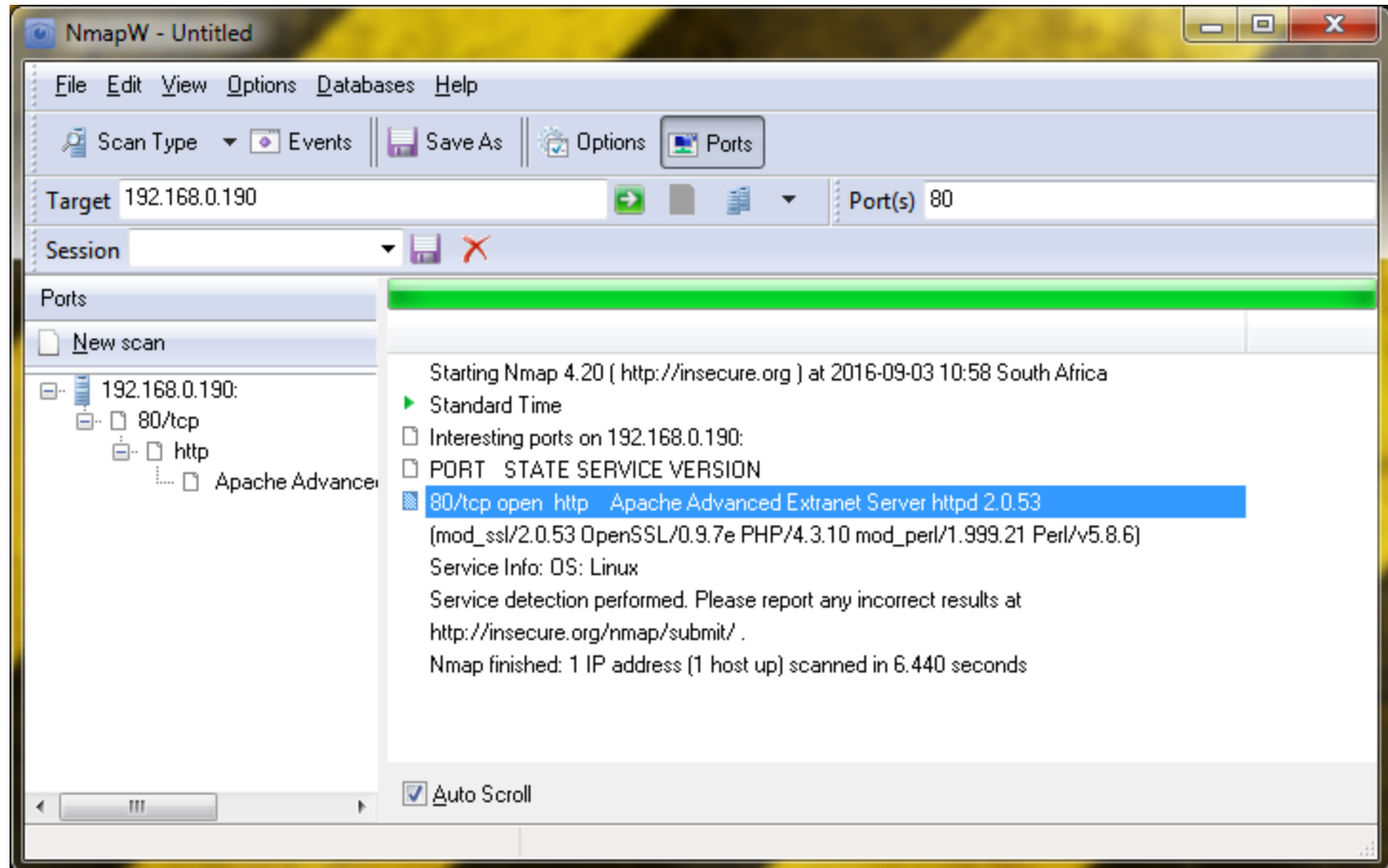
[walter@localhost ~]$ rpm -qa|grep apache
apache2-common-2.0.53-9mdk
apache2-mod_perl-2.0.53_2.0.0-0.RC4.6mdk
apache2-mod_php-2.0.53_4.3.10-7mdk
apache2-manual-2.0.53-9mdk
apache2-modules-2.0.53-9mdk
apache2-mod_ssl-2.0.53-8mdk
apache2-mod_suexec-2.0.53-7mdk
apache2-2.0.53-9mdk
apache-conf-2.0.53-5mdk
[walter@localhost ~]$
```

The terminal window has a status bar at the bottom with a gear icon, a "Shell" tab, and a close button.

2: **Attacker** finds open ports



3: **Attacker** scans port 80



4: **Attacker** finds vulns on CVE

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search

[View CVE](#)

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

Vulnerability Feeds & Widgets^{New}

www.itsecdb.com

[Home](#)

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

[Microsoft Bulletins](#)

Bugtraq Entries

CWE Definitions

[About & Contact](#)

— — —

[Apache](#) » [Http Server](#) » [2.0.53](#) : Security Vulnerabilities

Cpe Name: *cpe:/a:apache:http_server:2.0.53*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-0098	20		DoS	2014-03-18	2016-07-08	5.0	None	Remote	Low	Not required	None	None	Partial
The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.														
2	CVE-2013-6438	20		DoS	2014-03-18	2016-06-16	5.0	None	Remote	Low	Not required	None	None	Partial
The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.														
3	CVE-2013-2249				2013-07-23	2016-04-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.														
4	CVE-2012-0883	264		+Priv	2012-04-18	2013-09-17	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.														
5	CVE-2012-0031	399		DoS	2012-01-18	2013-10-10	4.6	None	Local	Low	Not required	Partial	Partial	Partial
scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.														

