Software Vulnerabilities

Software is designed (should) to meet requirements

A **software bug** is un *unmet specification*, a failure in meet the requirements.
If a bug is related to a security requirement, it is a **Software Vulnerability**
    Vulnerability is a subset of bug

A Vulnerability is a bug the has a reflect on constraints of CIA (Confidentiality, Integrity, Availability)

    Weakness or gap

Exploit is a set of instructions for abusing a sw vulnerability in order to cause unintended or unanticipated behavior.
There are no perfect softwares
There are only things that are secure “*enough*”..

VA&PT

A **Vulnerability Assessment** is the way to find as many flaws as possible and make a prioritized list of remediation items.

- List Oriented
- Don’t differentiate between flaws that can be exploited to cause damage and those that cannot.

A **Penetration Test** is an intrusive test, simulating real threat scenario and it is designed to evaluate also the defense measures in place.

- Goal oriented
- A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system

Often combined to achieve more cohmprensive security analysis

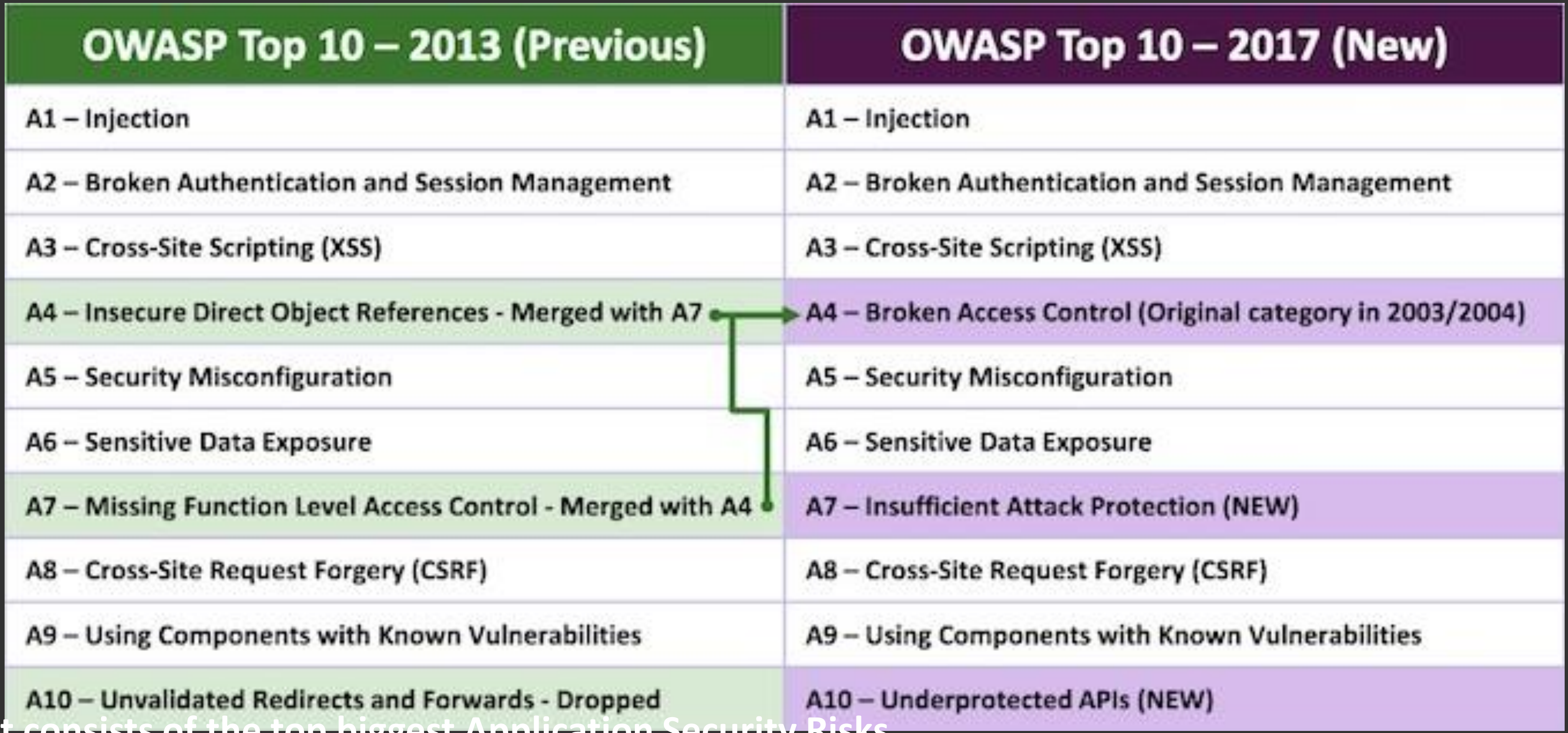
VA&PT

- **Vulnerability Assessment:** Find every flaws in a system
- **Vulnerability Assessment** is not Risk Assessment!

- **Penetration Test:** Evaluate how damaging a flaw could be in real attack.

- VAPT provides a detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks

OWASP TOP 10



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

he list consists of the top biggest Application Security Risks according to OWASP.

