INTRODUCTION TO ETHICAL HACKING AND PENETRATION TESTING

OMAR SANTOS

theartofhacking.org

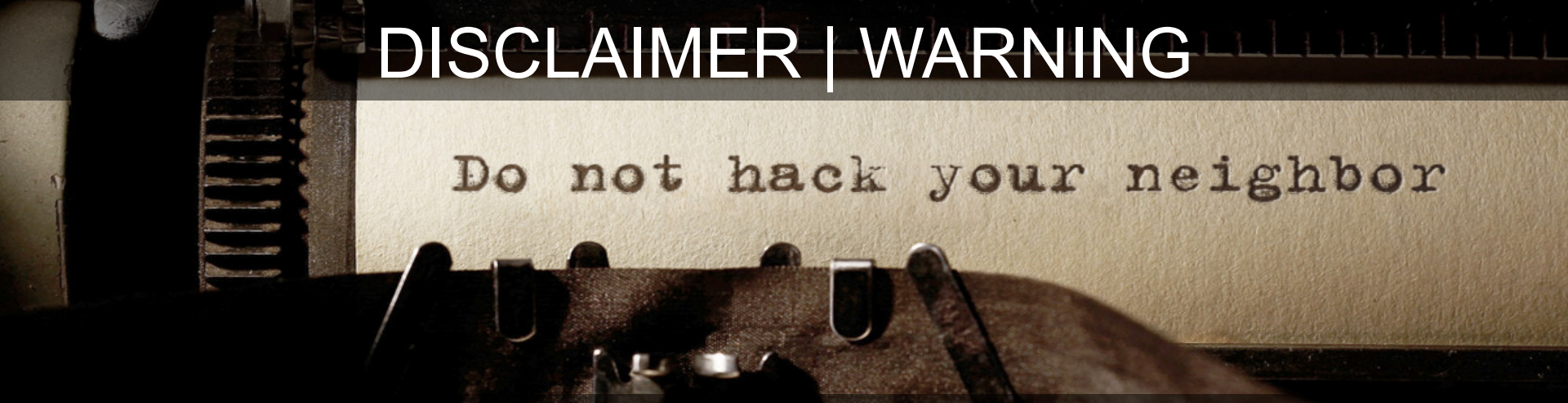
OMAR SANTOS

About Omar

- Principal Engineer at Cisco's Product Security Incident Response Team (PSIRT) – Security Research and Operations.
- Over 20 years of experience in cyber security.
- Author of over 20 books and video courses.

Follow @santosomar

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.

DAY 1:

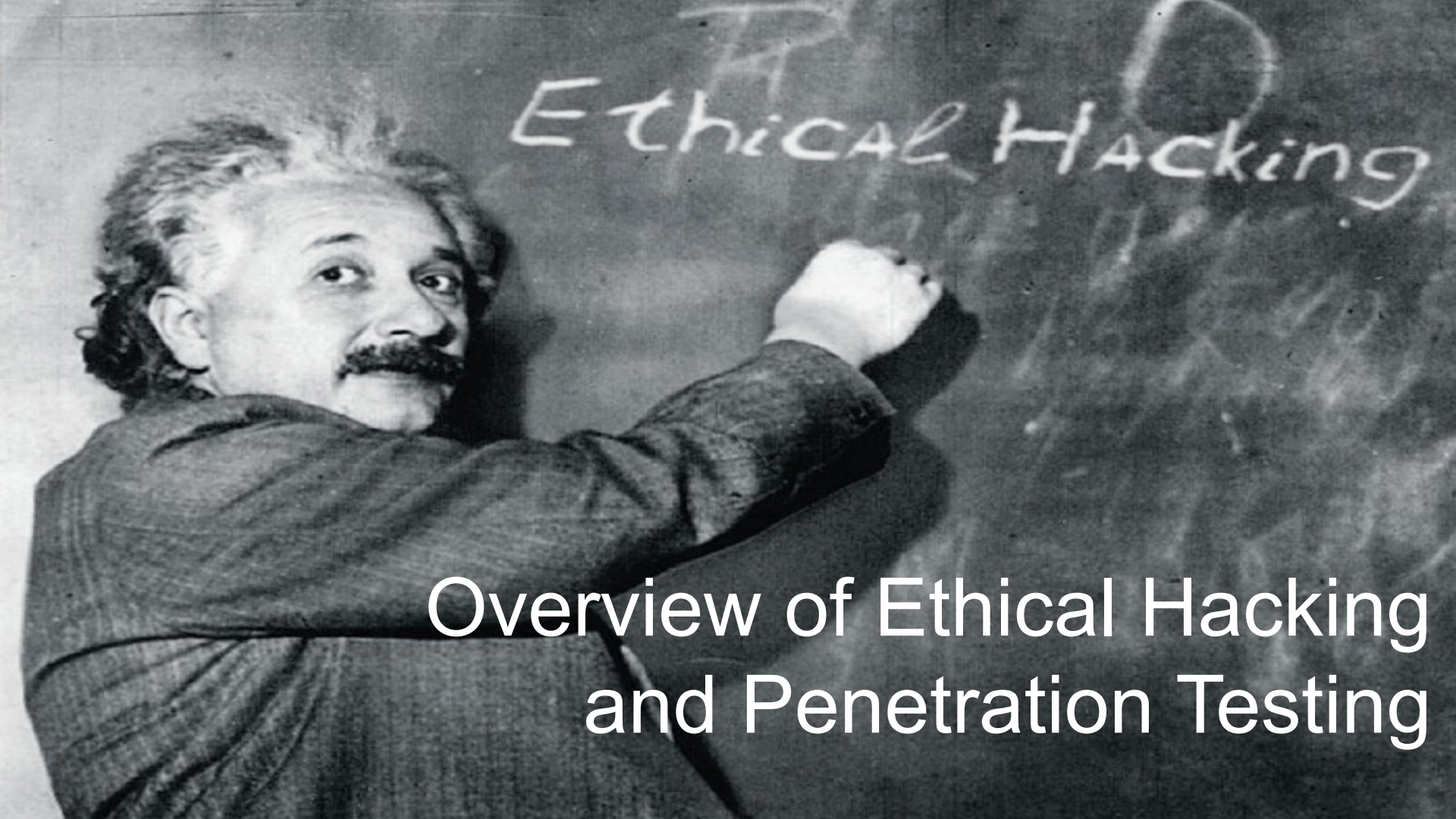
- Overview of Ethical Hacking and Penetration Testing
- Kali Linux
- Passive and Active Reconnaissance
- Introduction to Hacking Web Applications
- Introduction to Hacking User Credentials
- Introduction to Hacking Databases

DAY 2:

- Introduction to Hacking Networking Devices
- Fundamentals of Wireless Hacking
- Introduction to Buffer Overflows
- Fundamentals of Evasion and Post Exploitation Techniques
- Introduction to Social Engineering
- How to Write Penetration Testing Reports

POLL QUESTION: What is your level of familiarity with penetration testing (ethical hacking)?

A. Beginner (less than a year of experience)
B. Intermediate level (2-5 years of experience)
C. Advanced (more than 5 years of experience)



Overview of Ethical Hacking and Penetration Testing

RESOURCES FOR THIS CLASS

VIDEO COURSES IN SAFARI AND TONS OF REFERENCES

```
>> theartofhacking.org

>> theartofhacking.org/guide
```

EXERCISES AND LIVE TRAINING REFERENCES

What is Penetration Testing or Ethical Hacking?

- 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.
- The sole difference between the terms “malicious hacking” and “ethical hacking” is the permission.

What is a White Hat Hacker?

- Security professionals or security researchers that perform ethical hacking.
- Such hackers are employed by an organization and are permitted to attack an organization to find vulnerabilities that an attacker might be able to exploit.

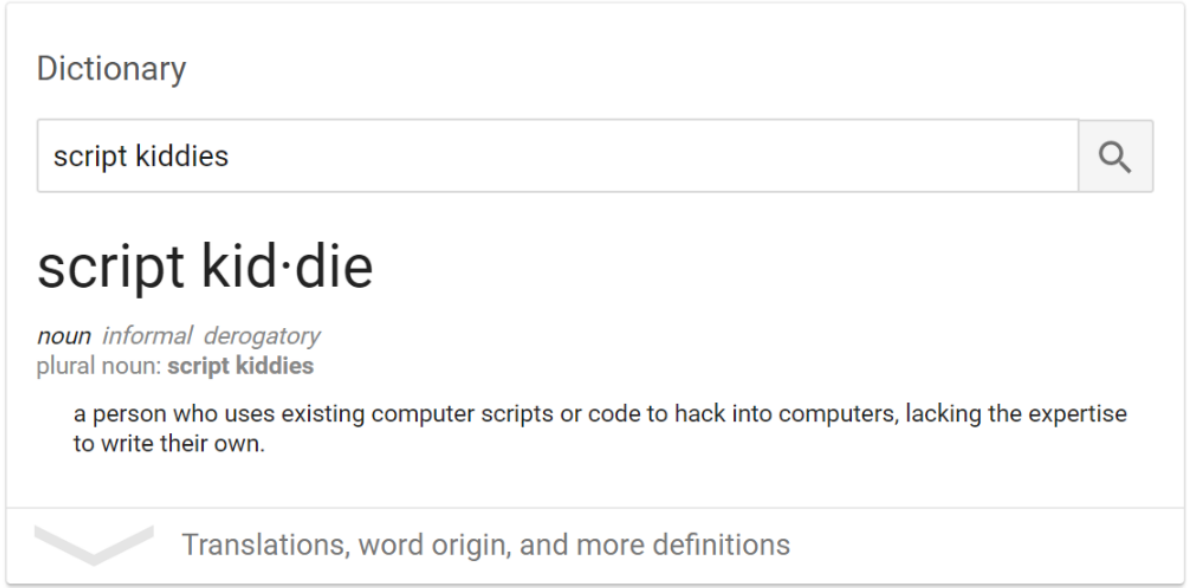
What is a Black Hat Hacker?

- Sometimes also referred to as a cracker, threat actor, bad actor, or malicious attacker.
- Uses his or her knowledge for negative purposes.
- Of course, they are often referred to by the media as *hackers*.

What is a Gray Hat Hacker?

- Somewhere in between a white hat and a black hat hacker.
- For instance, a gray hat hacker would work as a white hat hacker for an organization and then disclose everything to them.
- But might leave a backdoor to access it later and might also sell the confidential information or carry other attacks for his or her benefit.

What is a Script Kiddie?



Elite (l33t, 1337) Hacker

- Has deep knowledge on how an exploit works.
- Such hacker is able to create exploits, but also modify codes that someone else wrote.
- In other words, someone with elite skills of hacking.

Hacktivist

- Hacktivists are defined as group of hackers that hack into computer systems for a cause or purpose.
- The purpose may be political gain, freedom of speech, human rights, and so on.

QUICK DEFINITIONS BEFORE WE PROCEED WITH THE REST OF THE CLASS

ALSO AVAILABLE AT:

```
>> theartofhacking.org/guide
```

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.
- If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known— “the threat is latent and not yet realized.”

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.
- There are several methods of classifying exploits; however, the most common two categories are remote and local exploits.

What is an Exploit-Kit?

- An exploit kit is a compilation of exploits that are often designed to be served from web servers.

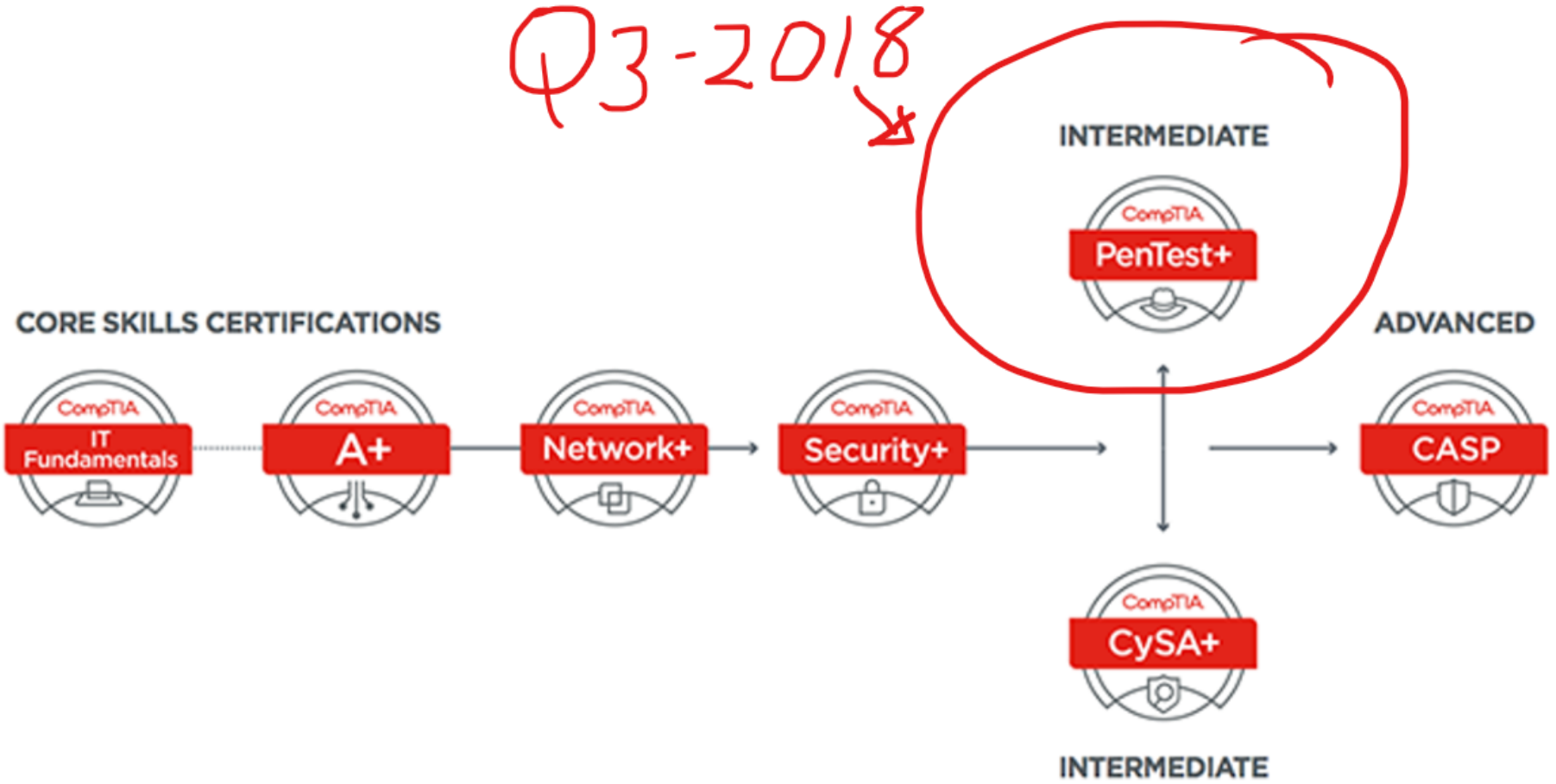
- Examples:
  - Angler
  - Mpack
  - Fiesta
  - Phoenix
  - Blackhole
  - Crimepack
  - RIG

POLL QUESTION: How are you planning to continue learning and enhancing your cybersecurity skills?

A. Not planning to continue to develop cybersecurity skills
B. Industry certifications
C. Two-year college degree
D. University / bachelors degree
E. Post-graduate degree

CYBERSECURITY AND ETHICAL HACKING CERTIFICATIONS

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh


Q3-2018
INTERMEDIATE
CompTIA
PenTest+
CORE SKILLS CERTIFICATIONS
ADVANCED
CompTIA
IT Fundamentals
CompTIA
A+
CompTIA
Network+
CompTIA
Security+
CompTIA
CASP
CompTIA
CySA+
INTERMEDIATE

OFFENSIVE SECURITY

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 your actual performance**. From the best penetration testing training comes the **best information security certifications**.

BECOME CERTIFIED NOW!
REGISTER TODAY

https://www.offensive-security.com

GIAC Penetration Testing Certification

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

Other Popular Cybersecurity Certificationsß

ISC² CERTIFICATIONS

https://www.isc2.org

CISCO CERTIFICATIONS

Certification Tracks	Entry	Associate	Professional	Expert	Architect
Cloud		CCNA Cloud	CCNP Cloud		
Collaboration		CCNA Collaboration	CCNP Collaboration	CCIE Collaboration	
Cybersecurity Operations		CCNA Cyber Ops			
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center	
Design	CCENT	CCDA	CCDP	CCDE	CCAr
Industrial		CCNA Industrial			
Routing and Switching	CCENT	CCNA Routing and Switching	CCNP Routing and Switching	CCIE Routing and Switching	
Security	CCENT	CCNA Security	CCNP Security	CCIE Security	
Service Provider		CCNA Service Provider	CCNP Service Provider	CCIE Service Provider	
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless	

http://www.cisco.com/go/certifications

- CompTIA Security +
- CompTIA Advanced Security Practitioner (CASP)

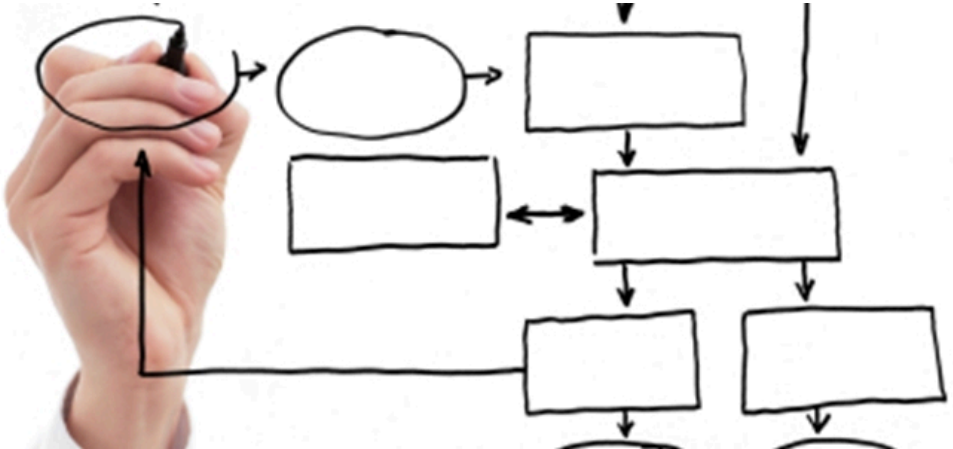
https://certification.comptia.org

ISACA


ISACA
Trust in, and value from, information systems
Support
Shopping Cart
Join ISACA
Reinstate
Sign In
ENGLISH
ISACA
My ISACA
Site Content
SEARCH
Advanced Search
ABOUT
MEMBERSHIP
CERTIFICATION
EDUCATION
COBIT
KNOWLEDGE & INSIGHTS
JOURNAL
BOOKSTORE
CSX
CYBERSECURITY NEXUS
Insights and resources for the cybersecurity professional from ISACA
LEARN MORE >
ISACA > Certification > CISA: Certified Information Systems Auditor
share
Certified Information Systems Auditor (CISA)
CISA Certified Information Systems Auditor
An ISACA Certification
Enhance your career by earning CISA—world-renowned as the standard of achievement for those who audit, control, monitor and assess information technology and business systems.
Why Certify?
Exam Registration
Computer-Based Testing Benefits
2017 Computer-Based Testing (CBT) Locations
ISACA Exam Candidate Information Guide
CISA: Certified Information Systems Auditor
Boost Your Credentials and Gain a Competitive Edge
The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.
Quick Links
I want to...
My Bookmarks
Saved Searches
Apply for CISA certification
CPE: How to report your hours
Earn CPE credits
Find a review course
Join ISACA
Understand the value of membership
View Candidate's Guide to the Exam
View CISA Fact Sheet