5: Attacker looks for an exploit

Search:

☒ Search content ☐ Search author

☐ Search in description

Category: Platform:

Price from: Price to:

Author login: CVE:

The minimum length of a search query is 3 symbols

Search results for exploits with selected filters

[remote exploits]

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
13-08-2016	FreePBX 13 / 14 Remote Command Execution Exploit	php	108		R	D	-	✓	free	pgt
22-01-2016	Tata Docomo Leak User details + Live Remote Access Exploit	php	1,534		R	D	-	✓	1 000	BadBoy17
19-12-2015	Joomla 1.5 - 3.4.5 - HTTP Header Unauthenticated Remote Code Execution Exploit	php	1,442		R	D	C	✓	free	metasploit
08-12-2015	phpFileManager 0.9.8 Remote Code Execution Exploit	php	999		R	D	-	✓	free	metasploit
02-11-2015	PHP yaml_parse_url Double Free Vulnerability	php	1,035		R	D	-	✓	free	John Leitch
02-11-2015	PHP yaml_parse_url Unsafe Deserialization Vulnerability	php	644		R	D	-	✓	free	John Leitch
27-10-2015	Th3 MMA mma.php Backdoor Arbitrary File Upload Exploit	php	743		R	D	-	✓	free	metasploit
22-10-2015	The World Browser 3.0 Final - Remote Code Execution Exploit	php	346		R	D	C	✓	free	Ehsan Noreddini
21-10-2015	Zpanel Remote Unauthenticated Remote Code Execute Exploit	php	579		R	D	C	✓	free	metasploit
19-10-2015	Nibbleblog File Upload Vulnerability	php	410		R	D	-	✓	free	metasploit
29-09-2015	WordPress 4.0 Directory Traversal Exploit 0day	php	4,478		R	D	-	✓	500	lulz0day
16-09-2015	Bolt CMS File Upload Vulnerability	php	1,085		R	D	-	✓	free	metasploit
10-08-2015	PHP SplDoublyLinkedList Use-After-Free Exploit	php	806		R	D	-	✓	free	Taoguang Chen
10-08-2015	PHP SplObjectStorage Use-After-Free Exploit	php	611		R	D	-	✓	free	Taoguang Chen
10-08-2015	PHP SPL ArrayObject Use-After-Free Exploit	php	601		R	D	-	✓	free	Taoguang Chen
08-05-2015	Wordpress RevSlider File Upload and Execute Vulnerability	php	4,054		R	D	-	✓	free	metasploit
25-04-2015	WordPress WPshop eCommerce 1.3.9.5 Shell Upload Exploit	php	4,349		R	D	-	✓	free	metasploit
25-04-2015	WordPress InBoundio Marketing 2.0 Shell Upload Exploit	php	2,569		R	D	-	✓	free	metasploit
20-04-2015	WordPress SlideShow Gallery Authenticated File Upload Exploit	php	2,958		R	D	C	✓	free	Jesus Ramirez
19-04-2015	Wordpress Work-The-Flow Plugin 2.5.2 Upload Exploit	php	2,490		R	D	-	✓	free	metasploit

[local exploits]

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
05-10-2015	PHP 5.6.13 Uninitialized pointer in phar_make_dirstream Vulnerability	php	852		R	D	-	✓	free	hugh
05-10-2015	PHP 5.6.13 phar_get_fp_offset() Null pointer dereference Vulnerability	php	940		R	D	-	✓	free	emmanuel
06-11-2014	ManageEngine EventLog Analyzer SQL / Credential Disclosure	php	1,610		R	D	C	✓	free	Pedro Ribeiro
26-04-2014	GeoCore MAX DB 7.3.3 Blind SQL Injection Vulnerability	php	1,873		R	D	-	✓	free	Esac

6: Defender scans server

The screenshot displays the Defender application window. The menu bar includes File, View, Task, Scope, Report, Extras, and Help. The left sidebar shows a tree view with 'Global Settings', 'scan', 'one', and 'mdk'. The 'mdk' folder is selected, showing a report for '20160813-065124'. The main pane is titled 'Report for scope: mdk (Task: scan)' and has tabs for 'Comments', 'Options', and 'Report'. The 'Report' tab is active, showing a list of 'Host/Port/Severity' on the left and detailed information on the right. The list includes '192.168.0.190', 'microsoft-ds (445/tcp)', 'http (80/tcp)', and a 'Security Hole'. The detailed information for the 'Security Hole' includes the 'Impact Level: Application', 'Affected Software/OS' (PHP versions), a 'Fix' description, 'References', 'CVSS Score' (Base: 2.1, Temporal: 1.9, Risk factor: Low), 'CVE: CVE-2009-0754', and 'BID: 33542'. The report also mentions 'Reported by NVT "PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability" (1.3.6.1.4.1.' and an 'Overview' section. The status bar at the bottom indicates 'not connected'.

File View Task Scope Report Extras Help

Report for scope: mdk (Task: scan)

Comments Options Report

Name

Global Settings

scan

one

mdk

Report 20160813-065124

Host/Port/Severity

- 192.168.0.190
 - microsoft-ds (445/tcp)
 - http (80/tcp)
 - Security Hole
 - Security Warning
 - Security Note
 - Log Message
 - ssh (22/tcp)
 - netbios-ns (137/udp)
 - x11 (6000/tcp)
 - unknown (987/tcp)
 - unknown (984/udp)
 - unknown (796/udp)
 - sunrpc (111/udp)
 - sunrpc (111/tcp)
 - nfs (2049/udp)
 - nfs (2049/tcp)
 - netbios-ssn (139/tcp)
 - https (443/tcp)
 - general/tcp
 - general/icmp
 - general/SMBClient

Impact Level: Application

Affected Software/OS:
PHP version 4.4.4 and prior
PHP 5.1.x to 5.1.6
PHP 5.2.x to 5.2.5

Fix: No solution or patch is available as on 17th March, 2009. Information regarding this issue will be updated once the solution details are available. For updates refer, <http://www.php.net>

References:
<http://bugs.php.net/bug.php?id=27421>
https://bugzilla.redhat.com/show_bug.cgi?id=479272

CVSS Score:
CVSS Base Score : 2.1 (AV:L/AC:L/Au:NR/C:N/I:P/A:N)
CVSS Temporal Score : 1.9
Risk factor : Low
CVE : **CVE-2009-0754**
BID : 33542

Reported by NVT "PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability" (1.3.6.1.4.1.

Overview:
PHP is prone to a vulnerability that an attacker could exploit to execute arbitrary code with the privileges of the user running the affected application. Successful exploits will compromise the application and possibly the computer.

Scan took place from Sat Aug 13 06:44:08 2016 to Sat Aug 13 06:51:24 2016

not connected

7: Defender looks up details

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#) [AddThis](#)

Vulnerability Feeds & Widgets^{New} www.itsecdb.com

[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

Vulnerability Details : [CVE-2009-0754](#)

PHP 4.4.4, 5.1.6, and other versions, when running on Apache, allows local users to modify behavior of other sites hosted on the same web server by modifying the mbstring.func_overload setting within .htaccess, which causes this setting to be applied to other virtual hosts on the same server.

Publish Date : 2009-03-03 Last Update Date : 2010-08-21

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	2.1
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	134

8: Defender finds remediation



[English](#) | [\[\]](#)

About: Dedicated | Advanced | Standard | Recurring | No Risk | Desktop | Basic | Single | Sec
Price/Feature Summary | Order | New Vulnerabilities | Confidentiality | Vulnerability Search

Vulnerability Search

☐ Tests ☐ CVE ☒ All

Test ID: 63483

Category: Mandrake Local Security Checks

Title: Mandrake Security Advisory MDVSA-2009:066 (php)

Summary: Mandrake Security Advisory MDVSA-2009:066 (php)

Description: Description:

The remote host is missing an update to php announced via advisory MDVSA-2009:066.

