Universidad del Rosario | Escuela de Ingeniería, Ciencia y Tecnología | MACC Matemáticas Aplicadas y Ciencias de la Computación | HINNT Hub de INNovación y Transferencia

Hacking Ético

Daniel Díaz-López

Líder de Ciberseguridad - MACC
Profesor principal de carrera

danielo.diaz@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur

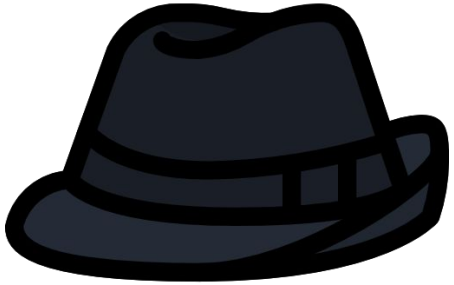
Agenda

i. ¿Qué es Hacking Ético?
ii. Tipos de hackers
iii. Tipos de pruebas
iv. Metodología de hacking: OSSTMM
v. Herramientas de Hacking: OWASP ZAP
vi. Software de aprendizaje: Mutillidae
vii. Caso de uso -> Replicar

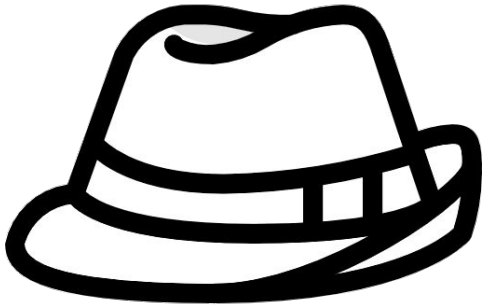
¿Qué es Hacking Ético?

Uso de conocimientos en informática y en seguridad de la información para encontrar **vulnerabilidades** en un sistema de información, con el objetivo de **reportarlas** a la organización propietaria de dicho sistema, para que se tomen las medidas necesarias que permitan **prevenir** un ataque a futuro.