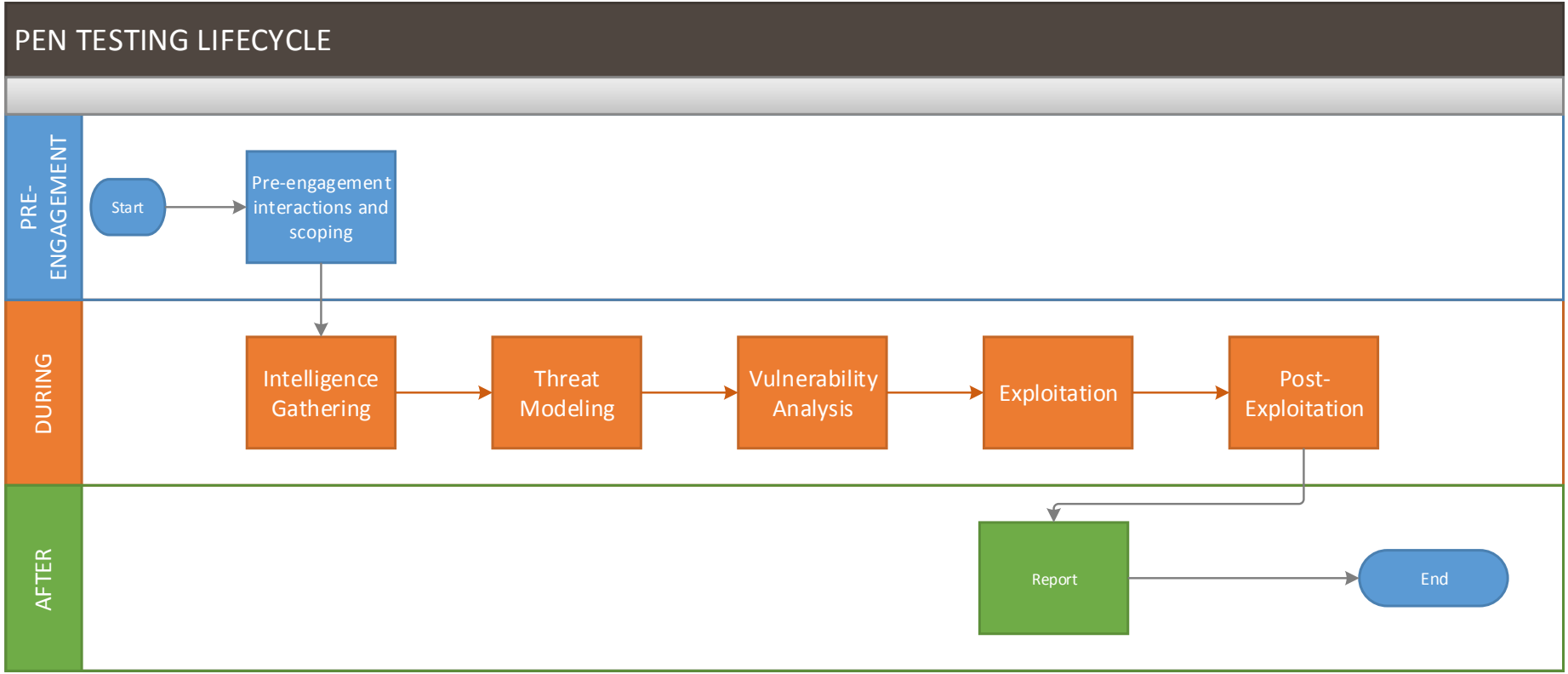
Hacking is a lot more than cool tools…

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



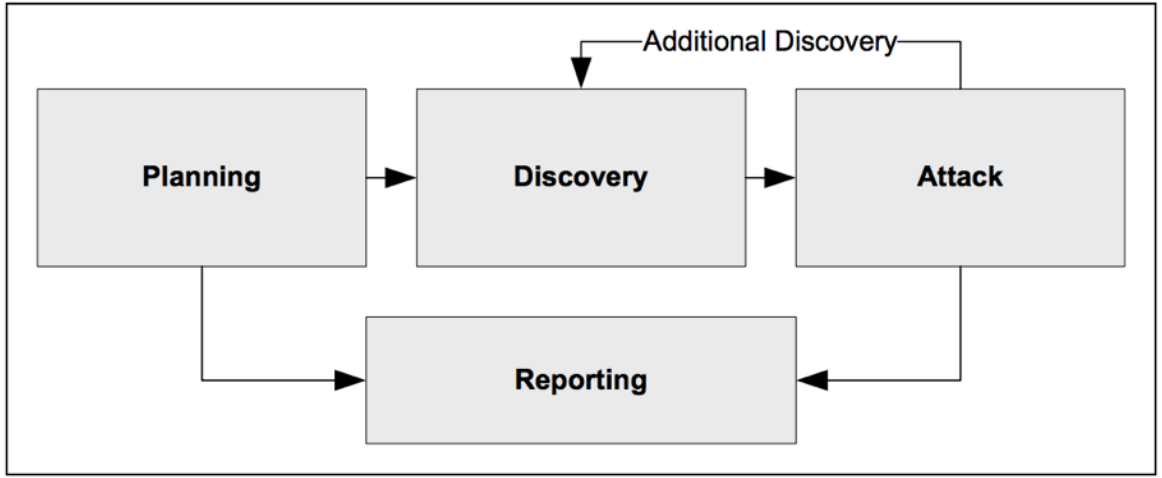
PEN TESTING METHODOLOGIES

- Penetration Testing Execution Standard
  http://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
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- Open Source Security Testing Methodology Manual (OSSTMM)
  http://www.isecom.org/research/



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

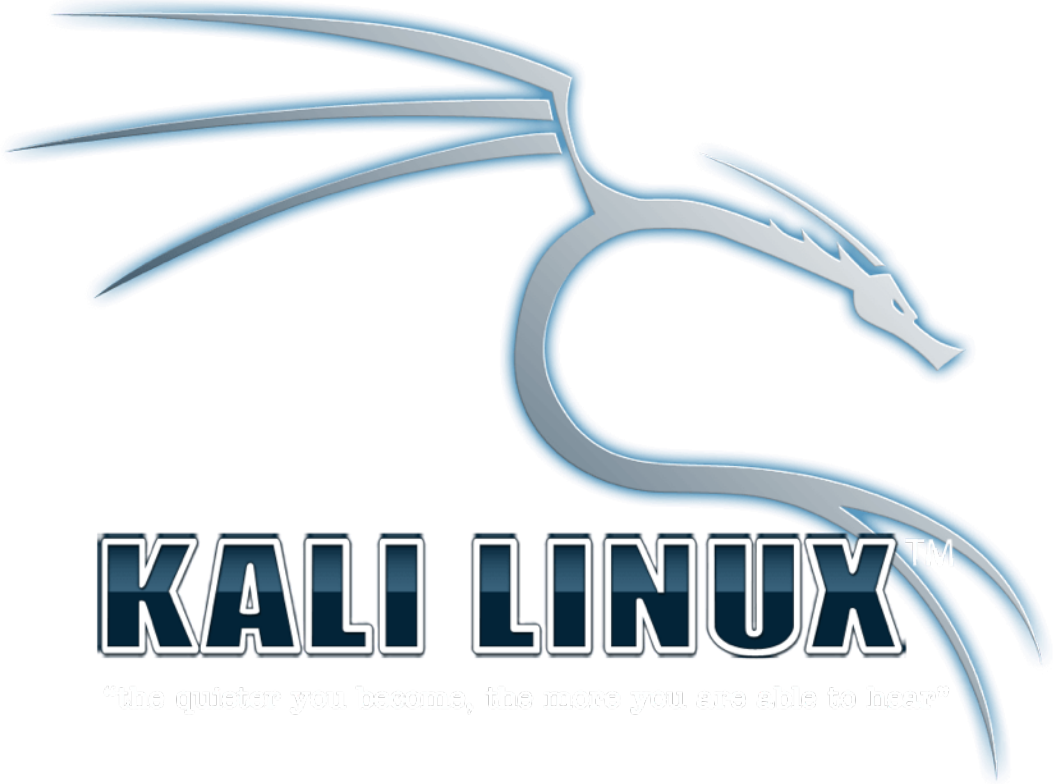
NIST 800-115



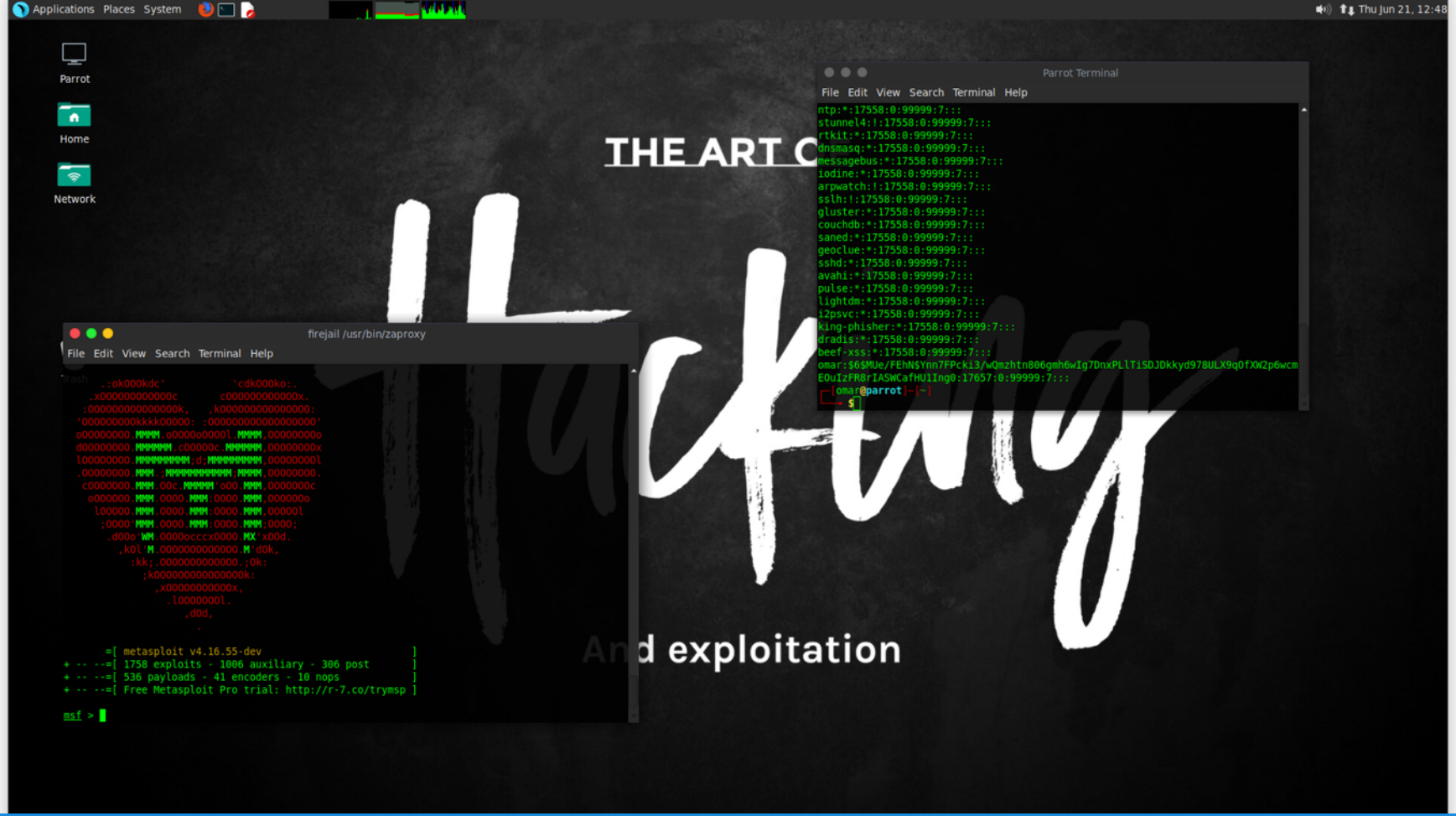
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Kali Linux

Toolz!



https://www.kali.org

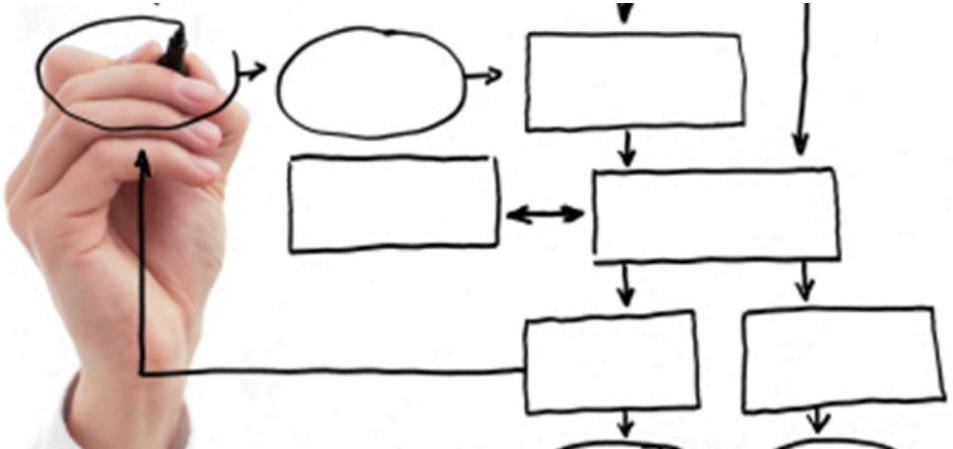

Applications Places System
Thu Jun 21, 12:48
Parrot
Home
Network
THE ART
Hacking
And exploitation
Parrot Terminal
File Edit View Search Terminal Help
ntp:*:17558:0:99999:7:::
stunnel4:!:17558:0:99999:7:::
rtkit:*:17558:0:99999:7:::
dnsmasq:*:17558:0:99999:7:::
messagebus:*:17558:0:99999:7:::
iodine:*:17558:0:99999:7:::
arpwatch:!:17558:0:99999:7:::
sslh:!:17558:0:99999:7:::
gluster:*:17558:0:99999:7:::
couchdb:*:17558:0:99999:7:::
saned:*:17558:0:99999:7:::
geoclue:*:17558:0:99999:7:::
sshd:*:17558:0:99999:7:::
avahi:*:17558:0:99999:7:::
pulse:*:17558:0:99999:7:::
lightdm:*:17558:0:99999:7:::
i2psvc:*:17558:0:99999:7:::
king-phisher:*:17558:0:99999:7:::
dradis:*:17558:0:99999:7:::
beef-xss:*:17558:0:99999:7:::
omar:6MUe/FEhN$Ynn7FPcki3/wQmzhtn806gmh6wIg7DnxPLlTiSDJDkkyd978ULX9qOfXW2p6wcm
EOuIzFR8rIASWCafHUlIng0:17657:0:99999:7:::
[omar@parrot]~[~]
$
firejail /usr/bin/zaproxy
File Edit View Search Terminal Help
=[metasploit v4.16.55-dev]
+ -- --=[1758 exploits - 1006 auxiliary - 306 post]
+ -- --=[536 payloads - 41 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

PARROT

Hacking is a lot more than cool tools…

REMEMBER!

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

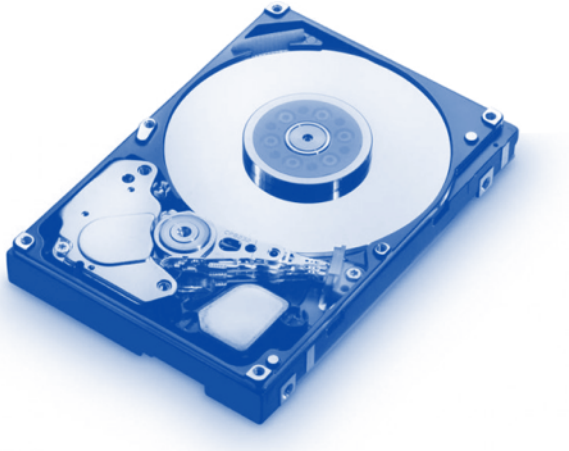
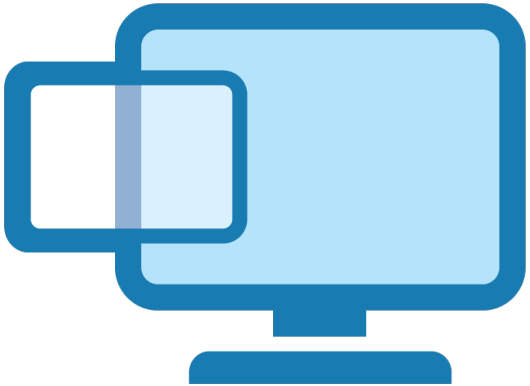


GUIDANCE ON HOW TO BUILD YOUR OWN LAB AND KALI LINUX EXERCISES

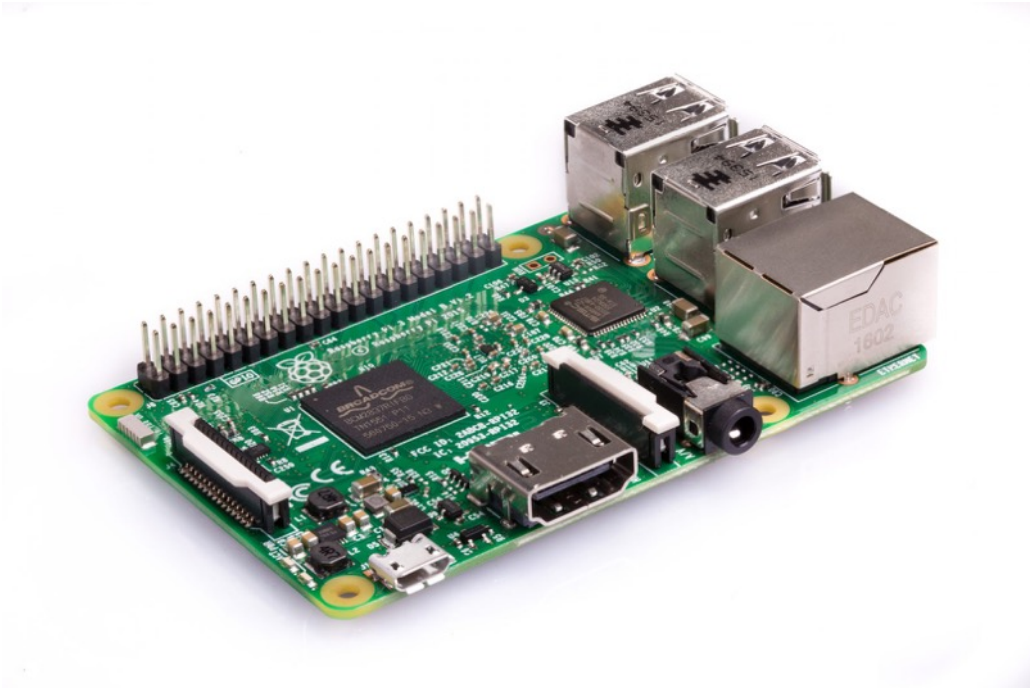
```
>> theartofhacking.org/guide
```

AMAZING FREE RESOURCE! - https://kali.training

DOWNLOADING and INSTALLING KALI

HDD INSTALL	VM INSTALL	LIVE MODE
		

ARM KALI IMAGES



https://www.offensive-security.com/kali-linux-arm-images

Kali Linux Users

- Default user: root
- Default password: toor

Let's change the default password and create a user.

https://kali.training/topic/managing-users-and-groups


Applications
Places
Terminal
Mon 14:12
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
METASPLOIT by Rapid7
EXPLOIT
RECON
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 – USER ACCOUNTS

DEMO – KALI ARCHITECTURE

Managing Kali Services

- SSH
- Web Services
- BUM

Managing Kali Services (video reference)

DEMO – ENABLING SERVICES

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
- Whois Information
- Tools like Recon-ng, Maltego, TheHarvester, Spiderfoot, etc.