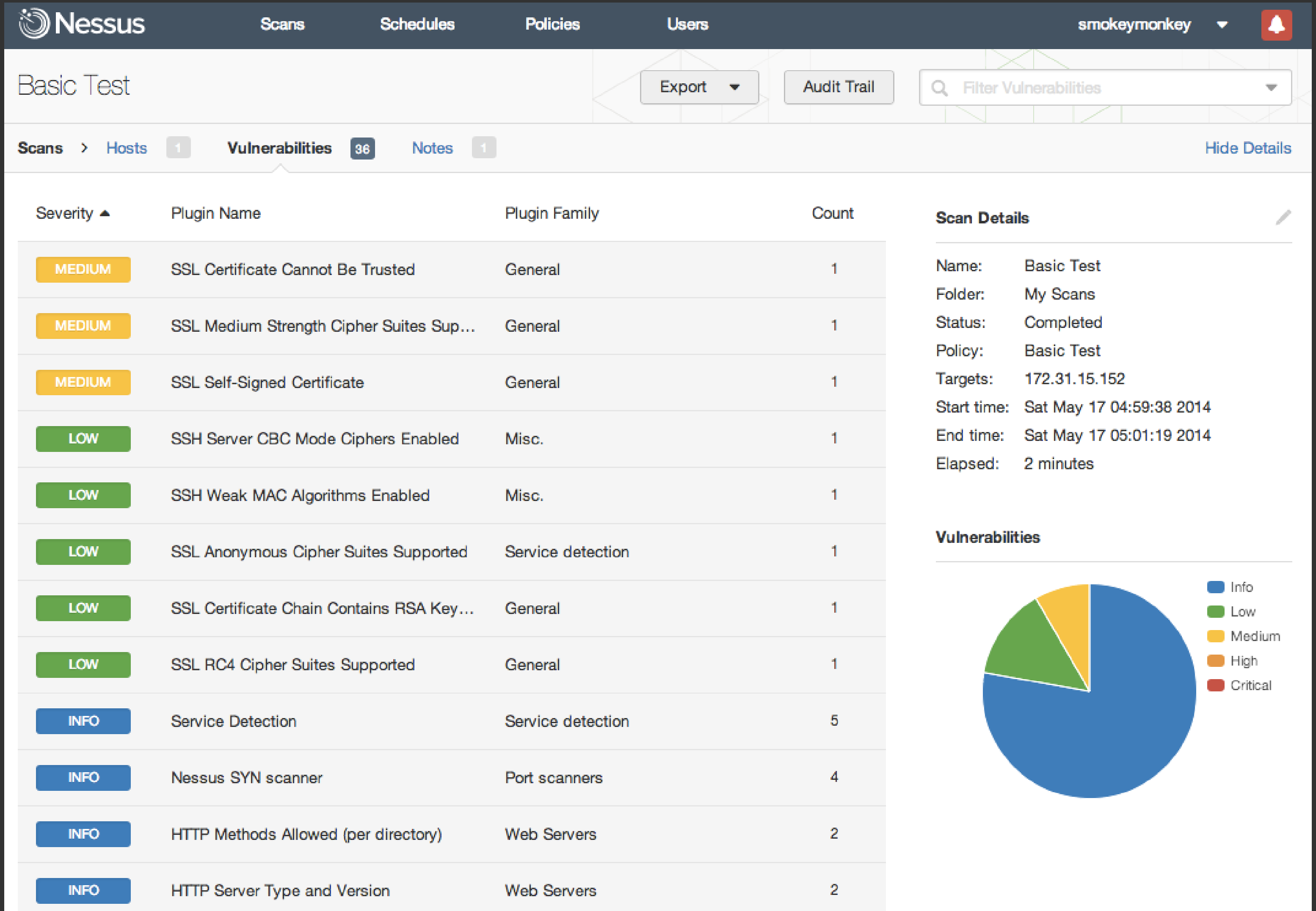
va, wapt, npt, eh...

- a vulnerability assessment is the process of identifying and quantifying security vulnerabilities in an environment.
  - An in-depth evaluation of your information security posture

  - Vulnerability Assessments Follow These General Steps:

    1. Catalog assets and resources in a system
    2. Assign quantifiable value and importance to the resources
    3. Identify the security vulnerabilities or potential threats to each resource
    4. Mitigate or eliminate the most serious vulnerabilities for the most valuable resources

NESSUS Demo



Basic Test

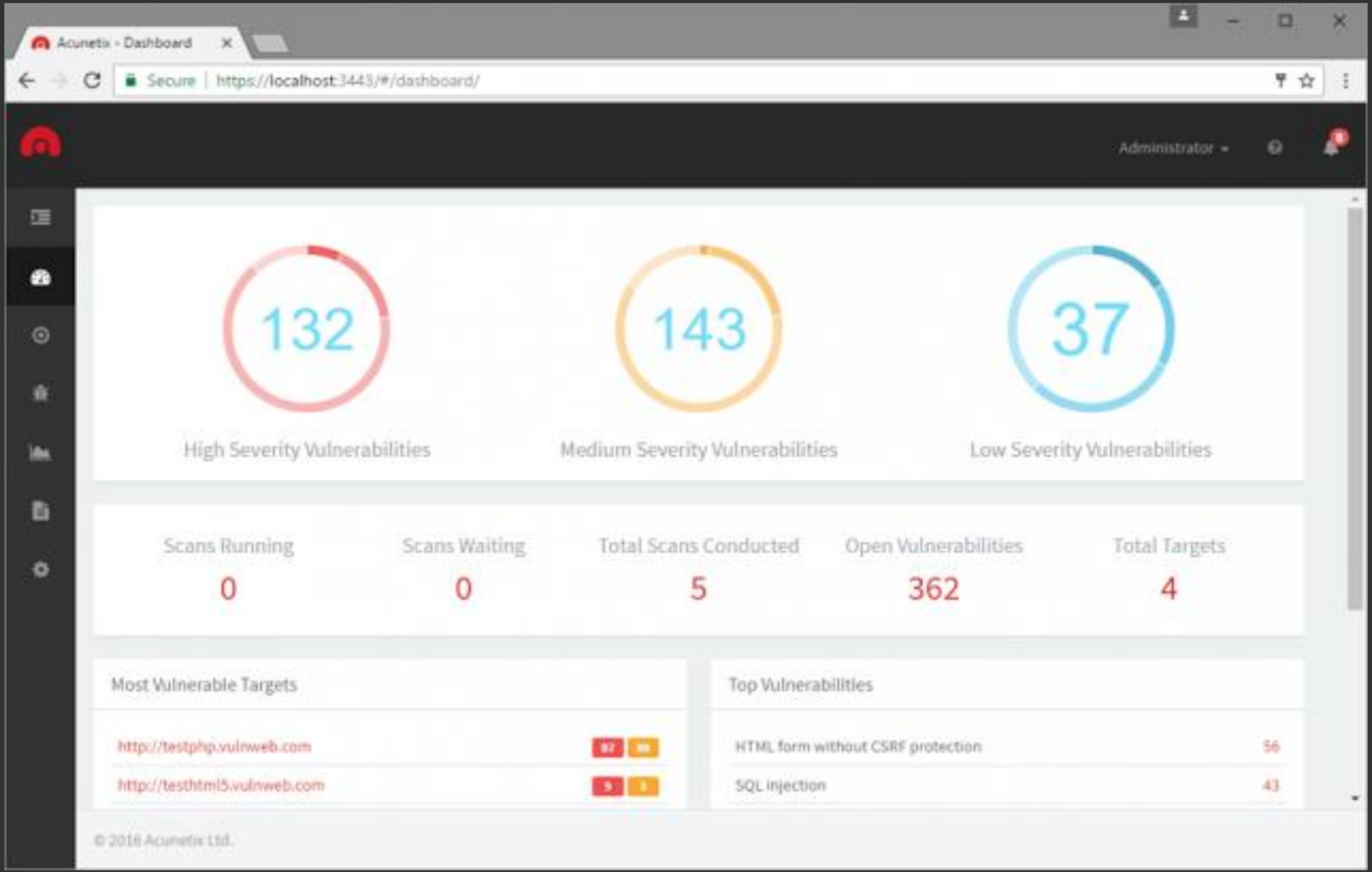
Severity ▲	Plugin Name	Plugin Family	Count
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Medium Strength Cipher Suites Sup...	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
LOW	SSL Anonymous Cipher Suites Supported	Service detection	1
LOW	SSL Certificate Chain Contains RSA Key...	General	1
LOW	SSL RC4 Cipher Suites Supported	General	1
INFO	Service Detection	Service detection	5
INFO	Nessus SYN scanner	Port scanners	4
INFO	HTTP Methods Allowed (per directory)	Web Servers	2
INFO	HTTP Server Type and Version	Web Servers	2

