Becoming a Hacker: An Introduction to Ethical Hacking, Penetration Testing, and Bug Hunting

DAY 1

Omar Santos

@santosomar

About // Omar Ωr Santos

https://h4cker.org

@santosomar

https://h4cker.org/discord

/in/santosomar

h4cker.org/github

Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar is the author of over 20 books and video courses; numerous white papers, articles, and security configuration guidelines and best practices. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities.

Omar is often presenting at many cybersecurity conferences and he is the co-lead of the DEF CON Red Team Village (redteamvillage.io). He is also the chair of the OASIS Common Security Vulnerability Framework (CSAF) Technical Committee and the co-chair of the Forum of Incident Response and Security Teams (FIRST) PSIRT Open Source Security Working Group.

Omar has been quoted by numerous media outlets, such as TheRegister, Wired, ZDNet, ThreatPost, CyberScoop, TechCrunch, Fortune Magazine, Ars Technica, and more.

Omar's PGP Key: 0x8e19a9d13af27edc

DISCLAIMER/ WARNING

- The information provided on this training is **for educational purposes only**. The **author**, O'Reilly, or any other entity **is in no way responsible for any misuse of the information**.

- Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.

- Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.

Agenda – Day 1

- An Overview of Ethical Hacking and Penetration Testing Methodologies
- Red Teaming vs. Pen Testing vs. Bug Bounties
- Building your own hacking lab with WebSploit Labs
- 🤖🔥AI-driven Ethical Hacking (throughout the course)
- Passive Reconnaissance and Open-Source Intelligence (OSINT)
- Active Reconnaissance, Scanning, and Fuzzing
- Introduction to Hacking Modern Web Applications
- Introduction to Hacking User Credentials and Cracking Passwords
- Introduction to Hacking Databases and SQL Injection

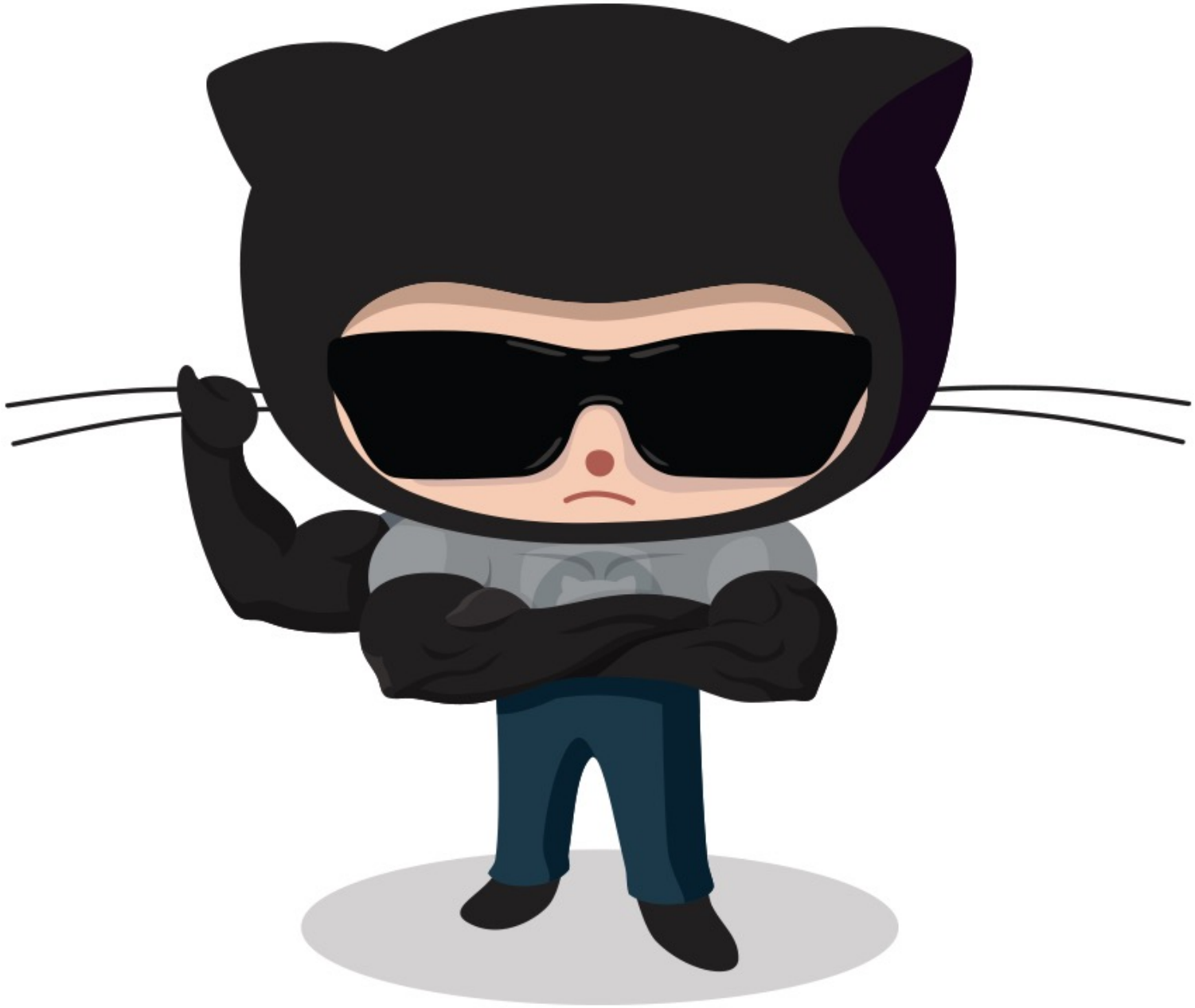
Agenda – Day 2

- Introduction to Hacking Networking Devices
- Fundamentals of Wireless Hacking
- Introduction to Buffer Overflows and Creating Payloads for Code Execution
- Introduction to Social Engineering
- Fundamentals of Evasion and Post Exploitation Techniques
- Command and Control, Exfiltration, and Privilege Escalation
- Best Practices on How to Write Penetration Testing Reports

Learning Path: https://h4cker.org/learning-path

GitHub Repo

https://hackerrepo.org



Hacking Labs

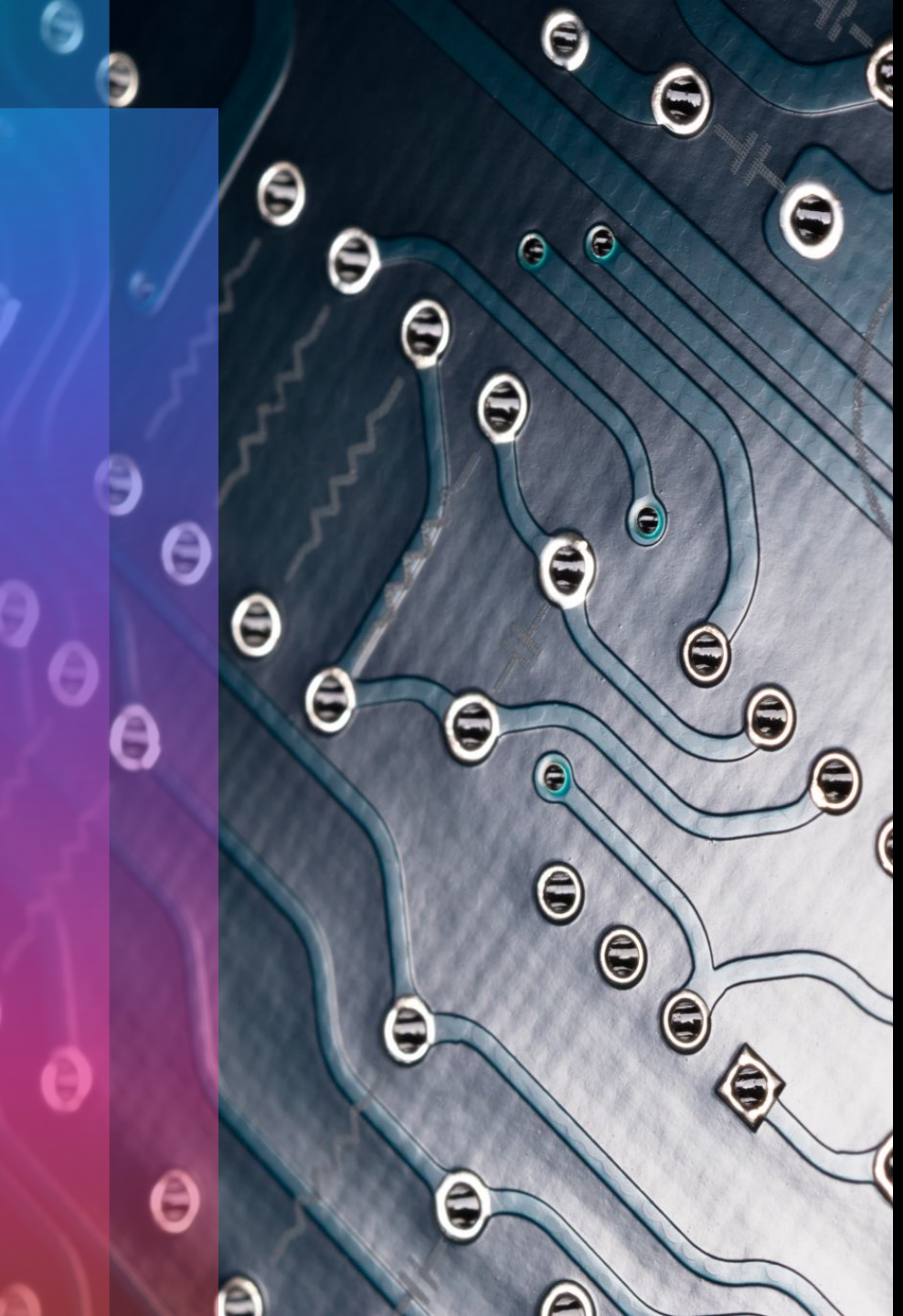
- https://hackingscenarios.com

An Overview of Ethical Hacking

Ethical Hacker?

An ethical hacker is as a person who is hired and permitted by an organization to attack its systems for the purpose of identifying vulnerabilities, which an attacker might take advantage of.

Boring Definitions



What is a Vulnerability?

- A vulnerability is an exploitable weakness in a system or its design.
- Vulnerabilities can be found in protocols, operating systems, applications, hardware, and system designs.

What is a threat?

A threat is any potential danger to an asset.

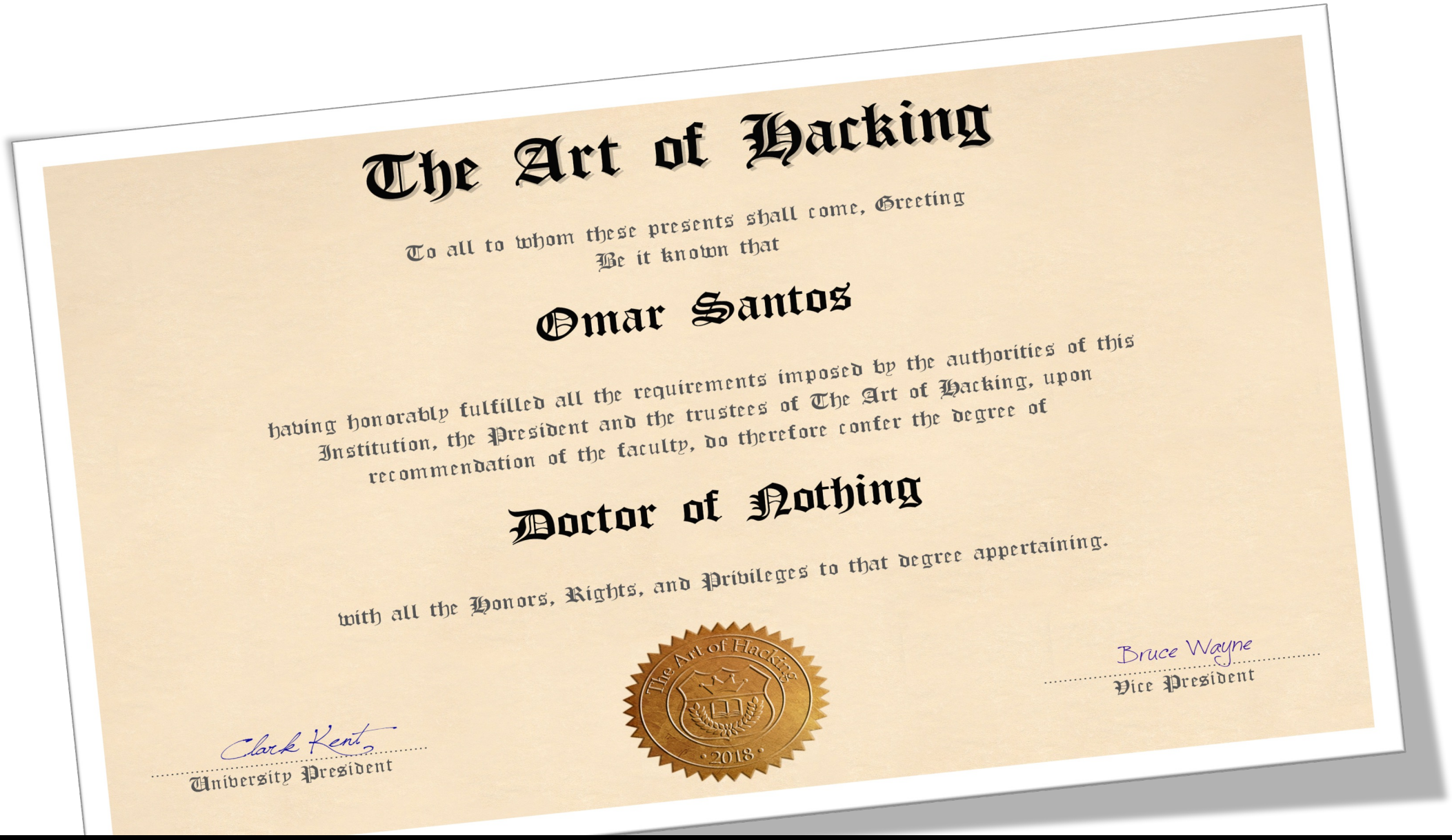
Vulnerabilities are threats, but not every threat is a vulnerability.

```
┌──(root㉿ websploit-kct1)-[~]
└─# searchsploit log4j
--------------------------------------------------------------- ---------------------------
 Exploit Title                                                 |  Path
--------------------------------------------------------------- ---------------------------
Apache Log4j 2 - Remote Code Execution (RCE)                   | java/remote/50592.py
Apache Log4j2 2.14.1 - Information Disclosure                  | java/remote/50590.py
--------------------------------------------------------------- ---------------------------
```

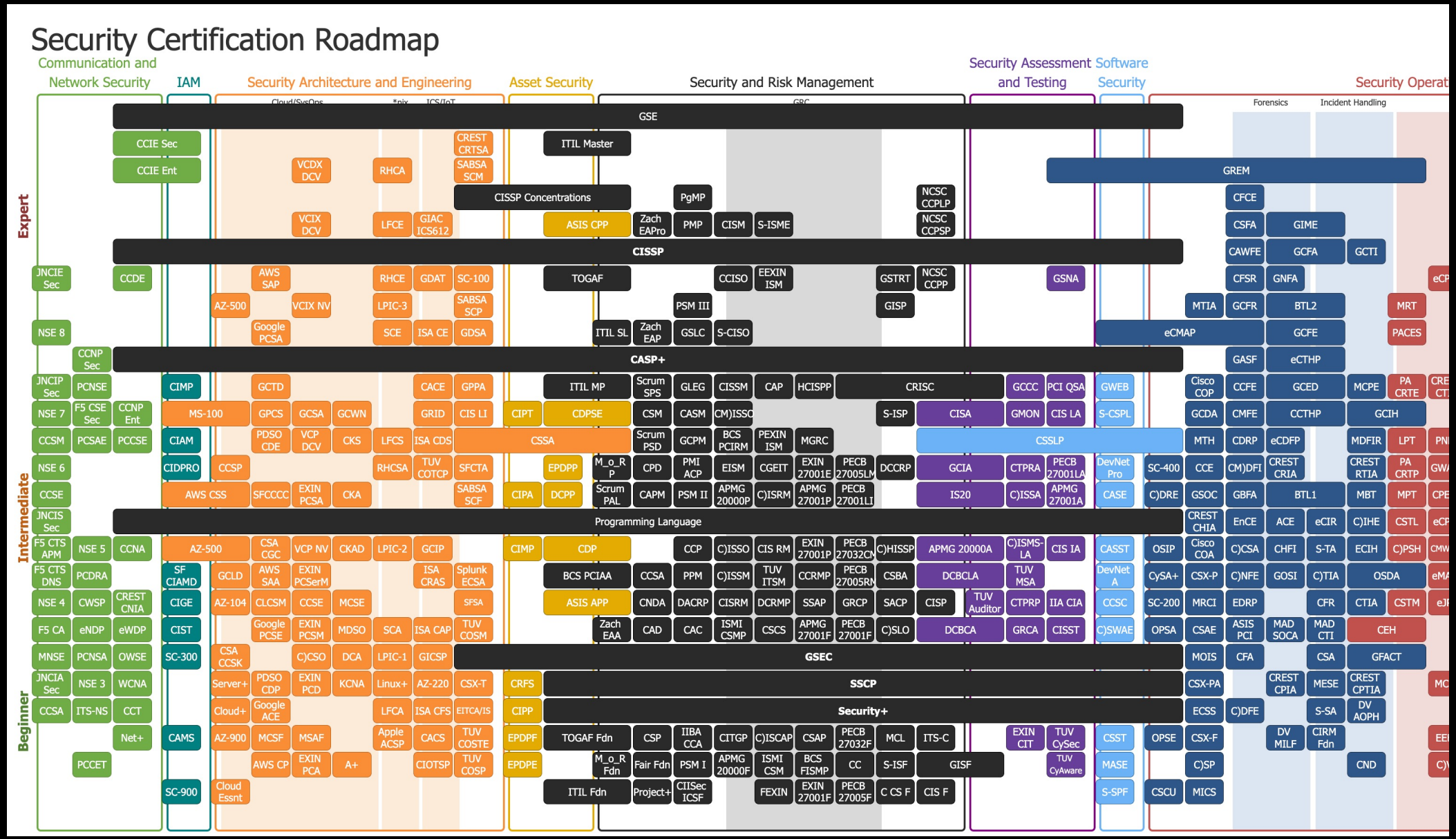
What is an Exploit?