Applications
Places
Terminal
Mon 14:12
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
METASPLOIT by Rapid7
RECON
EXPLOIT
LOOT
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 – Passive Recon

What is Active Recon?

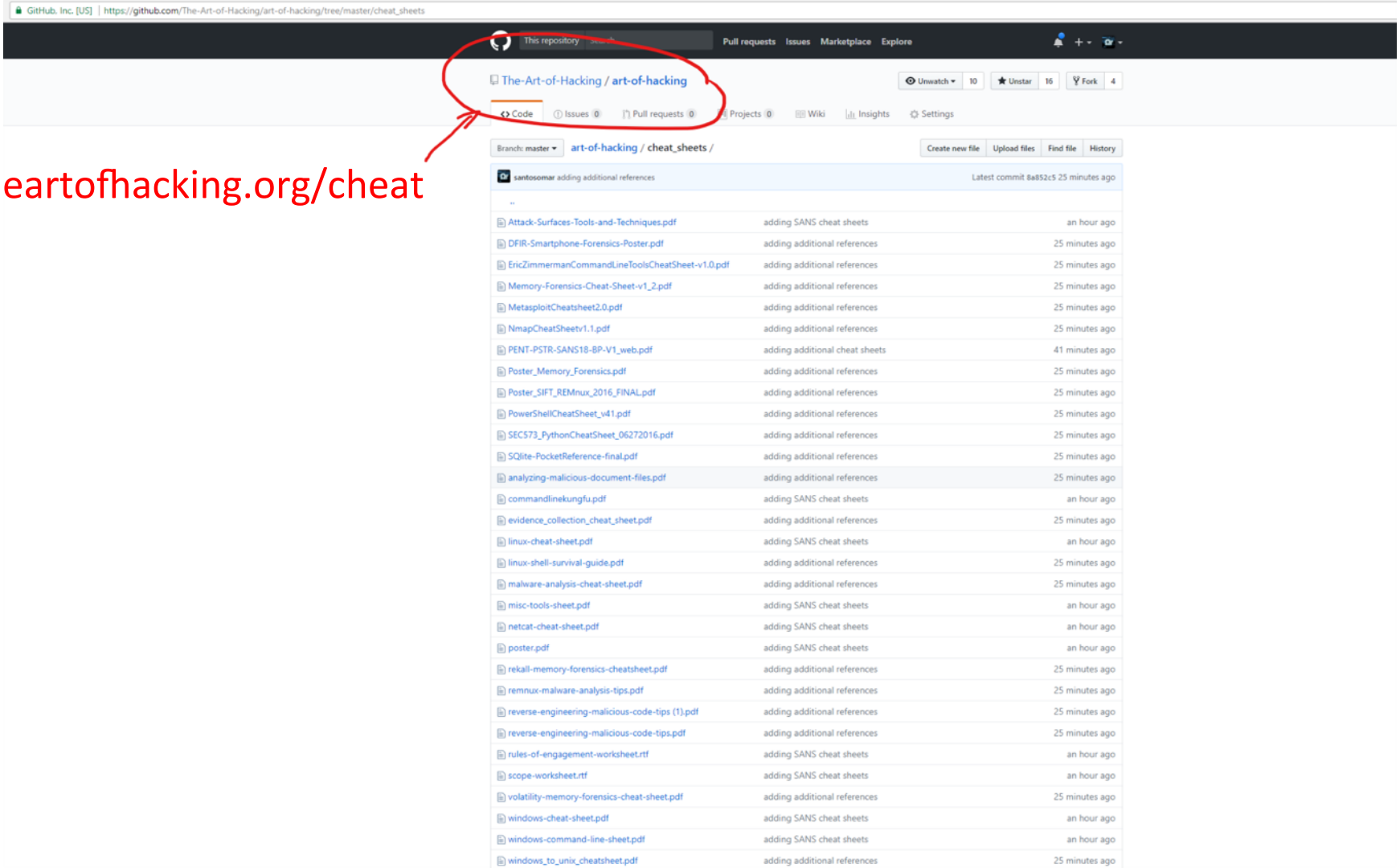
“Actively” performing a network or vulnerability scan and launching other tools against the victim.

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
EXPLOIT
RECON
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