PHP 4.4.4, 5.1.6, and other versions, when running on Apache, allows local users to modify behavior of other sites hosted on the same web server by modifying the mbstring.func_overload setting within .htaccess, which causes this setting to be applied to other virtual hosts on the same server (CVE-2009-0754).

The updated packages have been patched to correct these issues.

Affected: 2008.0, 2008.1, 2009.0, Corporate 4.0

Solution:

To upgrade automatically use MandrakeUpdate or urpmi. The verification of md5 checksums and GPG signatures is performed automatically for you.

<http://www.securityspace.com/smysecure/catid.html?in=MDVSA-2009:066>



← By Date →

← By Thread →

Search

CVE-2016-6662 - MySQL Remote Root Code Execution / Privilege Escalation (0day)

From: Dawid Golunski <dawid () legalhackers com>

Date: Mon, 12 Sep 2016 06:09:10 -0300

Vulnerability: MySQL Remote Root Code Execution / Privilege Escalation 0day

CVE: CVE-2016-6662

Severity: Critical

Affected MySQL versions (including the latest):

<= 5.7.15

<= 5.6.33

<= 5.5.52

Discovered by:

Dawid Golunski

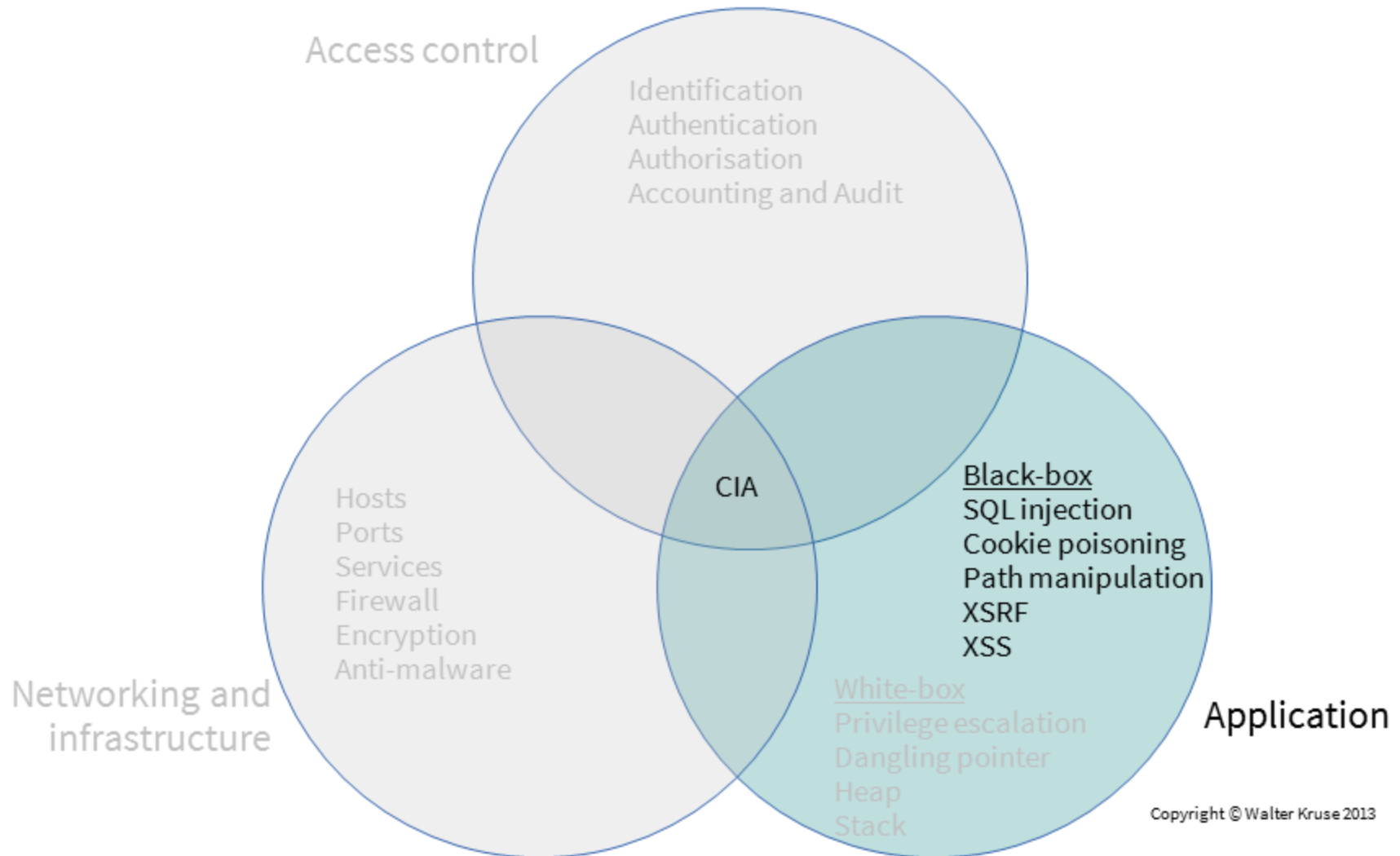
<http://legalhackers.com>

An independent research has revealed multiple severe MySQL vulnerabilities. This advisory focuses on a critical vulnerability with a CVEID of CVE-2016-6662. The vulnerability affects MySQL servers in all version branches (5.7, 5.6, and 5.5) including the latest versions, and could be exploited by both local and remote attackers. Both the authenticated access to MySQL database (via network connection or web interfaces such as phpMyAdmin) and SQL Injection could be used as exploitation vectors.

Successful exploitation could allow attackers to execute arbitrary code with root privileges which would then allow them to fully compromise the server on which an affected version of MySQL is running.