- An exploit is software or a sequence of commands that takes advantage of a vulnerability in order to cause harm to a system or network.

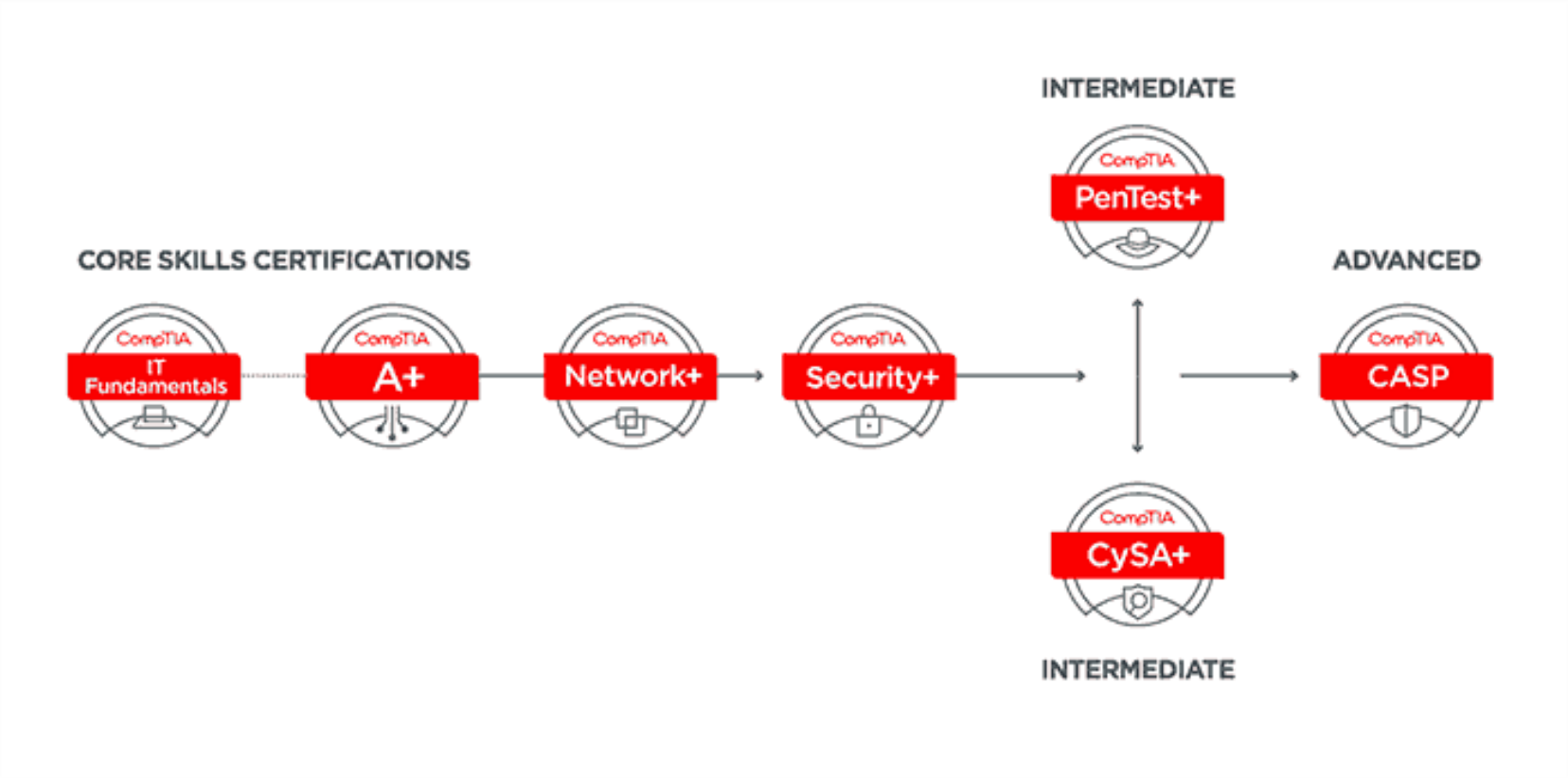
How Do You Get Started?

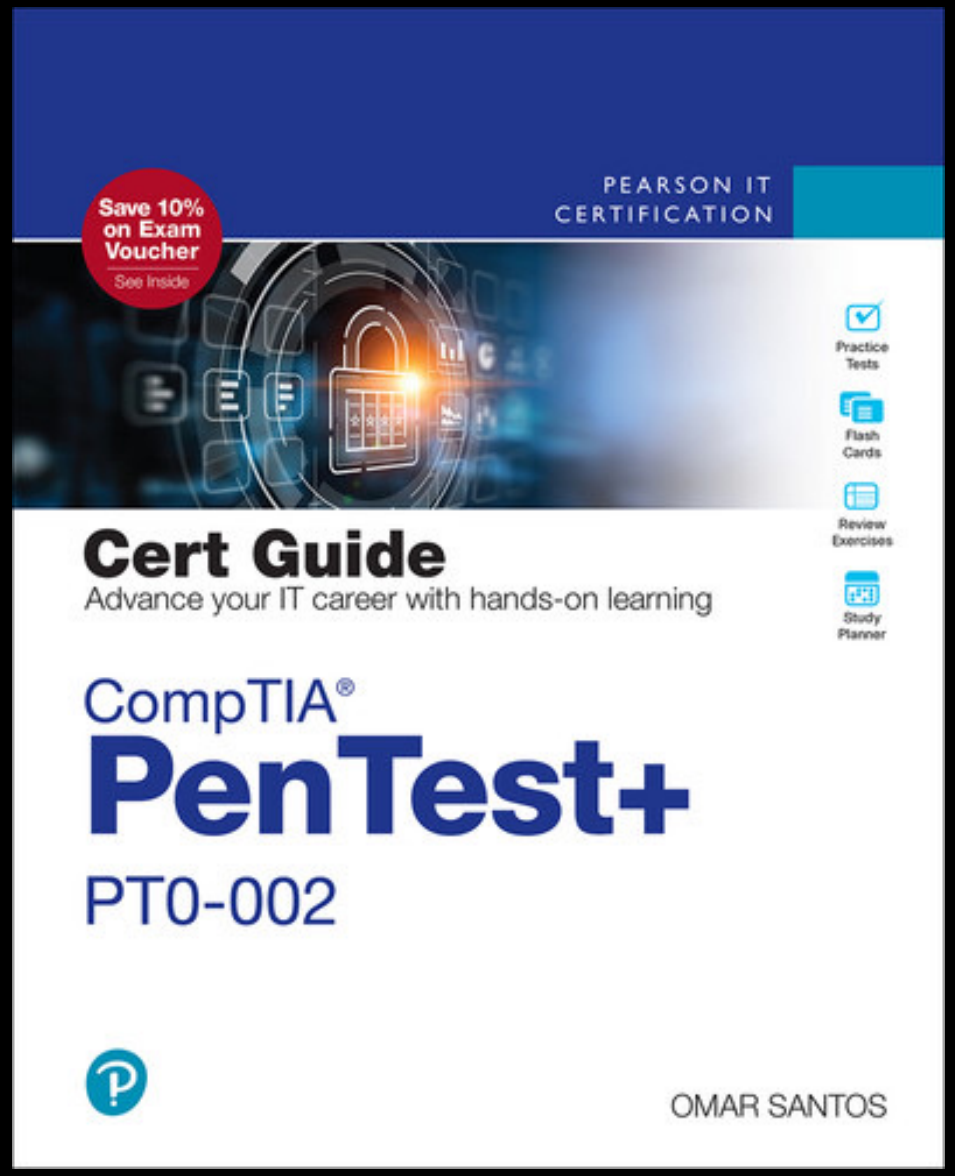


CYBERSECURITY AND ETHICAL HACKING CERTIFICATIONS



https://certs.h4cker.org


INTERMEDIATE
CompTIA
PenTest+
CORE SKILLS CERTIFICATIONS
ADVANCED
CompTIA
IT Fundamentals
CompTIA
A+
CompTIA
Network+
CompTIA
Security+
CompTIA
CASP
CompTIA
CySA+
INTERMEDIATE



You can use this as a guide for this class!

https://learning.oreilly.com/library/view/comptia-pentest-pt0-002/9780137566204

OFFENSIVE security

Courses | Certifications | Online Labs | Penetration Testing | Projects | Blog | About

Information Security Certifications

Hands-on information security certifications training by Offensive Security.

Information Security Certifications

For Pen Testers and IT Security Professionals

In-demand **Information Security Certifications** and hands-on ethical hacking courses for pen testers and IT security professionals. These ethical hacking certifications are provided by Offensive Security, the creators of Kali Linux.

Accompanying our **hands-on security training** programs are a set of industry leading **Information Security Certifications**, which are considered the most rigorous tests of skill available in the computer security field. These **performance-based certifications** rely entirely on **demonstrated ability and merit**. Instead of relying on outdated multiple choice questions, candidates are presented with a series of **real-world hacking challenges** which they must complete in a limited amount of time. Pass or fail is **based on**

BECOME CERTIFIED NOW!

OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP) and OTHERS

https://www.offensive-security.com

Ethical Hacking Bootcamp

Safari Live Training by Omar Santos

This is a comprehensive Ethical Hacking (security penetration testing) hands-on training! You will participate in live discussions, demos, whiteboard instruction and lab exercises. No prior experience is needed.
The author (Omar Santos) will walk you through numerous exercises and ethical hacking concepts.
If you are starting your cyber career, seeking your Certified Ethical Hacking (CEH), CompTIA PenTest+, or Offensive Security Certified Professional (OSCP) Certification, or just interested in learning more about cyber security, this three-day training session is a great resource!
This course provides step-by-step real-life scenarios. It starts by going over passive and active recon, then dives deep into scanning, target exploitation, password attacks, web application testing, buffer overflows, wired and wireless network hacking, and post-exploitation techniques.
You will use dozens of penetration testing tools and learn how to build your own lab!

https://bootcamp.h4cker.org

GIAC Penetration Testing Certification

GIAC Forensics, Manager

Secure | https://www.giac.org/certifications/pen-testing

GIAC CERTIFICATIONS

Login

Certifications | Exams | Certified Professionals | Programs | Resources | About

GIAC Certifications: Penetration Testing

High-value penetration testing doesn't involve just throwing a bunch of hacks at a target environment and declaring victory when a shell prompt magically pops up. Instead, the best penetration testers focus on understanding their craft in-depth. Pen Test Professionals provide significant value to organizations by improving their security stance through technical excellence and implementation of well-understood and repeatable methodologies. Ultimately, delivering real savings through information security to the business.

GIAC Certifications are developed with these principles in mind and to ensure penetration testers and ethical hackers achieve the status of certified expert penetration testers and ethical hackers.

Penetration Testing

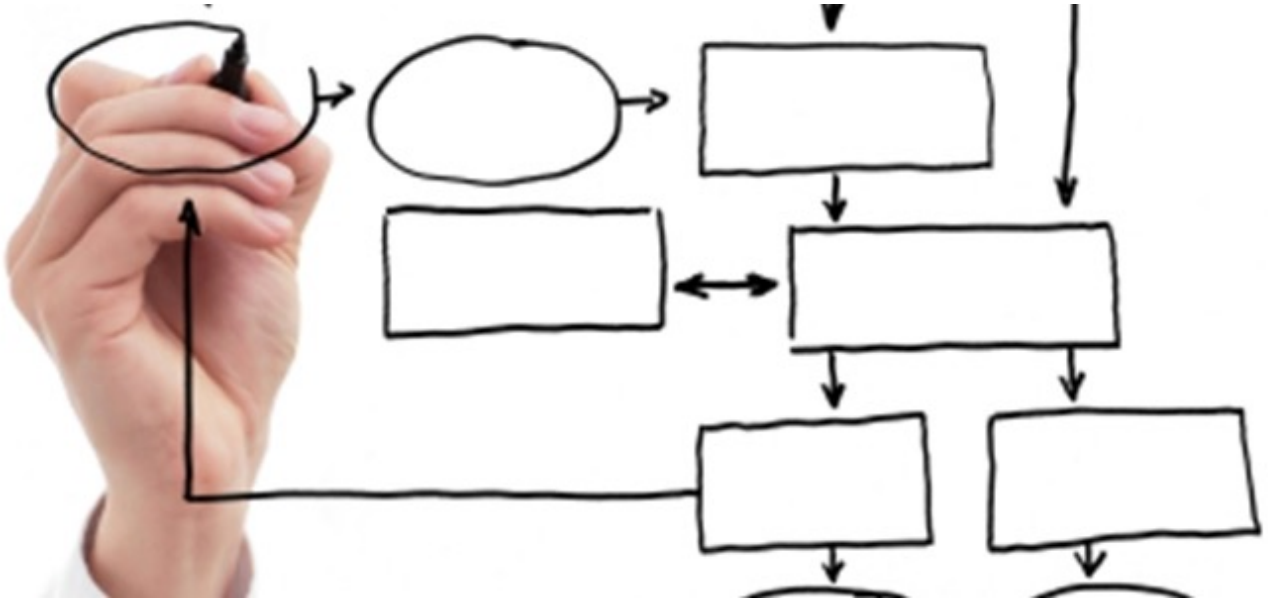
	Certification	Register
GCIH Certified Incident Handler	GCIH holders have demonstrated their ability to manage security incidents by understanding common attack techniques, vectors and tools as well as defending against and/or responding to such attacks when they occur. The GCIH certification focuses on methods used to detect, respond, and resolve computer security incidents. Affiliated Training: SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Register Now
	GPEN holders have demonstrated their ability to execute penetration testing and ethical hacking	