Scan Details

Name:	Basic Test
Folder:	My Scans
Status:	Completed
Policy:	Basic Test
Targets:	172.31.15.152
Start time:	Sat May 17 04:59:38 2014
End time:	Sat May 17 05:01:19 2014
Elapsed:	2 minutes

Vulnerabilities

Acunetix Web VS Demo



132	143	37
High Severity Vulnerabilities	Medium Severity Vulnerabilities	Low Severity Vulnerabilities

Scans Running	Scans Waiting	Total Scans Conducted	Open Vulnerabilities	Total Targets
0	0	5	362	4

Most Vulnerable Targets

http://testphp.vulnweb.com	87	88
http://testhtml5.vulnweb.com	9	3

Top Vulnerabilities

HTML form without CSRF protection	56
SQL injection	43

© 2018 Acunetix Ltd.

PT Phases

- Penetration Test Follow These General Steps:

    1. Pre-engagement activities (RoE, Scoping, Schedule, Formal permission)
    2. Reconnaissance and Info Gathering
    3. Enumeration,scanning
    4. Automated and Manual Testing, gaining access, exploitation
    5. Reporting
    6. Remediation Support

    Malicious Attackers go further:

    - Mantaining access with backdoord
    - Covering tracks

Types of Penetration Test

- Network service test
- Client-side test
- Web App Pen Test
- Wireless Pen Test
- Social Engineering Test
- Physical Security Test
- Cryptanalysis Attack

Determine the scope

- Network (PenTest, VA, wireless)
- Application (code or vuln scan)
- Process
- How critical is the system you assessing?
- High,medium – use external assessor
- Low self-assessment
- What are the concerns?
  - Disclosure of sensitive information
  - Interruption of production processing
  - Compromising of a particular machine..

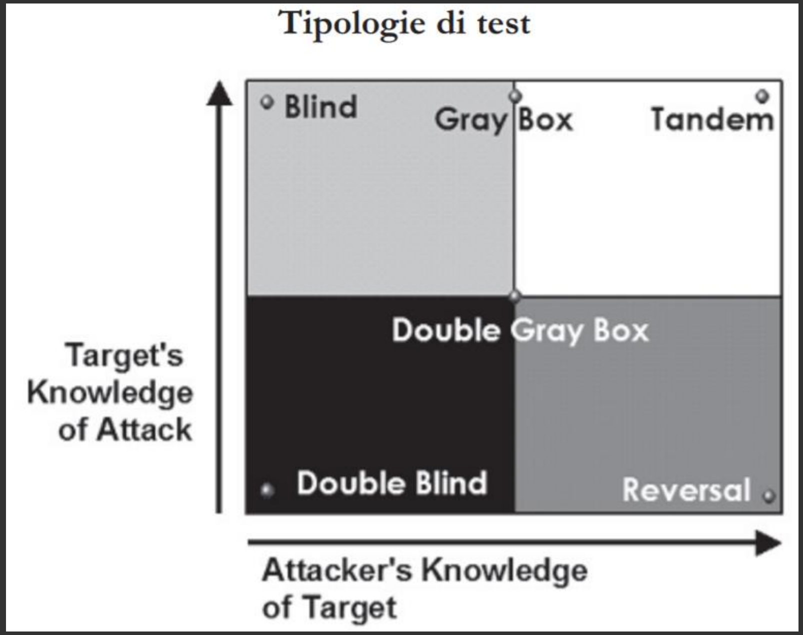
Testing Methodologies

- Open Source Security Testing Methodology (OSSTMM)
- Pen Testing Execution Standard (PTES)
- NIST Special Pubblication 800-15: Technical Guide to Information Security Assessment and testing
- Open Web Application Security Project (OWASP)
- Penetration Testing Framework

OSSTMM

OSSTMM is a scientific methodology developed by many volunteers worldwide through the peer model review.