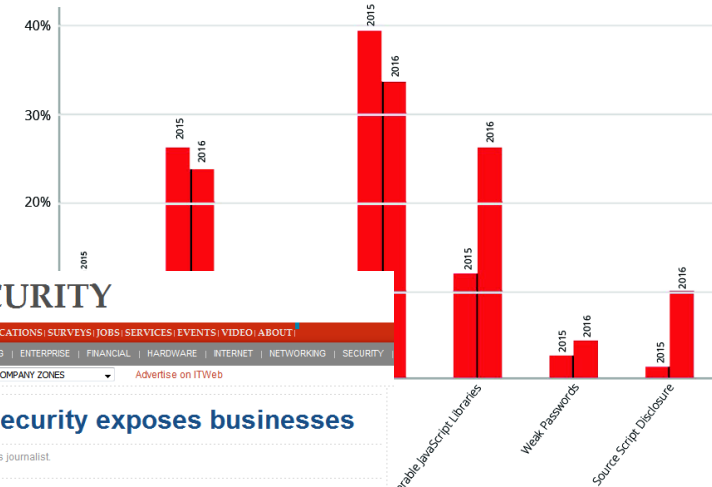
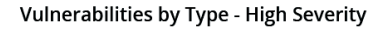
This advisory provides a (limited) Proof-Of-Concept MySQL exploit which demonstrates how Remote Root Code Execution could be achieved by attackers.

Black Box Scanning Demos



Recap: Application Security

- SANS Top 20, OWASP Top 10
 - *Cross-site Request Forgery (XSRF)*
 - *URL, Parameter tampering*
 - *Path, Header manipulation*
 - *Cross-site Scripting (XSS)*
 - *HTTP Response Splitting*
 - *Command Injection*
 - *Cookie poisoning*
 - *Session hijacking*
 - *Open redirects*
 - *SQL Injection*

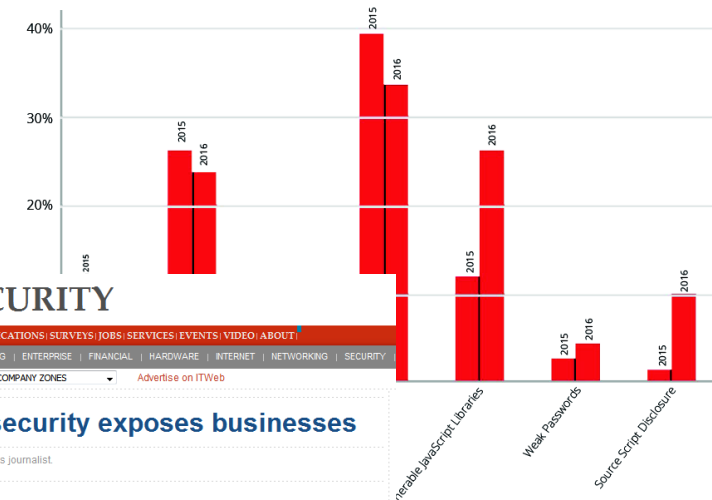


Recap: Application Security

- SANS Top 20, OWASP Top 10

- *Cross-site Request Forgery (XSRF)*
- *URL, Parameter tampering*
- *Path, Header manipulation*
- *Cross-site Scripting (XSS)*
- *HTTP Response Splitting*
- *Command Injection*
- *Cookie poisoning*
- *Session hijacking*
- *Open redirects*
- *SQL Injection*

Vulnerabilities by Type - High Severity



ITWeb SECURITY

HOME | OPINION | IN DEPTH | PUBLICATIONS | SURVEYS | JOBS | SERVICES | EVENTS | VIDEO | ABOUT

BUSINESS | CHANNEL | COMPUTING | ENTERPRISE | FINANCIAL | HARDWARE | INTERNET | NETWORKING | SECURITY

VIRTUAL PRESS OFFICES™ | COMPANY ZONES | Advertise on ITWeb

Application security exposes businesses

By Admire Moyo, ITWeb's senior news journalist
Johannesburg, 18 May 2016

Businesses are falling victim to breaches mostly because they are neglecting application security.

That was the word from Helen Bravo, head of product management at Israeli-based cyber security firm Checkmarx, speaking yesterday at ITWeb Security Summit 2016.

Citing a Gartner report, Bravo said 90% of successful cyber security attacks target the application layer. She added that



Helen Bravo, head of product management at Checkmarx

Most organisations is because most of



Software Error Category: Insecure Interaction Between Components

[1] CWE-79: Failure to Preserve Web Page Structure ('Cross-site Scripting')

Cross-site scripting (XSS) is one of the most prevalent, obstinate, and dangerous vulnerabilities in web applications...If you're not careful, attackers can...[MORE >>](#)

[2] CWE-89: Failure to Preserve SQL Query Structure (aka 'SQL Injection')

If attackers can influence the SQL that you use to communicate with your database, then they can...[MORE >>](#)

[4] CWE-352: Cross-Site Request Forgery (CSRF)

With cross-site request forgery, the attacker gets the victim to activate a request that goes to your site. Thanks to scripting and the way the web works in general, the victim...[MORE >>](#)

[8] CWE-434: Unrestricted Upload of File with Dangerous Type

You may think you're allowing uploads of innocent images...[MORE >>](#)

[9] CWE-78: Failure to Preserve OS Command Structure (aka 'OS Command Injection')

When you invoke another program on the operating system, but you allow untrusted inputs to be fed into the command string that you generate for executing the program, then you are inviting attackers...[MORE >>](#)