- Categories
- Cyber Defense
- Penetration Testing
- Incident Response and Forensics
- Management, Audit, Legal
- Developer
- Industrial Control Systems
- GSE

https://www.giac.org/certifications/pen-testing

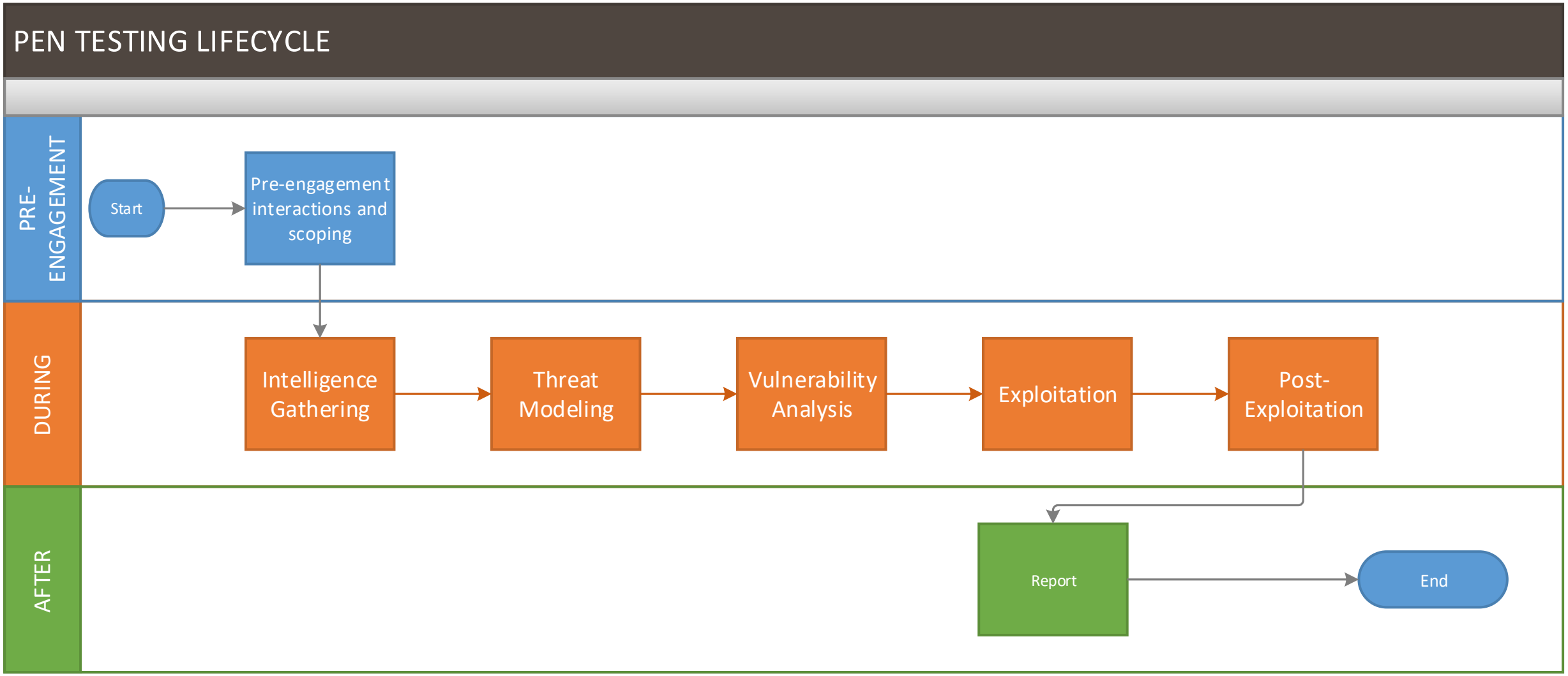
Hacking is a lot more than cool tools…

- Methodologies
- Research
- Think like an attacker
- Combine social engineering with technical capabilities



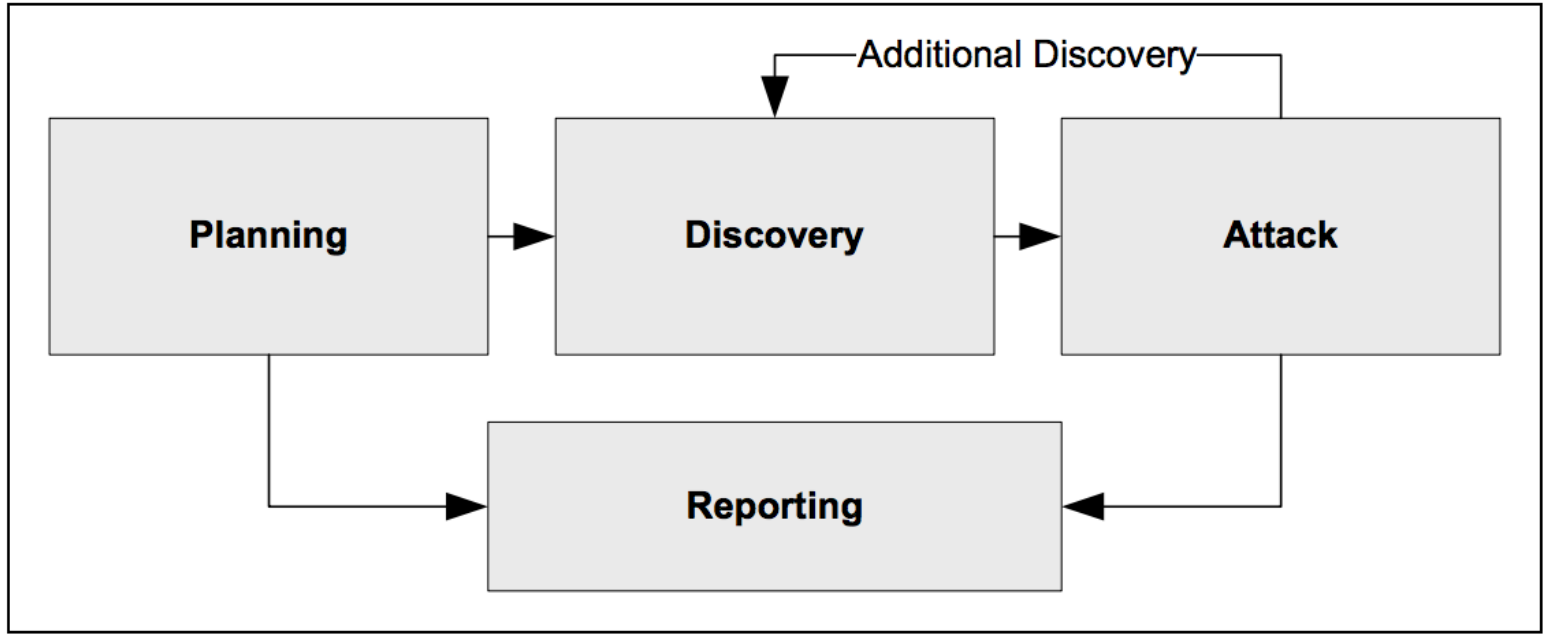
PEN TESTING METHODOLOGIES

- Penetration Testing Execution Standard
  https://www.pentest-standard.org
- OWASP Testing Guide
  https://www.owasp.org/index.php/OWASP_Testing_Project
- NIST 800-115: Technical Guide to Information Security Testing and Assessment
  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- Open Source Security Testing Methodology Manual (OSSTMM)
  https://www.isecom.org/research.html#content5-9d



Aligned with: http://www.pentest-standard.org

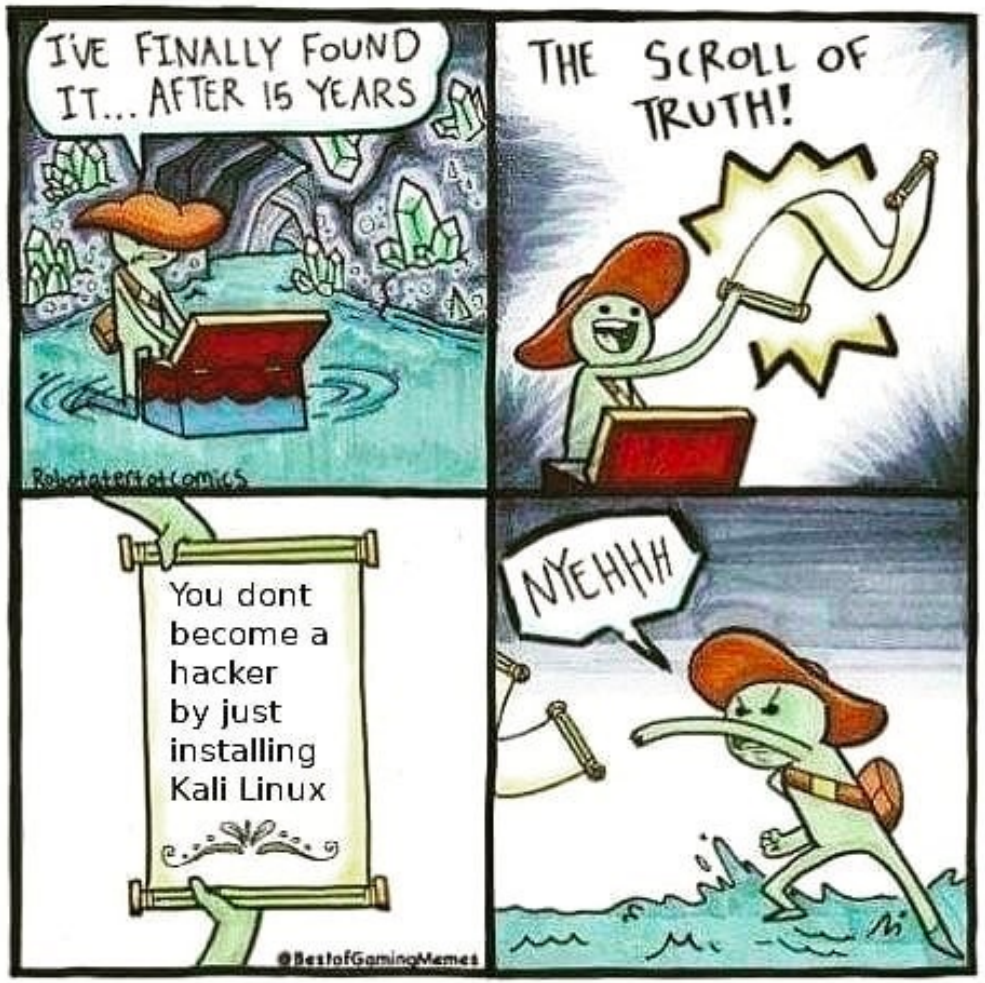
NIST 800-115



http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Penetration Testing Linux Distributions

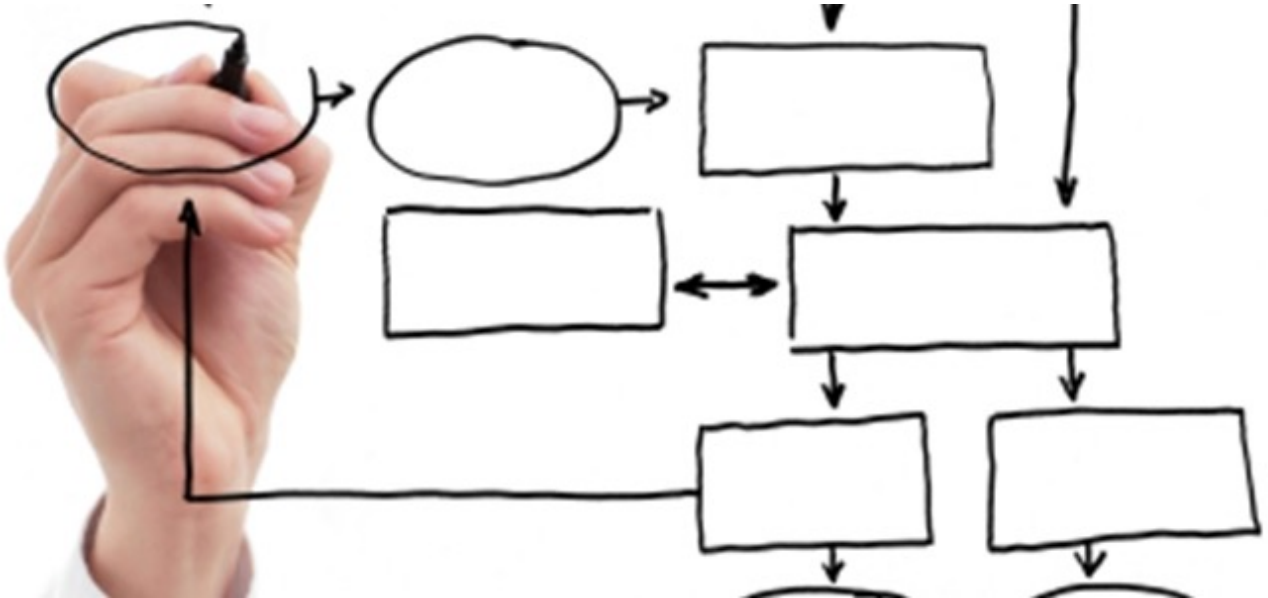
Kali Linux


I'VE FINALLY FOUND IT... AFTER 15 YEARS
THE SCROLL OF TRUTH!
You dont become a hacker by just installing Kali Linux
NYEHHH
@BestofGamingMemes

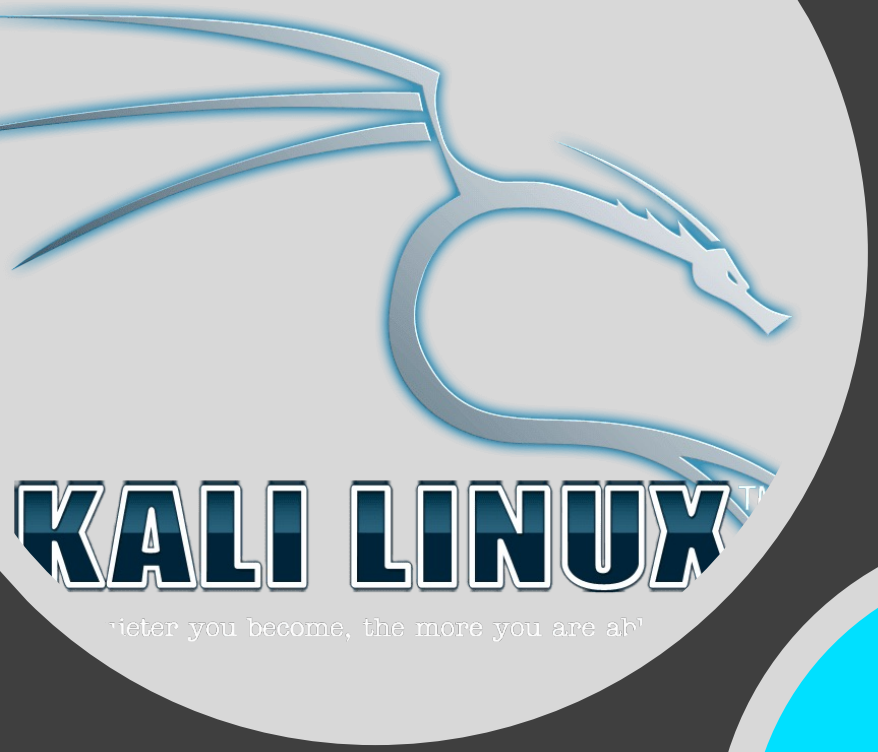
REMEMBER!

Hacking is a lot more than cool tools…

- Methodologies
- Research
- Think like an attacker
- Combine social engineering with technical capabilities

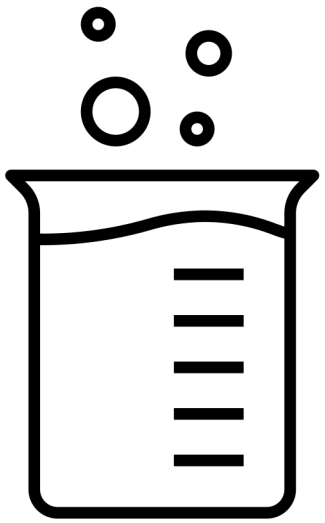


Pen Testing Linux Distributions



- Kali Linux https://www.kali.org
- Parrot Linux https://www.parrotsec.org
- BlackArch Linux https://blackarch.org

GUIDANCE ON HOW TO BUILD YOUR OWN LAB



The PenTesters Framework (PTF)

- A Python script designed for Debian/Ubuntu/ArchLinux based distributions to create a similar and familiar distribution for Penetration Testing.
- Created by David Kennedy and maintained by the community.
- https://github.com/trustedsec/ptf

Offensive Docker

- A Docker image with the most popular tools.
- https://github.com/aaaguirrep/offensive-docker
- docker pull aaaguirrep/offensive-docker

```
*****************************************************************************
     ___   __  __                _           ____             _
    / _ \ / _|/ _| ___ _ __  ___(_)_   _____  |  _ \  __   ___| | _____ _ __
   | | | | |_| |_ / _ \ '_ \/ __| \ \ / / _ \ | | | |/ _ \ / __| |/ / _ \ '__|
   | |_| |  _|  _|  __/ | | \__ \ |\ V /  __/ | |_| | (_) | (__|   <  __/ |
    \___/|_| |_|  \___|_| |_|___/_| \_/ \___| |____/ \___/ \___|_|\_\___|_|

Version: v0.2.7
-----------------------------------------------------------------------------
Creator: Arsenio Aguirre                          Email: a_aguirre117@hotmail.com
Repositories links:
Docker Hub: https://hub.docker.com/r/aaaguirrep/offensive-docker
Github: https://github.com/aaaguirrep/offensive-docker
*****************************************************************************
```

Bug Bounties vs. Red Teaming vs. Traditional Pen Testing

O'REILLY®

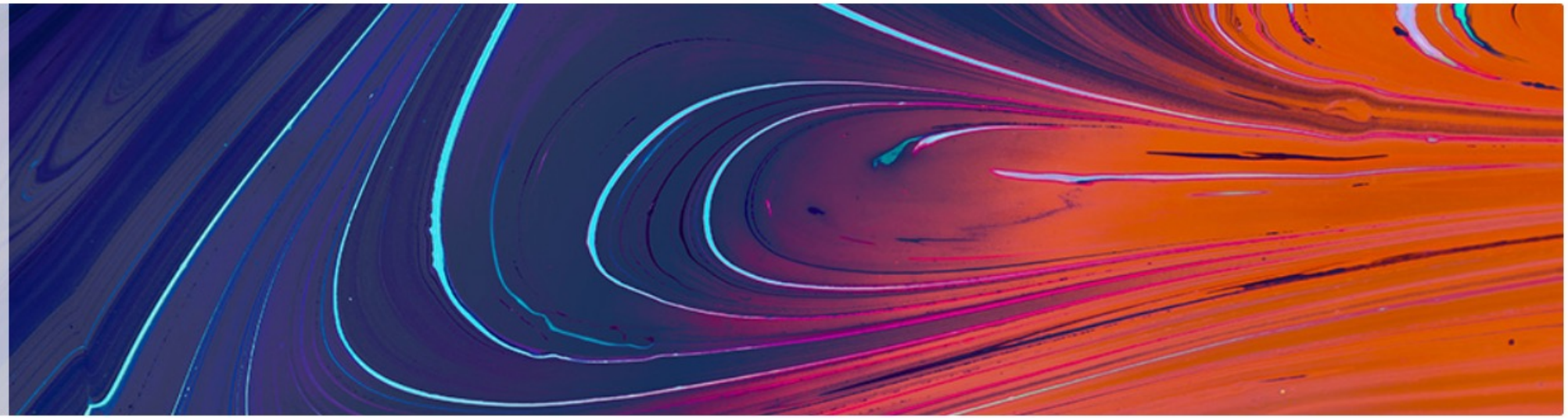
LIVE ONLINE TRAINING

Build Your Own Cybersecurity Lab and Cyber Range

Practice and Enhance Ethical Hacking and Defensive Security Skills

Topic: Security

OMAR SANTOS



BREAK

10 MINUTES

Passive and Active Reconnaissance

What is Passive Recon?