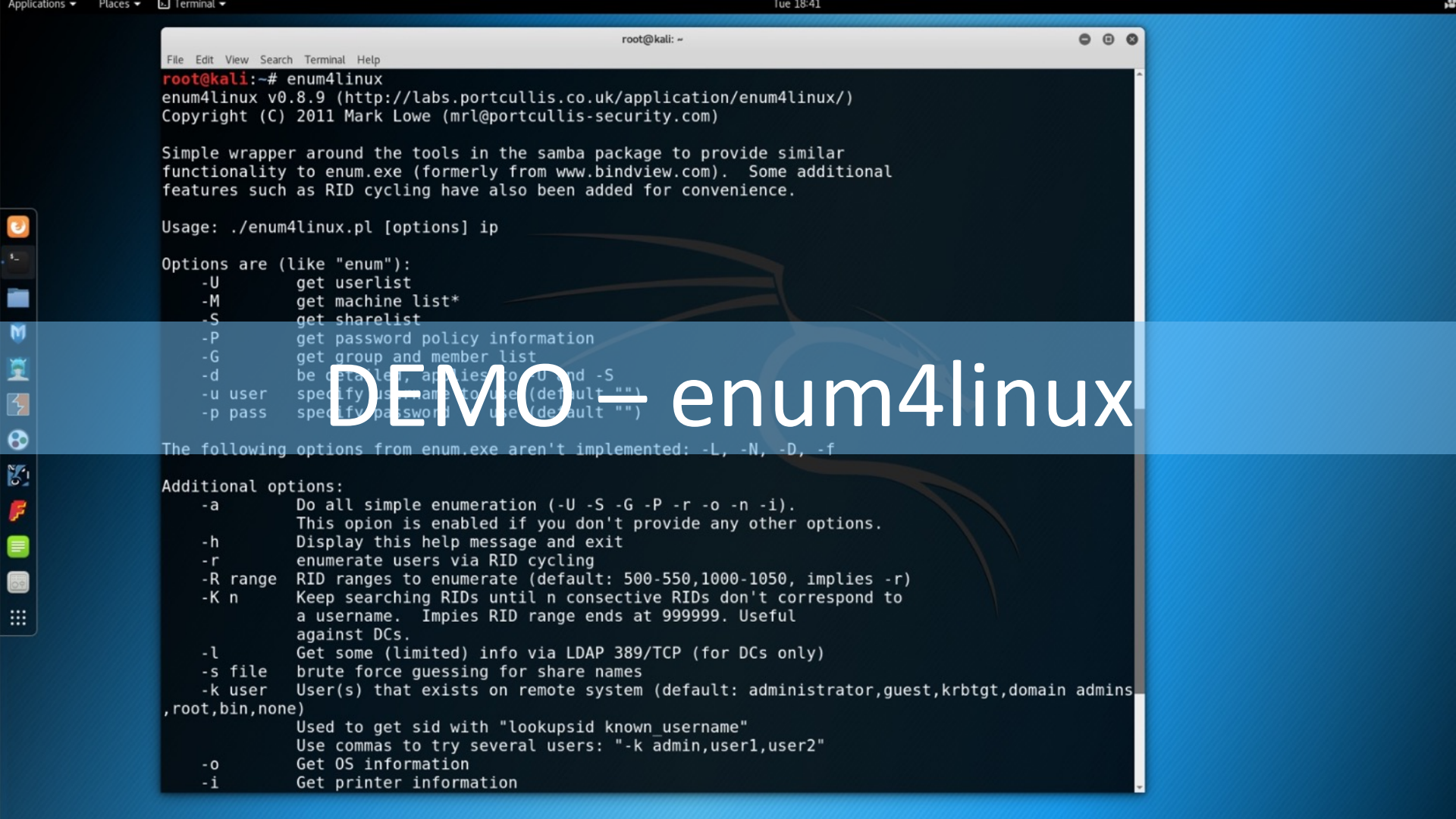


theartofhacking.org/cheat

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
```

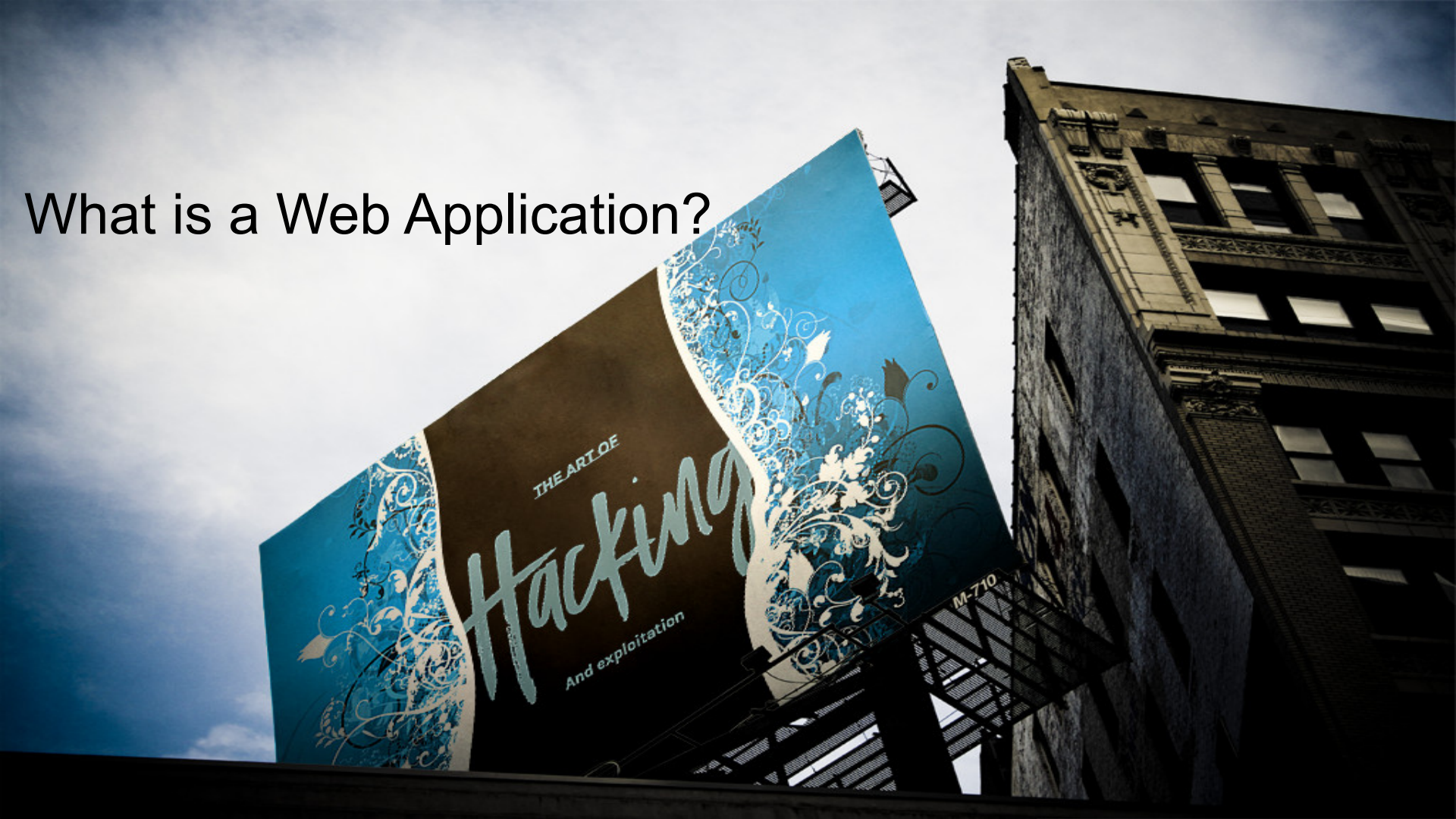


DEMO – enum4linux

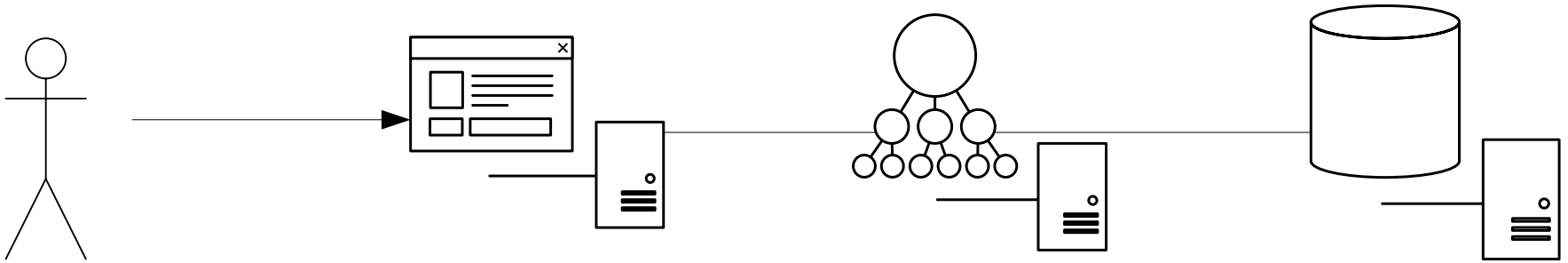
https://theartofhacking.org/guide

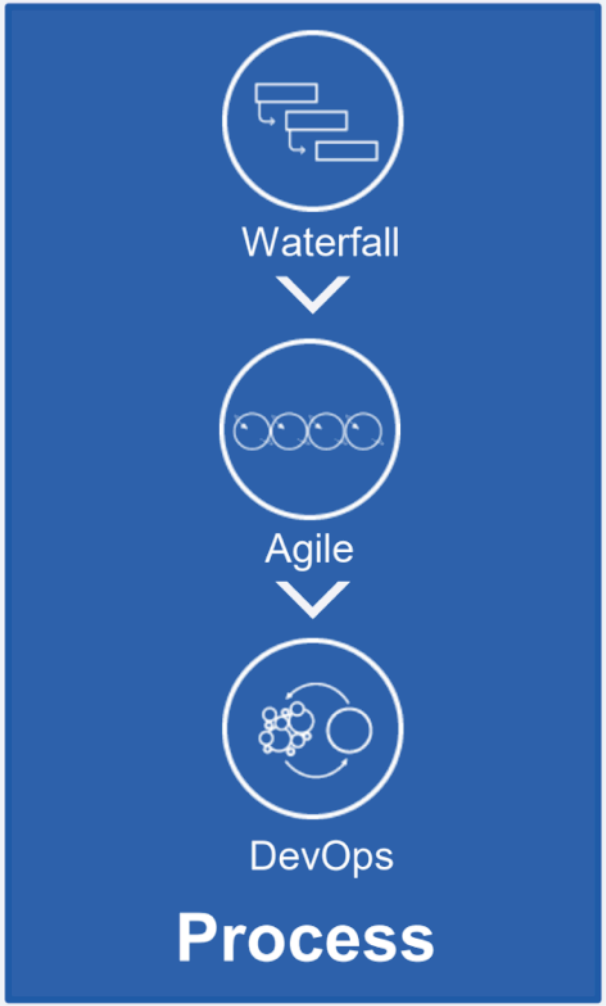
Introduction to Hacking Web Applications

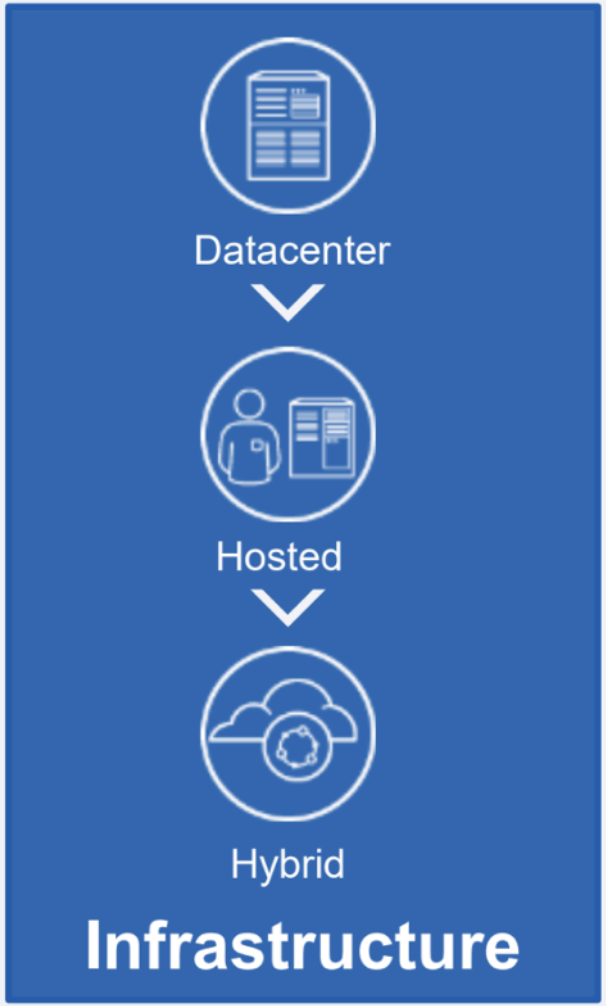
What is a Web Application?

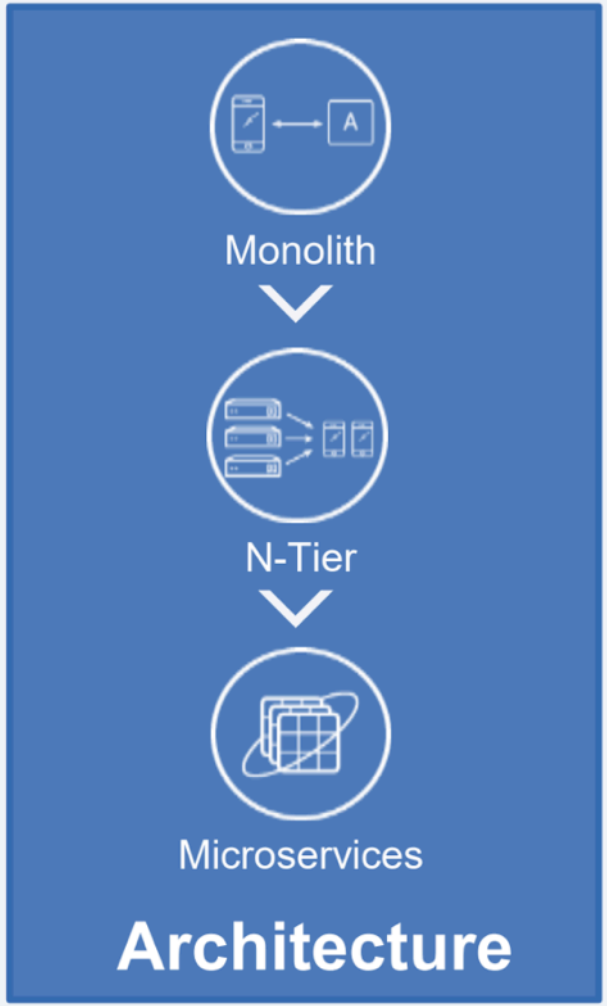


THE TRADITIONAL WEB APPLICATION ARCHITECTURE




Waterfall
Agile
DevOps
Process


Datacenter
Hosted
Hybrid
Infrastructure


A
Monolith
N-Tier
Microservices
Architecture

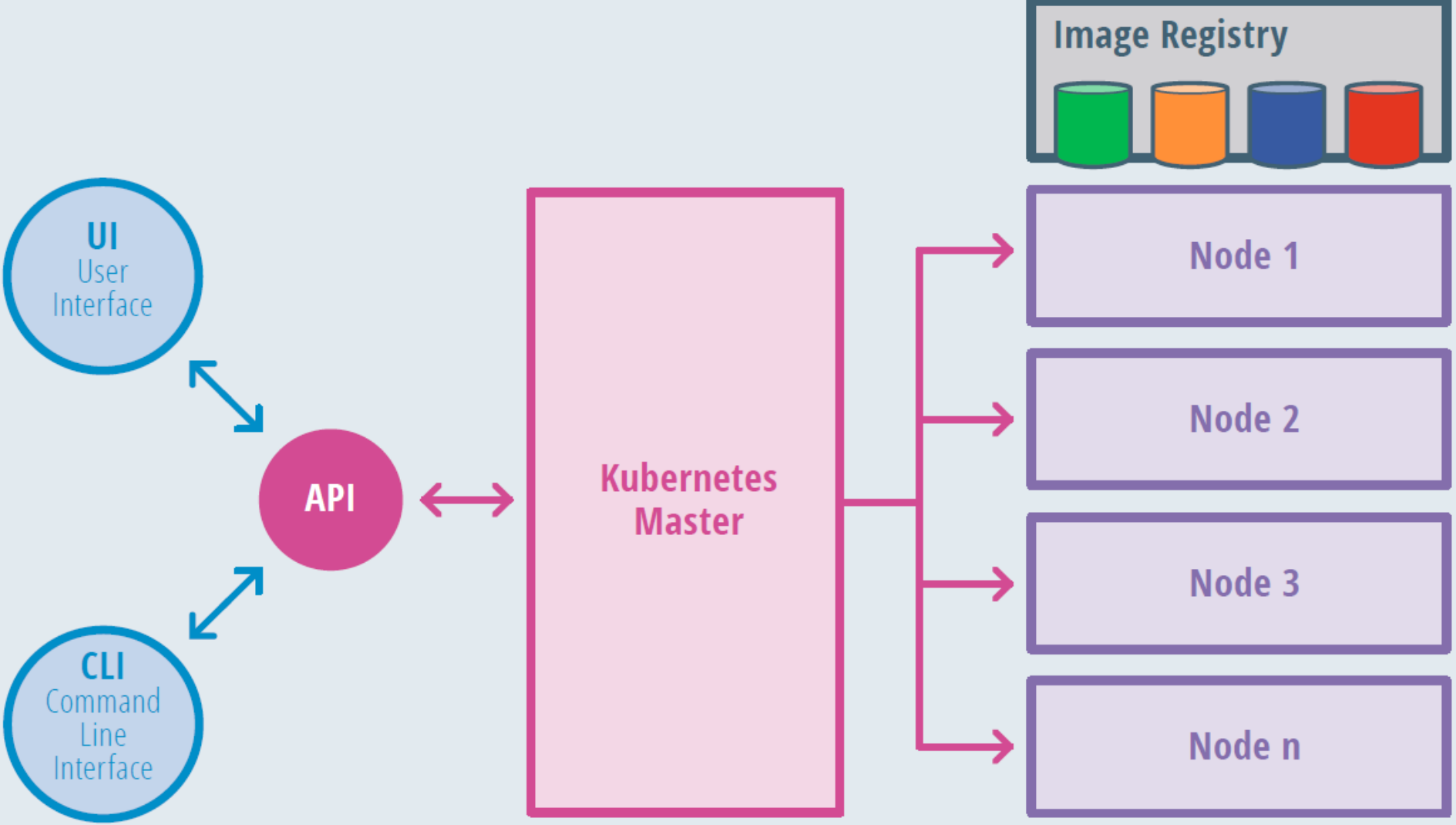
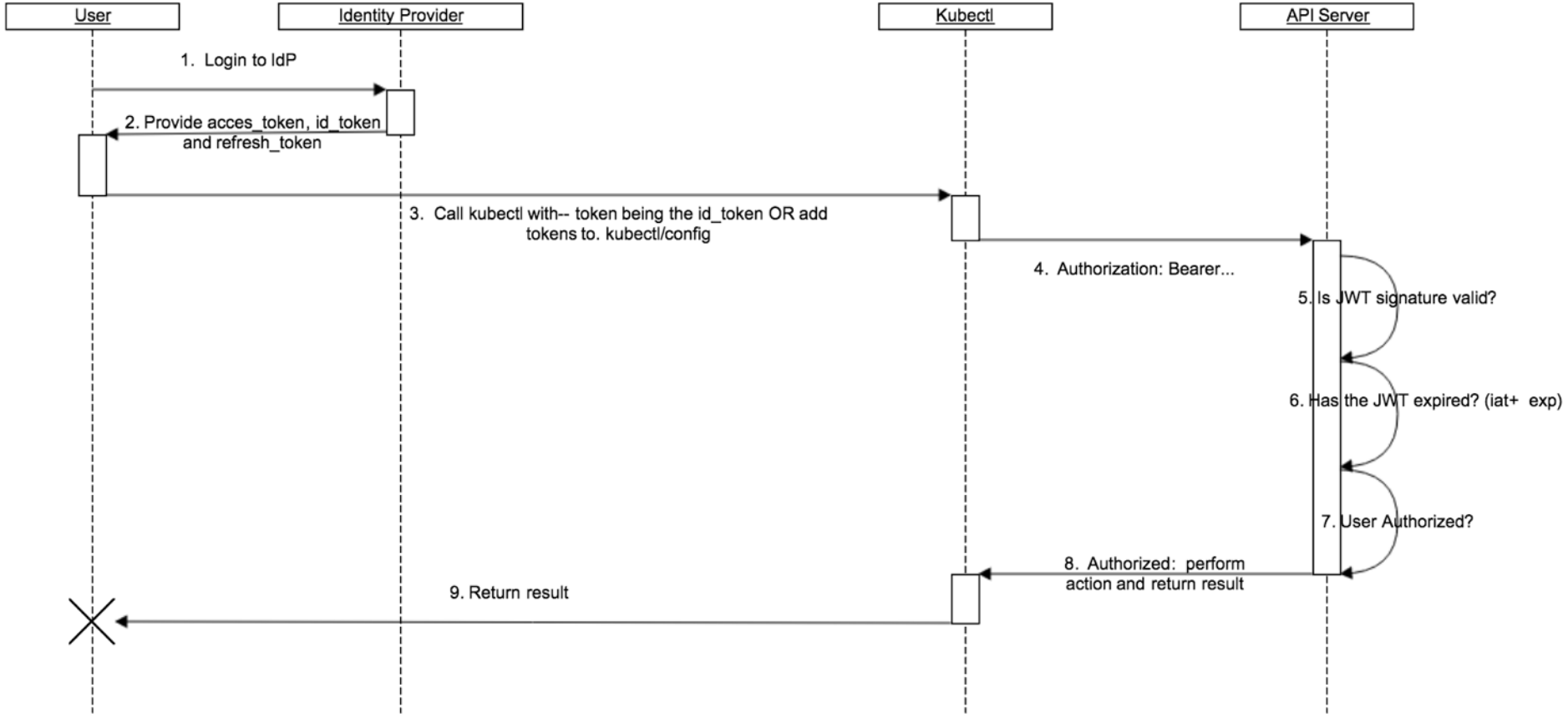


Image Registry
UI
User
Interface
API
CLI
Command
Line
Interface
Kubernetes
Master
Node 1
Node 2
Node 3
Node n

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"
    ]
  }
}
```