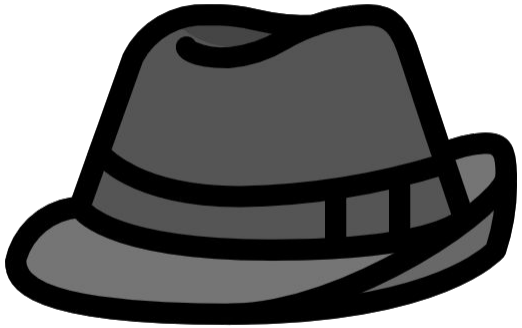
Tipos de hackers



Black hat

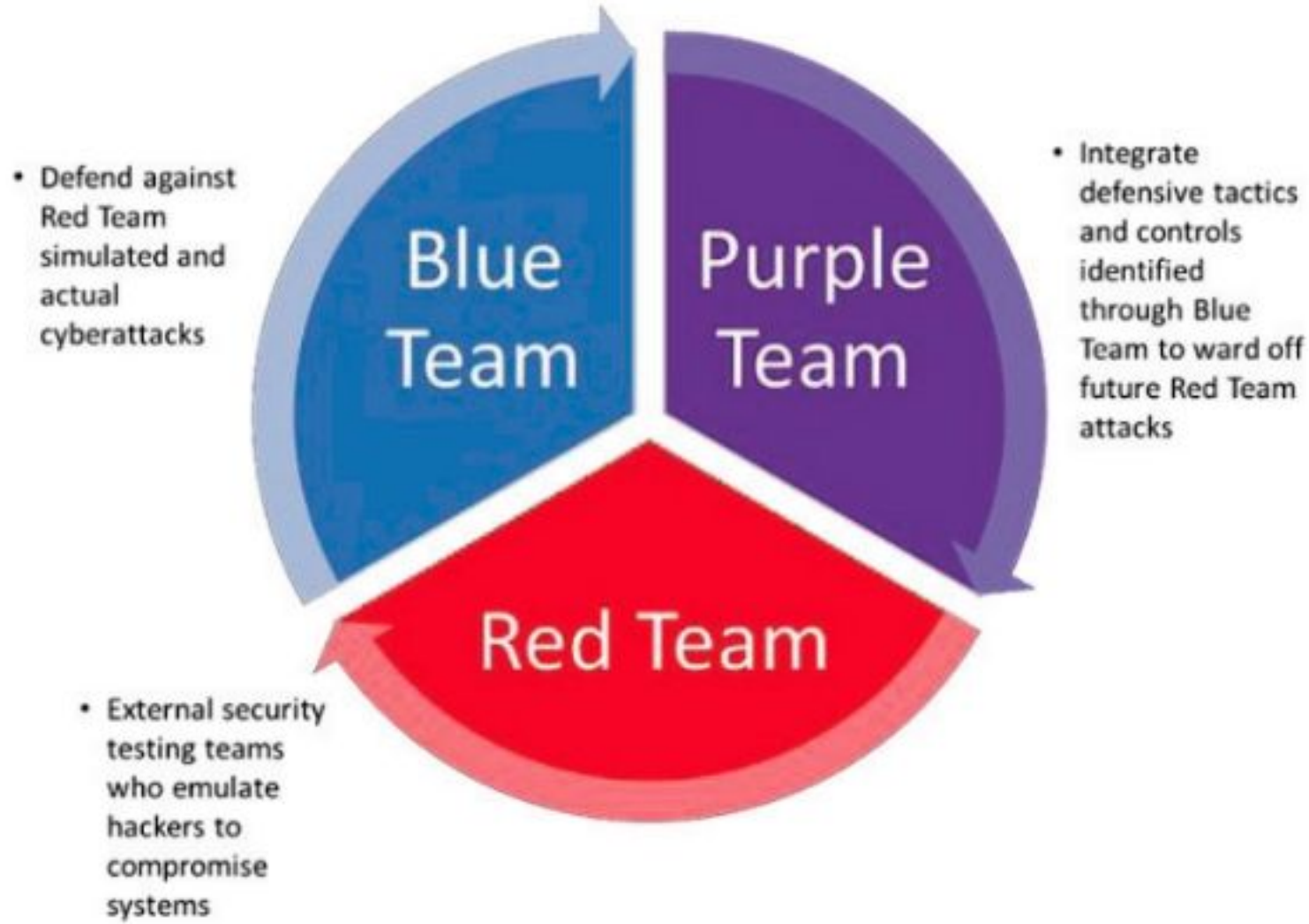


White hat

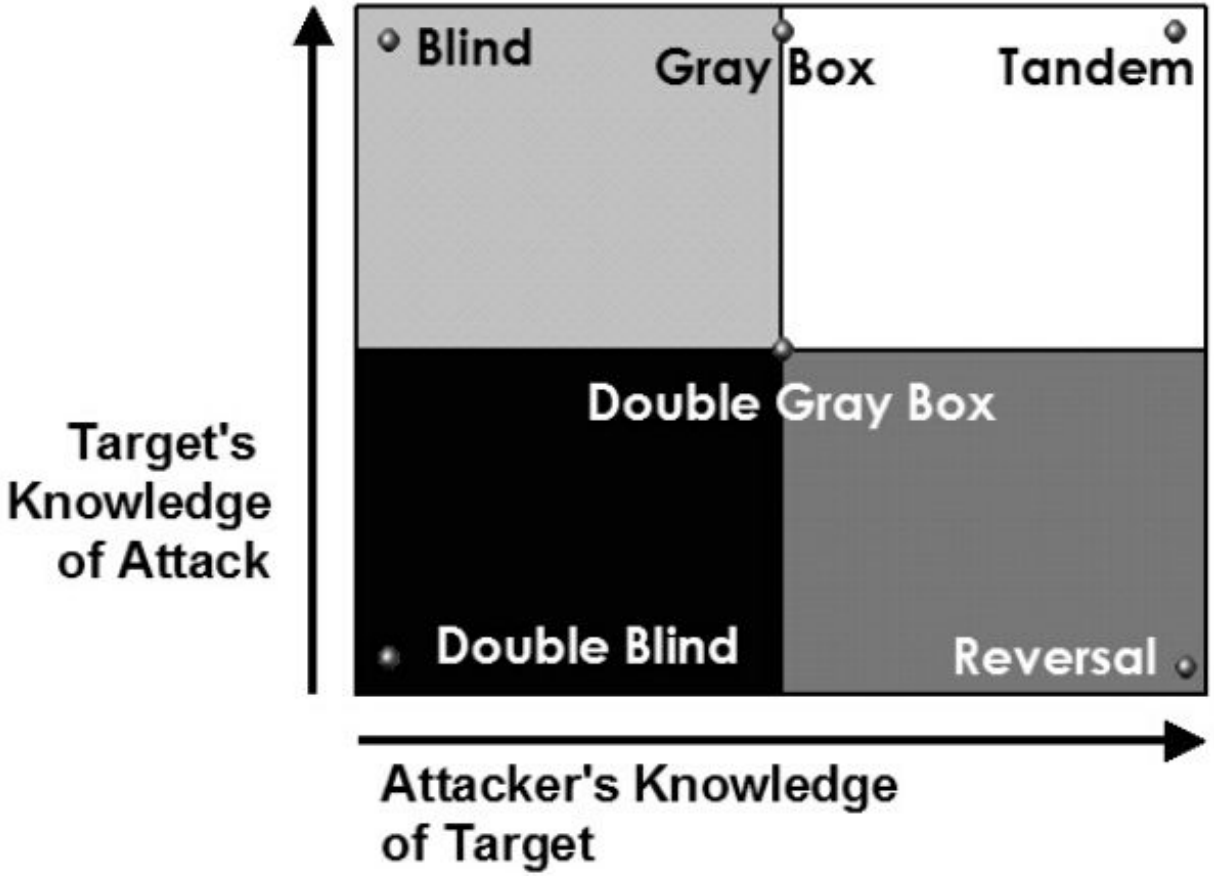


Gray hat

Security Testing Teams



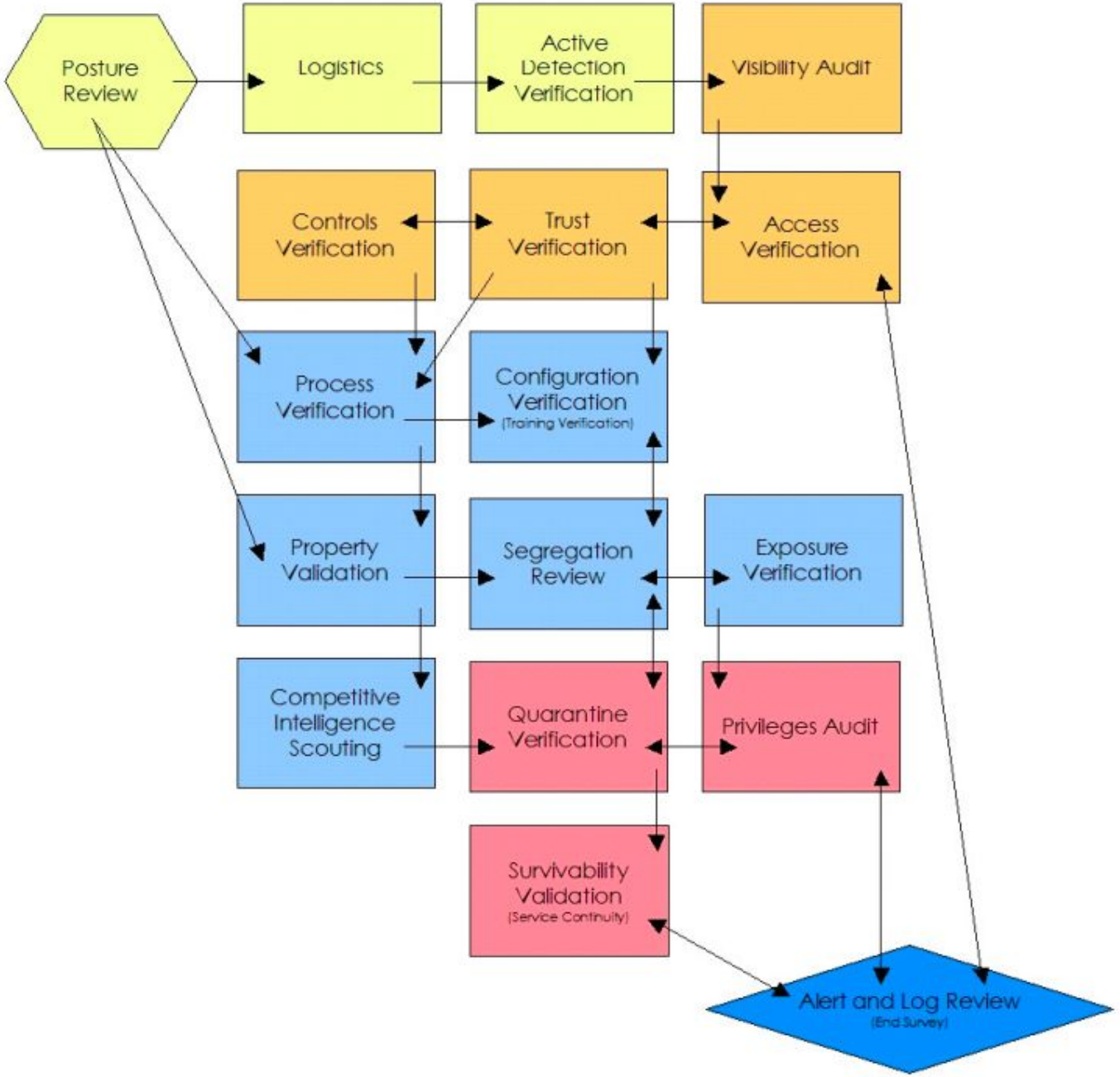
Tipos de pruebas



https://www.isecom.org/OSSTMM.3.pdf

Metodología de hacking

- OSSTMM (Open Source Security Testing Methodology Manual)



https://www.isecom.org/OSSTMM.3.pdf

HERRAMIENTAS DE HACKING

Information Gathering	Vulnerability Analysis	Wireless Attacks	Web Applications	Exploitation Tools
ace-voip Amap APT2 arp-scan Automater bing-ip2hosts braa CaseFile	BBQSQL BED cisco-auditing-tool cisco-global-exploiter cisco-ocs cisco-torch copy-router-config Doona	Airbase-ng Aircrack-ng Airdecap-ng and Airdecloak-ng Aireplay-ng airgraph-ng Airmon-ng Airodump-ng	apache-users Arachni BBQSQL BlindElephant Burp Suite CutyCapt DAVTest deblaze	Armitage Backdoor Factory BeEF cisco-auditing-tool cisco-global-exploiter cisco-ocs cisco-torch Commix

HERRAMIENTAS DE HACKING

Stress Testing	**Forensics Tools**	**Sniffing & Spoofing**	**Password Attacks**	**Maintaining Access**
DHCPig FunkLoad iaxflood Inundator inviteflood ipv6-toolkit mdk3	Binwalk bulk-extractor Capstone chntpw Cuckoo dc3dd ddrescue	bettercap Burp Suite DNSChef fiked hamster-sidejack HexInject iaxflood	BruteSpray Burp Suite CeWL chntpw cisco-auditing-tool CmosPwd creddump	CryptCat Cymothoa dbd dns2tcp HTTPTunnel Intersect Nishang

HERRAMIENTAS DE HACKING: ZAP

- Open Web Application Security Project (OWASP) es una comunidad sin ánimo de lucro que ayuda a las organizaciones a desarrollar y mantener aplicaciones seguras.