Reconnaissance without “actively” performing a scan, or launching any tools against the victim.

Examples:

- Google Hacking https://www.exploit-db.com/google-hacking-database/
- DNS Records
- Shodan
- Whois Information
- Tools like Recon-ng, Maltego, TheHarvester, Spiderfoot, etc.

OSINT Resources

https://github.com/The-Art-of-Hacking/h4cker/tree/master/osint

DEMO – Passive Recon

```
root@kali:~# msfconsole

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +-------------------------+-------------------------+
  |                         |                         |
  |   ==c(_____(o(_____(_()  |  |""""""""""""|======[***  |
  |             )=\         |  |  EXPLOIT   \          |
  |            // \\         |  |_____________\_______  |
  |           //   \\        |  |==[msf >]============\ |
  |          //     \\       |  |______________________\ |
  |         // RECON \\      |  \(@)(@)(@)(@)(@)(@)(@)/  |
  |        //         \\     |   *********************   |
  +-------------------------+-------------------------+
  |      o (( o             |   \'\/\/\/'/              |
  |          o0             |    '-----'                |
  |            o            |   .'  LOOT  '.            |
  | |^^^^^^^^^^^^^^|l___    |  /   _||__   \            |
  | |    PAYLOAD     |""\___, |  /   (_||_   \            |
  | |________________|__|)__| |  |    __||_)    |         |
  | |(@)(@)"""**|(@)(@)**|(@) |  "      ||      "         |
  |  = = = = = = = = = = = =  |   '--------------'        |
  +-------------------------+-------------------------+


       =[ metasploit v4.16.17-dev                         ]
+ -- --=[ 1703 exploits - 969 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

What is Active Recon?

"Actively" performing a network or vulnerability scan and launching other tools against the victim.

Examples:

- Scanners: Nmap, Nessus, Qualys, Nexpose, Retina

- Fuzzing (in some cases)

Applications Places Terminal Mon 14:12

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# msfconsole

  +-----------------------------------------------------+
  |  METASPLOIT by Rapid7                               |
  +---------------------------+-------------------------+
  |                           |                         |
  |   ==c(_____(o(_____(_()   | |""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT   \          |
  |            // \\          | |____________\_________|
  |           //   \\         | |==[msf >]============\ |
  |          //     \\        | |______________________\ |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/  |
  |        //         \\      |  ********************    |
  +---------------------------+-------------------------+
  |      o O o                |          \\/\\/ /        |
  |             o O           |          )======(        |
  |                o          |        .'  LOOT  '.      |
  | |^^^^^^^^^^^^^^|l___      |       /    _||__   \     |
  | |    PAYLOAD     |""\___, |      /    (_||_     \    |
  | |________________|__|)__| |     |     __||_)     |   |
  | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "   |
  | = = = = = = = = = = = = = |      '--------------'    |
  +---------------------------+-------------------------+


       =[ metasploit v4.16.17-dev                         ]
+ -- --=[ 1703 exploits - 969 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

DEMO – nmap

Cheat Sheets!

https://h4cker.org/cheat

O'REILLY Topics Start Learning Search 50,000+ courses, events, titles,...

Ethical Hacking: Introducing Network and Port Scanning using Nmap

58:59

Step 2 of 6

Introduction to Nmap

About Nmap

Nmap is by far one of the most popular network scanning tools available and can run on most operating systems found in the field.

Installing Nmap

Installing Nmap on Ubuntu is done by running the following:

```
sudo apt install nmap -y
```

To check the current version installed run:

```
nmap -
```

If install

```
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
...
```

Terminal | The Art of Hacking Gi... | WebSploit Labs | Ethical Hacking Labs

```
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,669 kB of archives.
After this operation, 26.8 MB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0-1build1 [142 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64 2.3.0+dfsg-3build1 [41.7
Get:3 http://us.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.3-0 amd64 5.3.3-1.1ubuntu2 [116 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 nmap-common all 7.80+dfsg1-2build1 [3,676
Get:6 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 nmap amd64 7.80+dfsg1-2build1 [1,662 kB]
Fetched 5,669 kB in 1s (4,298 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 135481 files and directories currently installed.)
Preparing to unpack .../0-libblas3_3.9.0-1build1_amd64.deb ...
Unpacking libblas3:amd64 (3.9.0-1build1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../1-liblinear4_2.3.0+dfsg-3build1_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Selecting previously unselected package liblua5.3-0:amd64.
Preparing to unpack .../2-liblua5.3-0_5.3.3-1.1ubuntu2_amd64.deb ...
Unpacking liblua5.3-0:amd64 (5.3.3-1.1ubuntu2) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../3-lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../4-nmap-common_7.80+dfsg1-2build1_all.deb ...
Unpacking nmap-common (7.80+dfsg1-2build1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../5-nmap_7.80+dfsg1-2build1_amd64.deb ...
Unpacking nmap (7.80+dfsg1-2build1) ...
Setting up libblas3:amd64 (3.9.0-1build1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-
libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up nmap-common (7.80+dfsg1-2build1) ...
Setting up liblua5.3-0:amd64 (5.3.3-1.1ubuntu2) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Setting up nmap (7.80+dfsg1-2build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
```

LAB 1: Intro to Network Scanning

https://learning.oreilly.com/scenarios/ethical-hacking-introducing/9780137673469X001/

O'REILLY Topics Start Learning Search 50,000+ courses, events, titles,...

< Ethical Hacking: Advanced Nmap Scanning and the Nmap Scripting Engine 56:01

Step 6 of 6

```
'02:42:0A:00:00:05', 'addrtype': 'mac'},
             'osmatch': {},
             'ports': [{'portid': '21',
                        'protocol': 'tcp',
                        'reason': 'syn-ack',
                        'reason_ttl': '64',
                        'scripts': [],
                        'service': {'conf':
'3',
                                    'method':
'table',
                                    'name':
'ftp'},
                        'state': 'open'},
                        'portid': '
                        'protocol
                        'reason': 'syn-ack',
                        'reason_ttl': '64',
                        'scripts': [],
'3',                                'method':
'table',
```

Terminal IDE The Art of Hacking Gi... WebSploit Labs Ethical Hacking Labs

```
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with
manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
$ pip3 install python3-nmap
Collecting python3-nmap
  Downloading python3_nmap-1.6.0-py3-none-any.whl (26 kB)
Requirement already satisfied: simplejson in /usr/lib/python3/dist-packages (from python3-nmap) (3.16.0
Installing collected packages: python3-nmap
Successfully installed python3-nmap-1.6.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with
manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
$ cat nmap.py
# Import Pretty Printing
from pprint import pprint

# Import the Nmap Module
import nmap3

# Create an nmap Object
nmap = nmap3.Nmap()

# Helper functions

def print_output(message: str, results: str) -> None:
    """Handle output message and printing results"""
    pprint("")
    pprint('-'*30)
    pprint(message)
    pprint(results)

# Define target host
HOST = "10.0.0.5"
SUBNET = "10.0.0.0/24"

# Nmap Top Ports Scan
results = nmap.scan_top_ports(HOST)
print_output(f"Top ports of {HOST}", results)

# Nmap OS Detection
results = nmap.nmap_os_detection(HOST)
```

LAB 2: Advanced NMap

https://learning.oreilly.com/scenarios/ethical-hacking-advanced/9780137673469X002

Applications Places Terminal Tue 18:41

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# enum4linux
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This opion is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins
,root,bin,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
```

DEMO – enum4linux

```
root@kali:~# enum4linux
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This opion is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins
,root,bin,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
```

LAB 3: Scanning Containers with Grype

https://learning.oreilly.com/scenarios/ethical-hacking-scanning/9780137673469X005

LAB 4: Scanning Containers Using Trivy

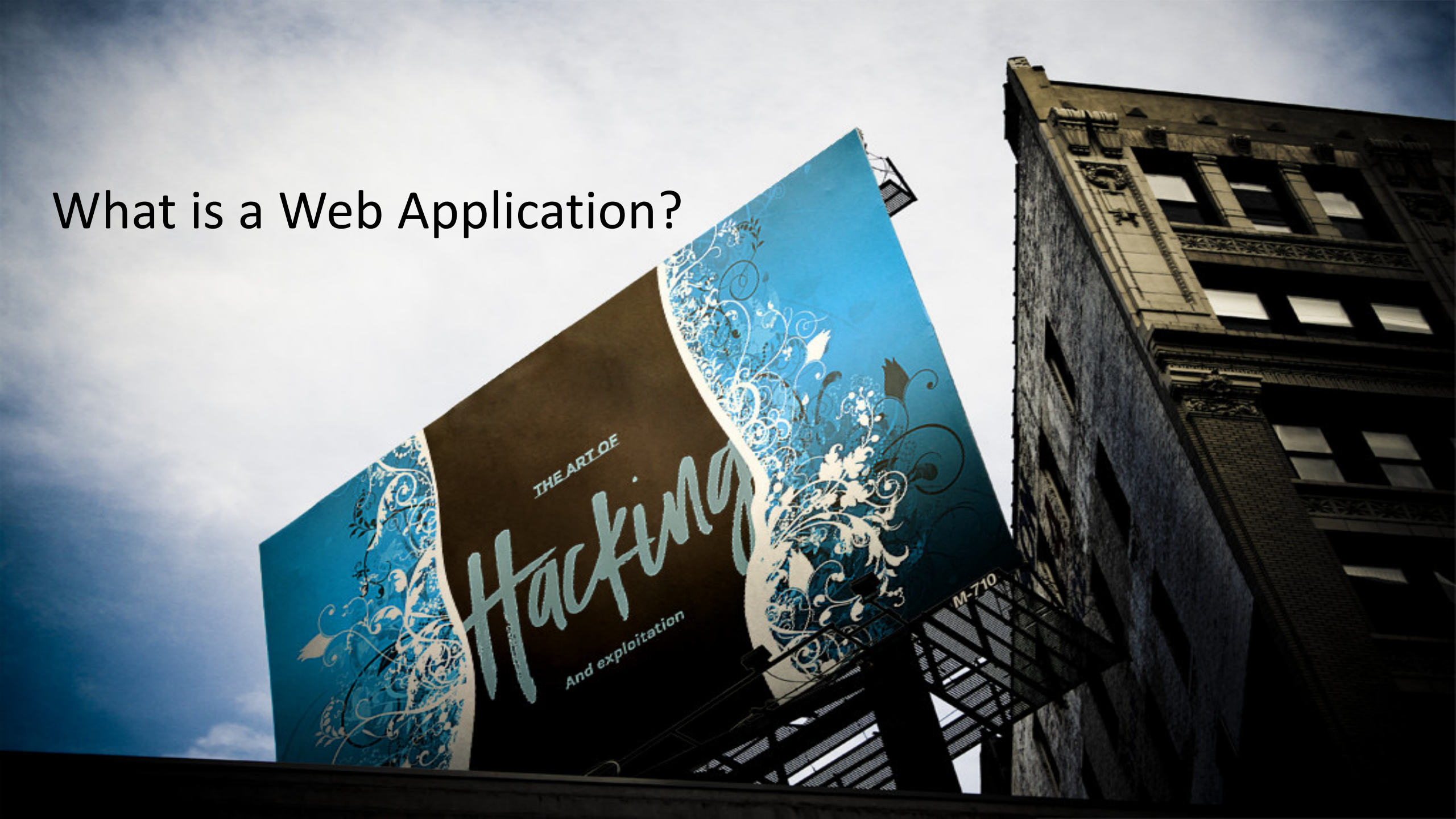
https://learning.oreilly.com/scenarios/ethical-hacking-active/9780137835720X005/

Introduction to Hacking Web Applications

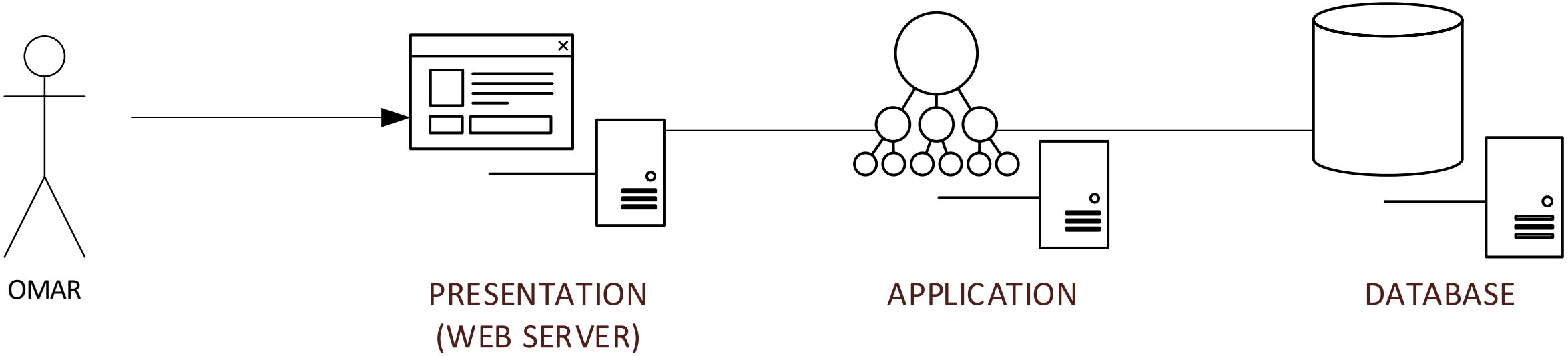
Free with your Safari subscription

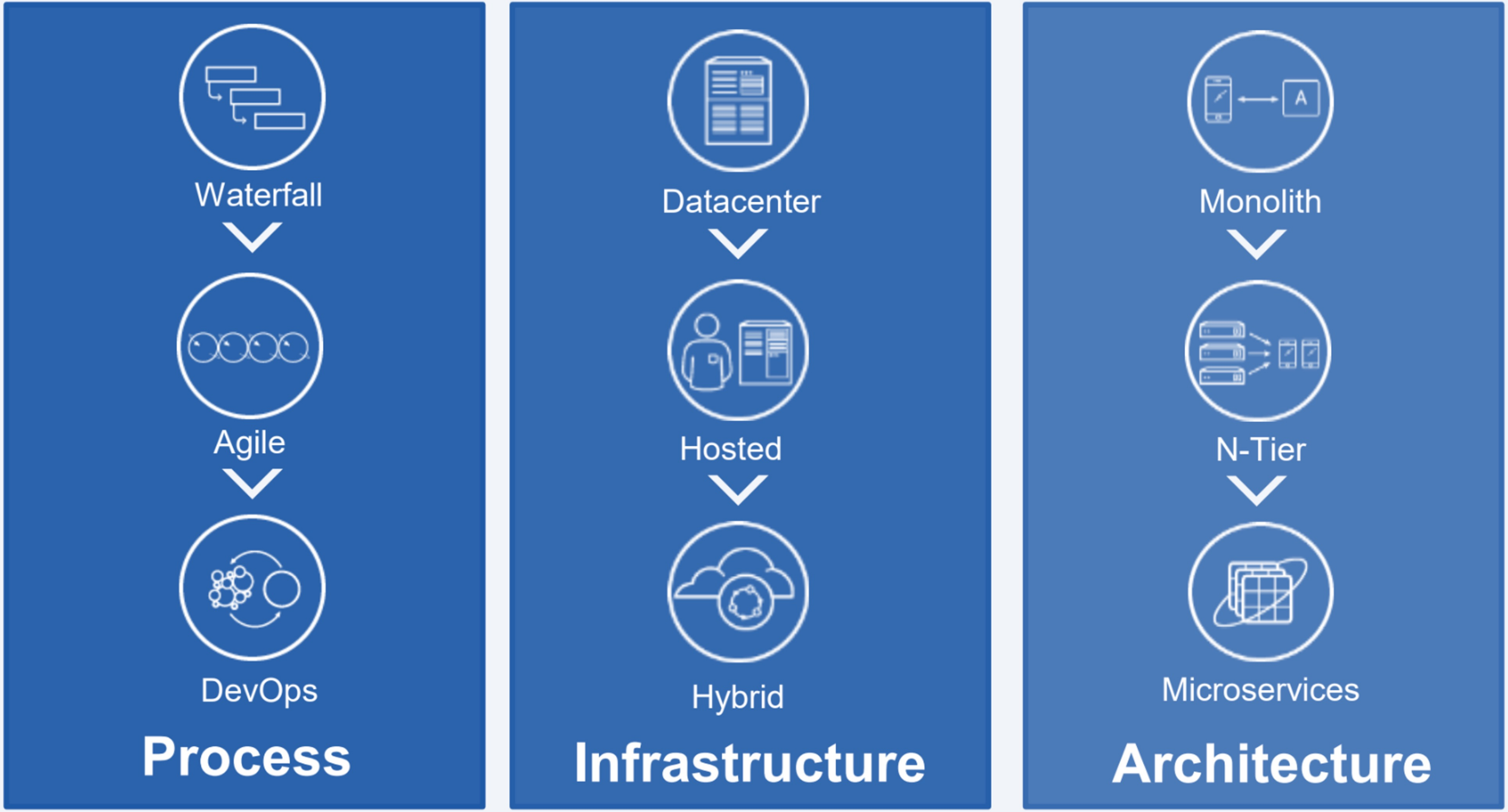
https://webapps.h4cker.org

What is a Web Application?