- Written by Pete Herzog and distributed by ISECOM
- Includes numeros information gathering templates
- Covers scoping,metrics,human security,data network security testing....
- This document strives:
- Repeatability
- Consistency
- High quality



OSSTMM

BLIND: quando l'attaccante non conosce minimamente il sistema da analizzare. E' conosciuto solamente il target (Indirizzi IP o URL) .

DOUBLE BLIND: simile a quello precedente con la differenza che alcune persone del committente sono al corrente del test. Viene tipicamente usato per verificare se il personale interno dedicato alla sicurezza è "vigile" e svolge con diligenza il proprio lavoro.

GRAY BOX: sia l'attaccante che l'attacco sono pienamente a conoscenza sia del sistema informatico da analizzare che delle modalità di attacco. Viene utilizzato quando si analizza il proprio sistema interno.

DOUBLE GRAY BOX: è un gray box che prevede la conoscenza delle credenziali di accesso. Viene usato per testare l'accesso ad informazioni più riservate rispetto al suo livello da parte di un utente.

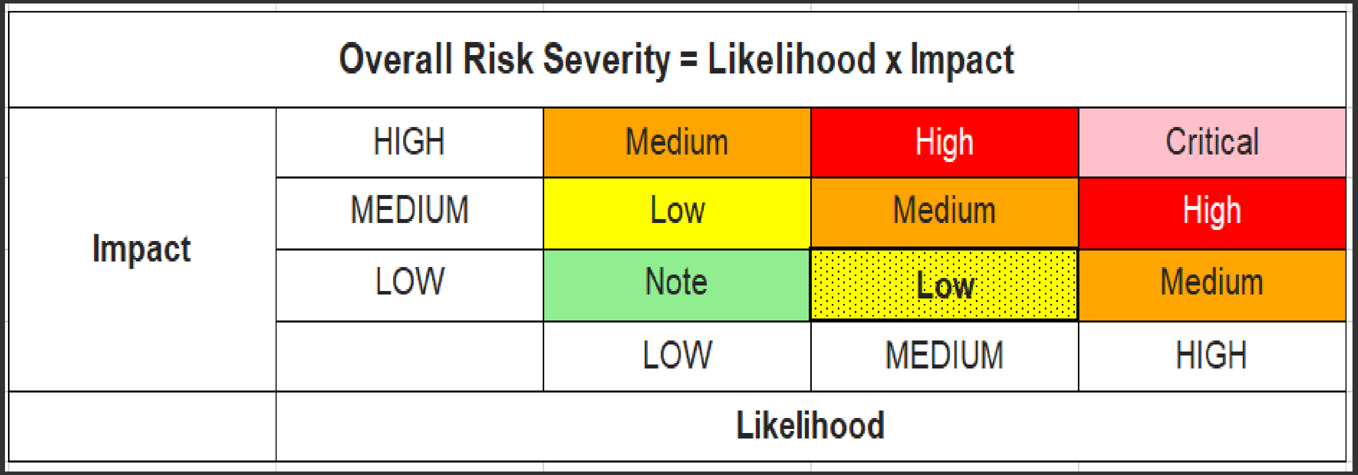
TANDEM: analisi del codice. Chi verifica e chi crea il codice collaborano

REVERSAL: test a uso interno. Il tester ha una grande quantità di informazione il committente non sa i tempi e le metodologie con cui verrà attaccato.

OWASP

Focused on Web Application Testing

- Owasp Testing Guide v.4.0 (https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)
- OWASP TOP TEN 2017 (https://www.owasp.org/index.php/Top_10-2017_Top_10)
    - Denial of service testing
    - Ajax testing
    - Web services testing
    - Data validation testing
    - Business logic testing
    - Session managmente testing