- Todo el contenido de OWASP es gratuito, abierto y sin sesgo comercial.

https://www.owasp.org

- Dentro de los contenidos disponibles en OWASP se encuentran:
  - ❑ Herramientas de seguridad
  - ❑ Documentos (Guías, estándares)
  - ❑ Librerías de código

- Igualmente, hay diferentes espacios para compartir conocimiento con la comunidad:
  - ❑ Capítulos locales: Bogotá, Lima, Quito, Sao Paulo, Ciudad de Panamá, etc
  - ❑ Conferencias: OWASP Latam Tour
  - ❑ Listas de correo

- Uno de los proyectos más populares de OWASP: ZAP
  - ❑ https://owasp.org/www-project-zap/

ZAP:

- Series of short form videos featuring Simon Bennetts, project lead of the OWASP Zed Attack Proxy (ZAP) project: https://www.alldaydevops.com/zap-in-ten
- Introducción a la API de Zap: https://www.zaproxy.org/docs/api/#introduction
- Coursera project: https://www.coursera.org/learn/web-application-security-testing-with-owsap-zap
- Instalación de multillidae https://github.com/webpwnized/mutillidae

SOFTWARE DE APRENDIZAJE: MUTILLIDAE

- Tiene más de 40 vulnerabilidades y desafíos.
- Contiene al menos una vulnerabilidad por cada categoría incluida en el OWASP Top Ten 2017.
- Actually Vulnerable (User not asked to enter “magic” statement)
- Mutillidae can be installed on Linux or Windows *AMP stacks making it easy for users who do not want to install or administrate their own webserver. Mutillidae is confirmed to work on XAMPP, WAMP, and LAMP.
- Preinstalled on Rapid7 Metasploitable 2, Samurai Web Testing Framework (WTF), and OWASP Broken Web Apps (BWA)
- System can be restored to default with single-click of "Setup" button
- Dos modos de operación: Seguro e inseguro
- Utilizado en educación a nivel universitario y corporativo
- Utilizado para probar la software de detección de vulnerabilidades
- Actualizado frecuentemente

Laboratorio

Laboratorio: Escaneo y explotación de vulnerabilidades

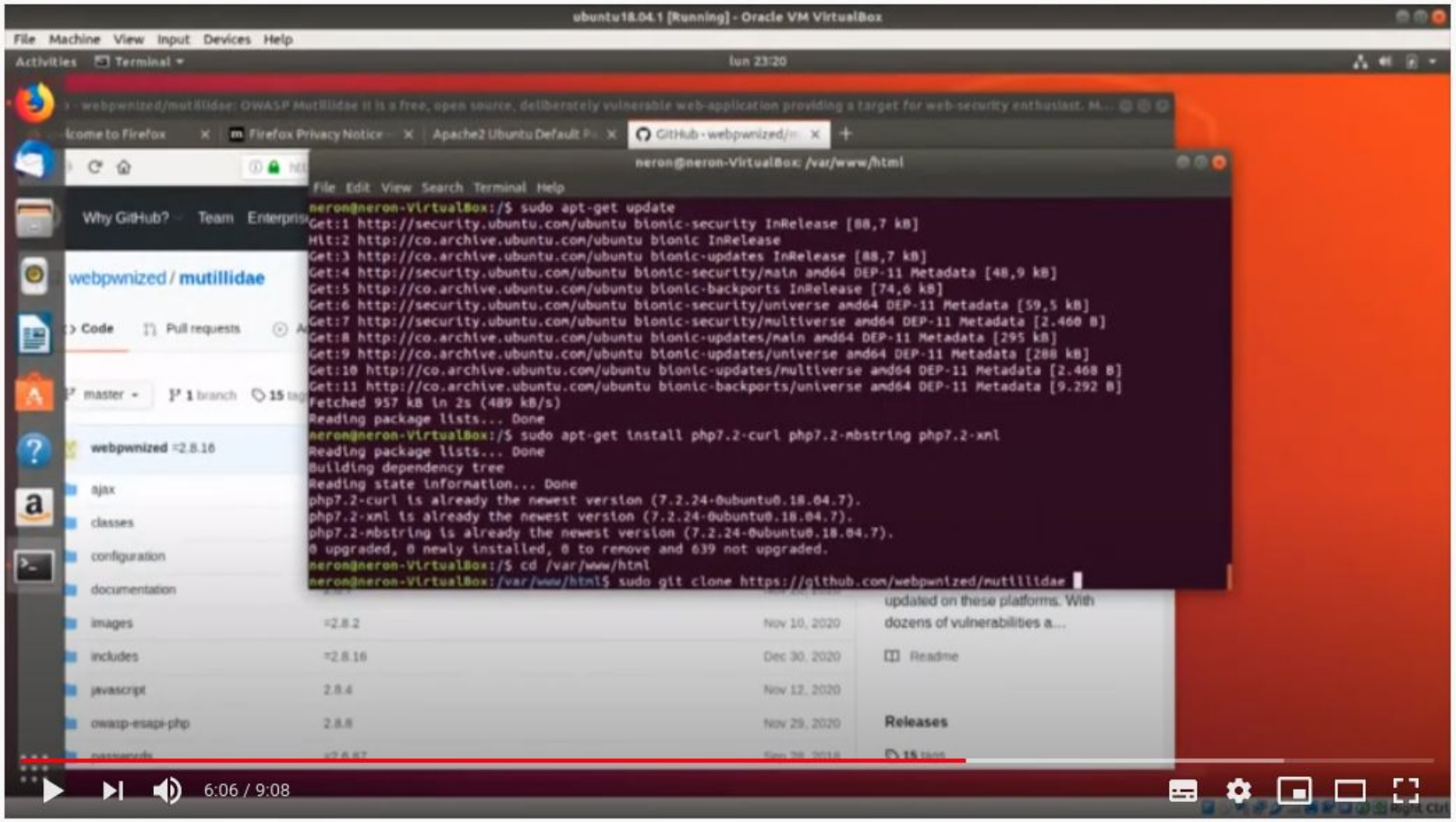
1. Instalar e Iniciar Mutillidae
2. Instalar e Iniciar ZAP
3. Primer ataque: Realización de un primer escaneo de vulnerabilidades usando ZAP y Mutillidae
4. Análisis de resultados (identificación de impactos): High, Medium and Low priority alerts
5. Explotación de una de las vulnerabilidades (SQL Injection)
6. Informe: Propuesta de medida de corrección

Otro ataque (Interceptación de http requests): Opcional!