THE TRADITIONAL WEB APPLICATION ARCHITECTURE




Waterfall
Agile
DevOps
Process
Datacenter
Hosted
Hybrid
Infrastructure
A
Monolith
N-Tier
Microservices
Architecture

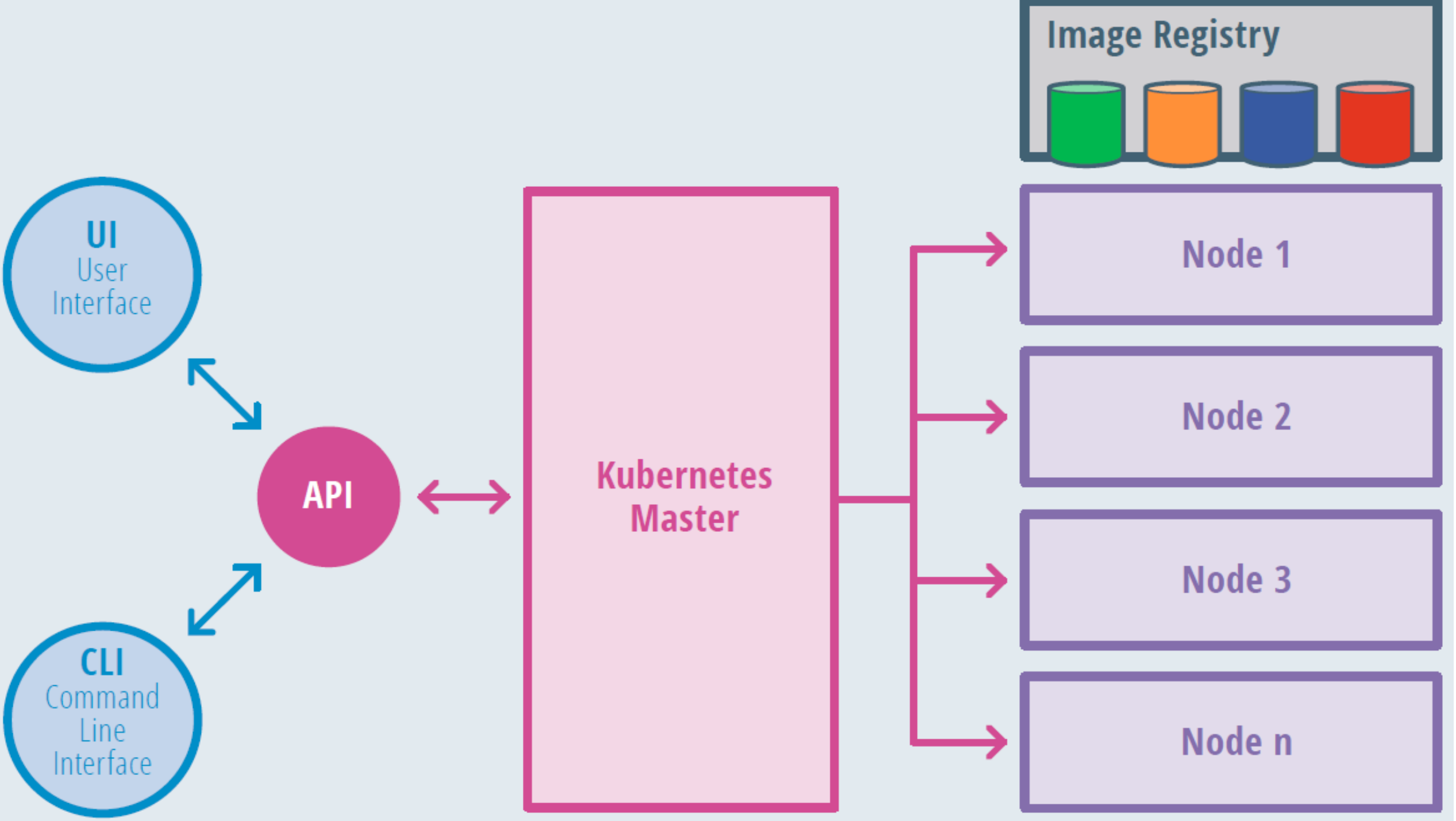
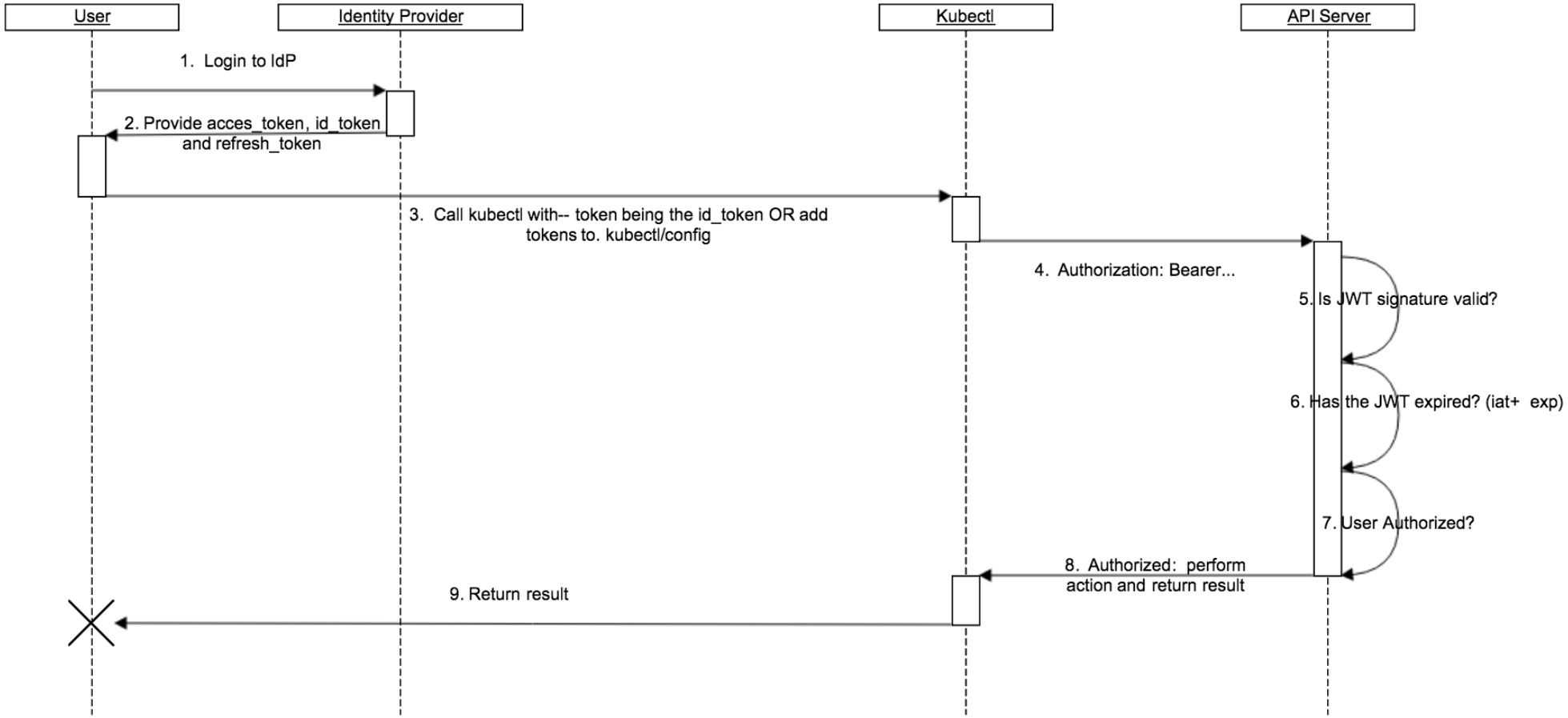


Image Registry
UI
User
Interface
API
CLI
Command
Line
Interface
Kubernetes
Master
Node 1
Node 2
Node 3
Node n

OPENID AUTHENTICATION FLOW



WEBHOOK MODE EXAMPLE REQUEST

```
{
  "apiVersion": "authorization.k8s.io/v1beta1",
  "kind": "SubjectAccessReview",
  "spec": {
    "resourceAttributes": {
      "namespace": "kittensandponies",
      "verb": "get",
      "group": "unicorn.example.org",
      "resource": "pods"
    },
    "user": "jane",
    "group": [
      "group1",
      "group2"
    ]
  }
}
```

```
{
  "apiVersion": "authorization.k8s.io/v1beta1",
  "kind": "SubjectAccessReview",
  "status": {
    "allowed": false,
    "reason": "user does not have read access to the namespace"
  }
}
```

Understand how the application works

- Purpose (e.g. app configuration)
- Functions (e.g. account provisioning)

Gather needed information

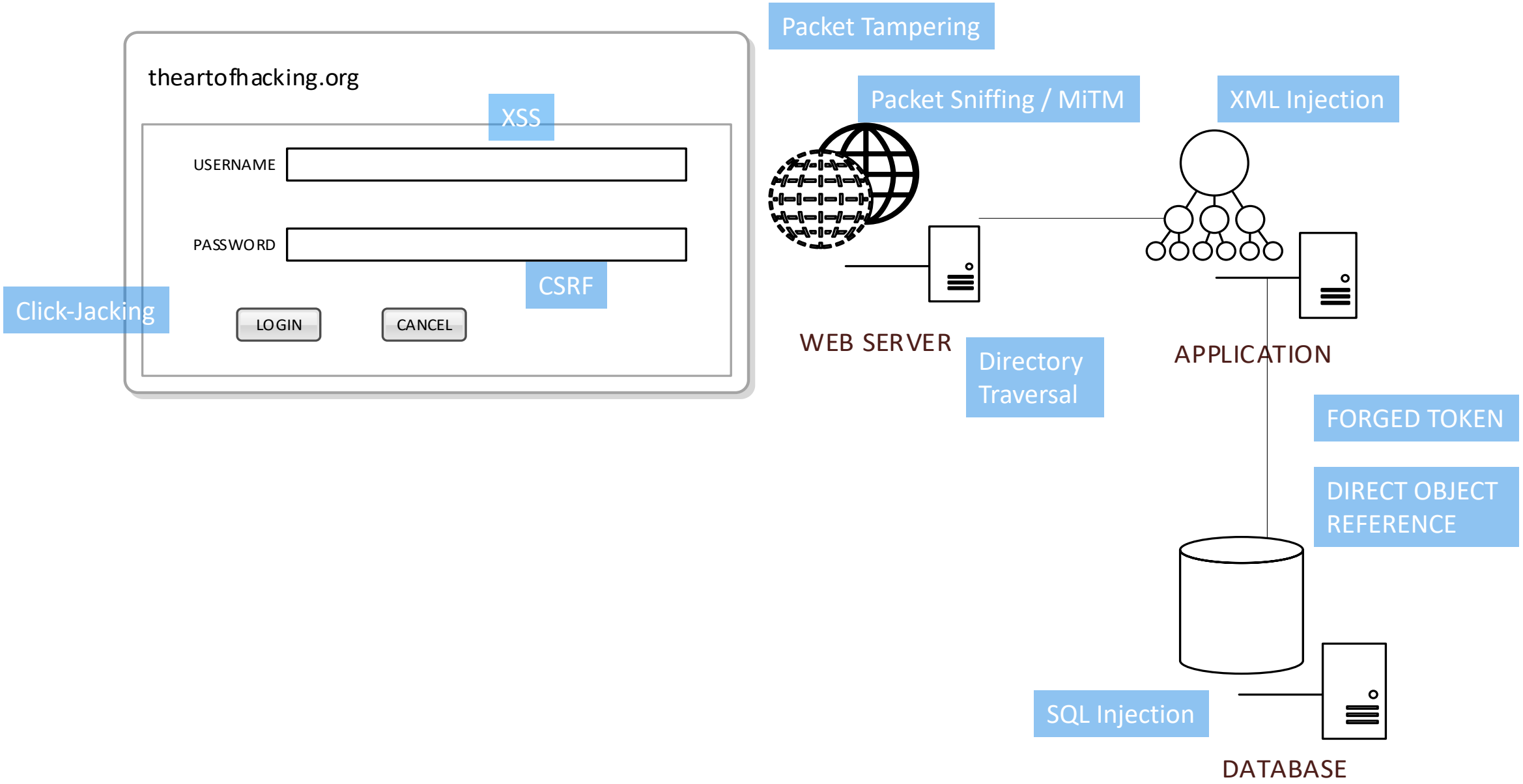
- credentials, tokens, API configurations

Break the application to manageable chunks

- Large app scans can take hours
- Functional breakout (admin, reporting)

Allot time to reset the application & purge backend database

- Scans inject bad data
- Can use VM snapshots


theartofhacking.org
XSS
USERNAME
PASSWORD
CSRF
Click-Jacking
LOGIN
CANCEL
Packet Tampering
Packet Sniffing / MiTM
XML Injection
WEB SERVER
Directory Traversal
APPLICATION
FORGED TOKEN
DIRECT OBJECT REFERENCE
SQL Injection
DATABASE

ASP®

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Store

Donate

Joi

Who is the OWASP® Foundation?

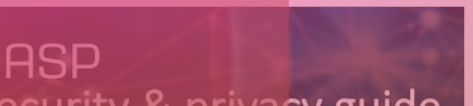
The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through communit led open-source software projects, hundreds of local chapters worldwide, ter of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and voluntee have supported the OWASP Foundation and its work. Donate, Join, or becor a Corporate Member today.

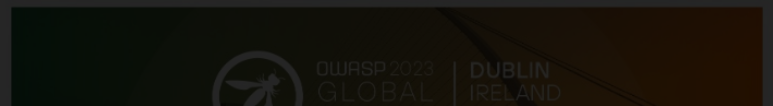
https://www.owasp.org

Spotlight: AI Security and Privacy Guide



AI applications are on the rise and so are the concerns regarding AI security

OWASP 2023 Global AppSec Dublin



Registration Open!