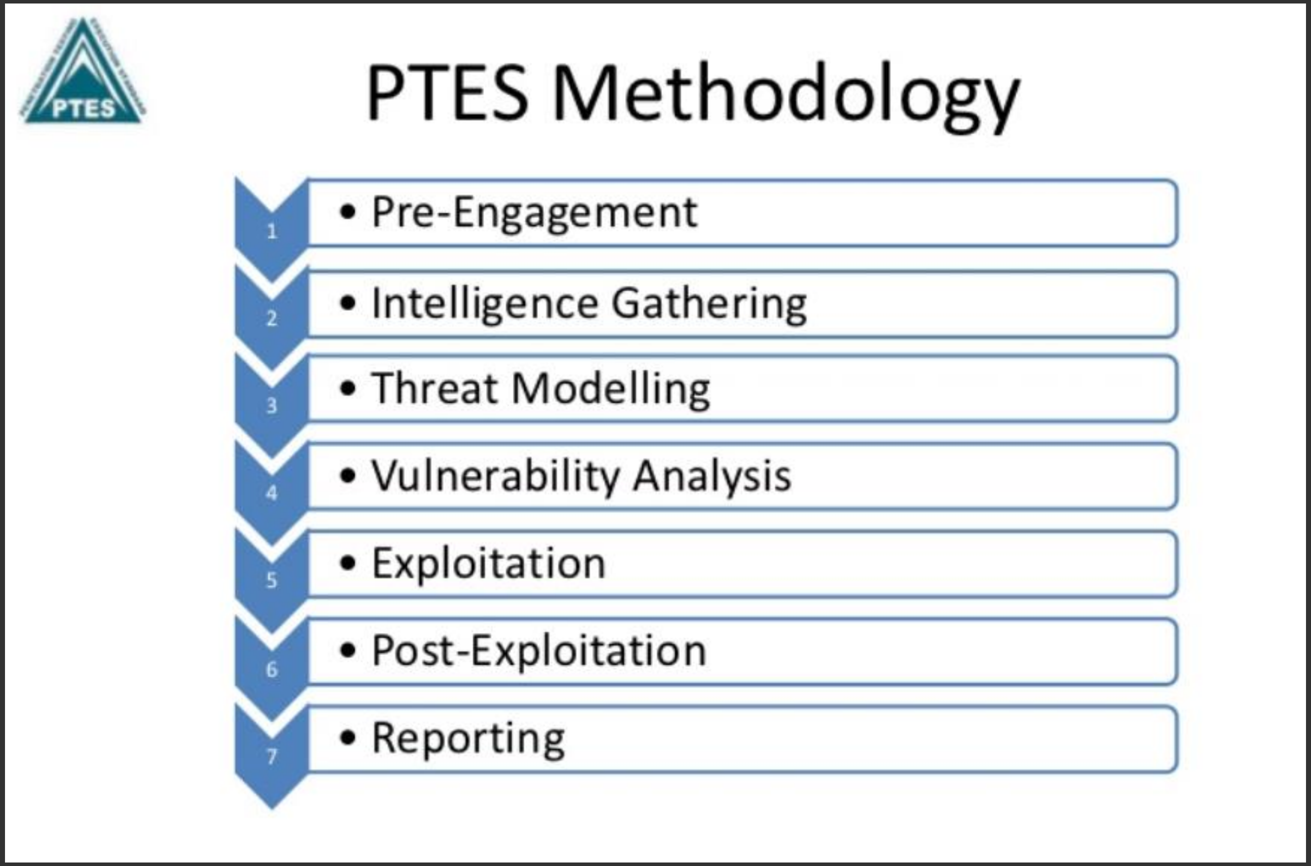


Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

PTES

Available at www.pentest-standard.org

- Pre-engagement interactions
- Intelligence gathering
- Threat modeling
- Vuln analysis
- Exploitation and post exploitation
- reporting



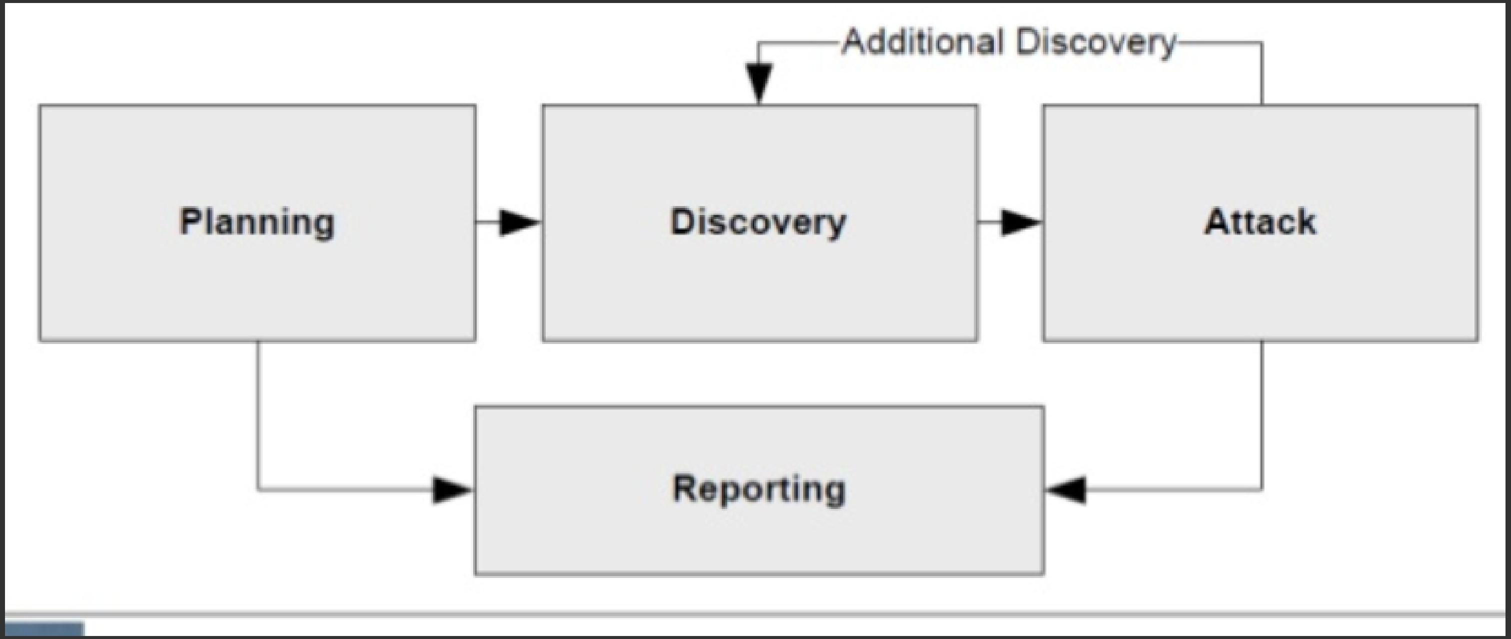
PTES Methodology

- Pre-Engagement
- Intelligence Gathering
- Threat Modelling
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting

NIST 800-15

Covers planning, process, analysis, validation.
It also includes appendix with a template for RoE
Three types of Assessment methods can be used to accomplish this:

- Testing
- Examination
- Interviewing



footprinting

DISCLOSED ORIENTED

- Organization website
- IP addresses
- Directories
- Email
- Domain name blocks
- AP
- …
- OSINT