[17] CWE-209: Information Exposure Through an Error Message

If you use chatty error messages, then they could disclose secrets to any attacker who dares to misuse your software. The secrets could cover a wide range of valuable data...[MORE >>](#)

[23] CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

While much of the power of the World Wide Web is in sharing and following links between web sites, typically there is...[MORE >>](#)

[25] CWE-362: Race Condition

Attackers will consciously look to exploit race conditions to cause chaos or get your application to cough up something valuable...[MORE >>](#)

Recap: Application Security

- SQL Injection:
 - Maliciously reconstruct parameterised SQL in order to make the system do what it was not intended to

```
SQLquery = "SELECT * FROM Users WHERE UserName = " + UserId;
```

User Name:

```
SELECT * FROM Users WHERE UserName = 'Johnny'
```

User Name:

```
SELECT * FROM Users WHERE UserName = 'Johnny' OR 1 = 1
```

```
SELECT * FROM Users WHERE UserName = TRUE
```

```
SELECT * FROM Users
```

Black Box Scanning Demos

- My own SQL injection testing tool *circ.* 2006
- w3af – open source web application vulnerability scanner

Black Box Scanning Demos

- My own SQL injection testing tool *circ.* 2006
- w3af – open source web application vulnerability scanner

InsecureWebApp - A vulnerable Web application - Mozilla Firefox

File Edit View History Bookmarks Tools Help

InsecureWebApp - A v... +

localhost:8080/insecure/public/index.jsp

Search





☆ 📁 ⬇️ 🏠 😊 🛡️ ☰

AS

American Services

Home Page American Services Corp

> Latest Products

Product Name	Description	Details	Qty Available	Image
Seasonal Product	Seasonal Product	Fall product	0	
First Product	Premier Product	Flagship Product	10	
Second Product	Regular Product	Best Value Product	5	
Third Product	Entry Product	Entry-level product	4	

Search


[Products](#)


[Customer Login](#)

[Instructions](#)

InsecureWebApp

Sponsored By

ISTHMUSGROUP

OWASP
The Open Web
Application Security Project

AS

American Services

- [Products](#)
- [Customer Login](#)

- [Instructions](#)

InsecureWebApp

Sponsored By



> Customer Login

Name :

'1 = 1 -

Password

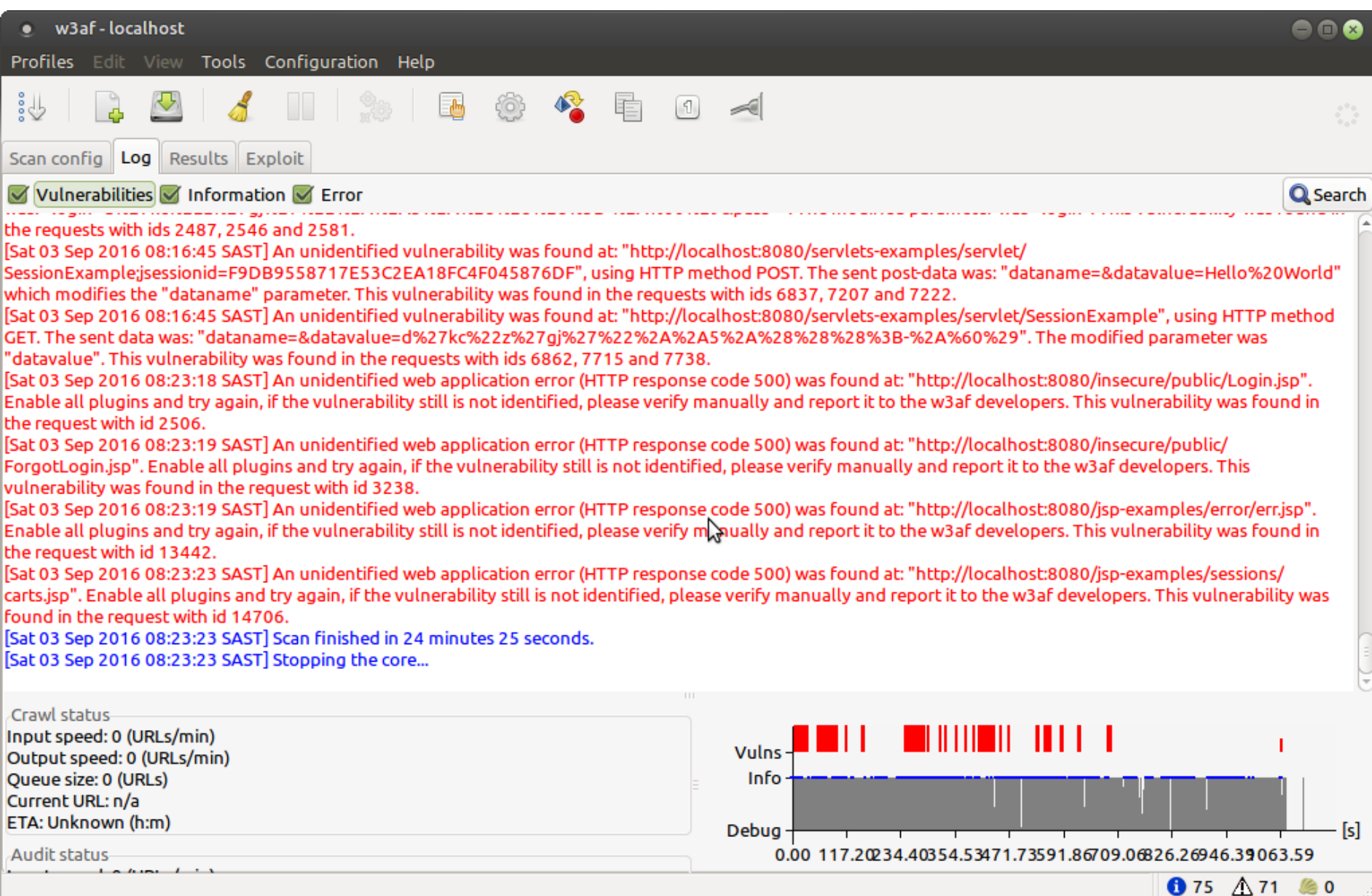
:

Login

[I need a new password](#)

Black Box Scanning Demos

- My own SQL injection testing tool *circ.* 2006
- w3af – open source web application vulnerability scanner



w3af - localhost

ProfilesEditViewToolsConfigurationHelp

Scan configLogResultsExploit

KB BrowserURLsRequest/Response navigator

☒ Vulnerabilities☒ Informations

Knowledge Base

server_header(1)

allowed_methods(1)

dav(1)

user_dir(1)

csrf(1)

blind_sql(1)

blind_sql(1)

Blind SQL injection vulnerability

xss(1)

lfi(1)

generic(1)

error_500(1)

Blind SQL injection was found at: "http://localhost:8080/insecure/public/ForgotLogin.jsp", using HTTP method GET. The injectable parameter is: "email". This vulnerability was found in the requests with ids 3258 to 3259.