OWASP Top 10

https://owasp.org/www-project-top-ten/

OWASP Cheat Sheet Series

https://cheatsheetseries.owasp.org

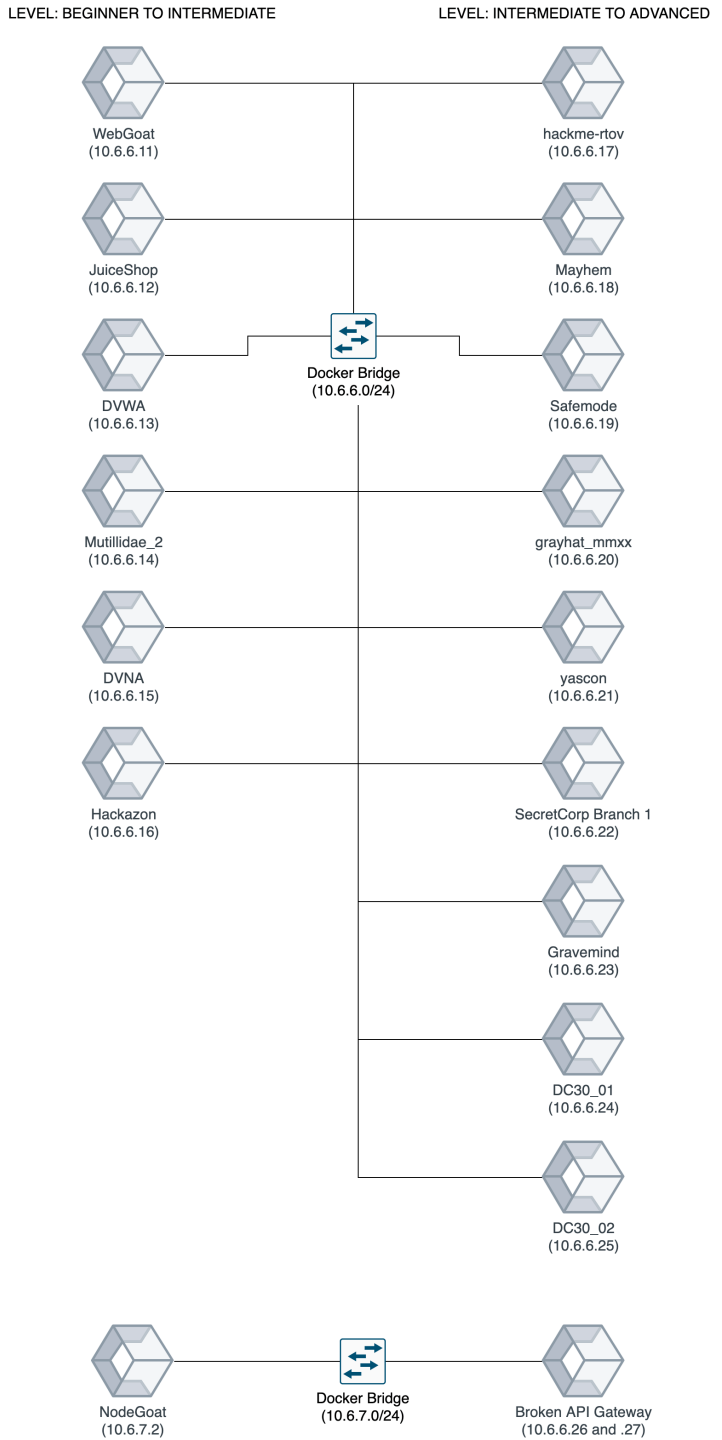
OWASP

CHEAT SHEET

SERIES PROJECT

WebSploit Containers

https://websploit.org



WebGoat - Mozilla Firefox

WebGoat | WebGoat/WebGoat: ... | art-of-hacking/vulner... | Vulnerability: File Upl...

192.168.78.8:8080/WebGoat/start.mvc#lesson/SqlInjectionAdvanced.lesson/3

Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums | NetHunter | Getting Started

WEBGOAT

- Introduction
- General
- Injection Flaws
  - SQL Injection
  - SQL Injection (advanced)
  - SQL Injection (mitigations)
  - XXE
- Authentication Flaws
- Cross-Site Scripting (XSS)
- Access Control Flaws
- Insecure Communication
- Request Forgeries
- Vulnerable Components - A9
- Client side
- Challenges

SQL Injection (advanced)

Reset lesson

1 2 3 4 5

Blind SQL Injection

Blind SQL injection is a type of SQL injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

Difference

Let's first start with the difference between a normal SQL injection and a blind SQL injection. In a normal SQL injection the error messages from the database are displayed and gives enough information to find out how the query is working. Or in the case of an union based SQL injection the application does not reflect the information directly on the webpage. So in the case where nothing is displayed you will need to start asking the database questions based on a true or false statement. That's why a blind SQL injection is much more difficult to exploit.

There are several different types of blind SQL injections: content based and time based SQL injections.

Example

In this case we are trying to ask the database a boolean question based on for example a unique id, for example suppose we have the following url: `https://my-shop.com?article=4` On the server side this query will be translated as follows:

```
SELECT * from articles where article_id = 4
```

When we want to exploit this we change the url into: `https://my-shop.com?article=4 AND 1=1` This will be translated to:

```
SELECT * from articles where article_id = 4 AND 1 = 1
```

If the browser will return the same page as it used to when using `https://my-shop.com?article=4` you know the website is vulnerable for a blind SQL injection. If the browser responds with a page not found or something else you know a blind SQL injection might not work. You can now change the SQL query and test for example: `https://my-shop.com?article=4 AND 1=2` which will not return anything because the query returns false.

So but how do we actually take advantage of this? Above we only asked the database for trivial question but you can for example also use the following url:
`https://my-shop.com?article=4 AND substring(database_version(),1,1) = 2`

Most of the time you start by finding which type of database is used, based on the type of database you can find the system tables of the database you can enumerate all the tables present in the database. With this information you can start getting information from all the tables and you are able to dump the database. Be aware that this approach might not work if the privileges of the database are setup correctly (meaning the system tables cannot be queried with the user used to connect from the web application to the database).

Another way is called a time based SQL injection, in this case you will ask the database to wait before returning the result. You might need to use this if you are totally blind so there is no difference between the response you can use for example:

Damn Vulnerable Web Application (DVWA) >> http://www.dvwa.co.uk

DVWA

- Home
- Instructions
- Setup / Reset DB

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- XSS (Reflected)
- XSS (Stored)

- DVWA Security
- PHP Info
- About

- Logout

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficultly levels**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

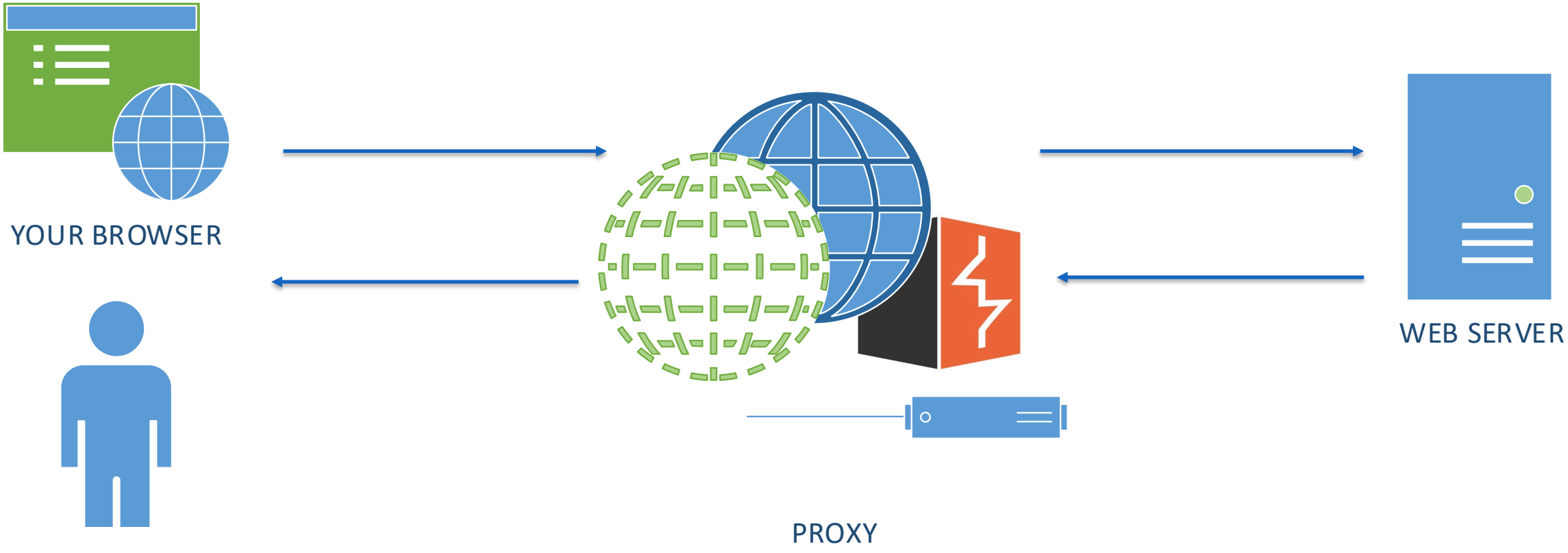
Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the

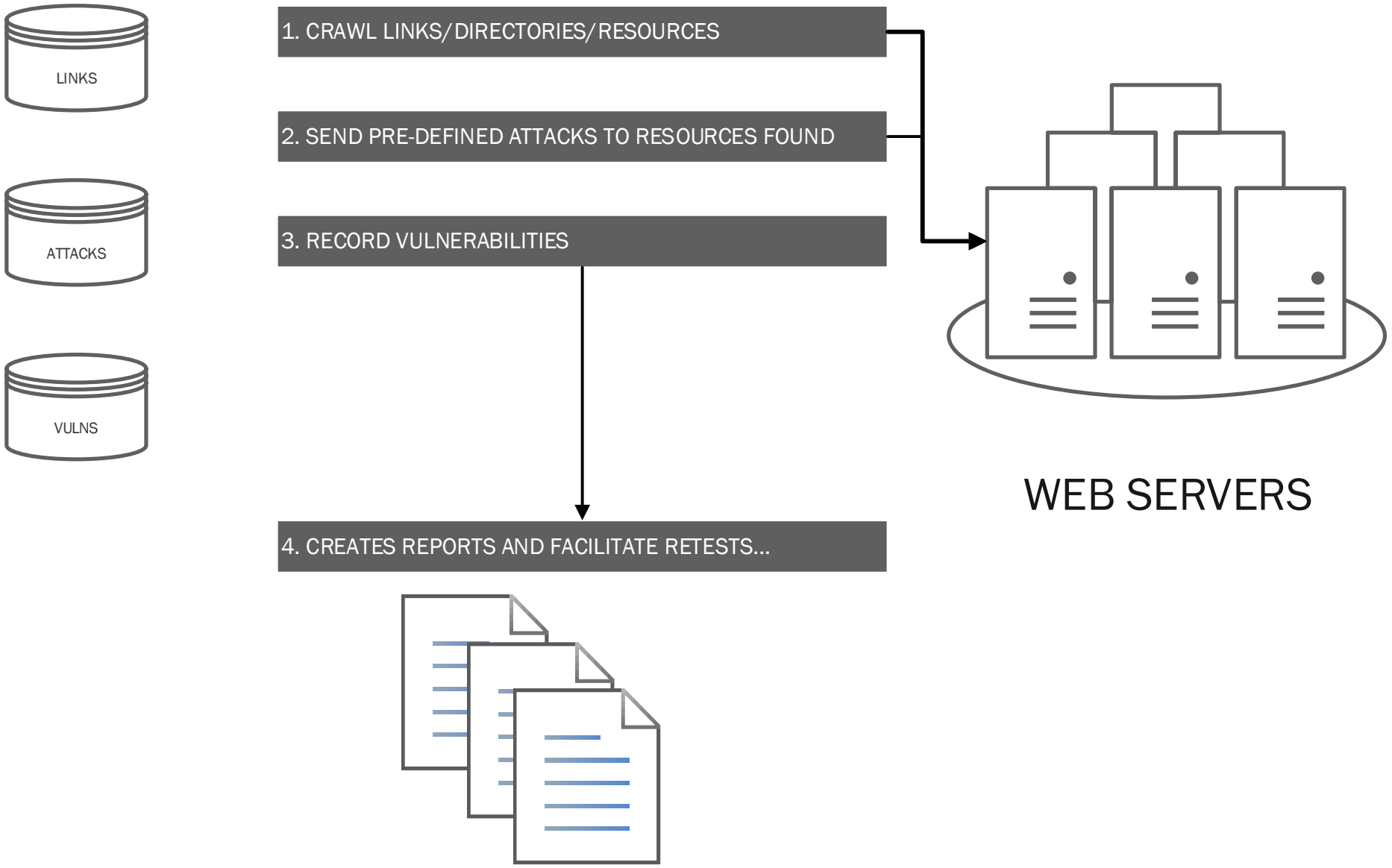
TYPES OF WEB TESTING TOOLS

- Web Vulnerability Scanners
- Proxies
- Browser Plugins
- Automation APIs
- Static Analysis Scanners
- Exploitation Frameworks



Modification
Analysis
Recording

HOW WEB SCANNERS WORK?


LINKS
ATTACKS
VULNS
1. CRAWL LINKS/DIRECTORIES/RESOURCES
2. SEND PRE-DEFINED ATTACKS TO RESOURCES FOUND
3. RECORD VULNERABILITIES
4. CREATES REPORTS AND FACILITATE RETESTS...
WEB SERVERS

This repository Search Pull requests Issues Marketplace Explore

fuzzdb-project / fuzzdb

Watch 206 Star 1,886 Fork 558

Code Issues 12 Pull requests 7 Projects 0 Wiki Insights

Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.

404 commits 2 branches 0 releases 11 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

amuntner committed on Jan 16, 2017 Strings which can be accidentally expanded into different strings if ... Latest commit ecb0850 on Jan 16, 2017

attack	Strings which can be accidentally expanded into different strings if ...	a year ago
discovery	Update SAP.txt	a year ago
docs	from https://github.com/attackercan/	a year ago
regex	cross-updating with https://github.com/andresriancho/w3af/blob/master...	a year ago
web-backdoors	Tiny php remote os commanding backdoor	a year ago
wordlists-misc	Innocuous strings which may be blocked by profanity filters (https://...	a year ago
wordlists-user-passwd	Refreshed 3/8/16	2 years ago
README.md	Update README.md	a year ago
_copyright.txt	Update date to 2017, add addtl license	a year ago

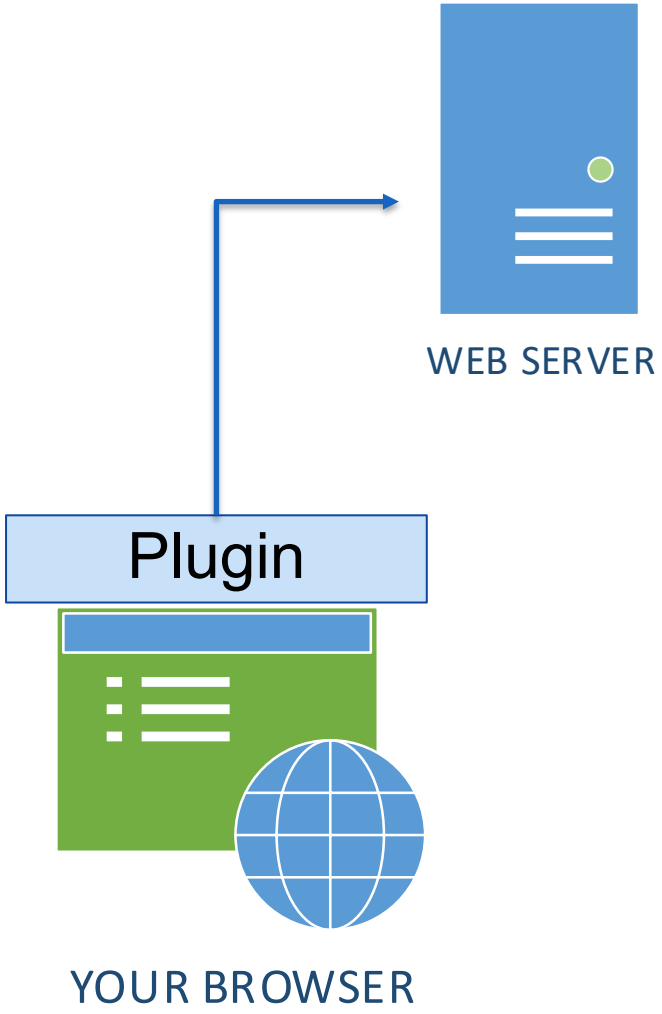
README.md

FuzzDB was created to increase the likelihood of causing and identifying conditions of security interest through dynamic application security testing. It's the first and most comprehensive open dictionary of fault injection patterns, predictable resource locations, and regex for matching server responses.

https://github.com/fuzzdb-project/fuzzdb

Browser Plugins

- How do they work?
- Many possible functions
  - Intercepting and modifying traffic
  - Manipulation of cookies
  - Attack injection
  - Debugging
  - Easily manage proxies
  - Password crackers, format translators, etc.



kali-linux-2017.3-vm-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali-linux-2017.3-vm-am...