EXTERNAL

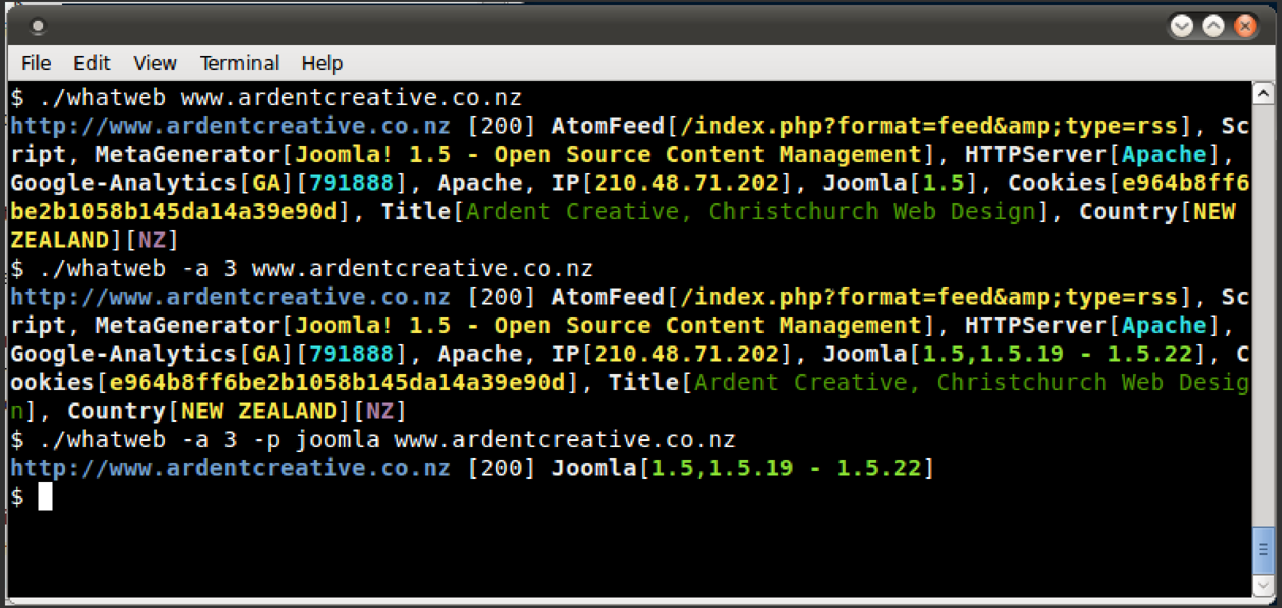
- Phone
- Network
- Websites
- Whois
- Google
- DNS
- Email header
- Social networks
- Job sites
- Ip blocks
- Net blocks

INTERNAL

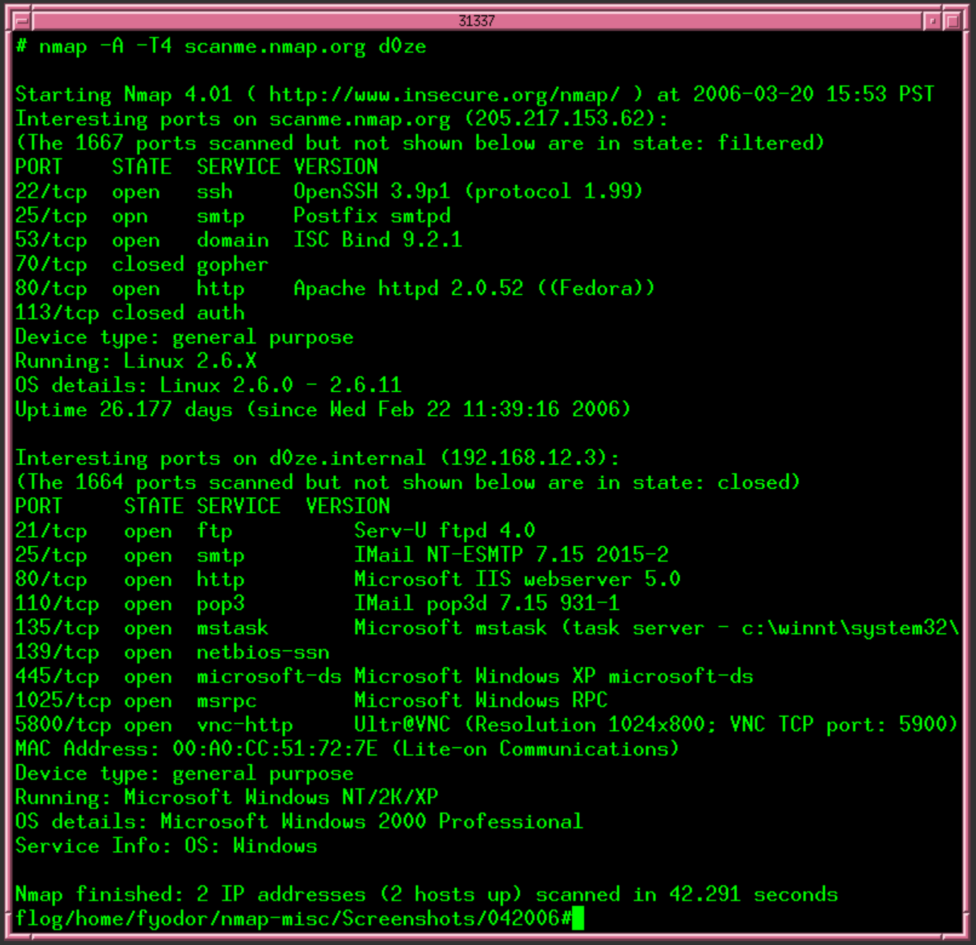
- Internal DNS
- Dumpster Diving
- Shoulder Surfing
- Evasedropping
- Private company stuff