Id: 3258

RequestResponse

RawHeaders

GET http://localhost:8080/insecure/public/ForgotLogin.jsp?email=81%27%20OR%20%2781%27%3D%2781 HTTP/1.1

Accept-encoding: gzip, deflate

Accept: /*/*

User-agent: w3af.org

Host: localhost:8080

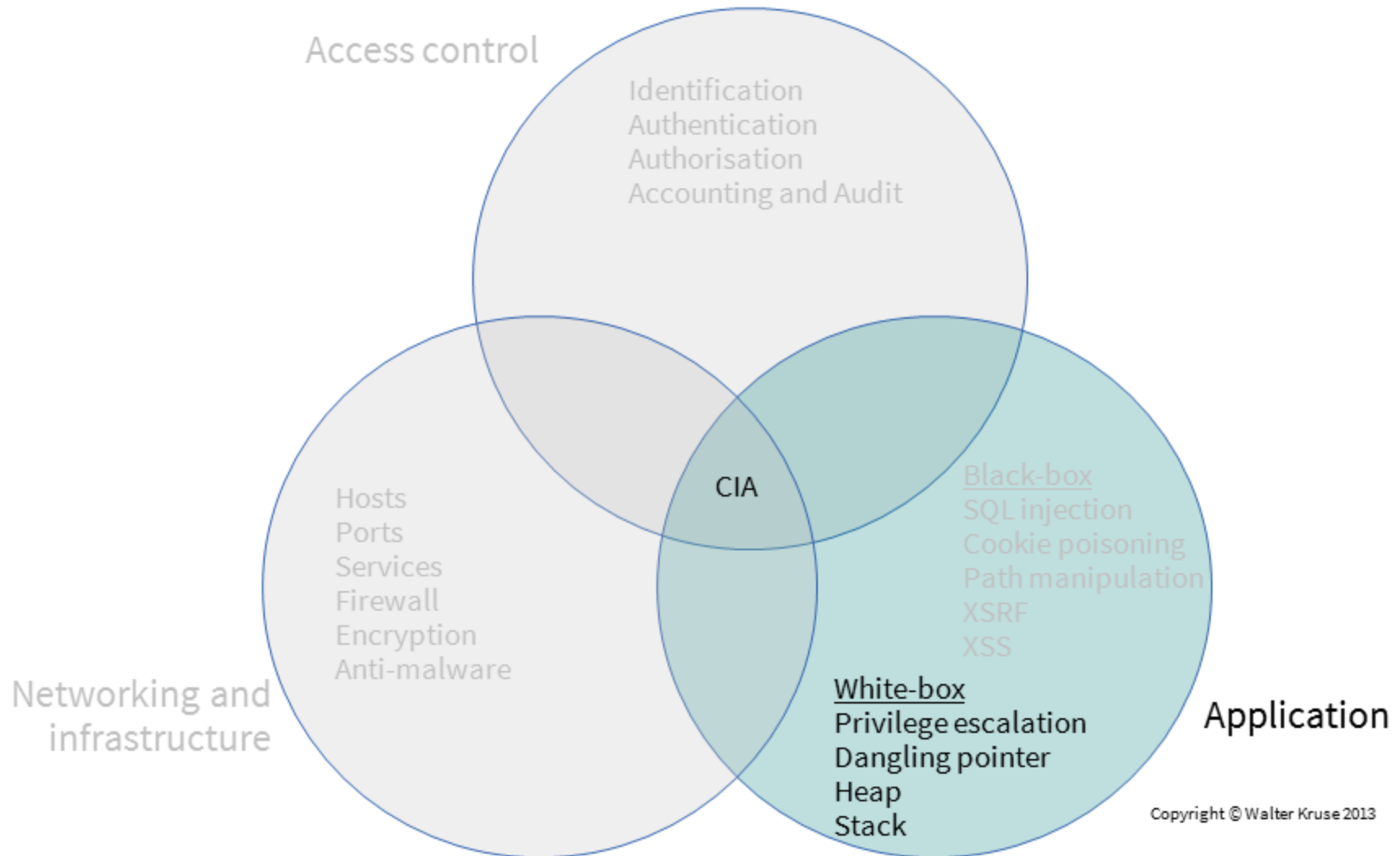
Referer: http://localhost:8080/

Cookie: JSESSIONID=069656142405261696DED9BA5409C73E

1 of 2

75710

White Box Scanning Demo



White Box Scanning Demo

- Eclipse plugins:
 - Lapse+
 - FindBugs
 - Google AnalytiX

White Box Scanning Demo

- Eclipse plugins:
 - Lapse+
 - FindBugs
 - Google AnalytiX

Lapse+

- Tests for known causes of: *Parameter Tampering, URL Tampering, Header Manipulation, Cookie Poisoning, SQL Injection, Cross-site Scripting (XSS), HTTP Response Splitting, Command Injection, Path Traversal, XPath Injection, XML Injection, LDAP Injection.*
- *Vulnerability Source*: Points of code that can be source of an attack of untrusted data injection.
- *Vulnerability Sink*: Points that can propagate the attack and manipulate the behaviour of the application.
- *Provenance Tracker*: Possibility to reach a source from a sink through backward propagation, if this occurs, we have a security vulnerability.

Static analysis - insecure/source/asc/db/DatabaseServiceImpl.java - Eclipse

File Edit Source Refactor Navigate Search Project CodePro Run Window Help

Static analy...

FindBugs

Resource

Java EE

Project Explorer

AltoroJ 2.1

bodgeit

cs6890hacmetravel.googlecode.com

HacmeBooks

insecure

Servers

wavsep

WebGoat

DatabaseServiceImpl.java

```
127 public Object perform() throws SQLException {
128     final String sql = "Update account set active=" + activateCd
129         + " WHERE accountId =" + accountId;
130
131     return new Integer(statement.executeUpdate(sql));
132 }
133 };
134 executeTask(task);
```

Vulnerability Sources

Suspicious call	Method	Type	Catego
rs.getString(2)	populateOneProduct	java.sql.ResultSet.getStr	Inform
rs.getString(3)	populateOneProduct	java.sql.ResultSet.getStr	Inform
rs.getString(4)	populateOneProduct	java.sql.ResultSet.getStr	Inform

Vulnerability Sinks

Suspicious call	Method	Cate
out.print(exception != null ? "Failed:" + exception.getMessage() : "Succeeded")	java.io.PrintWriter.	Cros
out.println("The Report could not be generated:" + e.getMessage())	java.io.PrintWriter.	Cros
statement.executeUpdate(sql)	java.sql.Statement	SQL

Provenance Tracker

Created a slice with 4 leaf element(s) and 9 element(s) located in 2 file(s) with 0 element(s) truncated with a max

sql (DatabaseServiceImpl.java:131) [initial]

sql="Update account set active=" + activateCd + " WHERE accountId =" + accountId (DatabaseService

"Update account set active=" + activateCd + " WHERE accountId =" + accountId (DatabaseServiceIm

"Update account set active=" (DatabaseServiceImpl.java:128) [string constant]

sql (DatabaseServiceImpl.java:131) [initial]

White Box Scanning Demo

- Eclipse plugins:
 - Lapse+
 - FindBugs
 - Google AnalytiX

FindBugs - insecure/source/asc/db/connection/DatasourceConnectionProvider.java - Eclipse

File Edit Source Refactor Navigate Search Project CodePro Run Window Help

FindBugs

Java EE Static analy... Resource

Package Explorer

AltoroJ 2.1