WEBHOOK MODE EXAMPLE RESPONSE

```
{
  "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

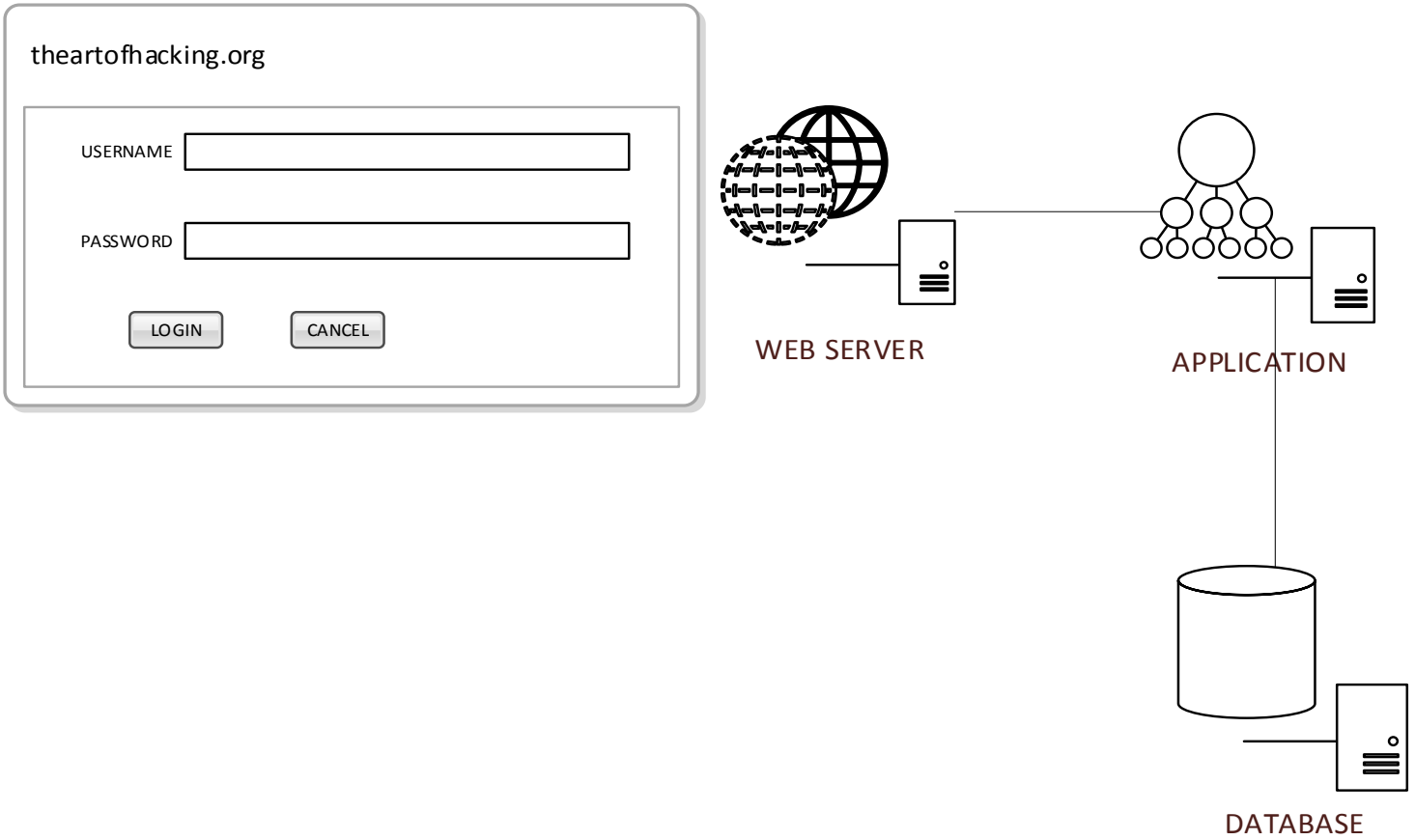
- credentials, tokens, API configurations

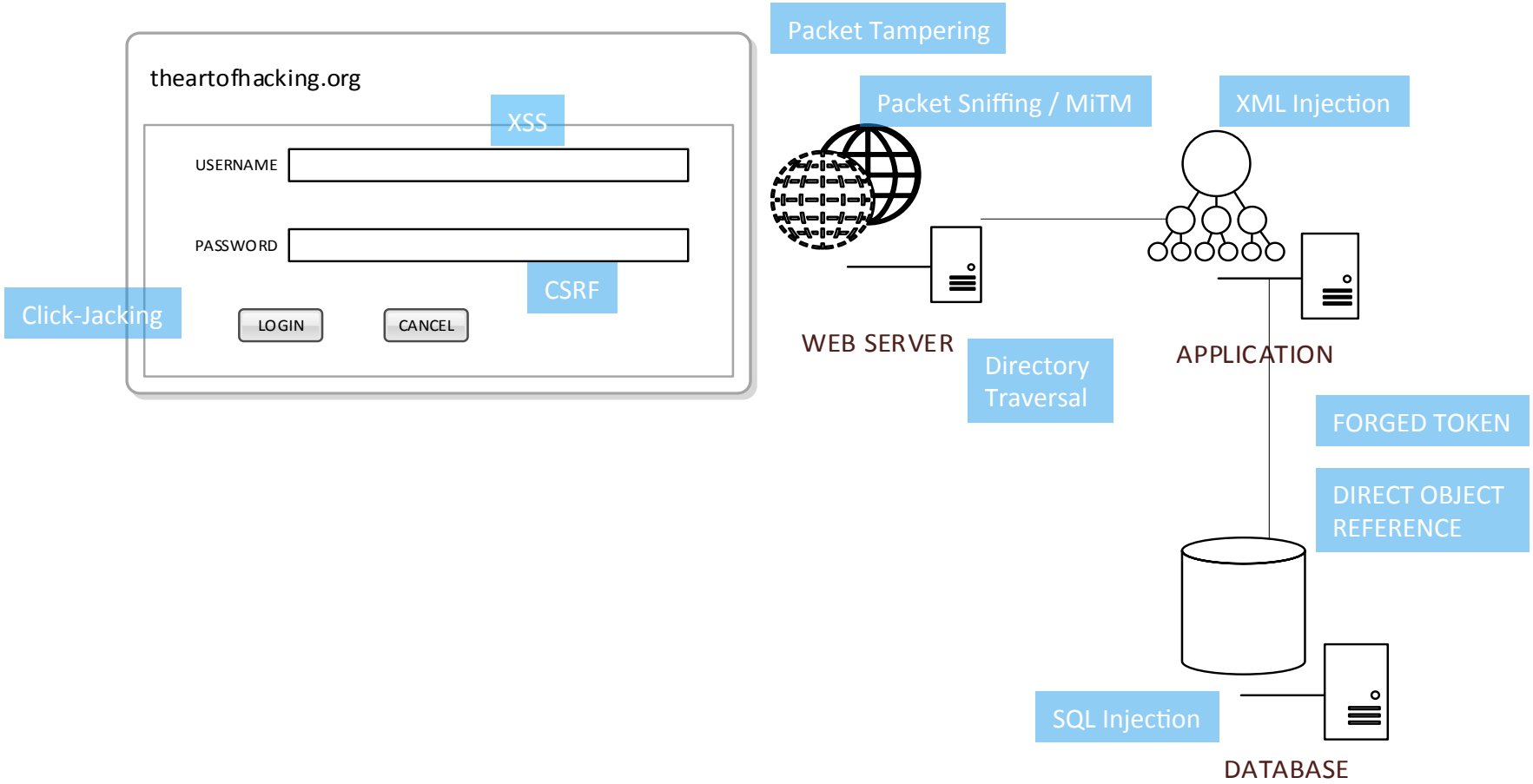
Break the application to manageable chunks

- 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
USERNAME
PASSWORD
LOGIN
CANCEL
WEB SERVER
APPLICATION
DATABASE


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

https://www.owasp.org

About The Open Web Application Security Project

(Redirected from About OWASP)

Last revision (mm/dd/yy): **01/30/2018**

[hide]

The OWASP Foundation

The OWASP Foundation came online on December 1st 2001 it was established as a not-for-profit charitable organization in the United States on April 21, 2004 to ensure the ongoing availability and support for our work at OWASP. OWASP is an international organization and the OWASP Foundation supports OWASP efforts around the world. OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. We can be found at www.owasp.org.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security. OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Similar to many open source software projects, OWASP produces many types of materials in a collaborative and open way. The OWASP Foundation is a not-for-profit entity that ensures the project's long term success.

https://www.owasp.org/index.php/Category:Attack

Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
News
Community portal
Presentations
Press
Projects
Video
Volunteer

Reference
Activities
Attacks
Code Snippets
Controls
Glossary
How To...
Java Project
.NET Project
Principles
Technologies
Threat Agents
Vulnerabilities

Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Category:Attack

Help

This category is for tagging common types of application security attacks.

What is an attack?

Attacks are the techniques that attackers use to exploit the vulnerabilities in applications. Attacks are often confused with vulnerabilities, so please try to be sure that the attack you are describing is something that an attacker would do, rather than a weakness in an application.

All attack articles should follow the Attack template.

Examples:

- Brute Force: Is an exhaustive attack that works by testing every possible value of a parameter (password, file name, etc.) Brute_force_attack
- Cache Poisoning: Is an attack that seeks to introduce false or malicious data into a web cache, normally via HTTP Response Splitting. Cache_Poisoning
- DNS Poisoning: Is an attack that seeks to introduce false DNS address information into the cache of a DNS server, where it will be served to other users enabling a variety of attacks. (e.g., Phishing)

Note: many of the items marked vulnerabilities and other places are really attacks. Some of the more obvious are:

- Resource exhaustion
- Reflection injection
- Reflection attack in an auth protocol

Subcategories

This category has the following 12 subcategories, out of 12 total.

A
- Abuse of Functionality (7 P)

D
- Data Structure Attacks (2 P)

E
- Embedded Malicious Code (3 P)
- Exploitation of Authentication (8 P)

I
- Injection (30 P)

P
- Path Traversal Attack (1 P)
- Probabilistic Techniques (4 P)
- Protocol Manipulation (1 P)

R
- Resource Depletion (2 P)
- Resource Manipulation (10 P)

S
- Sniffing Attacks (empty)
- Spoofing (5 P)

Pages in category "Attack"

The following 69 pages are in this category, out of 69 total.

B
- Binary planting
- Blind SQL Injection
- Blind XPath Injection
- Brute force attack
- Buffer overflow attack

C
- Cache Poisoning
- Cash Overflow
- Code Injection
- Command Injection
- Comment Injection Attack
- Content Security Policy
- Content Spoofing
- Cornucopia - Ecommerce Website Edition - Wiki Deck
- Execution After Redirect (EAR)

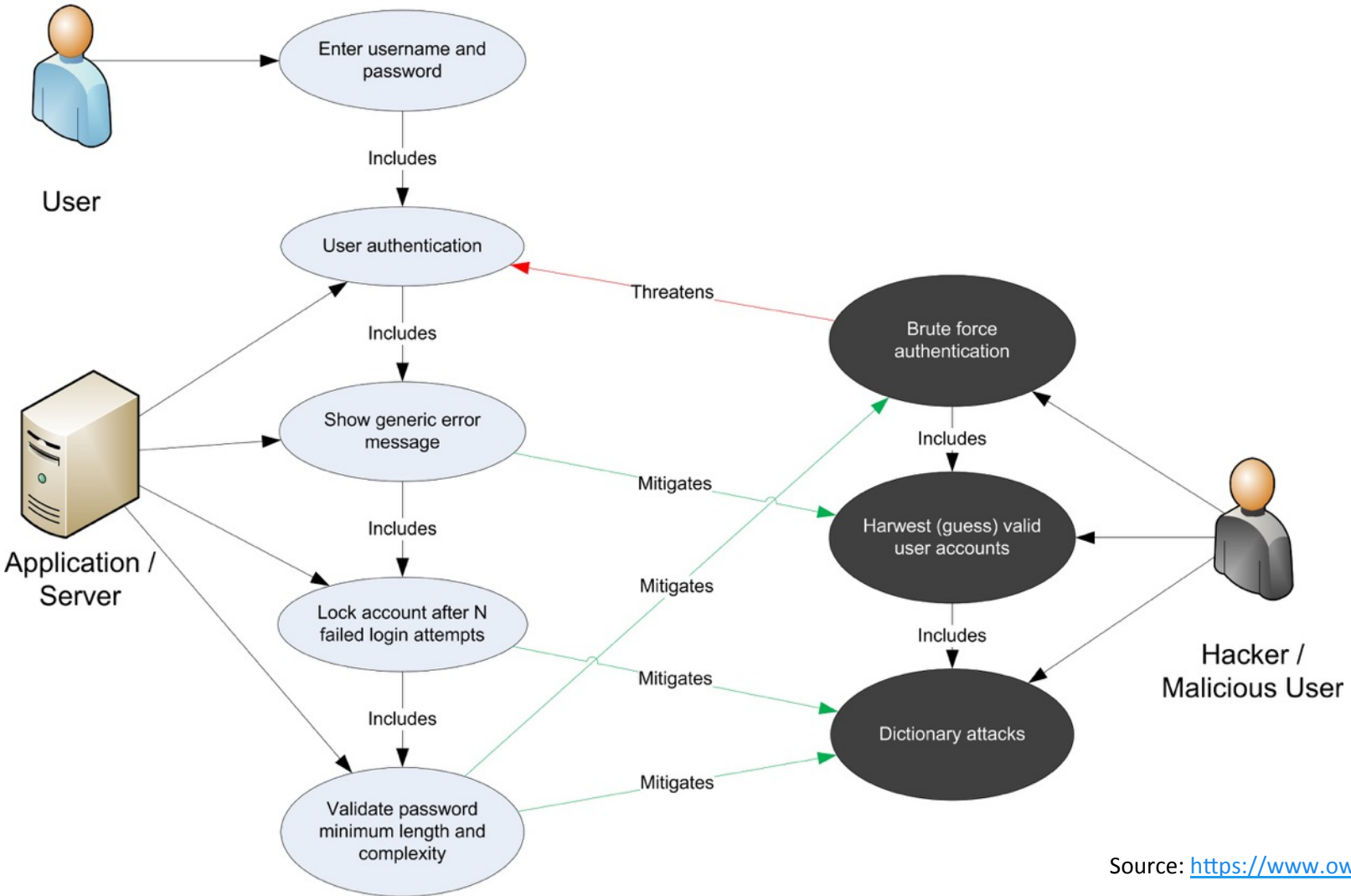
F
- Forced browsing
- Form action hijacking
- Format string attack
- Full Path Disclosure
- Function Injection

H
- HTTP Response Splitting

I
- Inyección de Código
- Inyección SQL
- Inyección SQL Ciega
- Inyección XPath
- Path Traversal

R
- Reflected DOM Injection
- Regular expression Denial of Service - ReDoS
- Repudiation Attack
- Resource Injection

S
- Server-Side Includes (SSI) Injection
- Session fixation
- Session hijacking attack
- Session Prediction
- Setting Manipulation
- Special Element Injection
- Spyware
- SQL Injection



Source: https://www.owasp.org

https://theartofhacking.org/github

Add topics

63 commits | 1 branch | 0 releases | 2 contributors

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

santosomar adding additional references — Latest commit 8a852c5 22 hours ago

capture_the_flag	adding CTF information	4 months ago
cheat_sheets	adding additional references	22 hours ago
cloud_resources	Rename Kali in AWS.md to README.md	6 months ago
exploit_development	adding exploit exercises	26 days ago
fuzzing_resources	Add fuzzing resources links	5 months ago
metasploit_resources	adding metasploit info	28 days ago
mobile_security	adding reverse engineering and mobile security references	2 months ago
osint	adding OSINT resources	28 days ago
pen_testing_reports	Rename public_reports.md to README.md	6 months ago
recon	adding recon info	26 days ago
reverse_engineering	adding exploit development references	2 months ago
useful_commands_and_scripts	Create reverse_shells.md	27 days ago
virl_topologies	Renumber VIRL topology files as reflected in the actual lesson numbers	27 days ago
vulnerable_servers	Update README.md	27 days ago
wireless_resources	Update z-wave.md	a month ago
README.md	Update README.md	3 months ago

README.md

The Art of Hacking Series

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

- 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)!

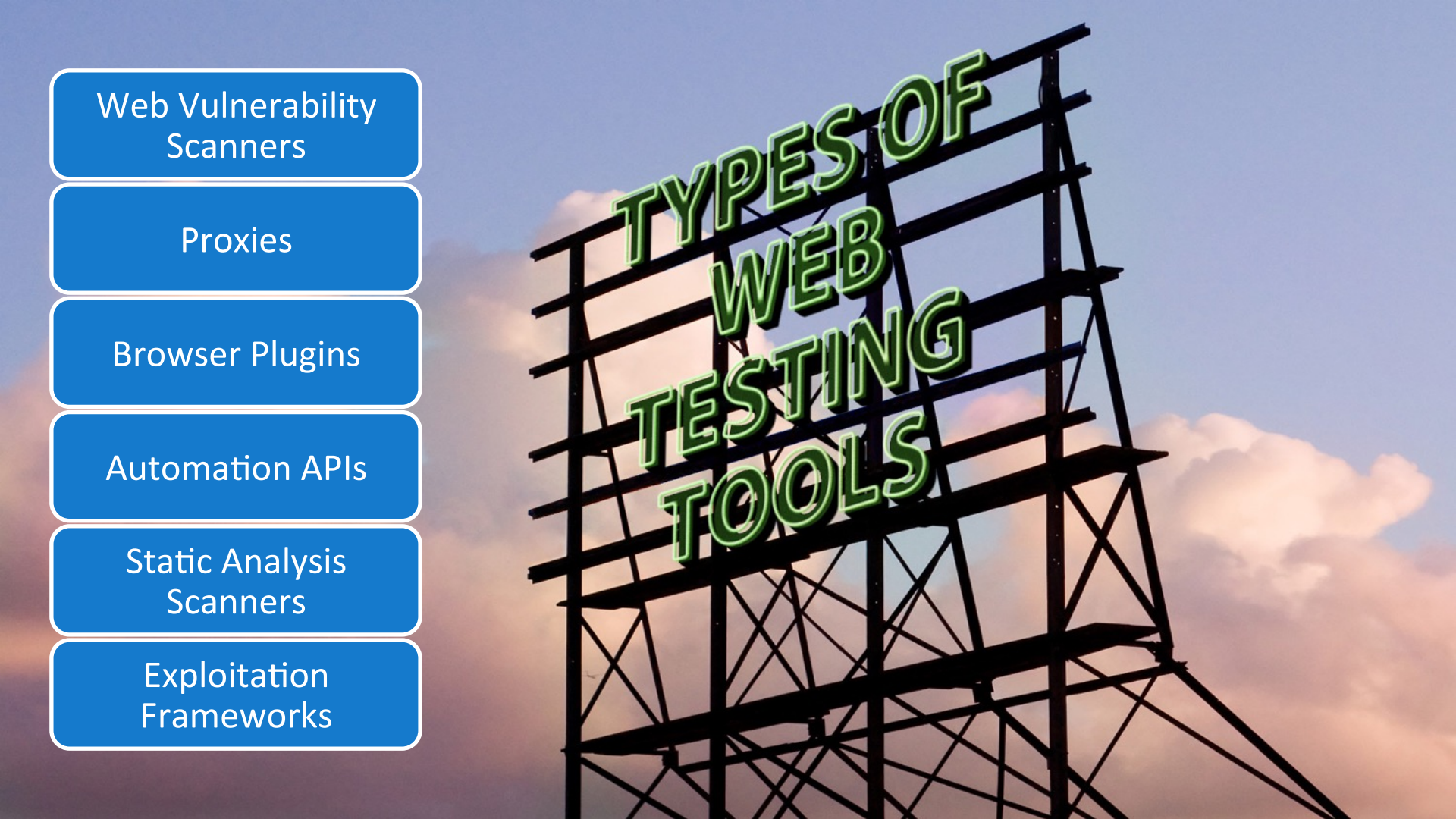
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

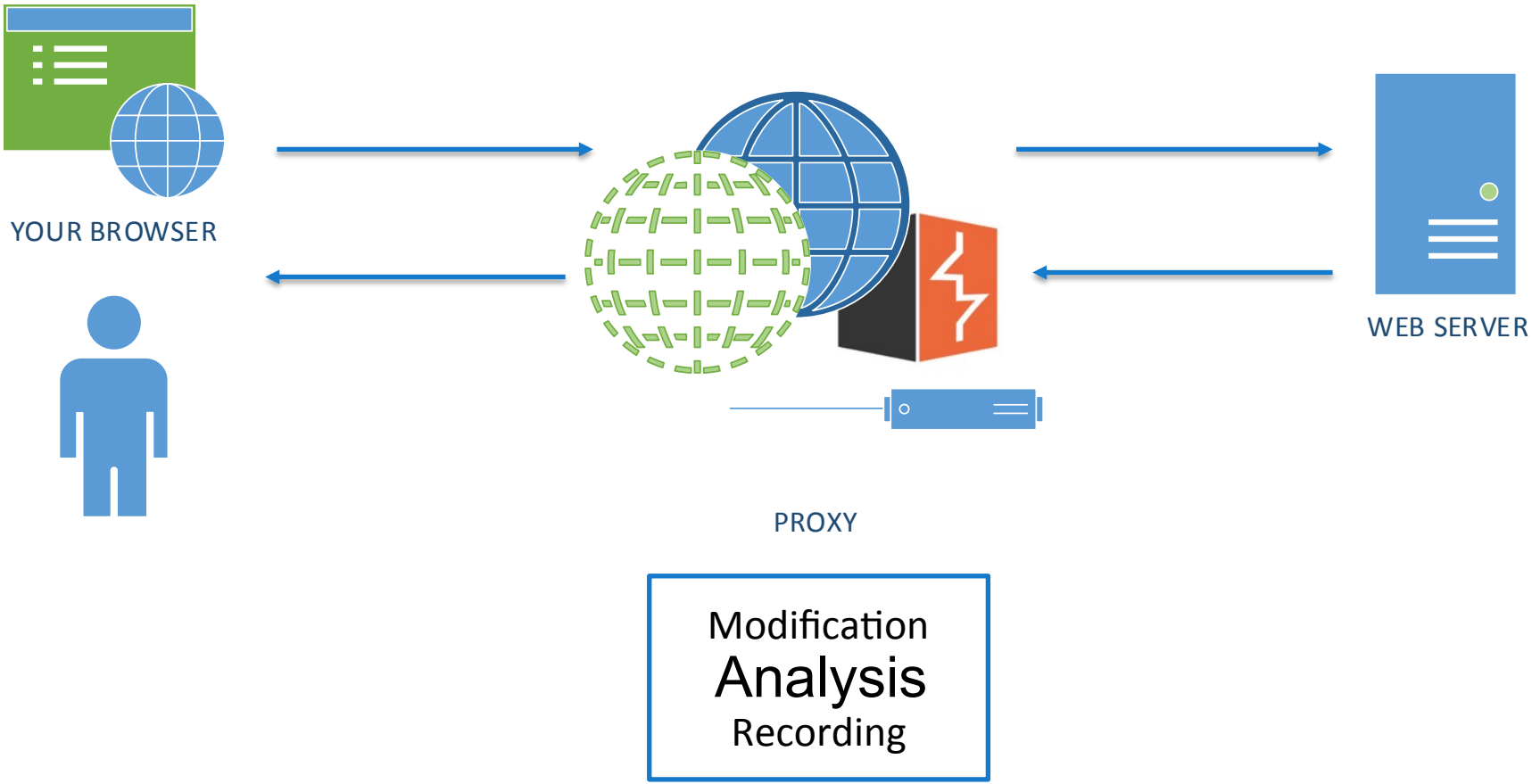
Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest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

Disclaimer

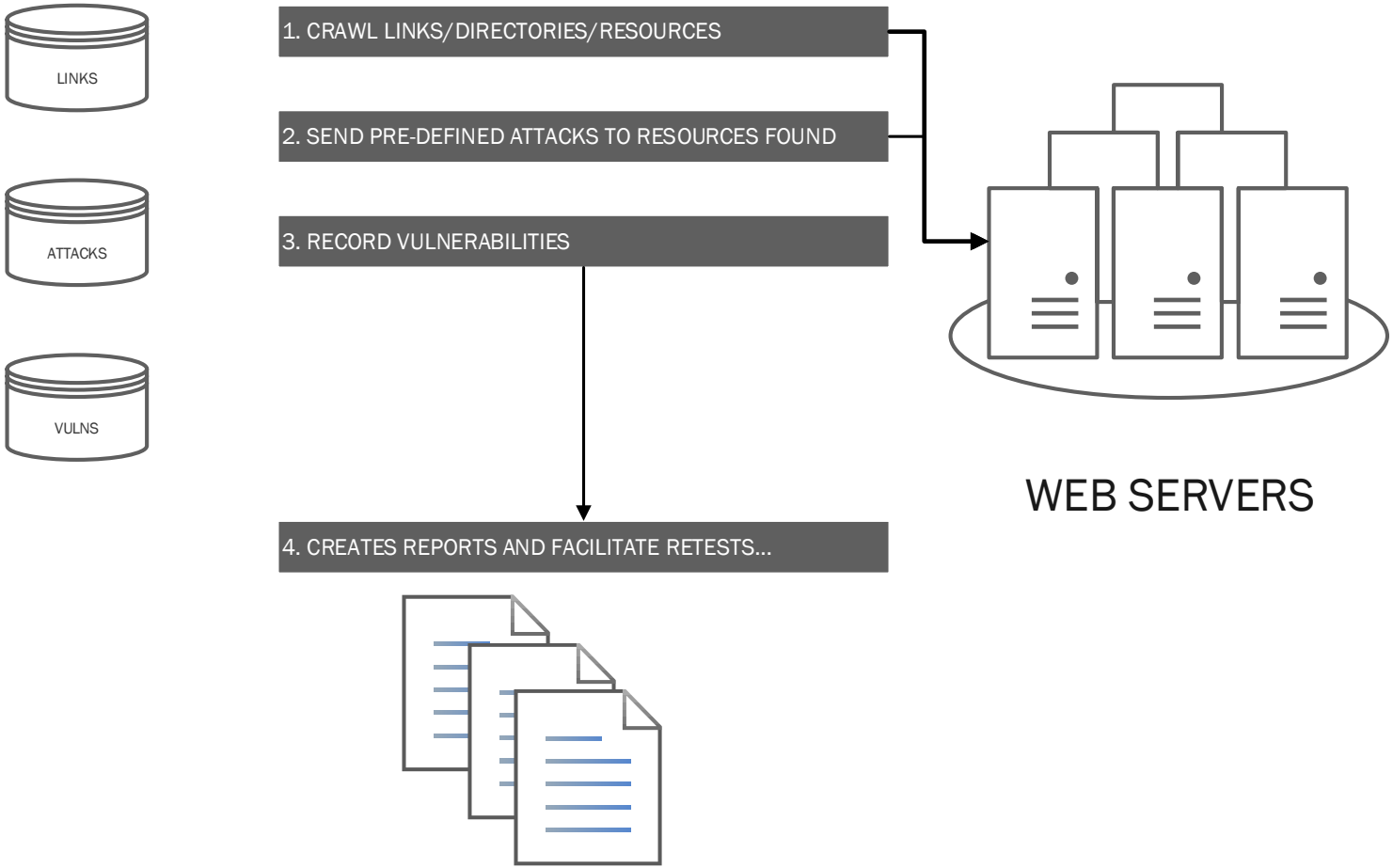
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the

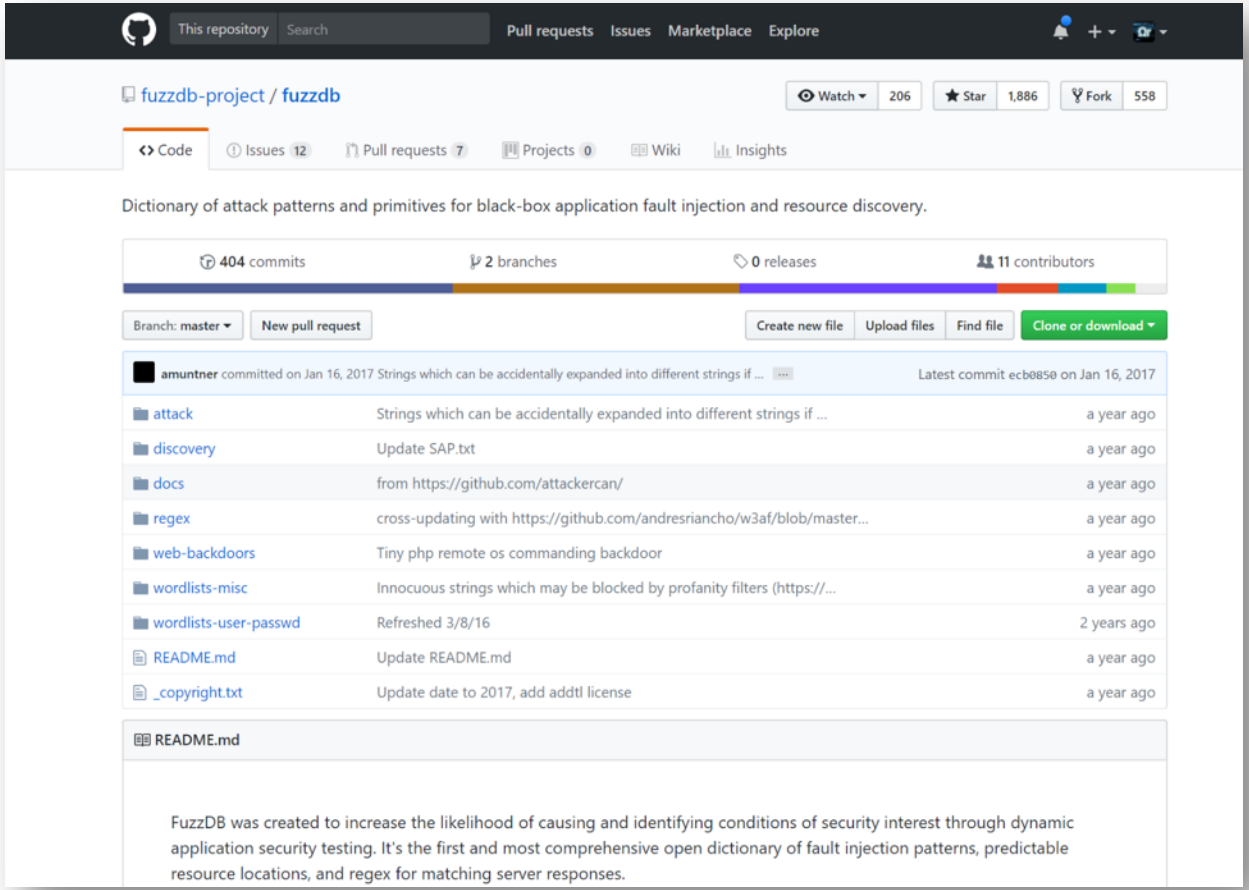


- Web Vulnerability Scanners
- Proxies
- Browser Plugins
- Automation APIs
- Static Analysis Scanners
- Exploitation Frameworks


YOUR BROWSER
WEB SERVER
PROXY
Modification
Analysis
Recording

HOW WEB SCANNERS WORK?

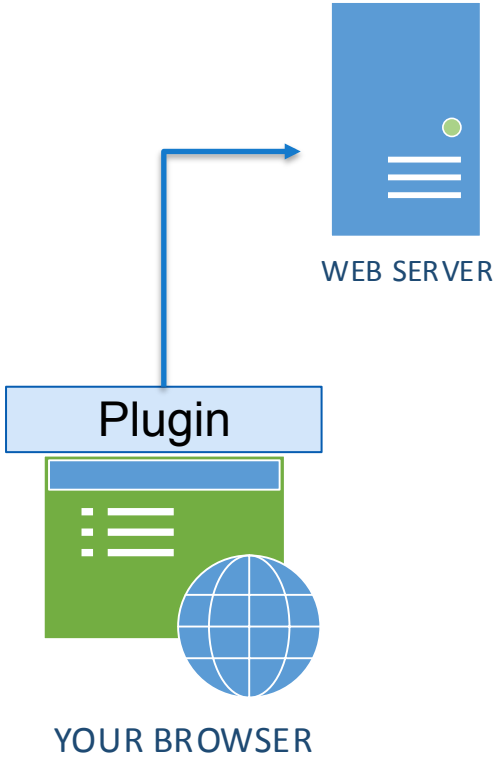

LINKS
ATTACKS
VULNS
1. CRAWL LINKS/DIRECTORIES/RESOURCES
2. SEND PRE-DEFINED ATTACKS TO RESOURCES FOUND
3. RECORD VULNERABILITIES
4. CREATES REPORTS AND FACILITATE RETESTS...
WEB SERVERS



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.



<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