1. Configuración de un proxy usando Foxyproxy para interceptar tráfico web
2. Encontrar archivos y fólderes de un web server con “Forced Browse Directory”

Laboratorio: Escaneo y explotación de vulnerabilidades

1. Realizar la instalación de Mutillidae en una máquina virtual (Esta será nuestra máquina víctima)



S3SB6C1 06PN Lab1 Instalación multillidae

https://www.youtube.com/watch?v=BgvTBN6lElM

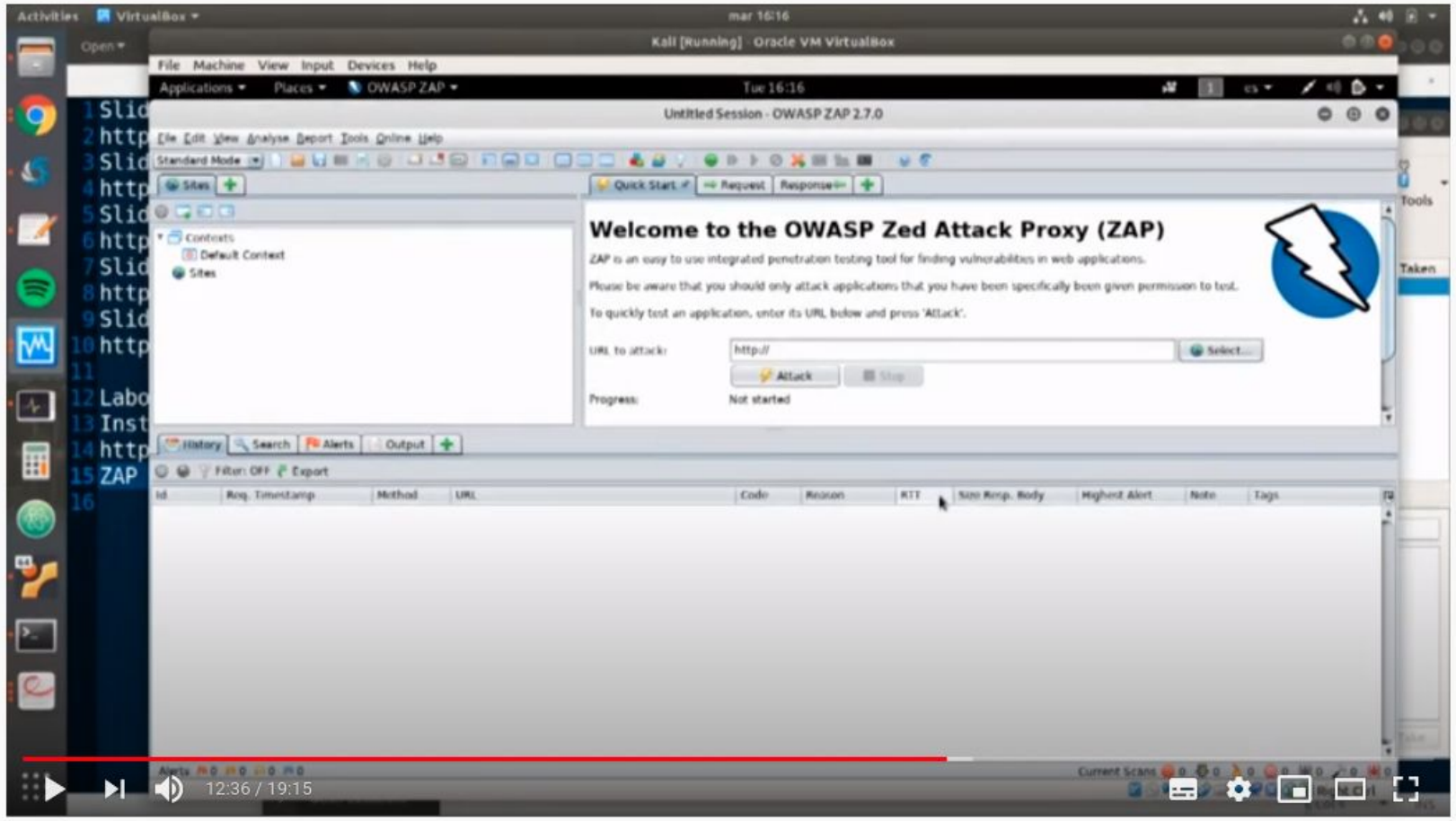
En este paso puede descargar la siguiente Máquina Virtual que ya trae mutillidae instalado:

https://uredu-my.sharepoint.com/:u:/g/personal/danielo_diaz_urosario_edu_co/EZ05pMwLf2REiK4V7I8EyacBLrLij1kypXEn0HgtSoM-uQ?e=gew0gW

Tambien puede validar que el sha256sum de la máquina descargada sea el correcto:
61681fdbbacfe558ddda51b4d5c25a6feacc2600065466d9ecce1194a85dfe81

Laboratorio: Escaneo y explotación de vulnerabilidades

2. Iniciar la máquina virtual de Kali Linux y la herramienta ZAP (Esta será nuestra máquina atacante)



S3SB6C2 07PN Lab2 Herramienta

https://www.youtube.com/watch?v=kJqXeA8HZvw

Usar el siguiente link de descarga a la versión **2021.4a** de Kali linux, en lugar del link de descarga indicado en el video:

http://old.kali.org/virtual-images/kali-2021.4a/kali-linux-2021.4a-virtualbox-amd64.ova

Usar las siguientes credenciales para acceder a la máquina virtual:

- User: kali
- Pwd: kali

Laboratorio: Escaneo y explotación de vulnerabilidades

2. Iniciar la máquina virtual de Kali Linux y la herramienta ZAP (Esta será nuestra máquina atacante)

ZAP no está incluido por default en las últimas versiones de kali linux, por ejemplo la 2021.4a, por ello se debe instalar con el siguiente comando: **sudo apt install zaproxy**