bodgeit

cs6890hacmetravel.googlecode.com

HacmeBooks

insecure (8)

source (8)

JRE System Library [jdk1.7.0]

Referenced Libraries

dist

doc

lib

temp

DatasourceConnectionProvider.java

```
23
24     DataSource dataSource;
25
26     public DatasourceConnectionProvider() throws Exception {
27         initContext = new javax.naming.InitialContext();
28         envContext = (Context) initContext.lookup("java:/comp/env");
29         dataSource = (DataSource)envContext.lookup("jdbc/asdb"); // see if datasou
30         Connection c = getConnection();
31         returnConnection(c,false);
32     }
33
34     public Connection getConnection() throws Exception {
35         return dataSource.getConnection();
36     }
37
38     public void returnConnection(Connection c, boolean sqlExceptionOccurred) {
39         try {
40             c.close();
41         } catch (Exception ignored) {}
42     }
43 }
```

Bug Explorer

insecure (8)

Scary (2)

Normal confidence (2)

Method throws alternative exception from catch t

Method asc.db.DatabaseServiceImpl.executeT

Constructor makes call to non-final method (1)

Constructor new asc.db.connection.Datasourc

Troubling (3)

Of Concern (3)

Bug Info

DatabaseServiceImpl.java: 40

Navigation

Method asc.db.DatabaseServiceImpl.executeTask(DatabaseTask) throws alternative exception from catch t

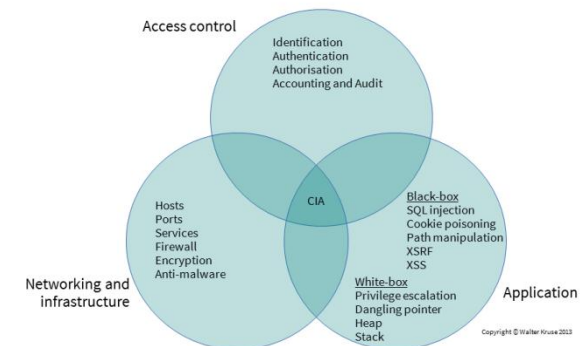
Method asc.db.DatabaseServiceImpl.executeTask(Dat...ock without history [Scary(7), Normal confidence]

White Box Scanning Demo

- Eclipse plugins:
 - Lapse+
 - FindBugs
 - Google AnalytiX

What can we *really* do about it ?

- You, as a tester can probably do very little about it
 - Must have a mandate
 - Must have permission
 - Socialise the fact that you want to do security testing
- Myriad of tools, most are targeted at Linux $\text{-}\backslash\text{-(}\text{ツ}\text{)}\text{-}\text{}$
 - Don't “run a scanner” and send a report and expect to be entertained if you can not interpret the results and possibly advise remedies for the findings
- Like performance testing, it is very technical and complex
- Lends itself well to in-scrum testing



Agenda

- Positioning security testing
- Infosec in South Africa
- Threats
- Significance of threats
- Security testing overview
- Demos
- Resources







Resources

- The Wolfpack report:
 - www.wolfpackrisk.com/research/south-african-cyber-threat-barometer/
- Acunetix Web Application Vulnerability Report
 - www.acunetix.com/acunetix-web-application-vulnerability-report-2016/
- ISECOM: www.isecom.org
 - OSSTMM, HHS
- OWASP: www.owasp.org
 - Top 10 list of web application vulnerabilities
 - Software Assurance Maturity Model
 - Tools, deliberately vulnerable apps, methodologies, community etc.

Resources Cont.

- National Institute for Standards and Technology:
 - <http://csrc.nist.gov>
- Web Application Security Consortium:
 - www.webappsec.org/
- SANS Institute:
 - www.sans.org
- Mitre Common Weaknesses Enumeration:
 - <http://cwe.mitre.org>
- sectooladdict.blogspot.com

sectooladdict.blogspot.com

Logo	Vulnerability Scanner	Benchmark Results							Pricing			
	IBM AppScan		WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup	Consultant	Enterprise	Any