Fw/IDS

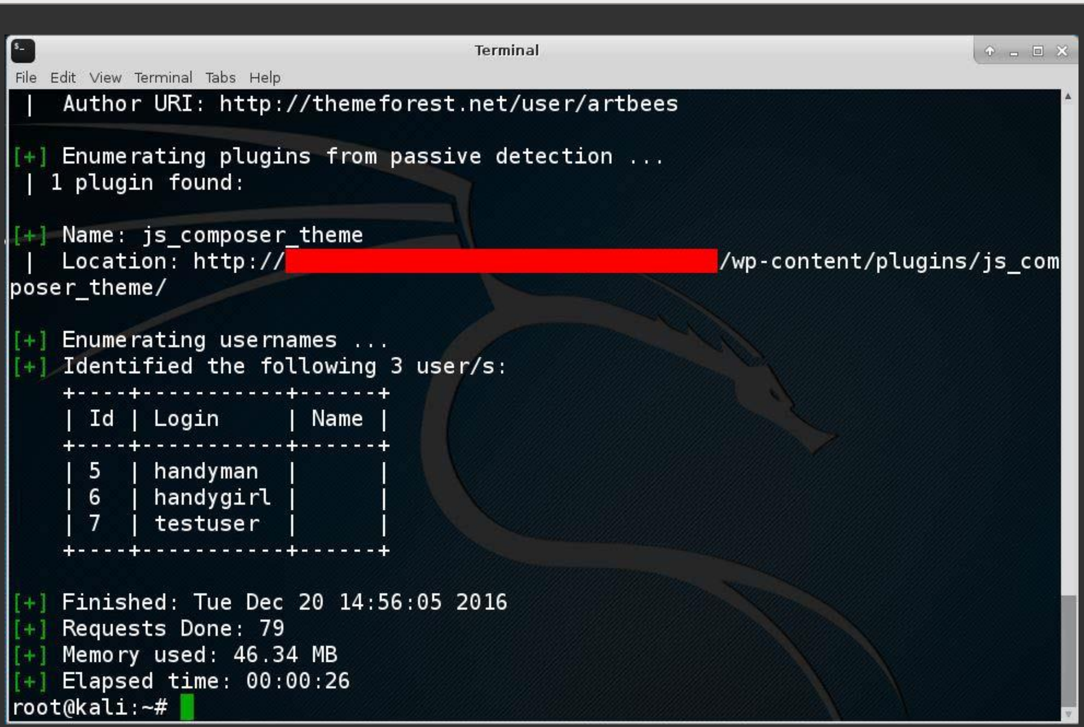
enumeration



```
$ ./whatweb www.ardentcreative.co.nz
http://www.ardentcreative.co.nz [200] AtomFeed[/index.php?format=feed&amp;type=rss], Sc
ript, MetaGenerator[Joomla! 1.5 - Open Source Content Management], HTTPServer[Apache],
Google-Analytics[GA][791888], Apache, IP[210.48.71.202], Joomla[1.5], Cookies[e964b8ff6
be2b1058b145da14a39e90d], Title[Ardent Creative, Christchurch Web Design], Country[NEW
ZEALAND][NZ]
$ ./whatweb -a 3 www.ardentcreative.co.nz
http://www.ardentcreative.co.nz [200] AtomFeed[/index.php?format=feed&amp;type=rss], Sc
ript, MetaGenerator[Joomla! 1.5 - Open Source Content Management], HTTPServer[Apache],
Google-Analytics[GA][791888], Apache, IP[210.48.71.202], Joomla[1.5,1.5.19 - 1.5.22], C
ookies[e964b8ff6be2b1058b145da14a39e90d], Title[Ardent Creative, Christchurch Web Desig
n], Country[NEW ZEALAND][NZ]
$ ./whatweb -a 3 -p joomla www.ardentcreative.co.nz
http://www.ardentcreative.co.nz [200] Joomla[1.5,1.5.19 - 1.5.22]
$ 
```

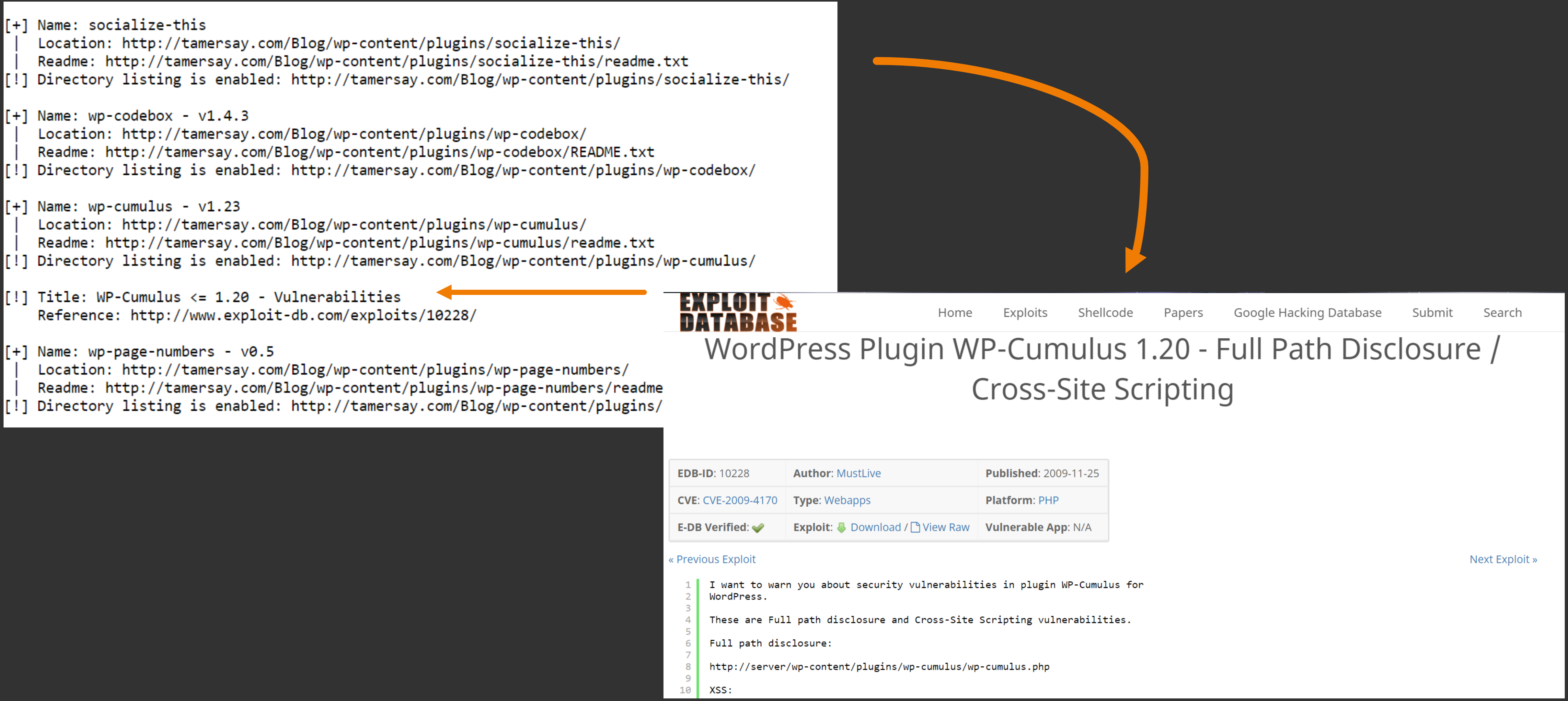


```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```