```
1  // ==UserScript==
2  // @name         Omar's new script
3  // @namespace    http://tampermonkey.net/
4  // @version      0.1
5  // @description  try to take over the world!
6  // @author       You
7  // @match        http://*/*
8  // @grant        none
9  // ==/UserScript==
10
11 (function() {
12     'use strict';
13
14     // Your code here...
15 })();
```

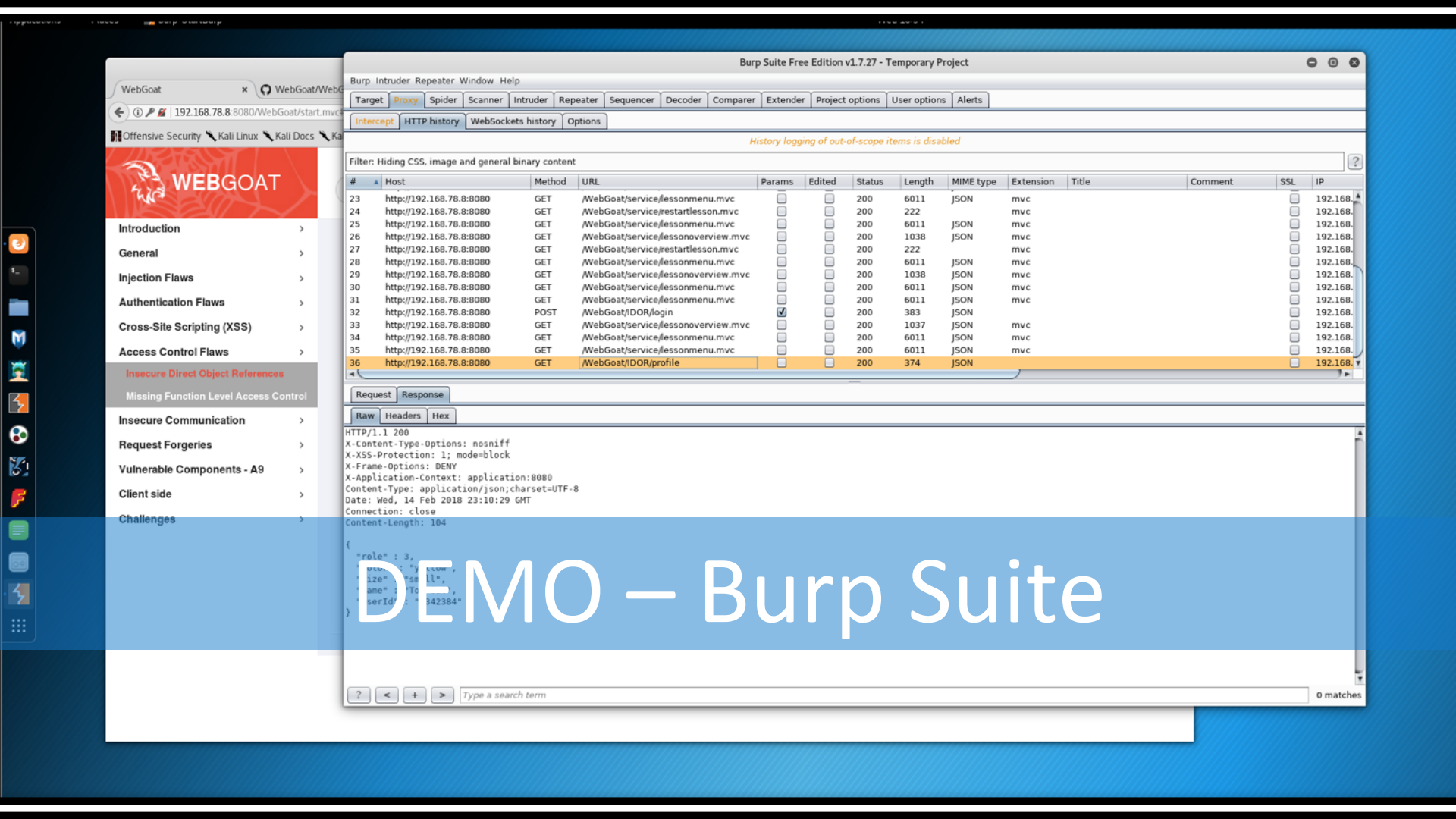
Exploitation Frameworks

- Metasploit
- Social Engineering Toolkit (SET)
- Browser Exploitation Framework (BeEF)

OWASP TOP 10

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project


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,
Type a search term
0 matches
DEMO – Burp Suite

Cross-site Scripting (XSS)

There are three forms of XSS, usually targeting users' browsers:

- **Reflected XSS**: The application or API includes unvalidated and unescaped 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**: unsanitized 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.

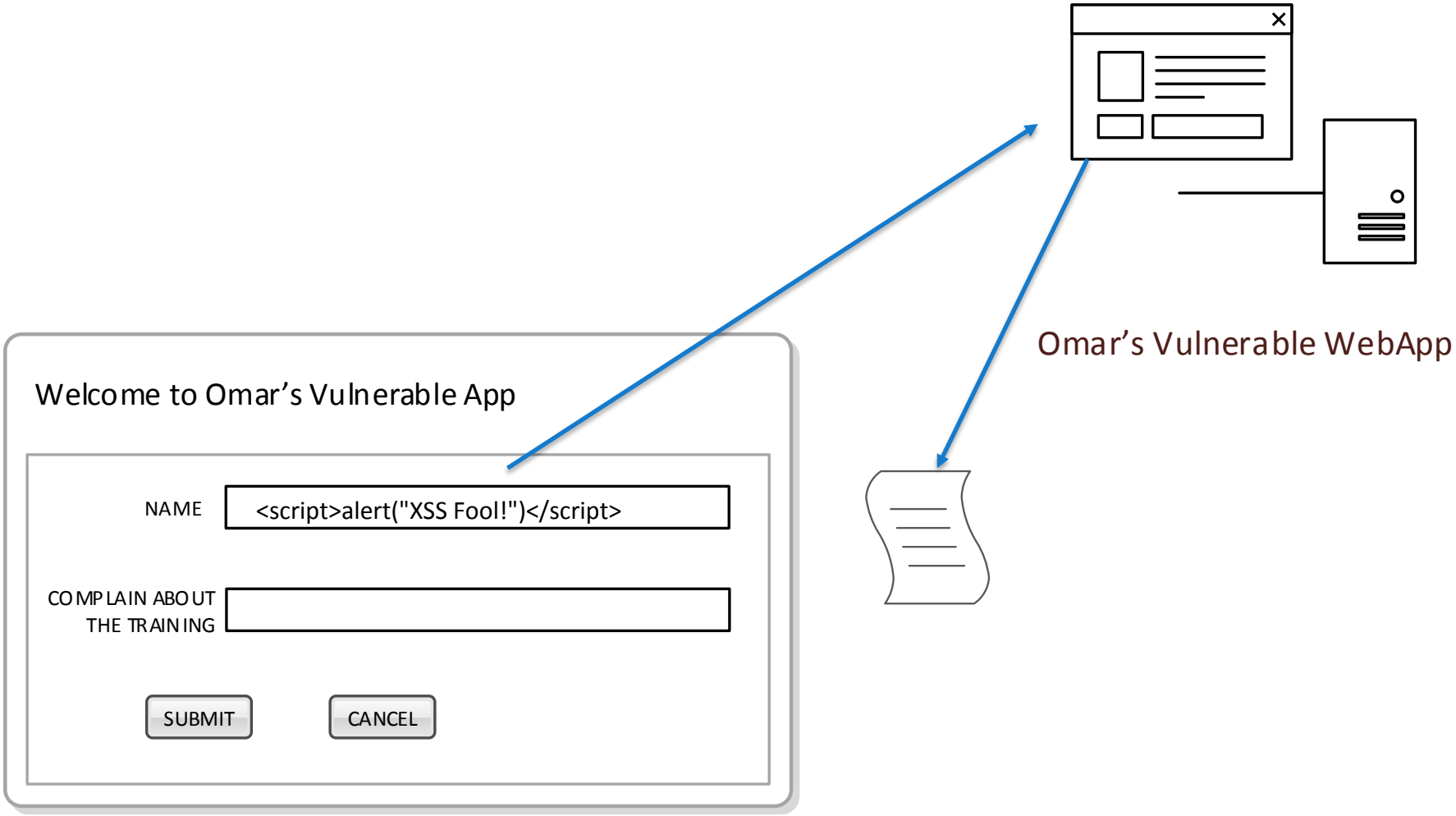
XSS attacks include session stealing, account takeover, MFA bypass, DOM node replacement or defacement (such as trojan login panels), attacks against the user's browser such as malicious software downloads, key logging, and other client-side attacks.

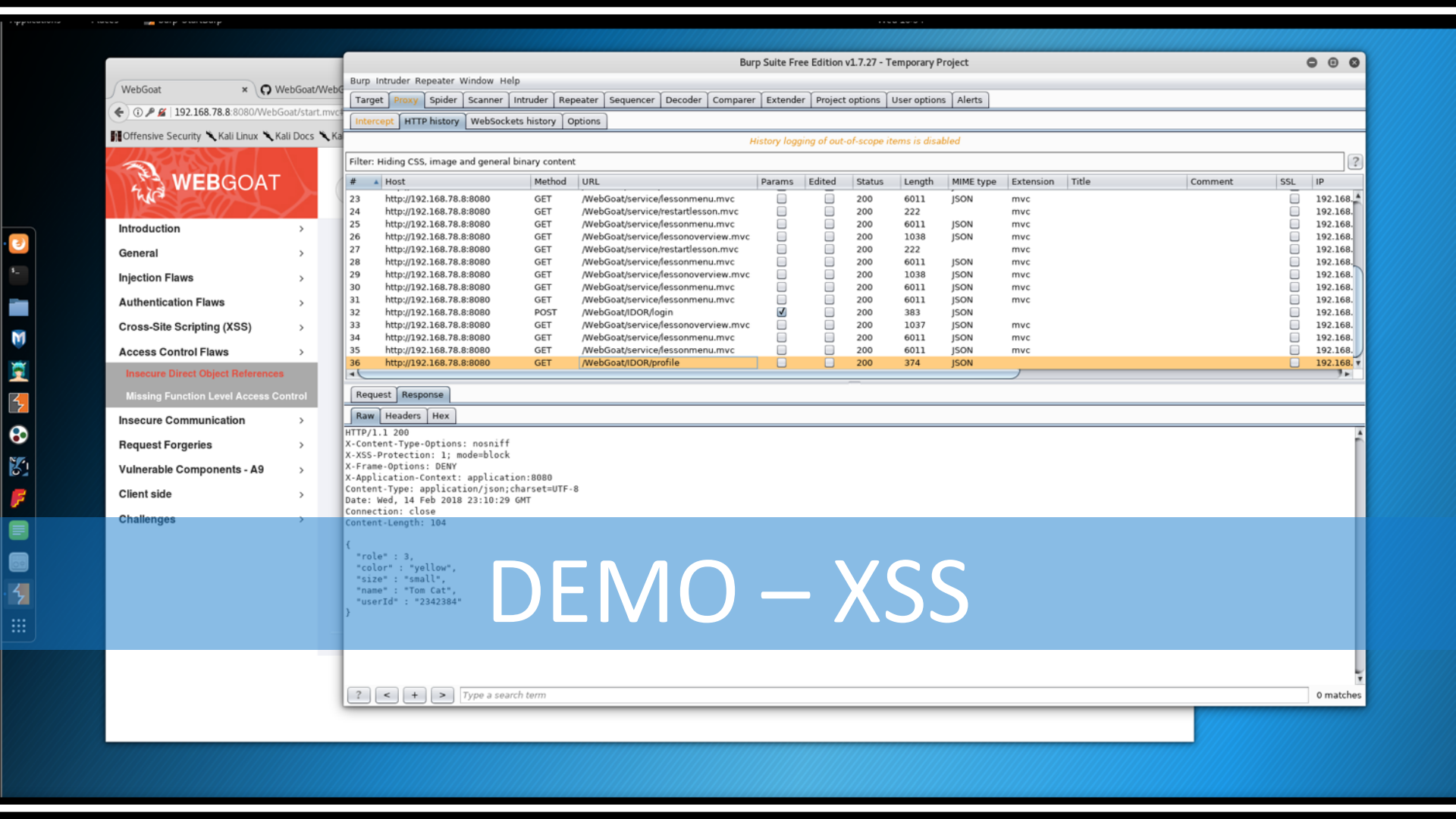
https://theartofhacking.org/go/top10.html

Cross-site Scripting (XSS)

Where do you typically 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

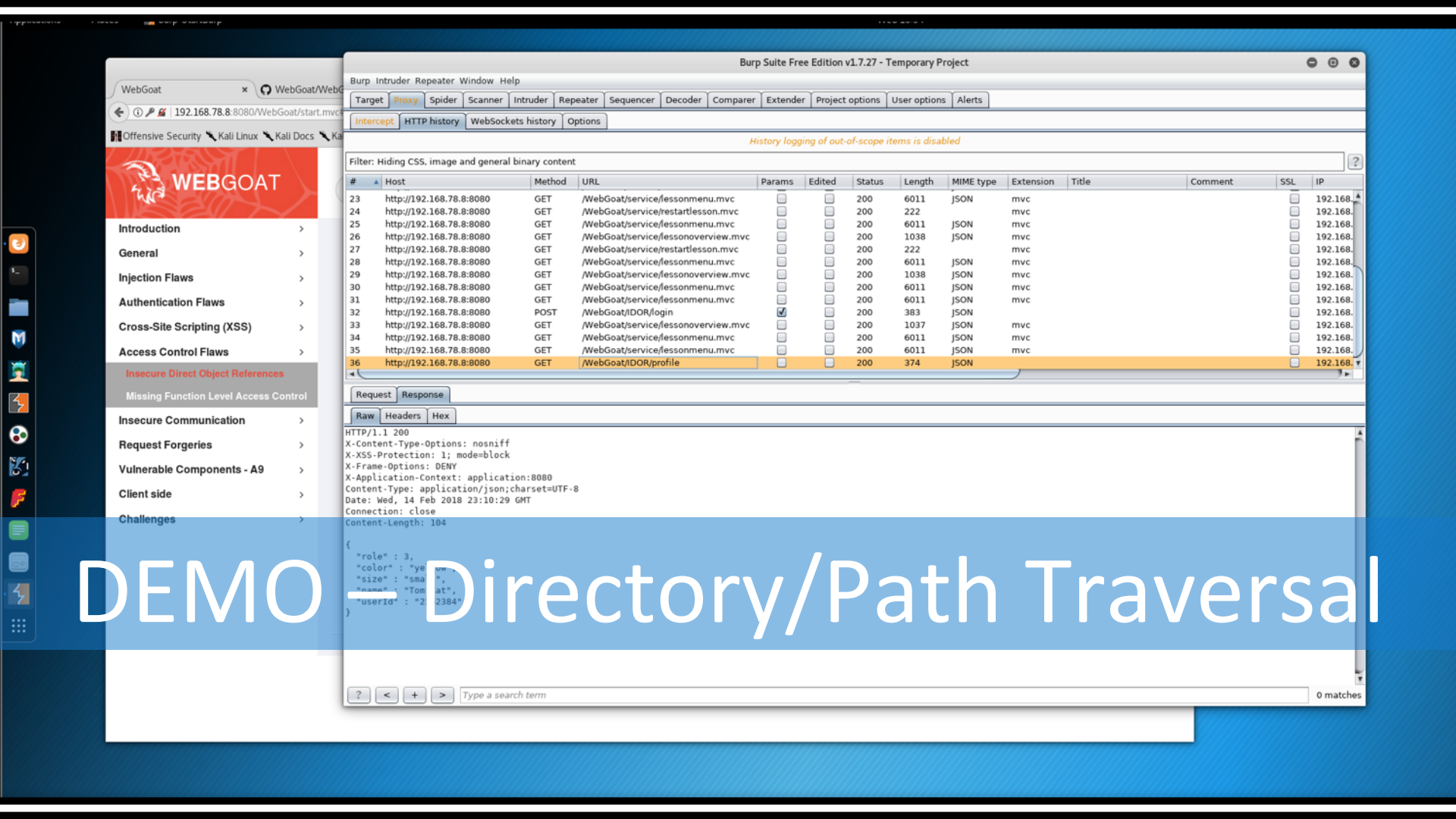

WebGoat
192.168.78.8:8080/WebGoat/start.mvc
Offensive Security
Kali Linux
Kali Docs
WEBGOAT
Introduction
General
Injection Flaws
Authentication Flaws