		Accuracy	92%	100.0%	100.0%	100.0%	100.0%	86.67%	5.43%	Seat/Year	Seat/Year	Website/Year
		False Positive		0.0%	0.0%	0.0%	0.0%	11.11%	86.67%	17700.0\$	×	×
		Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner	Seat/Perpetual	Seat/Perpetual	Website/Perpetual		
		30	17	✓	✓	✓	✓	37700.0\$	×	×		
	Webinspect		WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup	Consultant	Enterprise	Any
		Accuracy	96%	100.0%	100.0%	91.18%	100.0%	50.0%	2.17%	Seat/Year	Seat/Year	Website/Year
		False Positive		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	×	×	×
		Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner	Seat/Perpetual	Seat/Perpetual	Website/Perpetual		
		29	13	✓	✓	✓	✓	×	×	×		
	Acunetix WVS		WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup	Consultant	Enterprise	Any
		Accuracy	94%	100.0%	100.0%	94.12%	100.0%	100.0%	32.61%	Seat/Year	Seat/Year	Website/Year
		False Positive		0.0%	0.0%	0.0%	0.0%	11.11%	0.0%	3500.0\$	2495.0\$	345.0\$
		Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner	Seat/Perpetual	Seat/Perpetual	Website/Perpetual		
		26	7	✓	×	✓	✓	6995.0\$	4995.0\$	×		
	Tinfoil Security		WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup	Consultant	Enterprise	Any
		Accuracy	94%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	Seat/Year	Seat/Year	Website/Year
		False Positive		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	×	×	199.0\$
		Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner	Seat/Perpetual	Seat/Perpetual	Website/Perpetual		
		24	15	✓	×	✓	×	×	×	×		
	W3AF		WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup	Consultant	Enterprise	Any
		Accuracy	19%	35.29%	37.88%	57.48%	16.67%	63.33%	22.83%	Seat/Year	Seat/Year	Website/Year
		False Positive		30.0%	0.0%	12.5%	16.67%	11.11%	0.0%	0.0\$	0.0\$	0.0\$
		Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner	Seat/Perpetual	Seat/Perpetual	Website/Perpetual		
		23	8	✓	×	✓	×	0.0\$	0.0\$	0.0\$		
	arachni		WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup	Consultant	Enterprise	Any
		Accuracy	96%	100.0%	90.91%	100.0%	100.0%	100.0%	100.0%	Seat/Year	Seat/Year	Website/Year
		False Positive		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0\$	0.0\$	0.0\$
		Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner	Seat/Perpetual	Seat/Perpetual	Website/Perpetual		
		20	11	✓	×	✓	×	0.0\$	0.0\$	0.0\$		

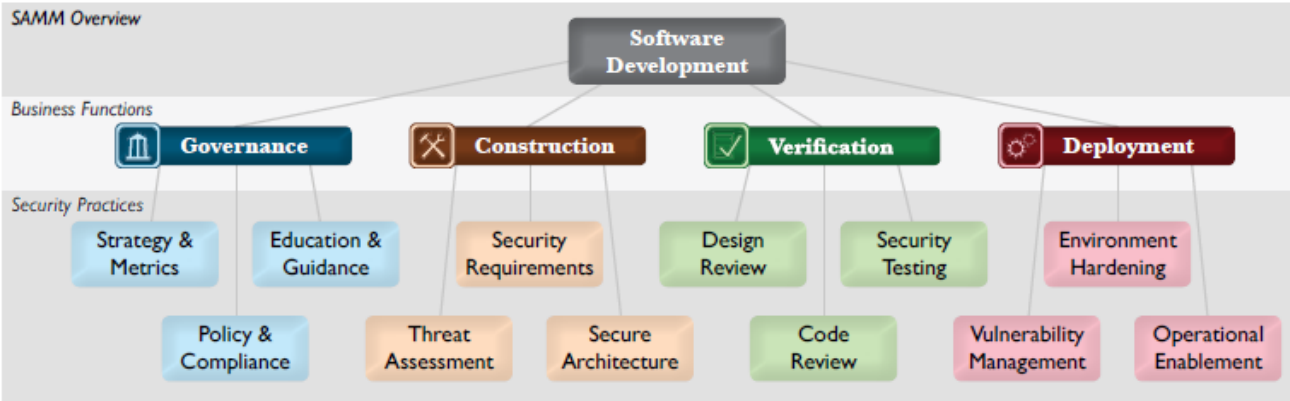


Software Assurance Maturity Model

A guide to building security into software development

VERSION - 1.0

SAMM Overview



OWASP WebGoat v5.4



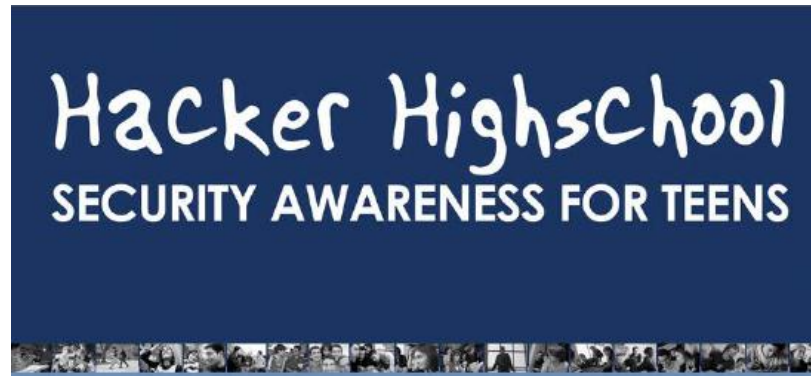
OWASP
Open Web Application
Security Project



ZAPROXY



ISECOM

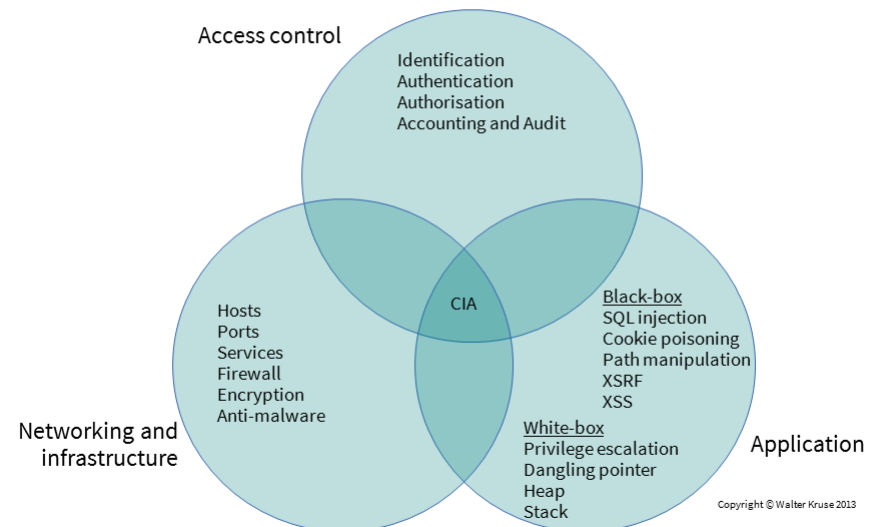


Conclusion

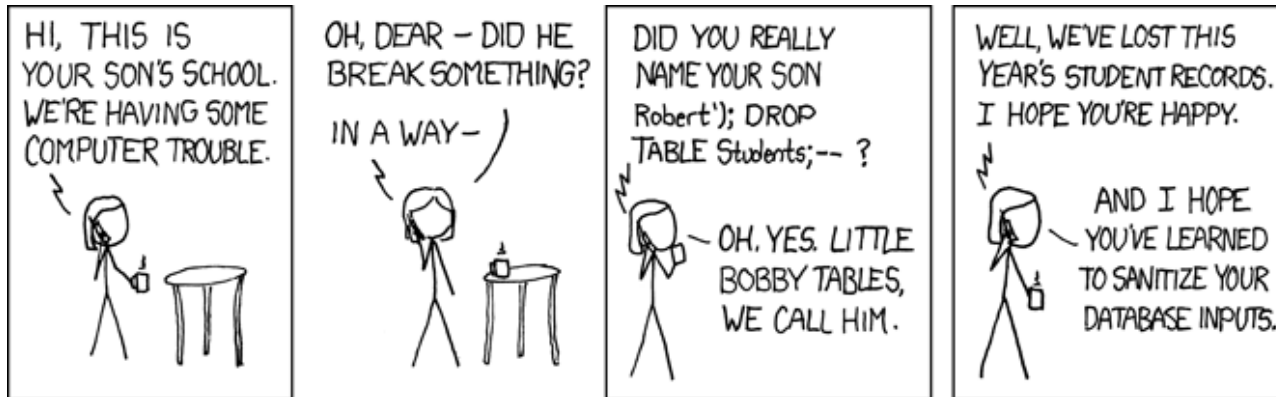
- Positioning Security Testing
- Infosec in South Africa
- Threats
- Significance of Threats
- Security Testing overview
- Demos
- Resources

Images attribution

- ITWeb.co.za
- timeslive.co.za
- ISECOM.org
- SANS.org
- OWASP.org
- w3schools.com
- xkcd.com



Questions ?



kruse.walter@gmail.com



Uhh yeah, I'm looking for a Mr. Jones, first name ";DROP TABLE *;--



Ok, let me just check.



Yo, is there a SELECT * FROM Drunks WHERE Name="";DROP TABLE *;-- Jones" here?