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zaproxy

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  zaproxy
0 upgraded, 1 newly installed, 0 to remove and 377 not upgraded.
Need to get 185 MB of archives.
After this operation, 232 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.11.1-0k
ali1 [185 MB]
Fetched 185 MB in 49s (3,787 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 267880 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.11.1-0kali1_all.deb ...
Unpacking zaproxy (2.11.1-0kali1) ...
Setting up zaproxy (2.11.1-0kali1) ...
Processing triggers for kali-menu (2021.4.2) ...
```

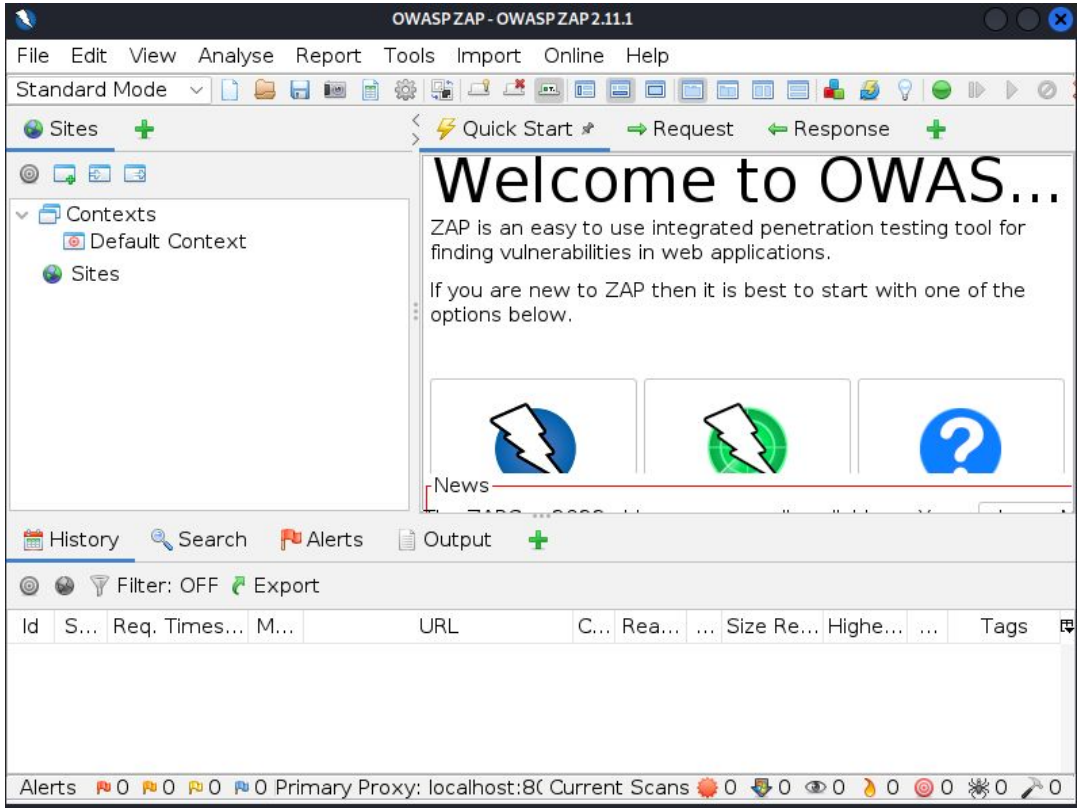
Mas información sobre el proceso de instalación: https://www.kali.org/tools/zaproxy/

Laboratorio: Escaneo y explotación de vulnerabilidades

2. Iniciar la máquina virtual de Kali Linux y la herramienta ZAP (Esta será nuestra máquina atacante)

Después de instalarse, ZAP puede iniciarse a través del siguiente comando: **zaproxy**

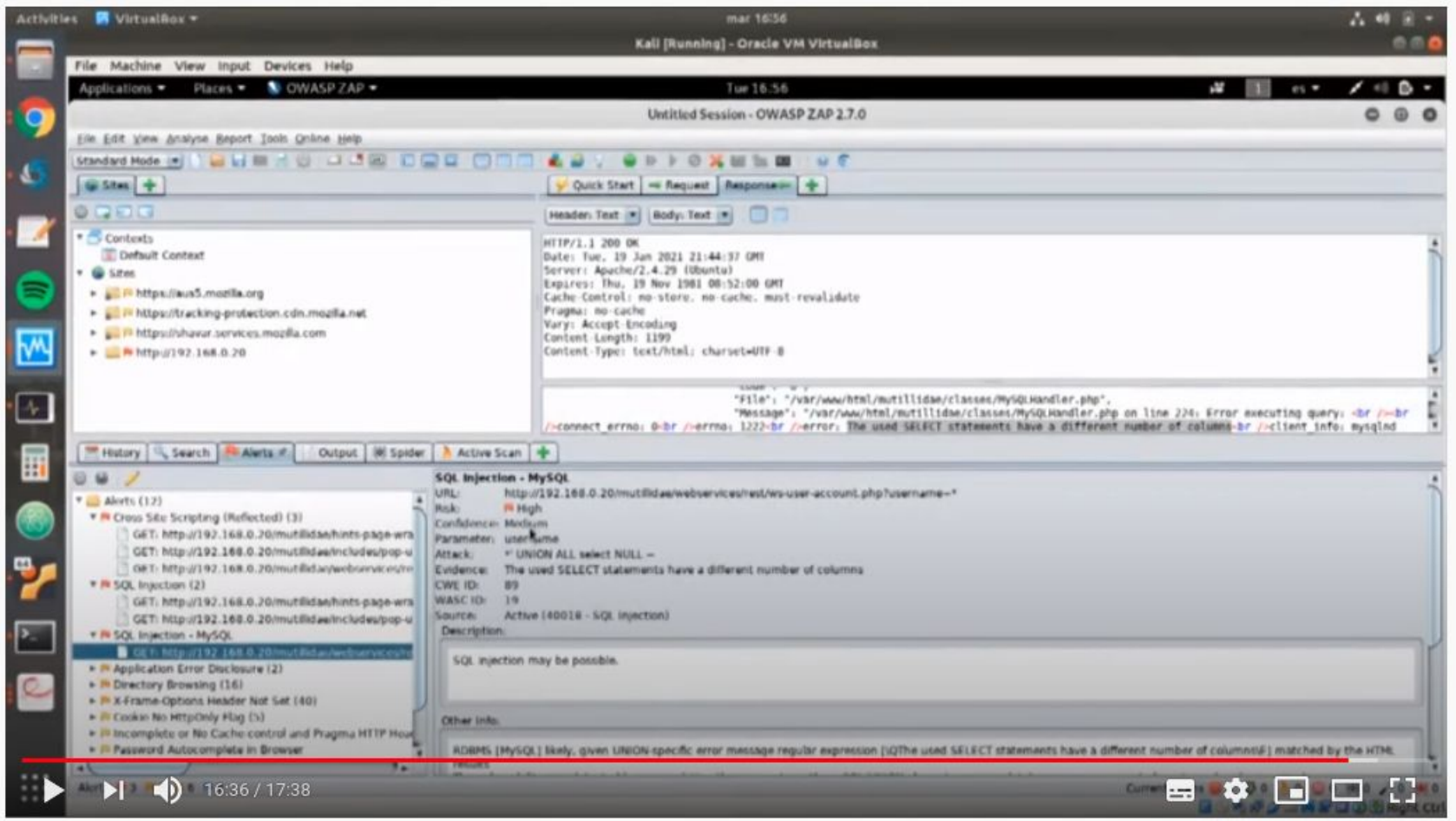
```
┌──(kali㉿kali)-[~]
└─$ zaproxy
Found Java version 11.0.13
Available memory: 1981 MB
Using JVM args: -Xmx495m
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
2371 [main] INFO  org.parosproxy.paros.Constant - Copying default configurati
on to /home/kali/.ZAP/config.xml
2853 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/ka
li/.ZAP/session
2854 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/ka
li/.ZAP/dirbuster
2854 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/ka
li/.ZAP/fuzzers
2854 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/ka
li/.ZAP/plugin
2968 [main] INFO  org.zaproxy.zap.GuiBootstrap - OWASP ZAP 2.11.1 started 23/
03/2022, 11:27:30 with home /home/kali/.ZAP/
```



Mas información sobre la instalación: https://www.kali.org/tools/zaproxy/

Laboratorio: Escaneo y explotación de vulnerabilidades

3. Realizar un escaneo de vulnerabilidades y explotar una de ellas

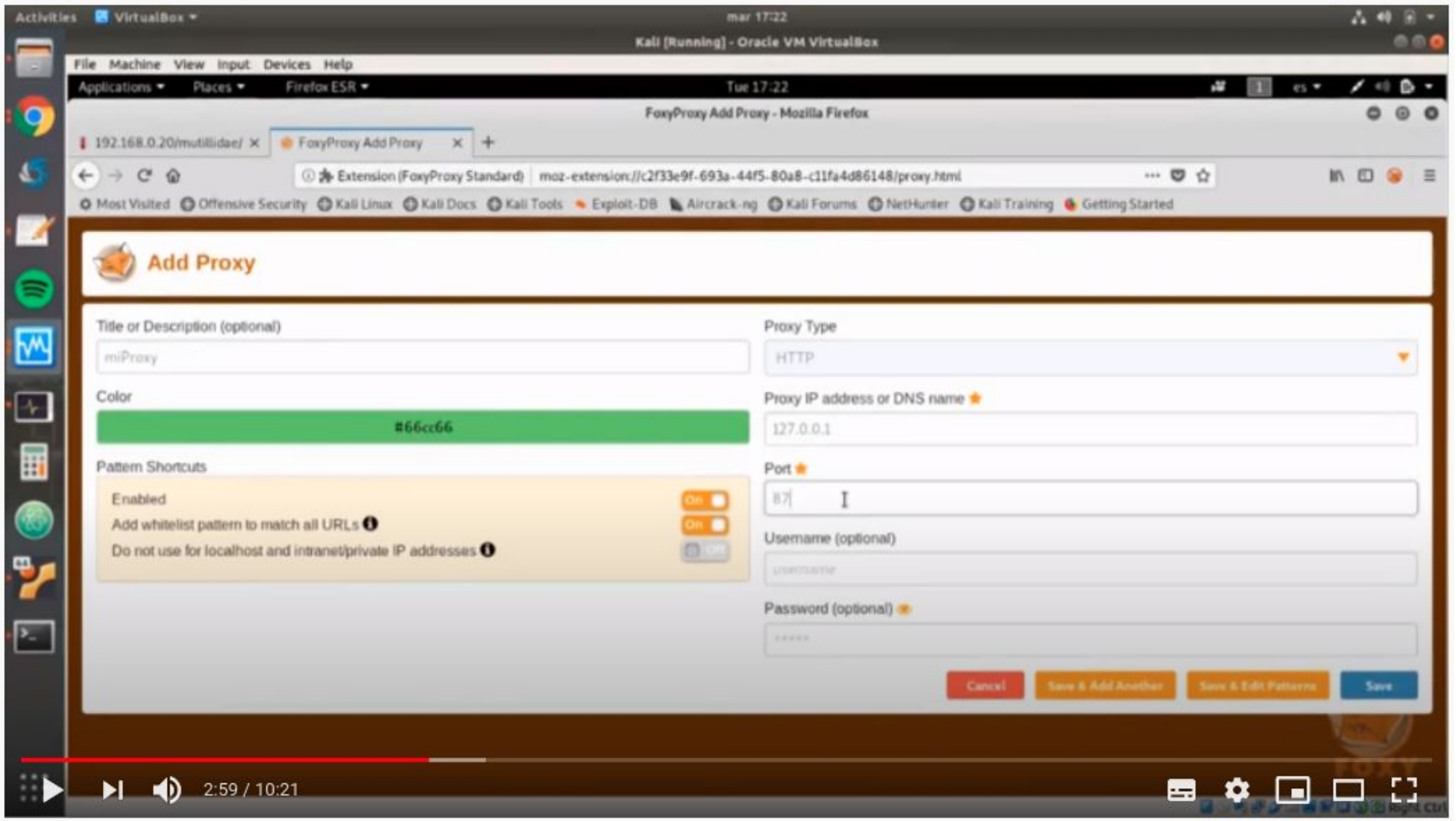