Cross-Site Scripting (XSS)
Access Control Flaws
Insecure Direct Object References
Missing Function Level Access Control
Insecure Communication
Request 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

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

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

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



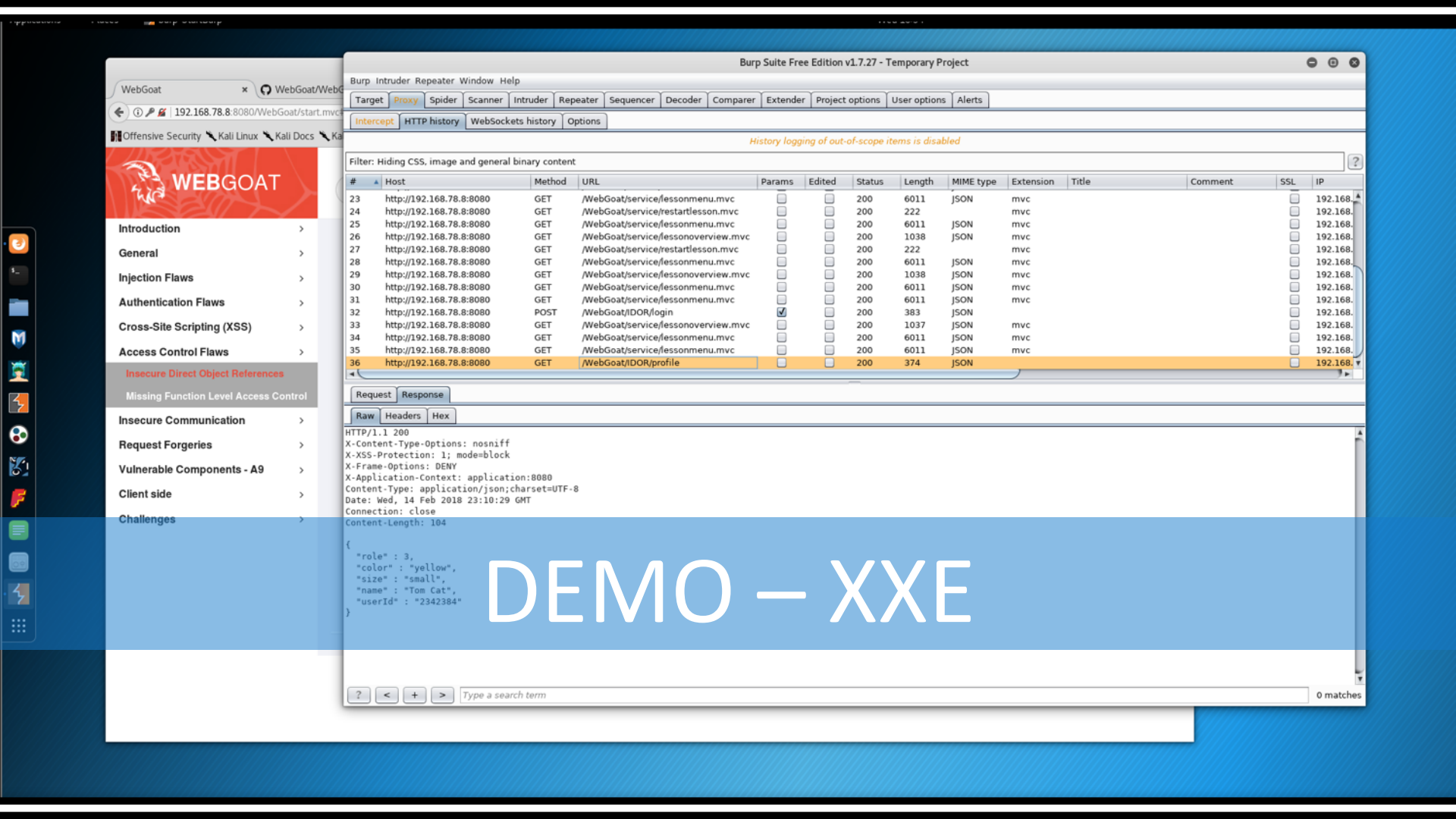
DEMO - Directory/Path Traversal

XML External Entity (XXE)

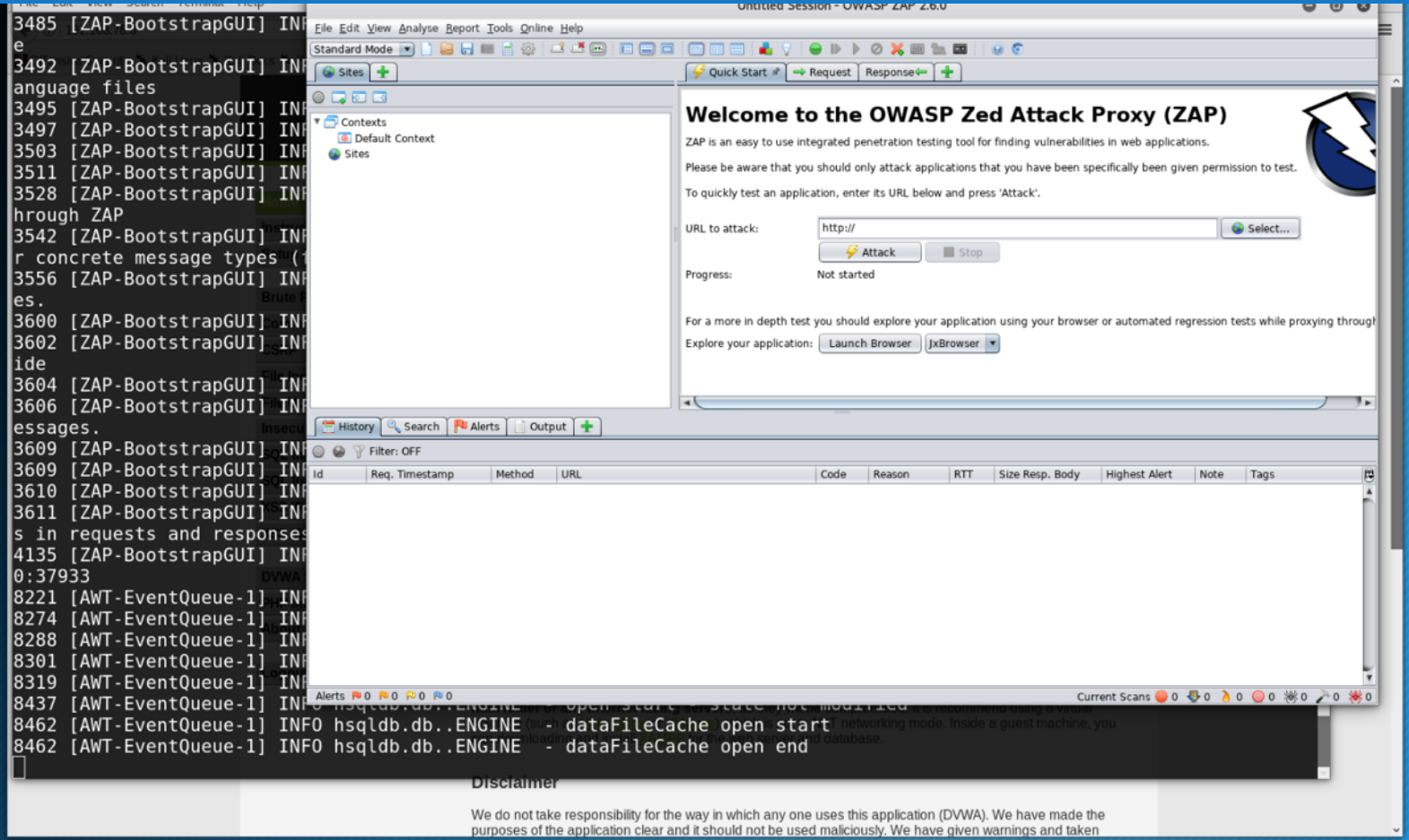
Poorly configured XML parsers evaluate external entity references within XML docs.

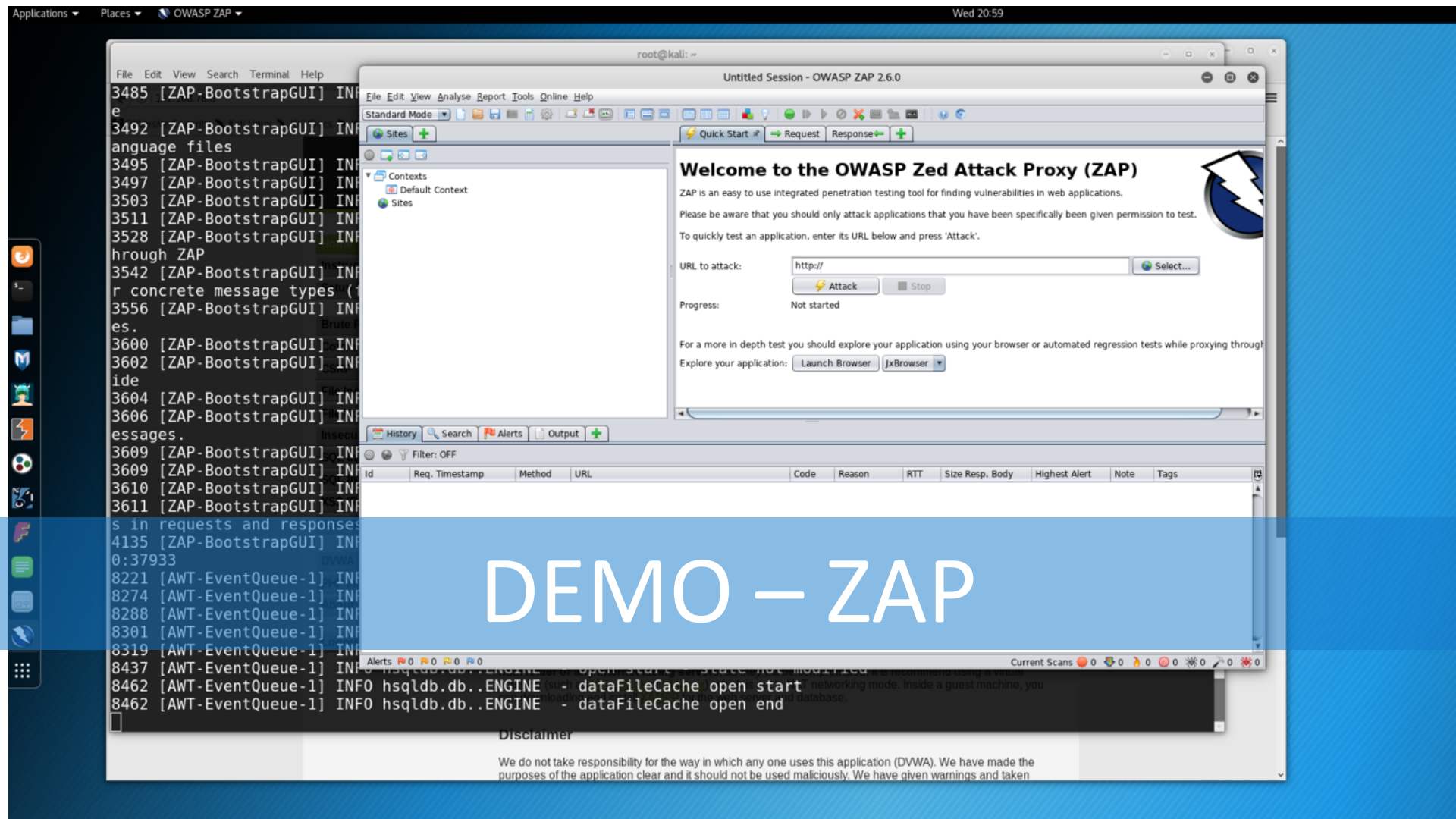
External entities can be used to:

* disclose internal files using the file URI handler
* internal file shares
* 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

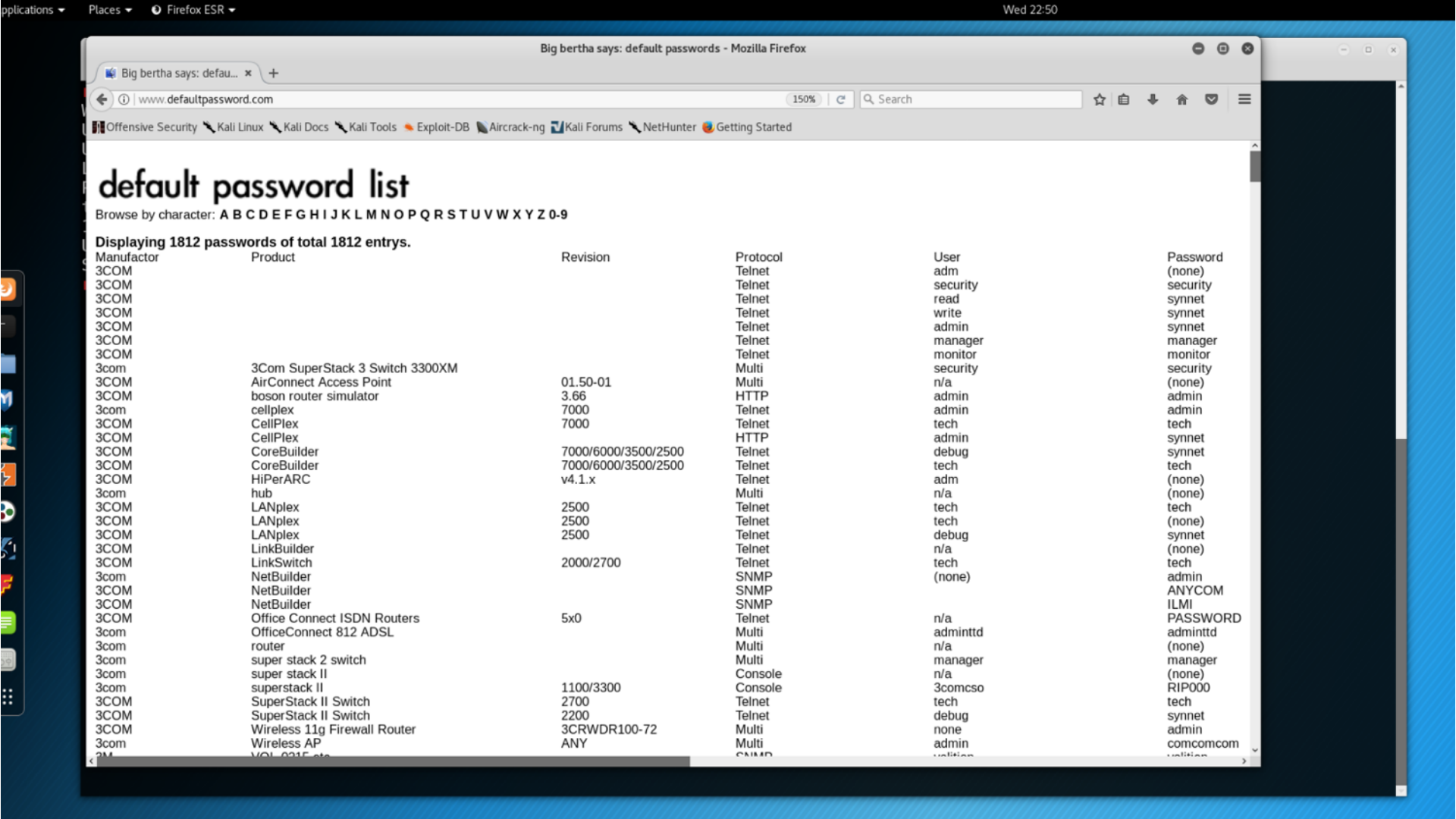
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project




Applications
Places
OWASP ZAP
Wed 20:59
root@kali: ~
File Edit View Search Terminal Help
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
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
DEMO – ZAP
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

Introduction to Hacking User Credentials

http://www.phenoelit-us.org/dpl/dpl.html
http://cirt.net/passwords
http://www.defaultpassword.com
http://www.passwordsdatabase.com
http://www.isdpodcast.com/resources/62k-common-passwords



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

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

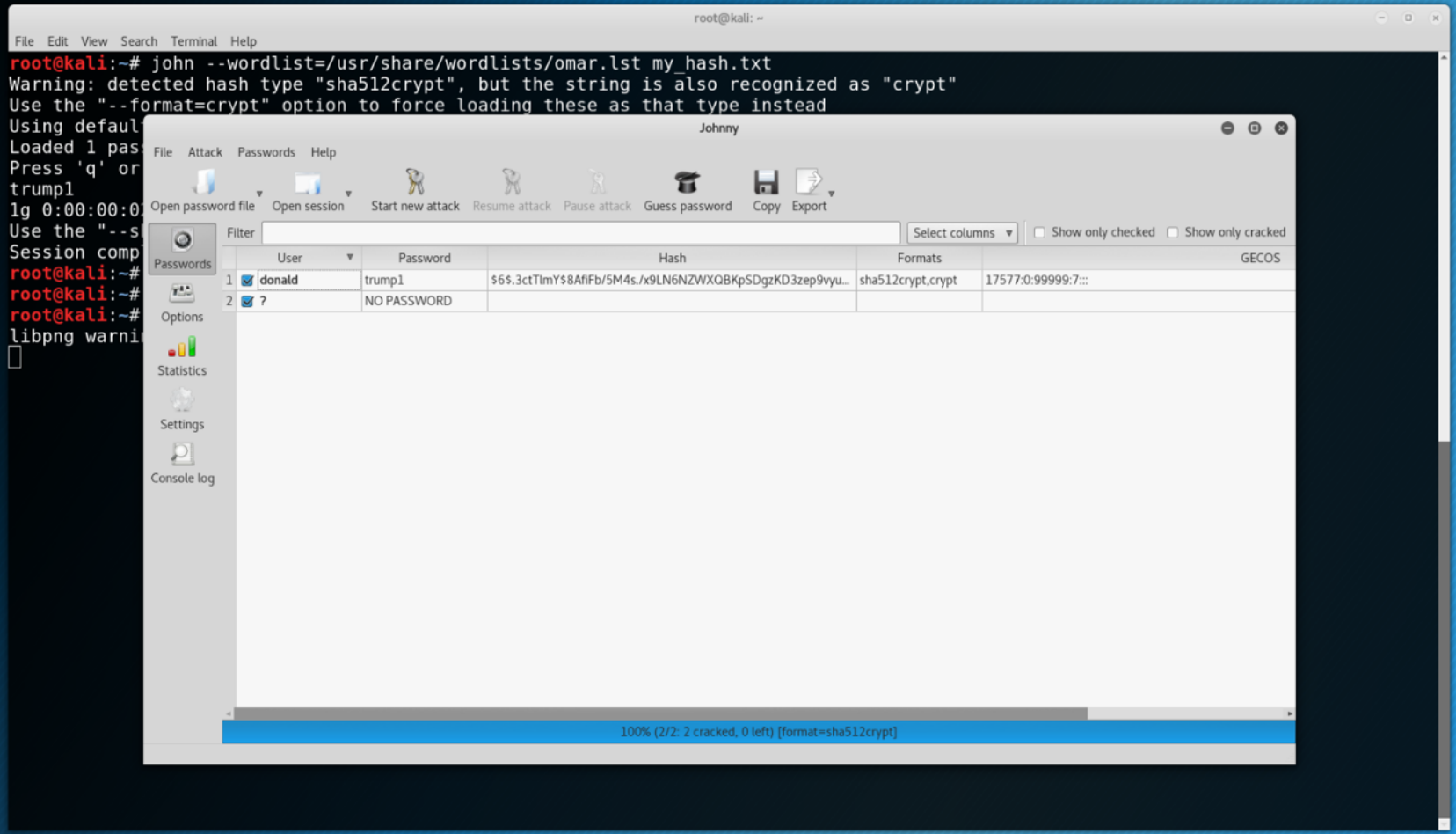
john -show passwd

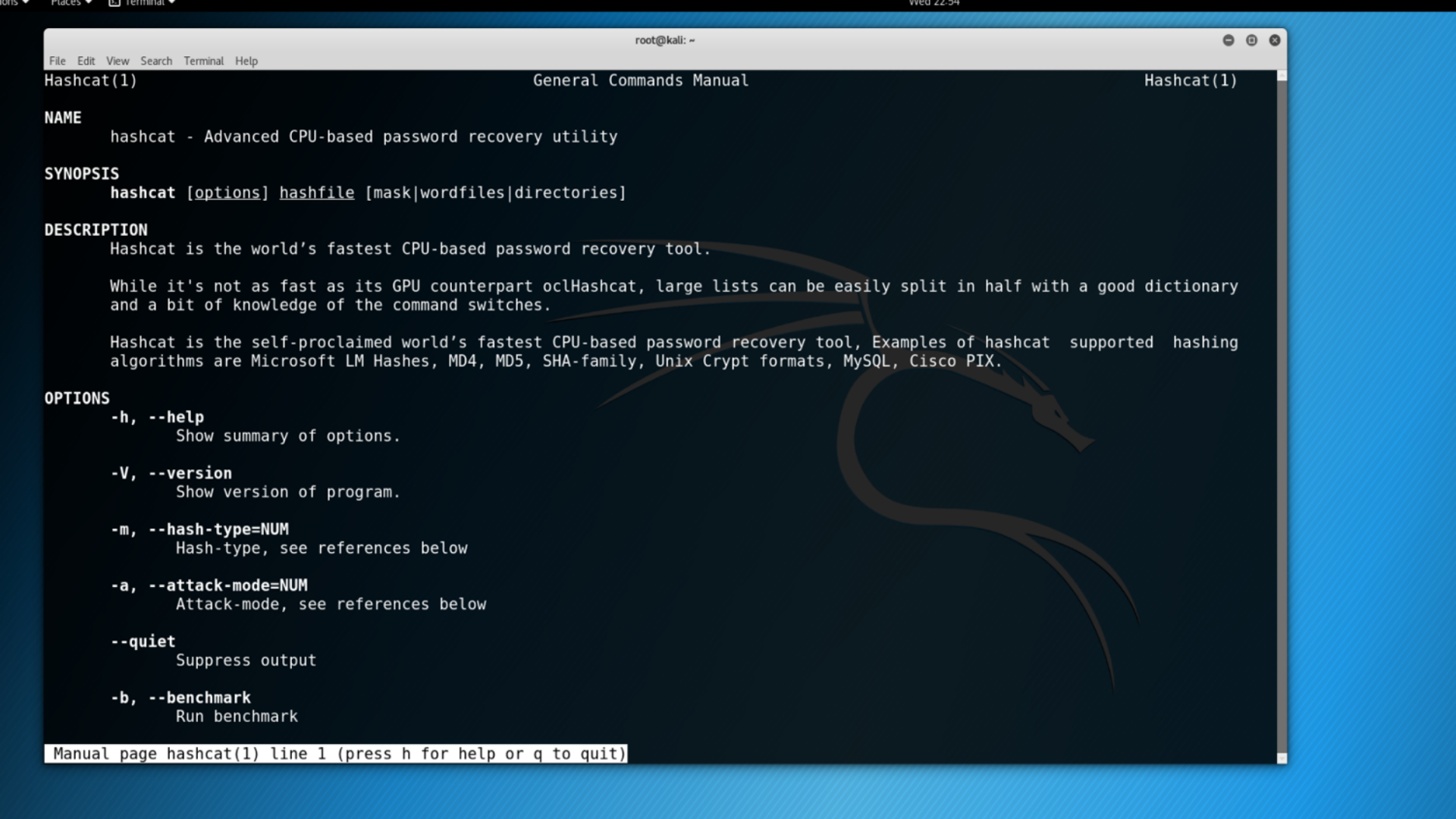