```
 |  Author URI: http://themeforest.net/user/artbees

[+] Enumerating plugins from passive detection ...
 | 1 plugin found:

[+] Name: js_composer_theme
 |  Location: http://[redacted]/wp-content/plugins/js_com
poser_theme/

[+] Enumerating usernames ...
[+] Identified the following 3 user/s:
    +----+-----------+------+
    | Id | Login     | Name |
    +----+-----------+------+
    | 5  | handyman  |      |
    | 6  | handygirl |      |
    | 7  | testuser  |      |
    +----+-----------+------+

[+] Finished: Tue Dec 20 14:56:05 2016
[+] Requests Done: 79
[+] Memory used: 46.34 MB
[+] Elapsed time: 00:00:26
root@kali:~# 
```

From enum to exploit…



```
[+] Name: socialize-this
 |  Location: http://tamersay.com/Blog/wp-content/plugins/socialize-this/
 |  Readme: http://tamersay.com/Blog/wp-content/plugins/socialize-this/readme.txt
[!] Directory listing is enabled: http://tamersay.com/Blog/wp-content/plugins/socialize-this/

[+] Name: wp-codebox - v1.4.3
 |  Location: http://tamersay.com/Blog/wp-content/plugins/wp-codebox/
 |  Readme: http://tamersay.com/Blog/wp-content/plugins/wp-codebox/README.txt
[!] Directory listing is enabled: http://tamersay.com/Blog/wp-content/plugins/wp-codebox/

[+] Name: wp-cumulus - v1.23
 |  Location: http://tamersay.com/Blog/wp-content/plugins/wp-cumulus/
 |  Readme: http://tamersay.com/Blog/wp-content/plugins/wp-cumulus/readme.txt
[!] Directory listing is enabled: http://tamersay.com/Blog/wp-content/plugins/wp-cumulus/

[!] Title: WP-Cumulus <= 1.20 - Vulnerabilities
    Reference: http://www.exploit-db.com/exploits/10228/

[+] Name: wp-page-numbers - v0.5
 |  Location: http://tamersay.com/Blog/wp-content/plugins/wp-page-numbers/
 |  Readme: http://tamersay.com/Blog/wp-content/plugins/wp-page-numbers/readme
[!] Directory listing is enabled: http://tamersay.com/Blog/wp-content/plugins/
```

WordPress Plugin WP-Cumulus 1.20 - Full Path Disclosure / Cross-Site Scripting

EDB-ID: 10228	**Author**: MustLive	**Published**: 2009-11-25
CVE: CVE-2009-4170	**Type**: Webapps	**Platform**: PHP
E-DB Verified: ✓	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

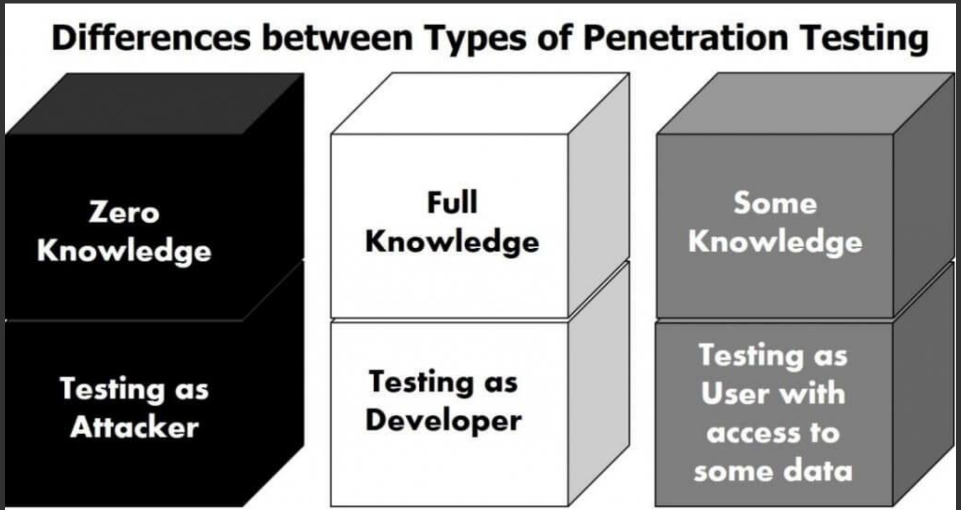
« Previous Exploit

Next Exploit »

```
I want to warn you about security vulnerabilities in plugin WP-Cumulus for
WordPress.

These are Full path disclosure and Cross-Site Scripting vulnerabilities.

Full path disclosure:

http://server/wp-content/plugins/wp-cumulus/wp-cumulus.php

XSS:
```

White / Black / Gray Box Testing

- **Black Box testing :** without credentials, without details on target, realistic. Black box PT evaluates both the underlying technology as well as the people and processes in place to identify and block real-world attacks.
- **White Box testing :** with credentials, maybe also the source code is available, deeper but also less realistic.
- **Gray box testing:** lies between black and white. Testers will have knowledge of some areas


Differences between Types of Penetration Testing
Zero Knowledge
Testing as Attacker
Full Knowledge
Testing as Developer
Some Knowledge
Testing as User with access to some data