S3SB6C3 08PN Lab3 Escaneo y explotación

https://www.youtube.com/watch?v=3aseMHFKRuk

Laboratorio: Escaneo y explotación de vulnerabilidades

4. Interceptación de tráfico y descubrimiento de directorios



S3SB6C4 09PN Lab4 Interceptacion y force

https://www.youtube.com/watch?v=lB581FNxgAw

Hacking Ético - SQL Injection

Daniel Díaz-López

Líder de Ciberseguridad - MACC
Profesor principal de carrera

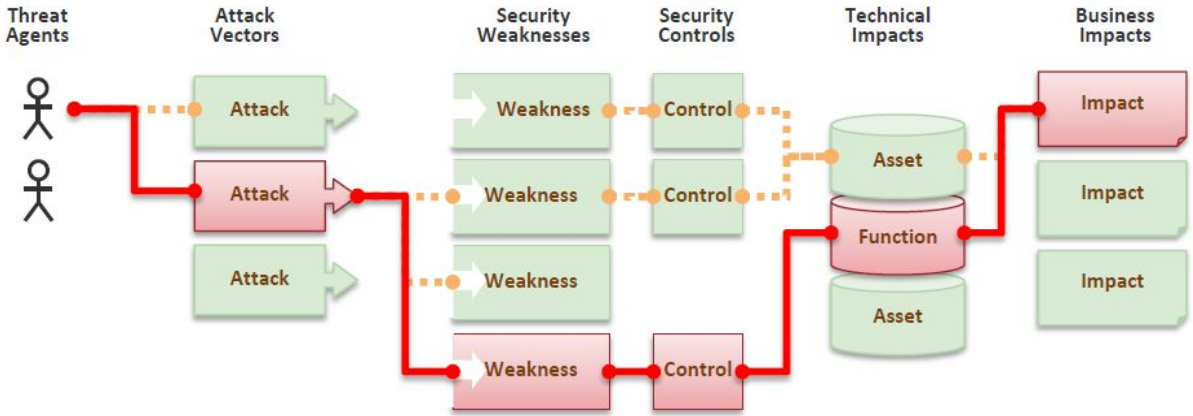
danielo.diaz@urosario.edu.co

Agenda

- ✔ What are application security risks?
- ✔ OWASP TOP10
  - ✔ Injection

What are application security risks?

What are application security risks?



- An attacker can use different paths to affect a business**: Each path is a risk**
- **One definition of risk:** *"When a threat agent materialize a threat (attack), which exploit a vulnerability (weakness) with certain probability, causing an impact (reputational, operational, legal)"*

Residual Risk = Probability_A * Impact_A

*A: It means **After** controls*

What are application security risks?

- These were the identified Risks for the Zion study case (Threat Modeling)

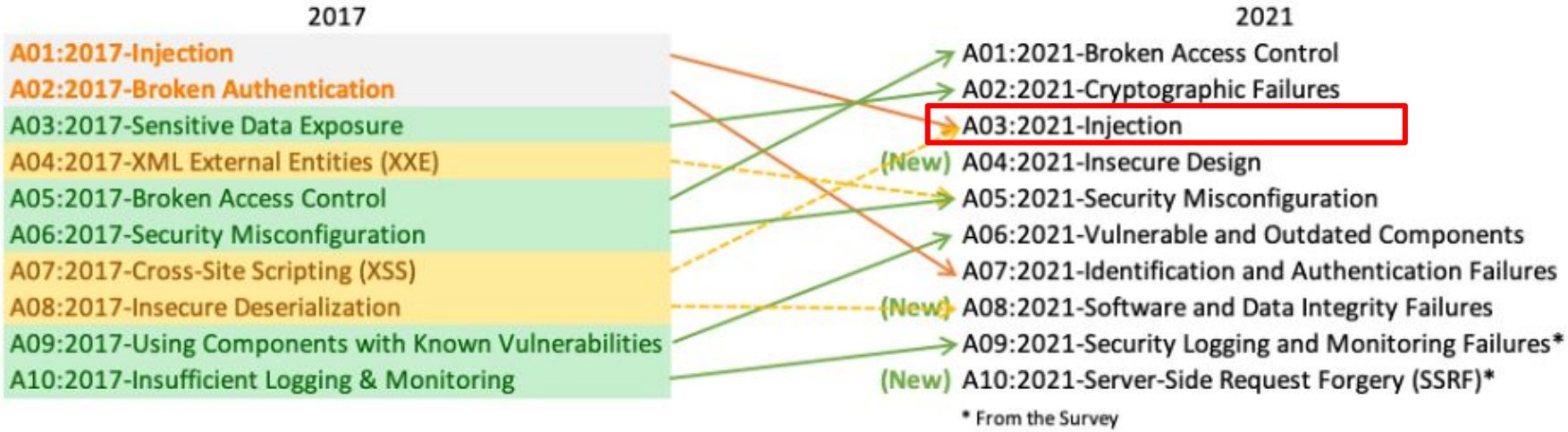
	Probability of Occurrence (P)			Business Impact (I)		P	I	Risk
Threat	**R**	**E**	**DI**	**D**	**A**	**(R+E+DI)**	**(D+A)**	**PxI**
SQL Injection	3	2	2	3	3	7	6	42
XSS	3	3	3	3	3	9	6	54
Cookie Replay	2	2	2	3	1	6	4	24
Session Hijacking	2	2	3	2	1	7	3	21
CSRF	1	1	1	3	1	3	4	12
Verbose Exception	1	2	1	2	3	4	5	20
Brute Forcing	1	1	2	2	3	4	5	20
Eavesdropping	1	2	2	2	3	5	5	25
Insecure Backup	1	2	2	1	1	5	2	10
Audit Log Deletion	0	0	3	1	1	3	2	06
Output Caching	3	2	3	3	3	8	6	48
Website Defacement	2	1	2	3	3	5	6	30
Logic Flaws	1	1	1	1	2	3	3	06

High: 41 to 60; Medium: 21 to 40; Low: 0 to 20

Table C.3 – **P x I ranking**

OWASP TOP 10

El proyecto OWASP TOP 10 agrupa las 10 vulnerabilidades más comunes en servicios web y su versión más reciente es la 2021.

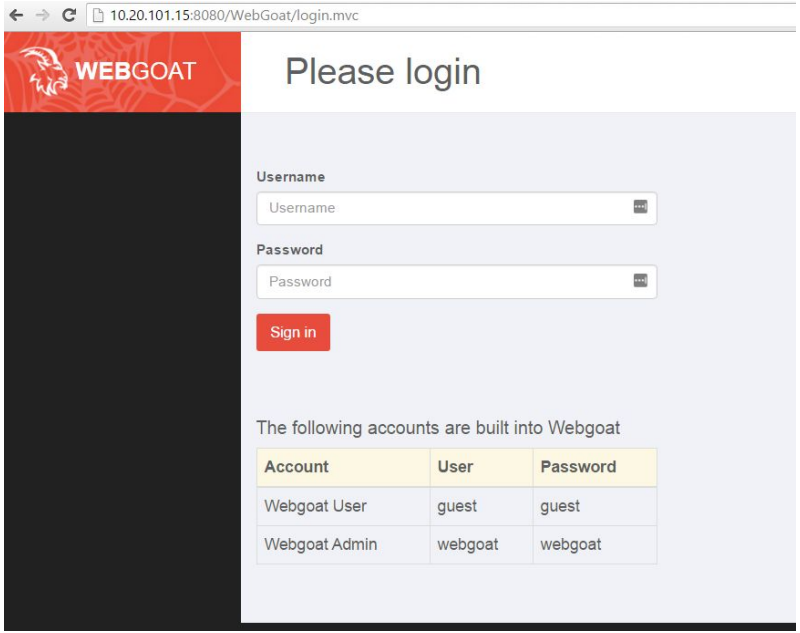