Important: do this under the same directory where the password was cracked (when using the cronjob, /var/lib/john), otherwise it won't work.

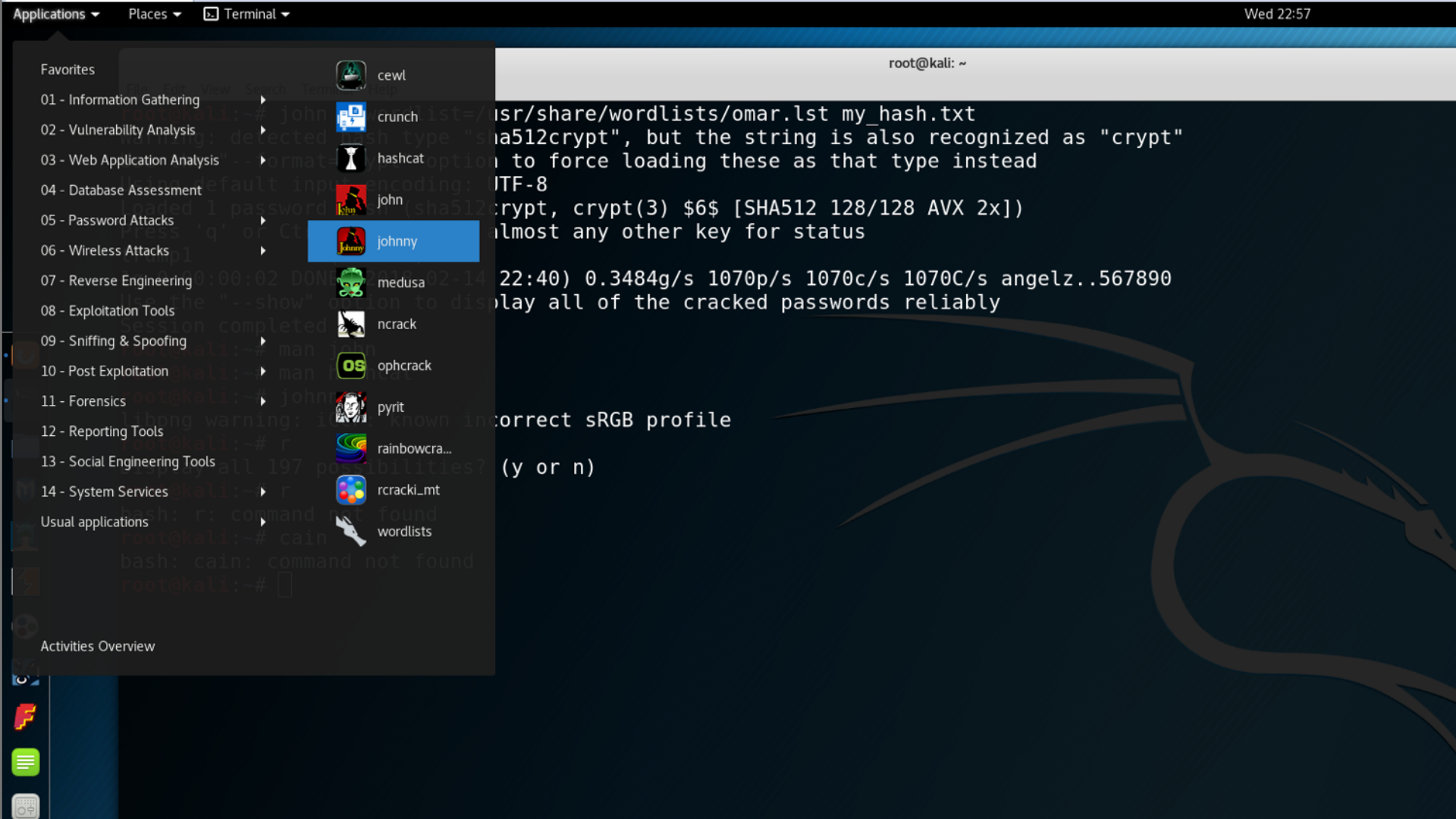
While cracking, you can press any key for status, or Ctrl+C to abort the session, saving point information to a file (~/.john/john.rec by default). By the way, if you press Ctrl+C twice John will abort immediately without saving. The point information is also saved every 10 minutes (configurable in the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

To continue an interrupted session, run:

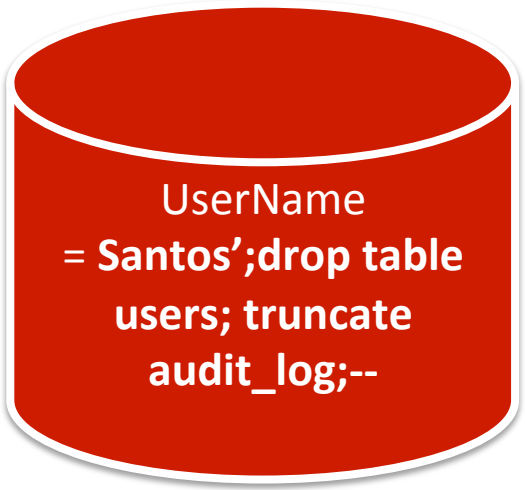
Manual page john(8) line 1 (press h for help or q to quit)


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
Filter
Select columns
Show only checked
Show only cracked
Passwords
Options
Statistics
Settings
Console log
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]

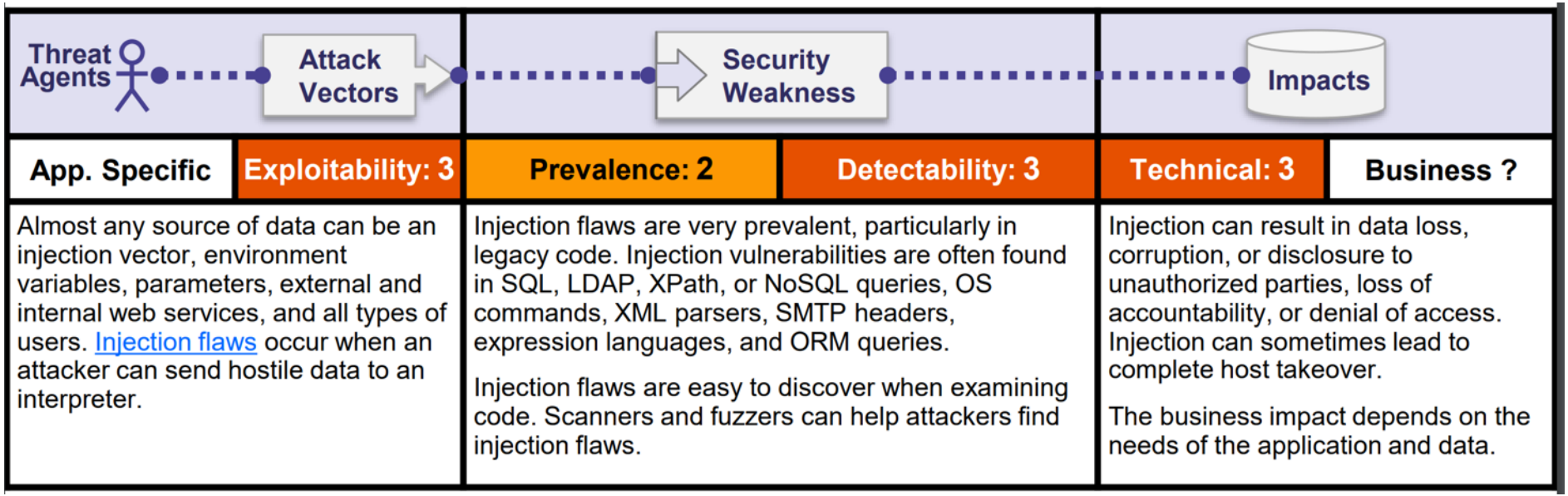

root@kali: ~
File Edit View Search Terminal Help
Hashcat(1) General Commands Manual Hashcat(1)
NAME
hashcat - Advanced CPU-based password recovery utility
SYNOPSIS
hashcat [options] hashfile [mask|wordfiles|directories]
DESCRIPTION
Hashcat is the world's fastest CPU-based password recovery tool.
While 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
root@kali: ~
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
sr/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
rypt, crypt(3) 6 [SHA512 128/128 AVX 2x])
lmost 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
orrect sRGB profile
(y or n)

DEMO – CRACKING PASSWORDS



Introduction to Hacking Databases

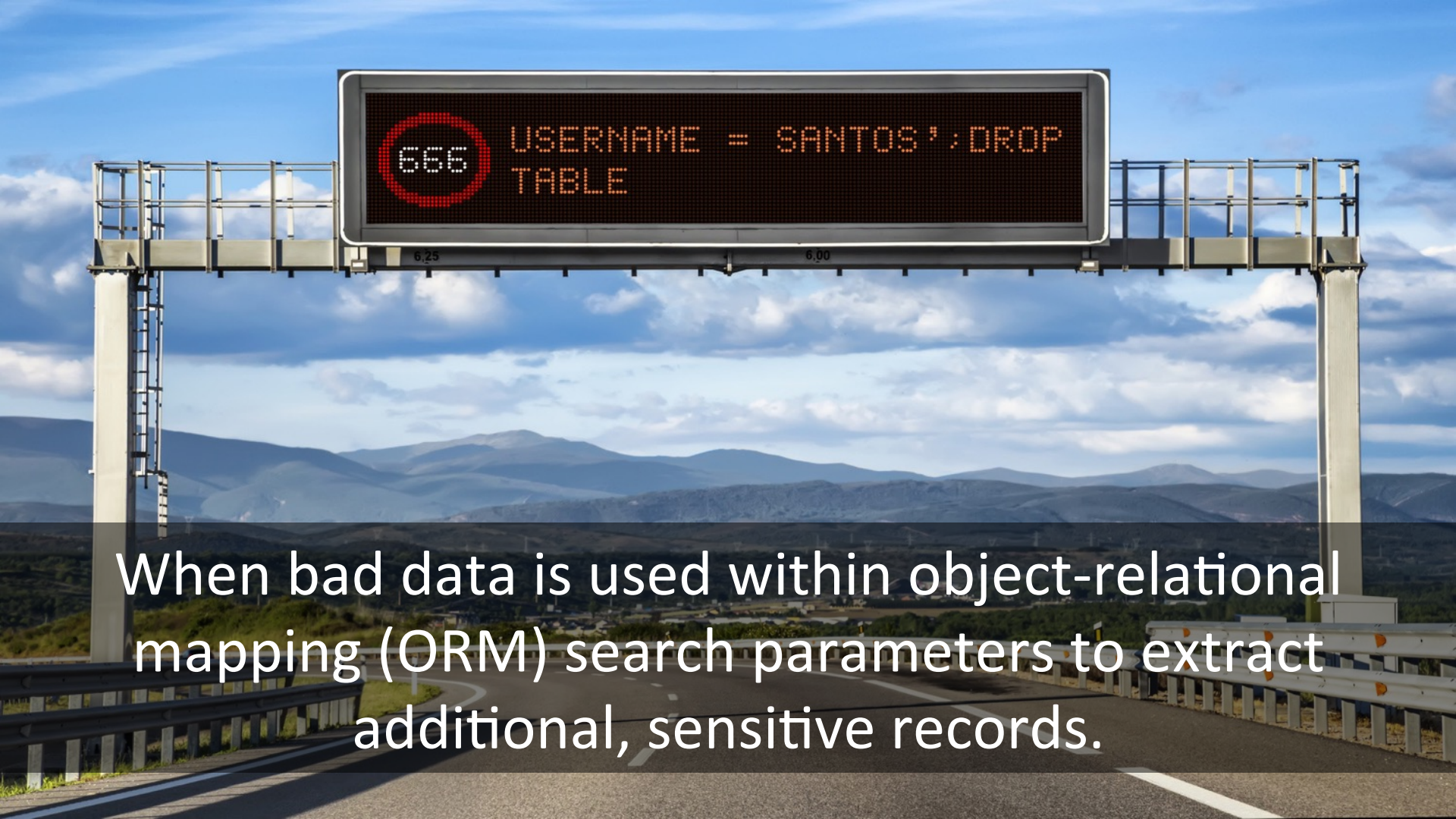


Source: OWASP

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

END OF DAY 1