Applications Places Thu 11:53

<New userscript> - Mozilla Firefox

Big bertha says: defau... | Add-ons Manager | <New userscript>

moz-extension://4ed95de2-98e6-4f1e-8d7c-f25d680eec51/options.html#nav=new-user-script+editor

Search

Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums | NetHunter | Getting Started

Tampermonkey®
v4.5.5660 by Jan Biniok

Installed userscripts | Settings | Utilities | Help

<New userscript>

Editor

ECMAScript 5 | Update URL:

Search | Replace | Jump to line | Insert constructor | Auto-Indent all

```
// ==UserScript==
// @name         Omar's new script
// @namespace    http://tampermonkey.net/
// @version      0.1
// @description  try to take over the world!
// @author       You
// @match        http://*/*
// @grant        none
// ==/UserScript==

(function() {
    'use strict';

    // Your code here...
})();
```

To direct input to this VM, click inside or press Ctrl+G.

Web Exploitation Frameworks

- Metasploit
- Browser Exploitation Framework (BeEF)

DEMO – Burp Suite

Burp Suite Free Edition v1.7.27 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Intercept | HTTP history | WebSockets history | Options

History logging of out-of-scope items is disabled

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
23	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
24	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
25	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
26	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
27	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
28	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
29	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
30	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
31	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
32	http://192.168.78.8:8080	POST	/WebGoat/IDOR/login	✓		200	383	JSON					192.168.
33	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1037	JSON	mvc				192.168.
34	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
35	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
36	http://192.168.78.8:8080	GET	/WebGoat/IDOR/profile			200	374	JSON					192.168.

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Application-Context: application:8080
Content-Type: application/json;charset=UTF-8
Date: Wed, 14 Feb 2018 23:10:29 GMT
Connection: close
Content-Length: 104

{
  "[illegible]": 3,
  "[illegible]olor": "y[illegible]llow",
  "[illegible]ize": "sm[illegible]ll",
  "[illegible]ame": "To[illegible] Cat",
  "[illegible]serI[illegible]": "[illegible]342384"
}
```

Type a search term

0 matches

WebGoat | WebGoat/WebG

192.168.78.8:8080/WebGoat/start.mvc#

Offensive Security | Kali Linux | Kali Docs | Ka

WEBGOAT

- Introduction
- General
- Injection Flaws
- Authentication Flaws
- Cross-Site Scripting (XSS)
- Access Control Flaws
  - Insecure Direct Object References
  - Missing Function Level Access Control
- Insecure Communication
- Request Forgeries
- Vulnerable Components - A9
- Client side
- Challenges

Cross-site Scripting (XSS)

Reflected XSS:

The application or API includes unvalidated and un-escaped user input as part of HTML output. A successful attack can allow the attacker to execute arbitrary HTML and JavaScript in the victim's browser.

Stored XSS:

Un-sanitized user input that is viewed at a later time by another user or an administrator. Stored XSS is often considered a high or critical risk.

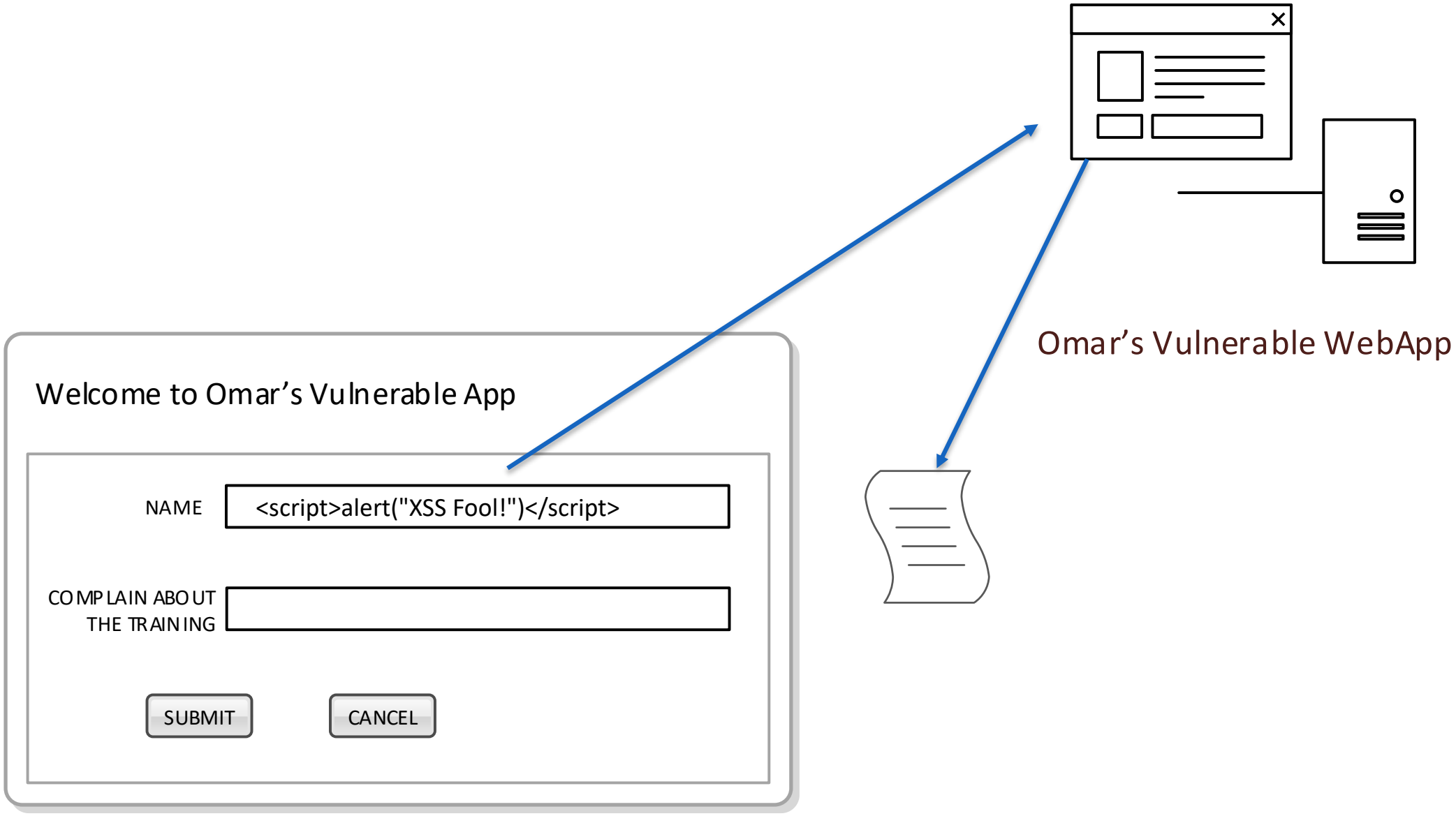
DOM XSS:

JavaScript frameworks, single-page applications, and APIs that dynamically include attacker-controllable data to a page are vulnerable to DOM XSS.

XSS attacks include session stealing, account takeover, MFA bypass, DOM node replacement or defacement (such as trojan login panels), attacks against the user's browser such as malicious software downloads, key logging, and other client-side attacks.

Where do you find XSS?

- Search fields that echo a search string back to the user
- Input fields that echo user data
- Error messages that return user supplied text
- Hidden fields that contain user supplied data
- Any page that displays user supplied data
- HTTP Headers


Omar's Vulnerable WebApp
Welcome to Omar's Vulnerable App
NAME
<script>alert("XSS Fool!")</script>
COMPLAIN ABOUT THE TRAINING
SUBMIT
CANCEL

WebGoat

192.168.78.8:8080/WebGoat/start.mvc

Offensive Security | Kali Linux | Kali Docs

WEBGOAT

- Introduction
- General
- Injection Flaws
- Authentication Flaws
- Cross-Site Scripting (XSS)
- Access Control Flaws
  - Insecure Direct Object References
  - Missing Function Level Access Control
- Insecure Communication
- Request Forgeries
- Vulnerable Components - A9
- Client side
- Challenges

Burp Suite Free Edition v1.7.27 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Intercept | HTTP history | WebSockets history | Options

History logging of out-of-scope items is disabled

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
23	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
24	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
25	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
26	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
27	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
28	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
29	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
30	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
31	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
32	http://192.168.78.8:8080	POST	/WebGoat/IDOR/login	✓		200	383	JSON					192.168.
33	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1037	JSON	mvc				192.168.
34	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
35	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
36	http://192.168.78.8:8080	GET	/WebGoat/IDOR/profile			200	374	JSON					192.168.

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Application-Context: application:8080
Content-Type: application/json;charset=UTF-8
Date: Wed, 14 Feb 2018 23:10:29 GMT
Connection: close
Content-Length: 104

{
  "role" : 3,
  "color" : "yellow",
  "size" : "small",
  "name" : "Tom Cat",
  "userId" : "2342384"
}
```

? < + > Type a search term 0 matches

DEMO – XSS

File Inclusion and Directory Traversal

1

Used to access files and directories that are stored outside the web root folder.

2

You can manipulate variables that reference files with “dot-dot-slash (../)” or by using absolute file paths.

3

You may be able access arbitrary files and directories stored on file system including application source code or configuration and critical system files, like the /etc/passwd

DEMO – Directory/Path Traversal

WebGoat

192.168.78.8:8080/WebGoat/start.mvc#

Offensive Security · Kali Linux · Kali Docs

WEBGOAT

- Introduction
- General
- Injection Flaws
- Authentication Flaws
- Cross-Site Scripting (XSS)
- Access Control Flaws
  - Insecure Direct Object References
  - Missing Function Level Access Control
- Insecure Communication
- Request Forgeries
- Vulnerable Components - A9
- Client side
- Challenges

Burp Suite Free Edition v1.7.27 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Intercept | HTTP history | WebSockets history | Options

History logging of out-of-scope items is disabled

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
23	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
24	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
25	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
26	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
27	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
28	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
29	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
30	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
31	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
32	http://192.168.78.8:8080	POST	/WebGoat/IDOR/login	✓		200	383	JSON					192.168.
33	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1037	JSON	mvc				192.168.
34	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
35	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
36	http://192.168.78.8:8080	GET	/WebGoat/IDOR/profile			200	374	JSON					192.168.

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Application-Context: application:8080
Content-Type: application/json;charset=UTF-8
Date: Wed, 14 Feb 2018 23:10:29 GMT
Connection: close
Content-Length: 104

{
  "role" : 3,
  "color" : "yellow",
  "size" : "small",
  "name" : "Tom Cat",
  "userId" : "2342384"
}
```

? < + > Type a search term 0 matches

XML External Entity (XXE)

- Poorly configured XML parsers evaluate external entity references within XML docs.
- External entities can be used to:
  - disclose internal files using the file URI handler
  - internal port scanning
  - remote code execution
  - denial of service attacks

WebGoat

192.168.78.8:8080/WebGoat/start.mvc#

Offensive Security | Kali Linux | Kali Docs

WEBGOAT

- Introduction
- General
- Injection Flaws
- Authentication Flaws
- Cross-Site Scripting (XSS)
- Access Control Flaws
  - Insecure Direct Object References
  - Missing Function Level Access Control
- Insecure Communication
- Request Forgeries
- Vulnerable Components - A9
- Client side
- Challenges

Burp Suite Free Edition v1.7.27 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Intercept | HTTP history | WebSockets history | Options

History logging of out-of-scope items is disabled

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
23	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
24	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
25	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
26	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
27	http://192.168.78.8:8080	GET	/WebGoat/service/restartlesson.mvc			200	222		mvc				192.168.
28	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
29	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1038	JSON	mvc				192.168.
30	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
31	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
32	http://192.168.78.8:8080	POST	/WebGoat/IDOR/login	✓		200	383	JSON					192.168.
33	http://192.168.78.8:8080	GET	/WebGoat/service/lessonoverview.mvc			200	1037	JSON	mvc				192.168.
34	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
35	http://192.168.78.8:8080	GET	/WebGoat/service/lessonmenu.mvc			200	6011	JSON	mvc				192.168.
36	http://192.168.78.8:8080	GET	/WebGoat/IDOR/profile			200	374	JSON					192.168.

Request | Response

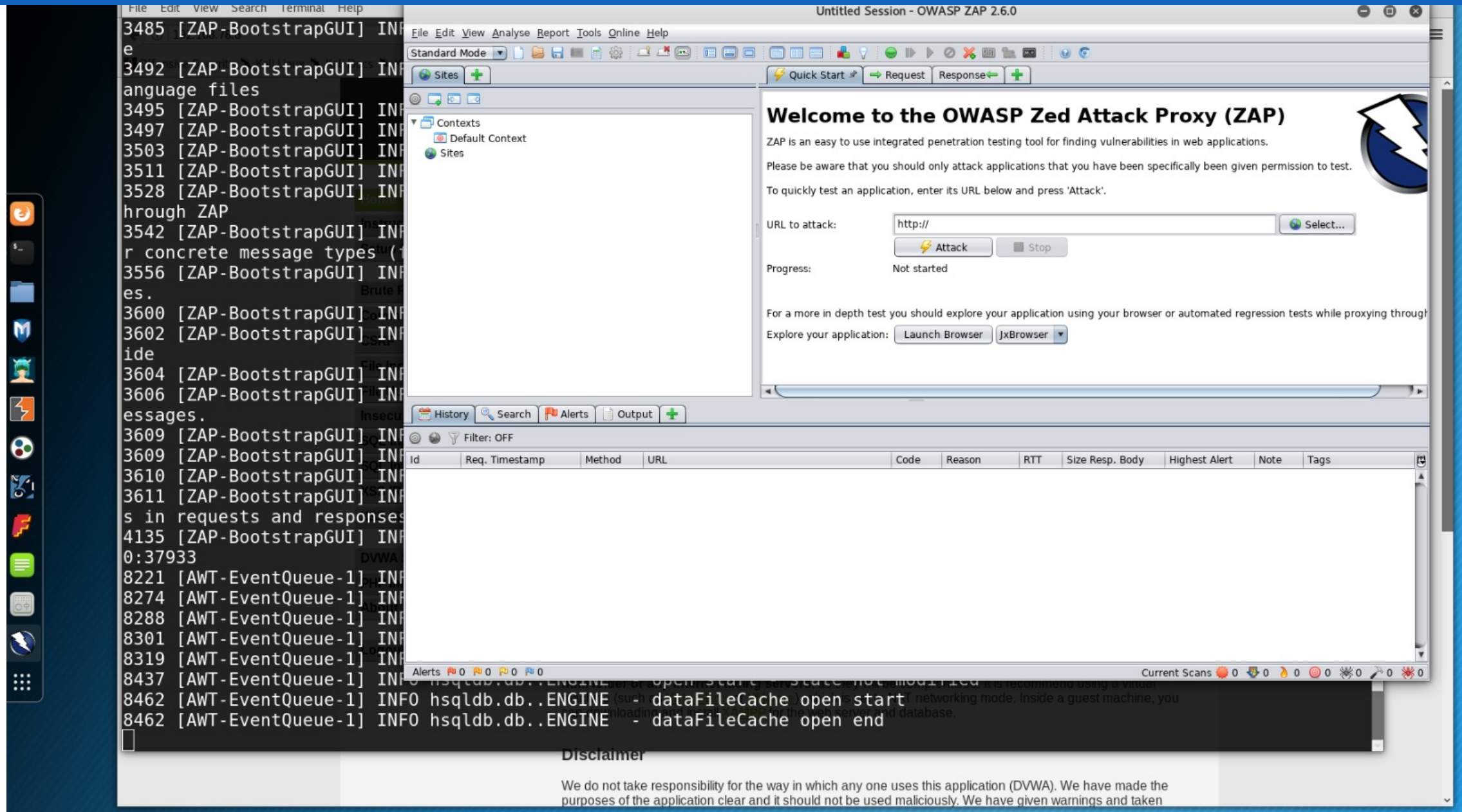
Raw | Headers | Hex

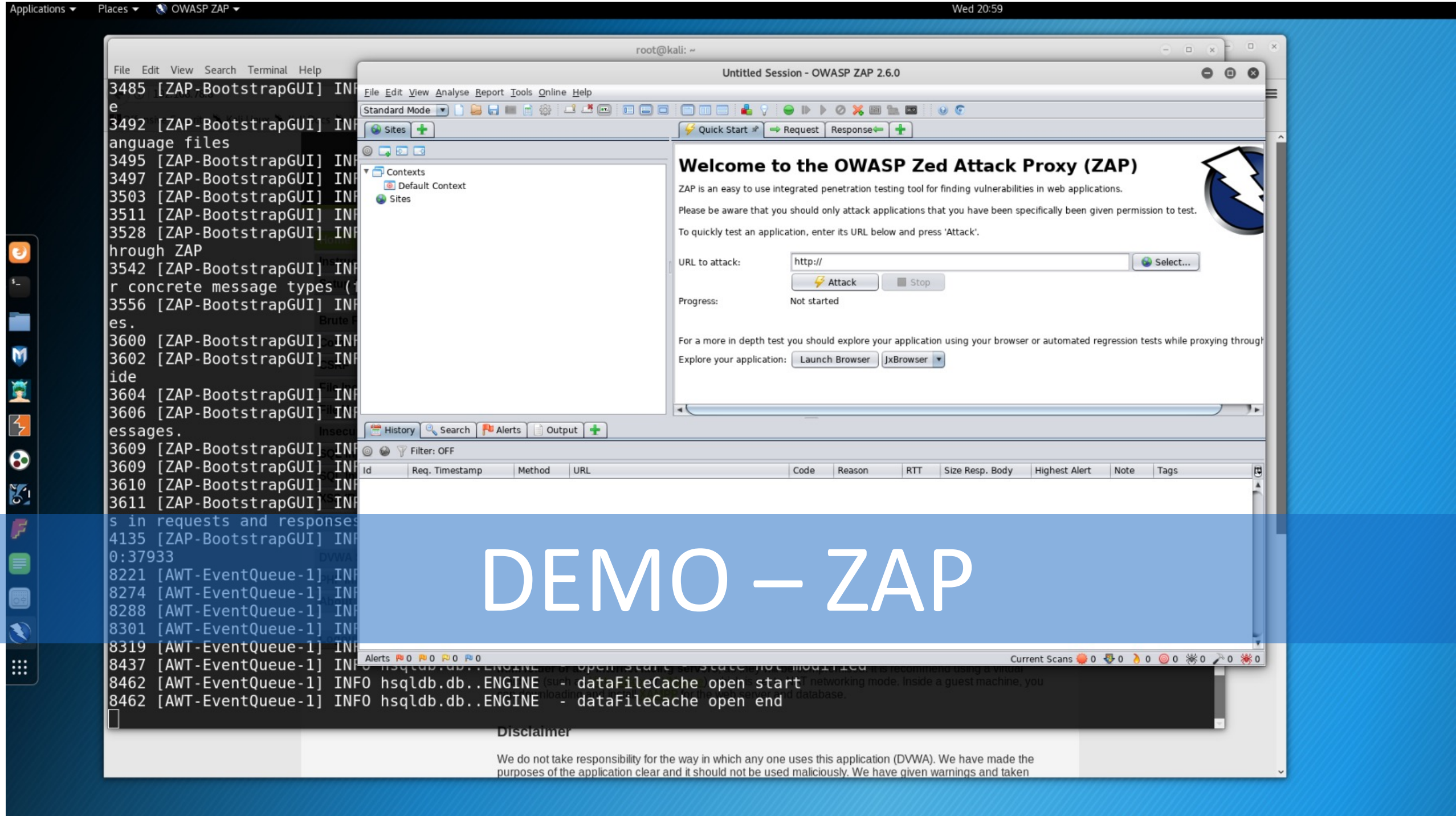
```
HTTP/1.1 200
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Application-Context: application:8080
Content-Type: application/json;charset=UTF-8
Date: Wed, 14 Feb 2018 23:10:29 GMT
Connection: close
Content-Length: 104

{
  "role" : 3,
  "color" : "yellow",
  "size" : "small",
  "name" : "Tom Cat",
  "userId" : "2342384"
}
```

? < + > Type a search term 0 matches

DEMO – XXE

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




Applications
Places
OWASP ZAP
Wed 20:59
root@kali: ~
File Edit View Search Terminal Help
3485 [ZAP-BootstrapGUI] INF
e
3492 [ZAP-BootstrapGUI] INF
anguage files
3495 [ZAP-BootstrapGUI] INF
3497 [ZAP-BootstrapGUI] INF
3503 [ZAP-BootstrapGUI] INF
3511 [ZAP-BootstrapGUI] INF
3528 [ZAP-BootstrapGUI] INF
hrough ZAP
3542 [ZAP-BootstrapGUI] INF
r concrete message types (
3556 [ZAP-BootstrapGUI] INF
es.
3600 [ZAP-BootstrapGUI] INF
3602 [ZAP-BootstrapGUI] INF
ide
3604 [ZAP-BootstrapGUI] INF
3606 [ZAP-BootstrapGUI] INF
essages.
3609 [ZAP-BootstrapGUI] INF
3609 [ZAP-BootstrapGUI] INF
3610 [ZAP-BootstrapGUI] INF
3611 [ZAP-BootstrapGUI] INF
s in requests and responses
4135 [ZAP-BootstrapGUI] INF
0:37933
8221 [AWT-EventQueue-1] INF
8274 [AWT-EventQueue-1] INF
8288 [AWT-EventQueue-1] INF
8301 [AWT-EventQueue-1] INF
8319 [AWT-EventQueue-1] INF
8437 [AWT-EventQueue-1] INF
8462 [AWT-EventQueue-1] INFO hsqldb.db..ENGINE - dataFileCache open start
8462 [AWT-EventQueue-1] INFO hsqldb.db..ENGINE - dataFileCache open end
Untitled Session - OWASP ZAP 2.6.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
To quickly test an application, enter its URL below and press 'Attack'.
URL to attack:
http://
Select...
Attack
Stop
Progress:
Not started
For a more in depth test you should explore your application using your browser or automated regression tests while proxying through
Explore your application:
Launch Browser
JxBrowser
History
Search
Alerts
Output
Filter: OFF
Id
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Alerts
Current Scans
Disclaimer
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken

DEMO – ZAP

Introduction to Hacking User Credentials

Take Advantage Default Usernames and Passwords

http://www.phenoelit-us.org/dpl/dpl.html
http://cirt.net/passwords
http://www.passwordsdatabase.com

Applications Places Firefox ESR Wed 22:50

Big bertha says: default passwords - Mozilla Firefox

Big bertha says: defau...

www.defaultpassword.com 150% Search

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

default password list

Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

Displaying 1812 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password
3COM			Telnet	adm	(none)
3COM			Telnet	security	security
3COM			Telnet	read	synnet
3COM			Telnet	write	synnet
3COM			Telnet	admin	synnet
3COM			Telnet	manager	manager
3COM			Telnet	monitor	monitor
3com	3Com SuperStack 3 Switch 3300XM		Multi	security	security
3COM	AirConnect Access Point	01.50-01	Multi	n/a	(none)
3COM	boson router simulator	3.66	HTTP	admin	admin
3com	cellplex	7000	Telnet	admin	admin
3COM	CellPlex	7000	Telnet	tech	tech
3COM	CellPlex		HTTP	admin	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3com	hub		Multi	n/a	(none)
3COM	LANplex	2500	Telnet	tech	tech
3COM	LANplex	2500	Telnet	tech	(none)
3COM	LANplex	2500	Telnet	debug	synnet
3COM	LinkBuilder		Telnet	n/a	(none)
3COM	LinkSwitch	2000/2700	Telnet	tech	tech
3com	NetBuilder		SNMP	(none)	admin
3COM	NetBuilder		SNMP		ANYCOM
3COM	NetBuilder		SNMP		ILMI
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3com	OfficeConnect 812 ADSL		Multi	adminttd	adminttd
3com	router		Multi	n/a	(none)
3com	super stack 2 switch		Multi	manager	manager
3com	super stack II		Console	n/a	(none)
3com	superstack II	1100/3300	Console	3comcso	RIP000
3COM	SuperStack II Switch	2700	Telnet	tech	tech
3COM	SuperStack II Switch	2200	Telnet	debug	synnet
3COM	Wireless 11g Firewall Router	3CRWDR100-72	Multi	none	admin
3com	Wireless AP	ANY	Multi	admin	comcomcom

Applications Places Terminal Wed 22:53

root@kali: ~

File Edit View Search Terminal Help

JOHN(8) System Manager's Manual JOHN(8)

NAME

john - a tool to find weak passwords of your users

SYNOPSIS

john [options] password-files

DESCRIPTION

This manual page documents briefly the **john** command. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. **john**, better known as John the Ripper, is a tool to find weak passwords of users in a server. John can use a dictionary or some search pattern as well as a password file to check for passwords. John supports different cracking modes and understands many ciphertext formats, like several DES variants, MD5 and blowfish. It can also be used to extract AFS and Windows NT passwords.

USAGE

To use John, you just need to supply it a password file and the desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental".

Once John finds a password, it will be printed to the terminal and saved into a file called ~/.john/john.pot. John will read this file when it restarts so it doesn't try to crack already done passwords.

To see the cracked passwords, use

john -show passwd

Important: do this under the same directory where the password was cracked (when using the cronjob, /var/lib/john), otherwise it won't work.

While cracking, you can press any key for status, or Ctrl+C to abort the session, saving point information to a file (~/.john/john.rec by default). By the way, if you press Ctrl+C twice John will abort immediately without saving. The point information is also saved every 10 minutes (configurable in the configuration file, ~/.john/john.ini or ~/.john/john.conf) in case of a crash.

To continue an interrupted session, run:

Manual page john(8) line 1 (press h for help or q to quit)

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# john --wordlist=/usr/share/wordlists/omar.lst my_hash.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using defaul
Loaded 1 pas
Press 'q' or
trump1
1g 0:00:00:0
Use the "--s
Session comp
root@kali:~#
root@kali:~#
root@kali:~#
libpng warni
```

Johnny

File Attack Passwords Help

Open password file | Open session | Start new attack | Resume attack | Pause attack | Guess password | Copy | Export

Passwords | Options | Statistics | Settings | Console log

Filter | Select columns | Show only checked | Show only cracked

	User	Password	Hash	Formats	GECOS
1	donald	trump1	6.3ctTlmY$8AfiFb/5M4s./x9LN6NZWXQBKpSDgzKD3zep9vyu...	sha512crypt,crypt	17577:0:99999:7:::
2	?	NO PASSWORD			

100% (2/2: 2 cracked, 0 left) [format=sha512crypt]

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Hashcat(1)                    General Commands Manual                    Hashcat(1)

NAME
       hashcat - Advanced CPU-based password recovery utility

SYNOPSIS
       hashcat [options] hashfile [mask|wordfiles|directories]

DESCRIPTION
       Hashcat is the world's fastest CPU-based password recovery tool.

       While it's not as fast as its GPU counterpart oclHashcat, large lists can be easily split in half with a good dictionary
       and a bit of knowledge of the command switches.

       Hashcat is the self-proclaimed world's fastest CPU-based password recovery tool, Examples of hashcat  supported  hashing
       algorithms are Microsoft LM Hashes, MD4, MD5, SHA-family, Unix Crypt formats, MySQL, Cisco PIX.

OPTIONS
       -h, --help
              Show summary of options.

       -V, --version
              Show version of program.

       -m, --hash-type=NUM
              Hash-type, see references below

       -a, --attack-mode=NUM
              Attack-mode, see references below

       --quiet
              Suppress output

       -b, --benchmark
              Run benchmark

 Manual page hashcat(1) line 1 (press h for help or q to quit)
```

Applications Places Terminal Wed 22:57

Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications

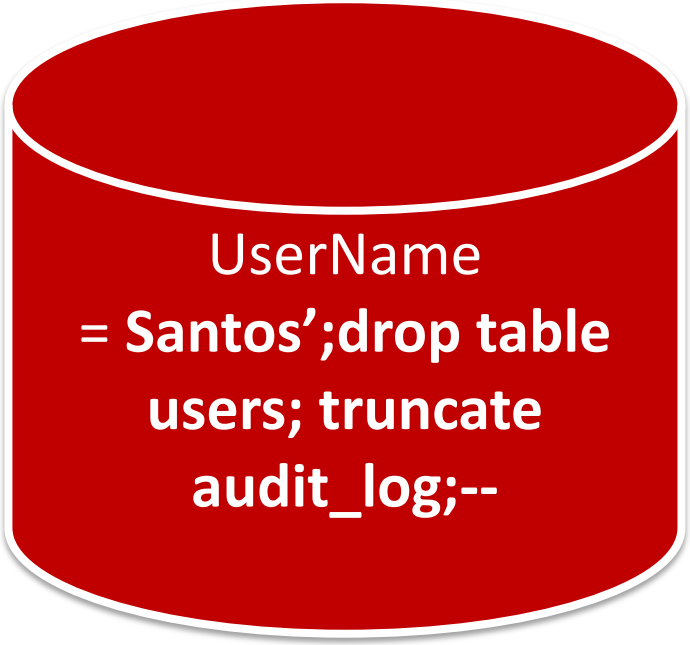
cewl
crunch
hashcat
john
johnny
medusa
ncrack
ophcrack
pyrit
rainbowcra...
rcracki_mt
wordlists

Activities Overview

root@kali: ~

```
usr/share/wordlists/omar.lst my_hash.txt
a512crypt", but the string is also recognized as "crypt"
 to force loading these as that type instead
TF-8
crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
almost any other key for status

22:40) 0.3484g/s 1070p/s 1070c/s 1070C/s angelz..567890
lay all of the cracked passwords reliably

correct sRGB profile

(y or n)
```

DEMO – CRACKING PASSWORDS



Introduction to Hacking Databases

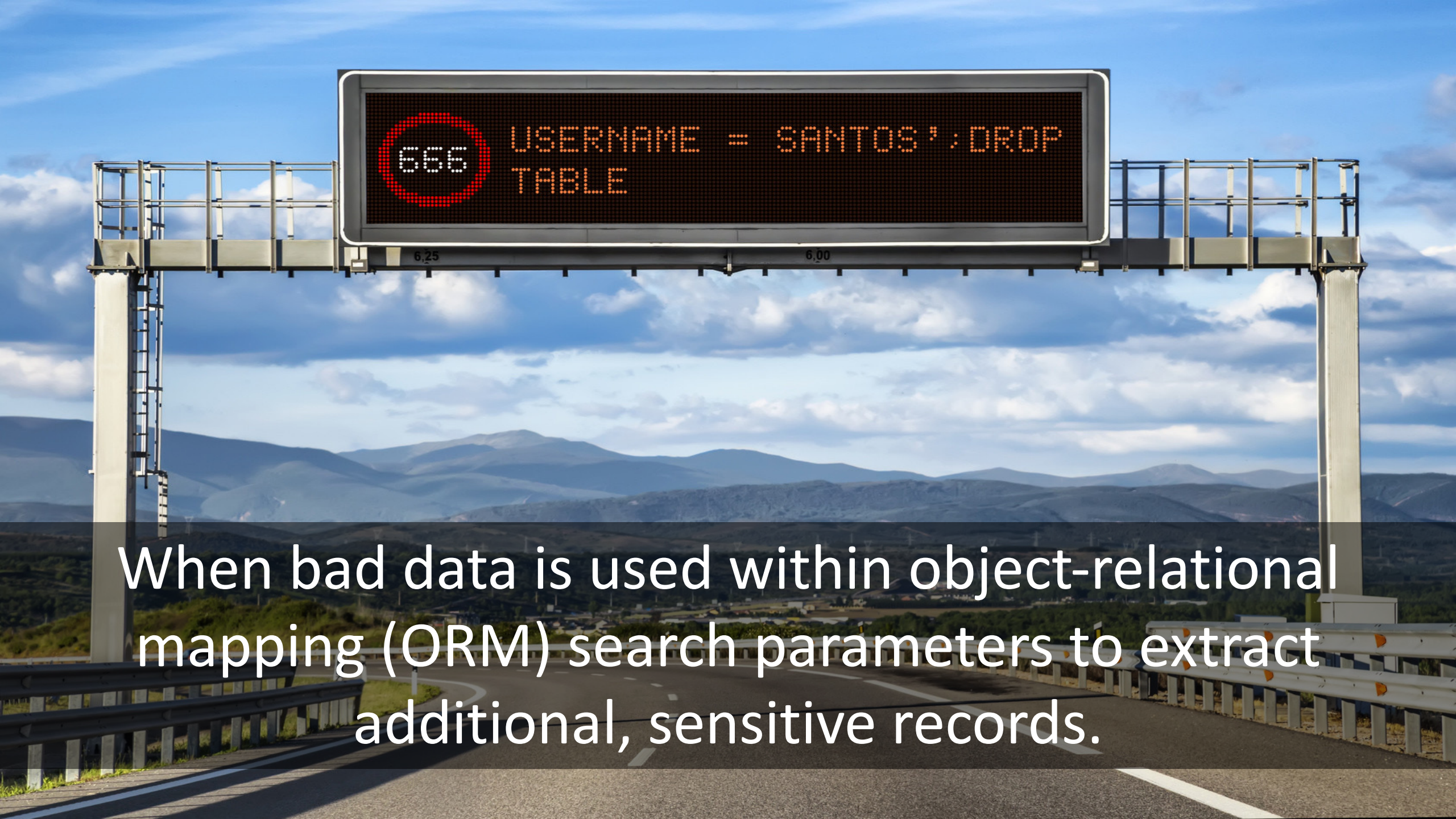
App. Specific	Exploitability: 3	Prevalence: 2	Detectability: 3	Technical: 3	Business ?
Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.		Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.		Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact depends on the needs of the application and data.	

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

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

When does SQL injection happen?

Data is not validated, filtered, or sanitized by the application.



When bad data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.

Data is not validated, filtered, or sanitized by the application.

DEMO
SQL INJECTION