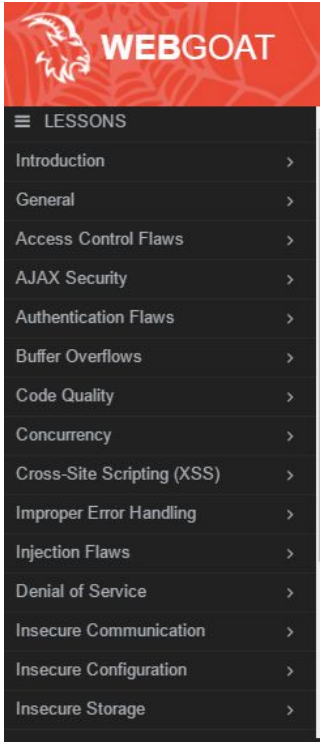
https://owasp.org/Top10/A03_2021-Injection/

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

WebGoat

- **WebGoat:** Deliberately insecure web application for interactive teaching of web application security

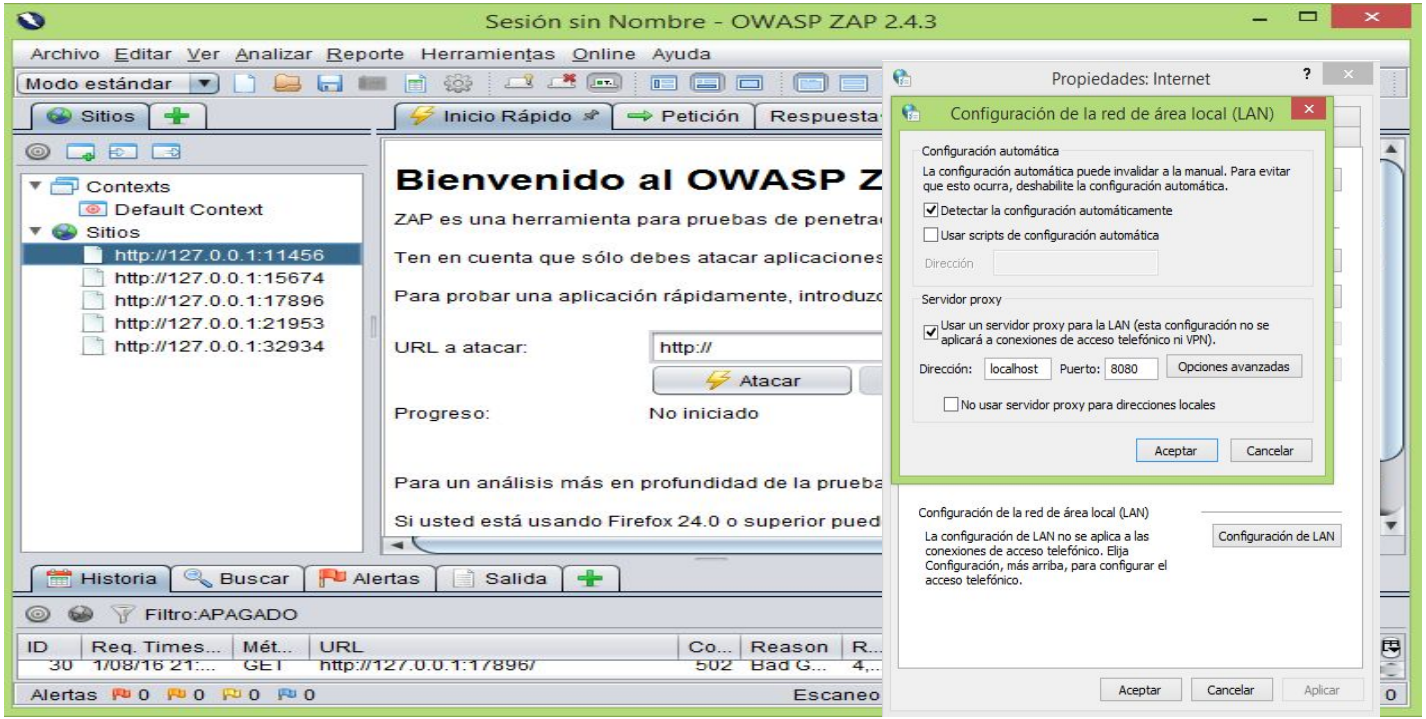




https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
https://github.com/WebGoat/WebGoat/tree/7.1

ZAP

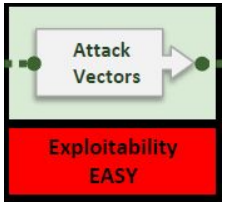
- **Zed Attack Proxy (ZAP):** Software de interceptación de comunicaciones



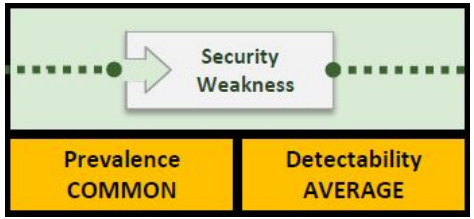
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Injection

INJECTION



- ¿Como? El intruso envía ataques basados en **texto** que explotan la sintaxis del interpreter de la aplicación. Casi cualquier fuente de datos (incluidas las internas) puede ser un vector de ataque.



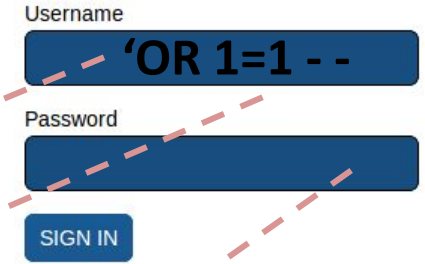
- ¿Por qué? Ocurre cuando los datos que provee el usuario no son validados antes de ser procesados por el interpreter. Pueden existir en código SQL, LDAP, XPATH, OS Commands, XML parsers, SMTP Headers, argumentos de programa, etc.

- Impacto: Pérdida de datos, modificación de datos, ejecución de actividades por fuera de logs, denegación de servicio

INJECTION

SQL INJECTION

- It is the most well-known form of injection
- The business databases are the main target
- The problem is that a database query is built with **user input** which is NOT sanitized or validated



string sSQLQuery = " SELECT * FROM USERS WHERE user_id = ' ' +
txtUserID.Text + " ' AND user_password = ' ' + **txtPassword.Text** + " '

string sSQLQuery = " SELECT * FROM USERS WHERE user_id = ' ' +
'OR 1=1 - - + " ' AND user_password = ' ' + txtPassword.Text + " '

SELECT * FROM USERS WHERE user_id = ' ' OR 1=1 - -

Everything after the -- in SQL is ignored

INJECTION

SQL INJECTION

Attack methodology:

1. Use **SQL commands that cause error** to force the database to respond with messages that **disclose internal database structure** (The Query structure)
2. Discover the **SQL query**
3. Inject a SQL command to achieve **modify, add, retrieve or delete** data from the database

Which can be the solution? → Suppressing database error messages!

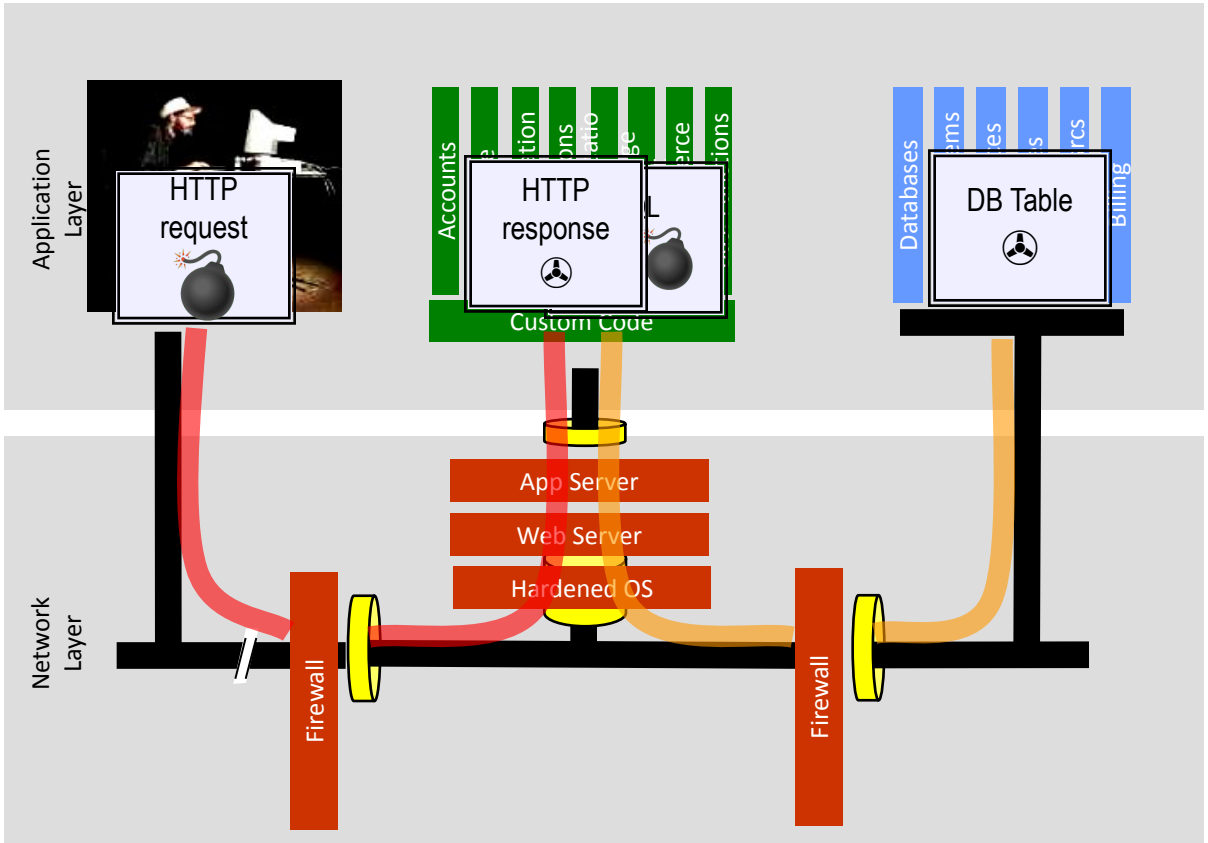
Not enough…

Blind SQL injection:

- Simple boolean SQL expression (true/false)
- Use the **response time** to determine if the result was TRUE or FALSE

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

SQL Injection – Illustrated



1. Application presents a form to the attacker
2. Attacker sends an attack in the form data
3. Application forwards attack to the database in a SQL query
4. Database runs query containing attack and sends encrypted results back to application
5. Application decrypts data as normal and sends results to the user

Injection means…

- Tricking an application into including unintended commands in the data sent to an interpreter

Interpreters…

- Take strings and interpret them as commands
- SQL, OS Shell, LDAP, XPath, Hibernate, etc…

SQL injection is still quite common

- Many applications still susceptible
- Even though it's usually very simple to avoid

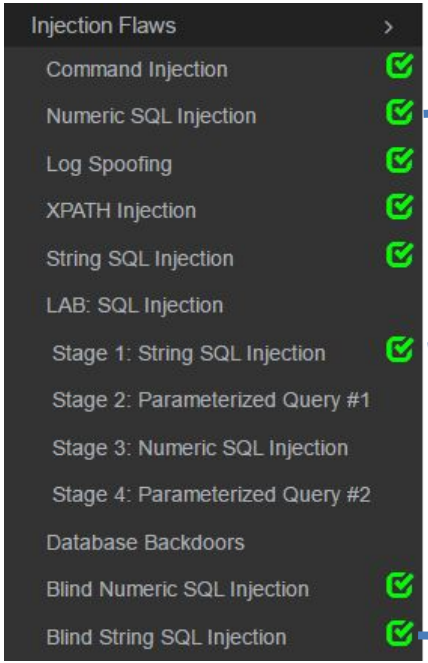
Typical Impact

- Usually severe. Entire database can usually be read or modified
- May also allow full database schema, or account access, or even OS level access

SQL Injection Laboratory

INJECTION

- **<u>Laboratory</u>**:



Do **Numeric SQL Injection** Lesson in your webgoat
https://www.youtube.com/watch?v=E_TPEcssMdU

Do **String SQL Injection** Lesson in your webgoat
https://www.youtube.com/watch?v=pt9nVSLy3Nk

Do **Blind Numeric SQL Injection** Lesson in your webgoat
https://www.youtube.com/watch?v=ffm73WEoup0

Do **Blind String SQL Injection** Lesson in your webgoat
https://www.youtube.com/watch?v=Lfo4hHS4yP8

GRACIAS

Daniel Díaz-López

Líder de Ciberseguridad - MACC
Profesor principal de carrera

danielo.diaz@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur