Universidad del Rosario

MACC
Matemáticas Aplicadas y Ciencias de la Computación

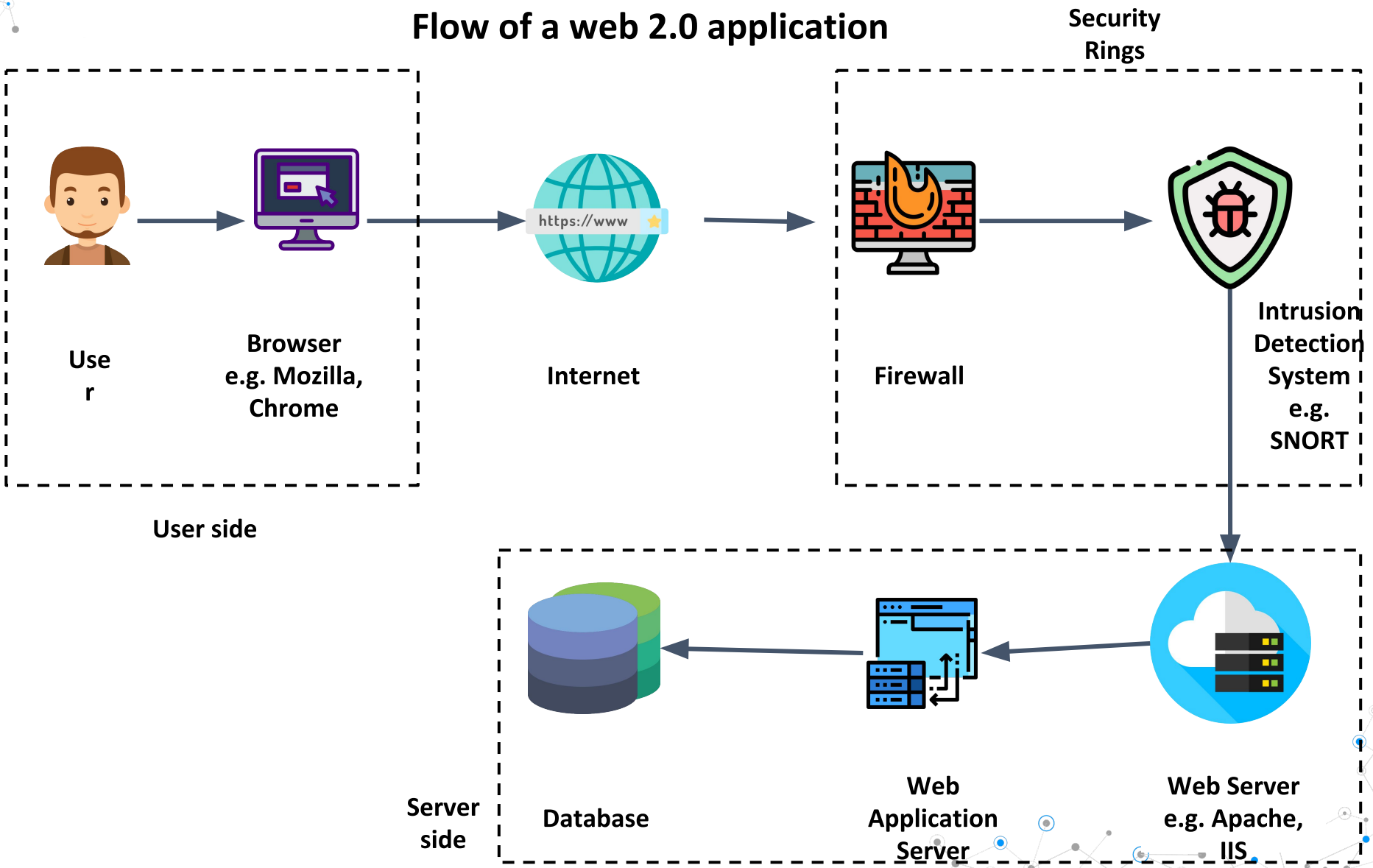
Hacking Web Applications

Hacking Ético

Daniel Orlando Díaz López, PhD

Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co

Flow of a web 2.0 application



Web 1.0

Sitios web con las siguientes características:

- Unidireccional (el usuario ve el contenido de manera pasiva)
- Mayoritariamente consumidores de contenido
- Páginas estáticas (HTML estático)
- Contenido desplegado desde un sistema de archivos local en lugar de una base de datos
- Uso de SSI o CGI (Common Gateway Interface)

Web 2.0

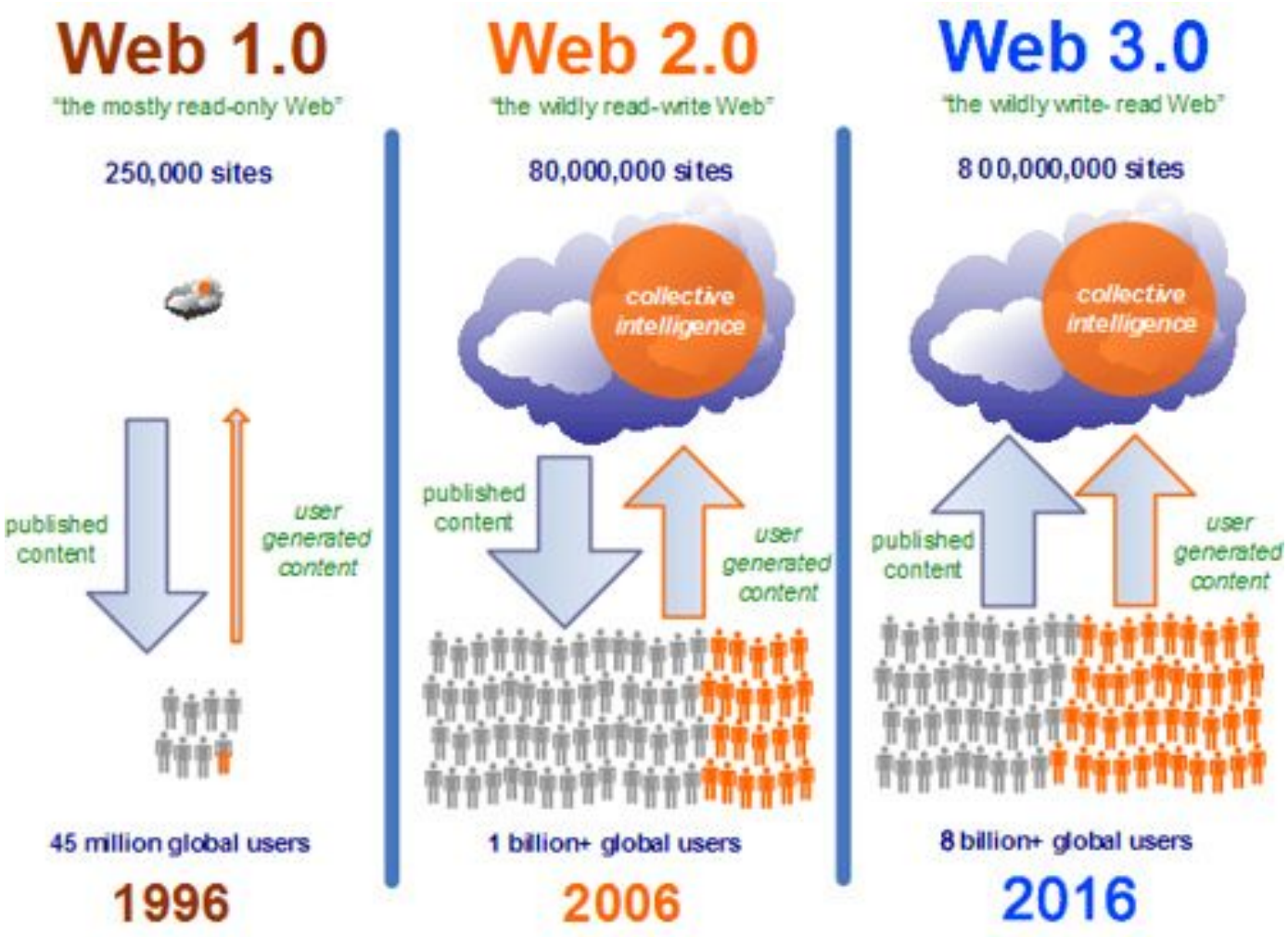
Sitios web con las siguientes características:

- Participativo
- Contenido generado por el usuario
- Cultura participativa
- Interoperabilidad
- Uso de lenguajes de programación dinámicos (PHP, Perl, Python, Ruby)

Hacking Web Applications

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Web 1.0	Web 2.0
Banner ads on websites	Automatic text, image, video, and interactive media advertisements, that are targeted to website content and audience
Ofoto, an online digital photography website, on which users could store, share, view and print digital photos	Flickr, an image hosting and video hosting website and web services suite
content delivery networks (CDN)	BitTorrent and eMule, communications protocols of peer-to-peer file sharing (P2P) which is used to distribute data and electronic files over the Internet
mp3.com, a website providing information about digital music and artists, songs, services, community, and technologies and a legal, free music-sharing service	Napster, a pioneering peer-to-peer (P2P) file sharing Internet service that emphasized sharing digital audio files, typically songs, encoded in MP3 format
Britannica Online, written by professionals and experts	Wikipedia, can be written and edited by any person, even amateurs and non-experts
personal websites	blogging
evite	upcoming.org and EVDB
domain name speculation	search engine optimization (SEO)
page views	cost per click
"screen scraping"	web services
publishing of online documents, once approved by gatekeepers and editorial staff	mass user participation, without approval of content by gatekeepers or editorial staff
content management systems	wikis that allow almost any users to contribute
directories (taxonomy)	"tagging" of websites, images and videos (folksonomy)
"stickiness"	syndication


Web 1.0
"the mostly read-only Web"
250,000 sites
published content
user generated content
45 million global users
1996
Web 2.0
"the wildly read-write Web"
80,000,000 sites
collective intelligence
published content
user generated content
1 billion+ global users
2006
Web 3.0
"the wildly write- read Web"
800,000,000 sites
collective intelligence
published content
user generated content
8 billion+ global users
2016

Web 1.0	Web 2.0	Web 3.0
The Web	The Social Web	The Semantic Web
Read-only Web	Read and Write Web	Read, Write and Execute Web
Information sharing	Interaction	Immersion
Connect Information	Connect People	Connect context, people and knowledge
All about static content (one-way interaction)	Two-way communication through social networking, blogging etc.	Visualization
Owning content	Sharing content	Consolidating content
Web Forms	Web Applications	Smart Applications
HTML Portals	XML/RSS	RDF/RDFS/OWL
Banner Advertising	Interactive advertising	Behavioral Advertising
Britannica Online	Wikipedia	Semantic Web

OWASP TOP 10

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- Open Web Application Security Project (OWASP) is a non-profit community which help organizations to develop and maintain secure application
- Everything is free, open and without commercial influence
- OWASP products:
  - ❑ Security tools
  - ❑ Documents, standards, books,
  - ❑ Local chapters
  - ❑ Conferences
  - ❑ Mailing lists

https://www.owasp.org

- One of the most popular products: **OWASP TOP 10**

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

OWASP
The Open Web Application Security Project

Laboratorio

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Realización de un ataque a una aplicación web a partir de una interceptación de tráfico

Laboratorio

1. Implementar un servidor de aplicaciones web vulnerable (WebGoat)
2. Instalar una herramienta de interceptación de tráfico (ZAP)
3. Realizar un ataque de inyección de código sobre el servidor víctima

Preguntas

1. Explique la forma de mitigar un ataque de inyección de código sobre una aplicación web

WebGoat

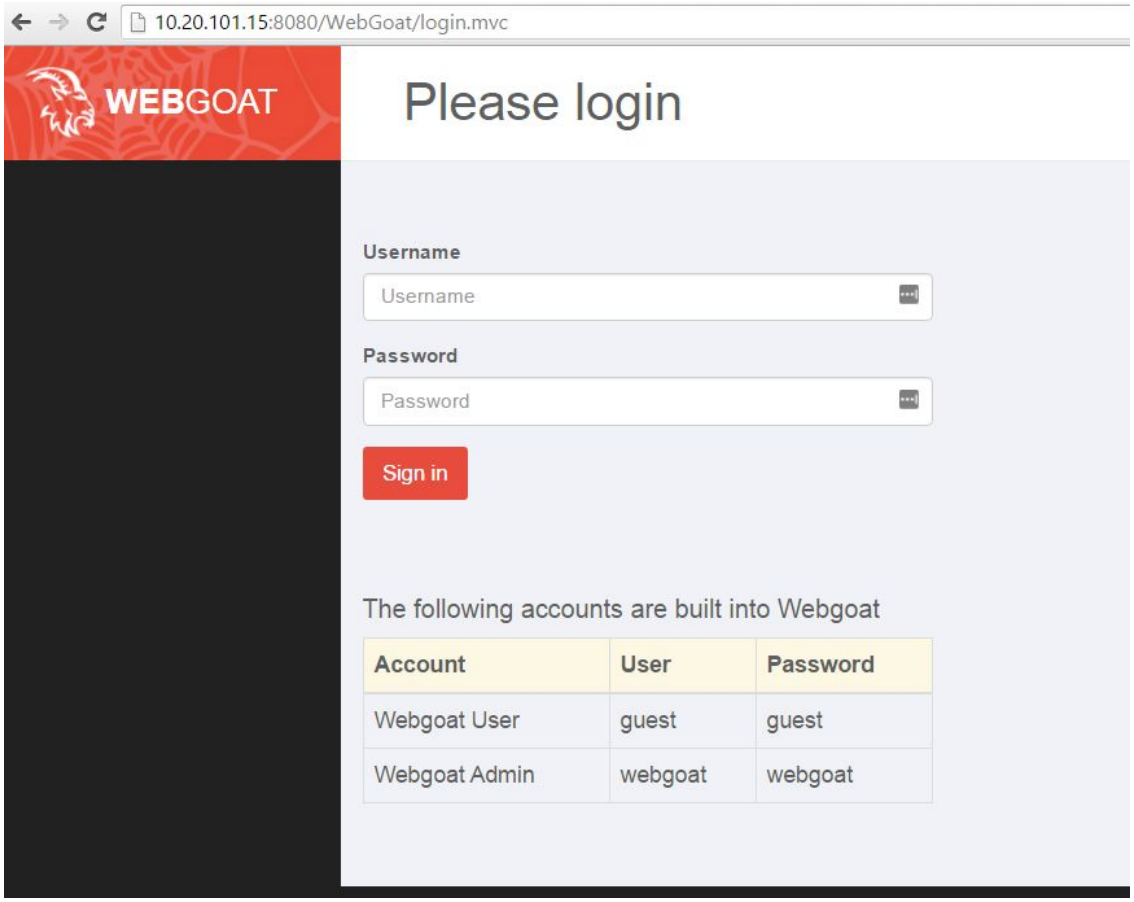
Universidad del Rosario

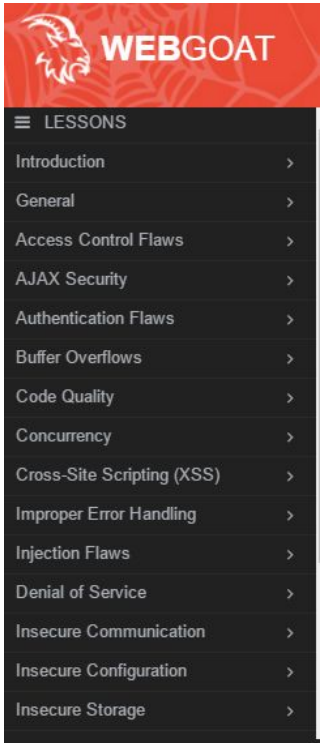
MACC
Matemáticas Aplicadas y Ciencias de la Computación

¡Instalemos un servidor web vulnerable!

Webgoat

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

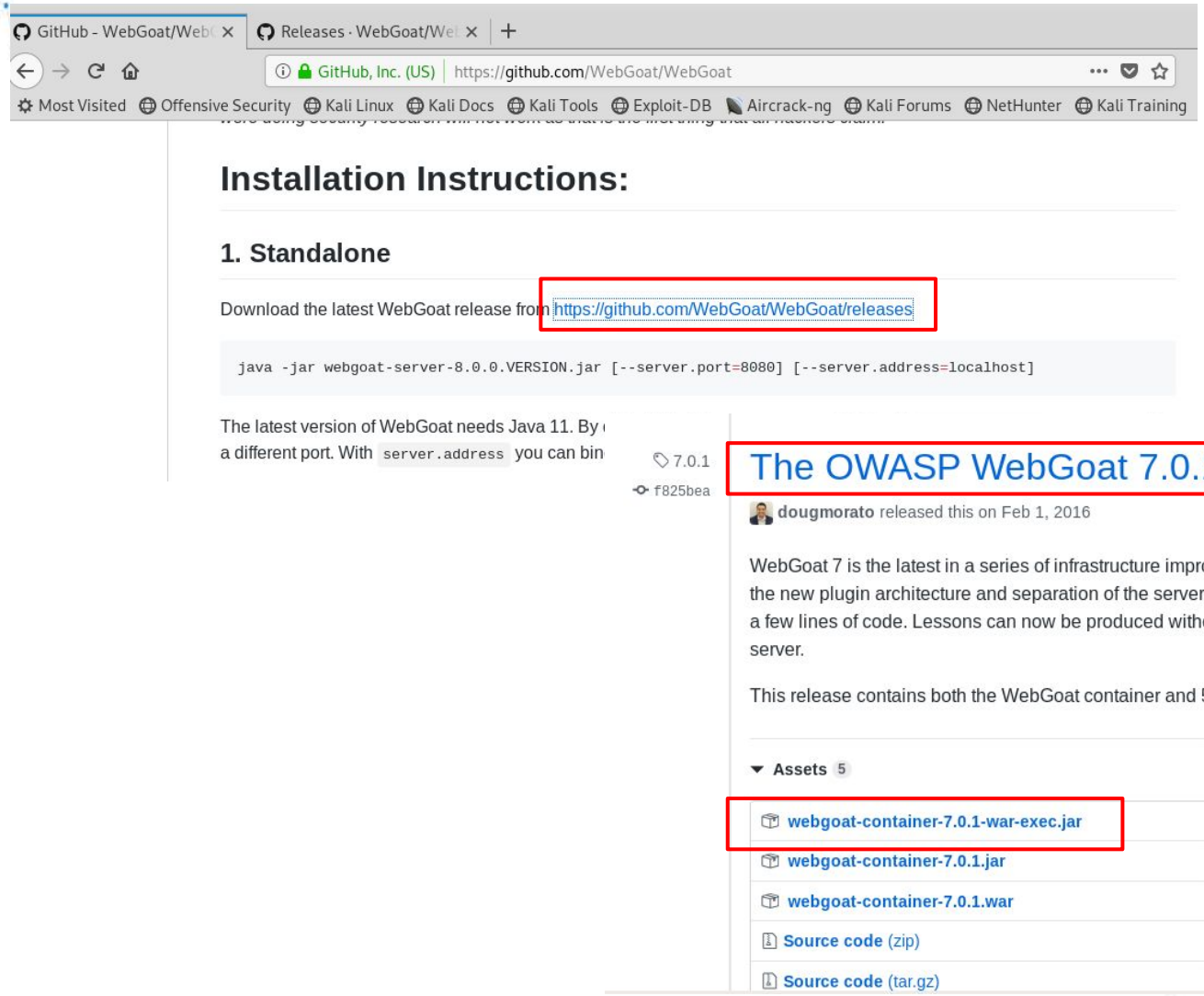




https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Webgoat

https://github.com/WebGoat/WebGoat
https://github.com/WebGoat/WebGoat/releases



Webgoat

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Seleccionar la versión de java a utilizar. En este caso seleccionar la versión Java 1.8.0 de la siguiente forma:

```
root@kali:~/Downloads# update-alternatives --install /usr/bin/java java /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java 1
root@kali:~/Downloads# update-alternatives --set java /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java
```

Validar que la versión de Java sea la correcta con el siguiente comando:

```
root@kali:~/Downloads# java -version
openjdk version "1.8.0_171"
OpenJDK Runtime Environment (build 1.8.0_171-8u171-b11-2-b11)
OpenJDK 64-Bit Server VM (build 25.171-b11, mixed mode)
```

Ejecutar Webgoat desde la ruta donde se haya descargado (en mi caso /root/Downloads)

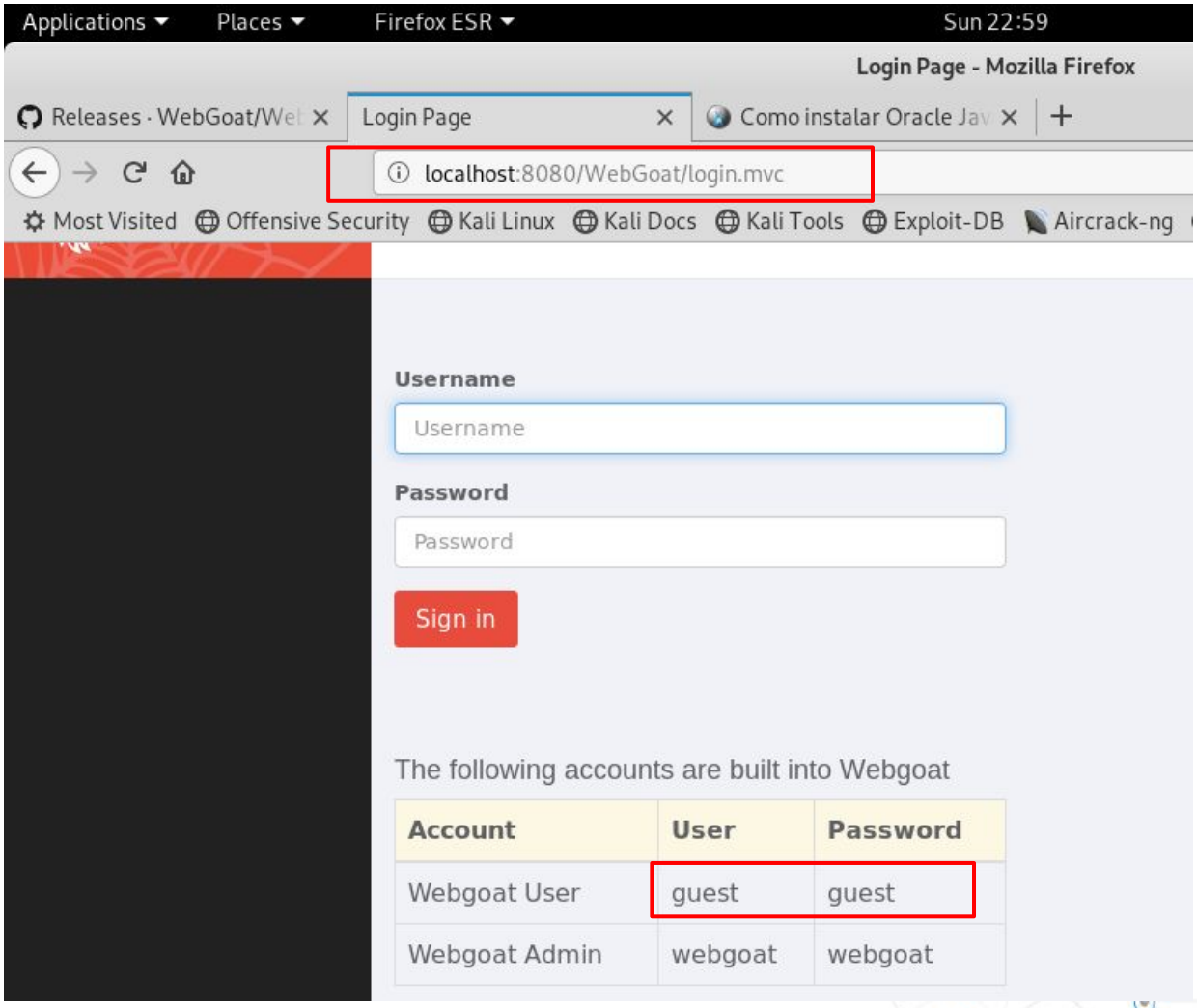
```
root@kali:~/Downloads# java -jar webgoat-container-7.0.1-war-exec.jar
```

```
2019-10-20 22:53:33,826 INFO  - FrameworkServlet 'mvc-dispatcher': initialization completed in 514 ms
2019-10-20 22:53:33,840 INFO  - Initializing main webgoat servlet
2019-10-20 22:53:33,845 INFO  - Browse to http://localhost:8080/WebGoat and happy hacking!
Oct 20, 2019 10:53:34 PM org.apache.coyote.http11.Http11Protocol start
INFO: Starting ProtocolHandler ["http-bio-8080"]
```

Webgoat

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

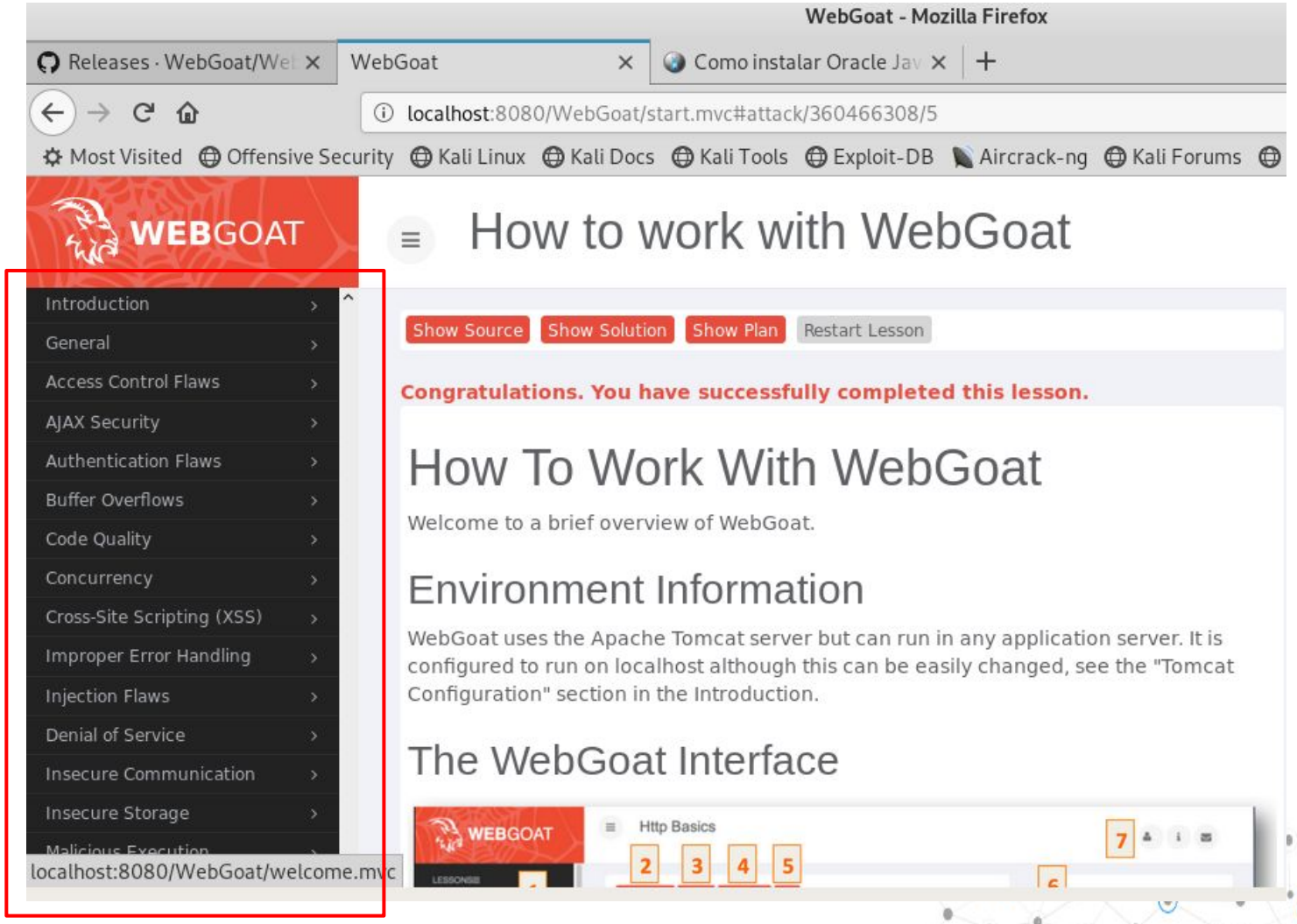
Acceder desde el navegador a la URL http://localhost:8080/WebGoat



Webgoat

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Autenticarse con las credenciales **guest/guest**



ZAP

Universidad del Rosario

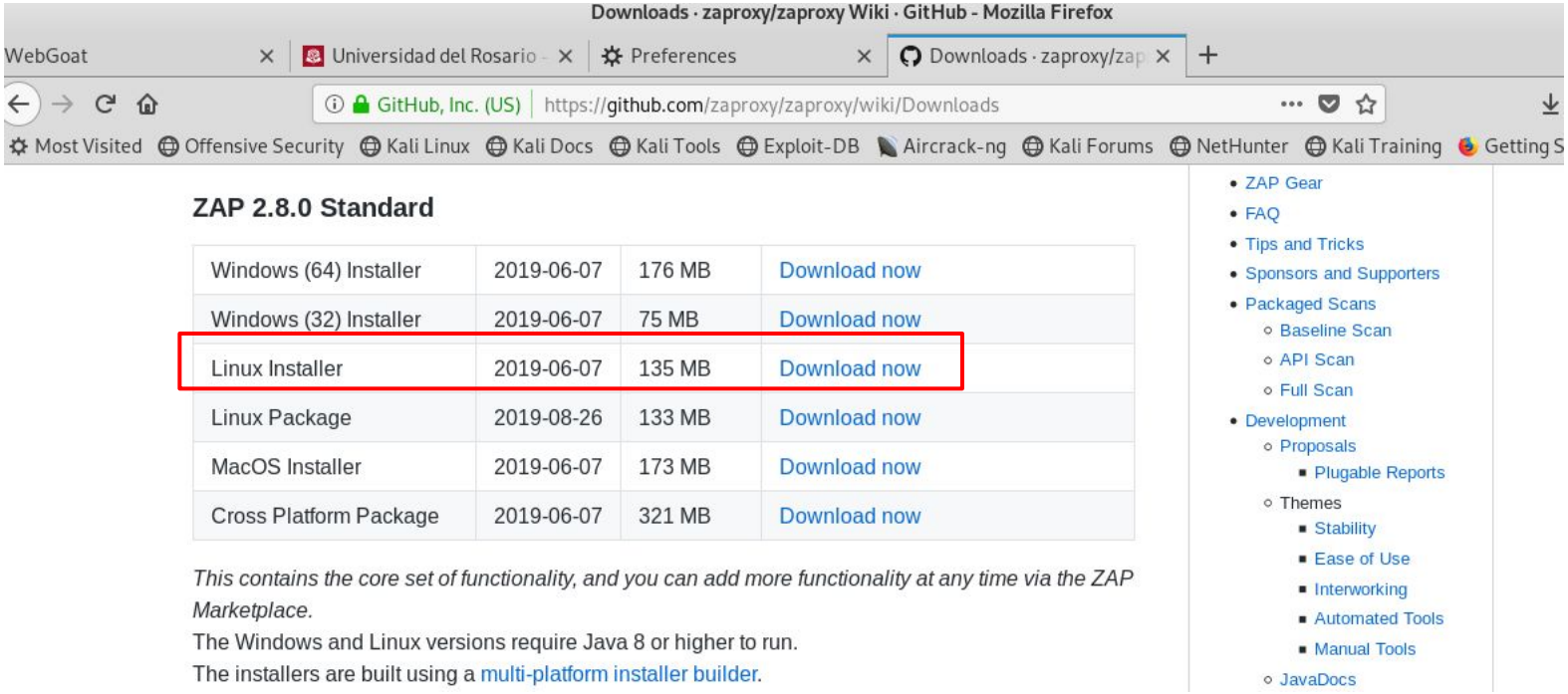
MACC
Matemáticas Aplicadas y Ciencias de la Computación

¡Ahora instalemos nuestro software de interceptación!

ZAP

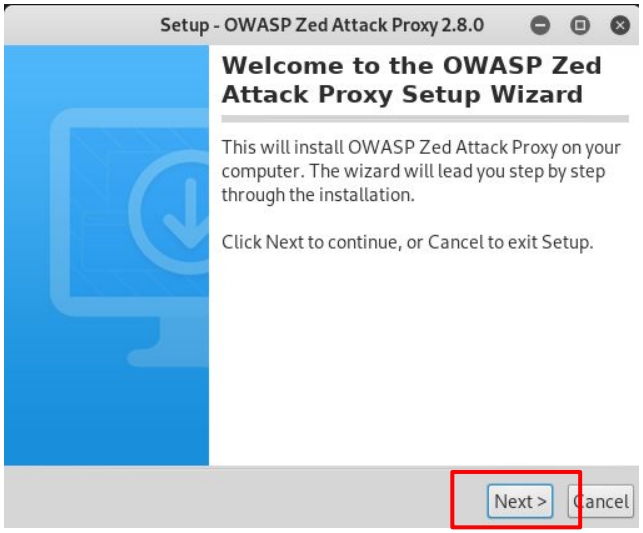
- **Zed Attack Proxy (ZAP):** Software de interceptación de comunicaciones

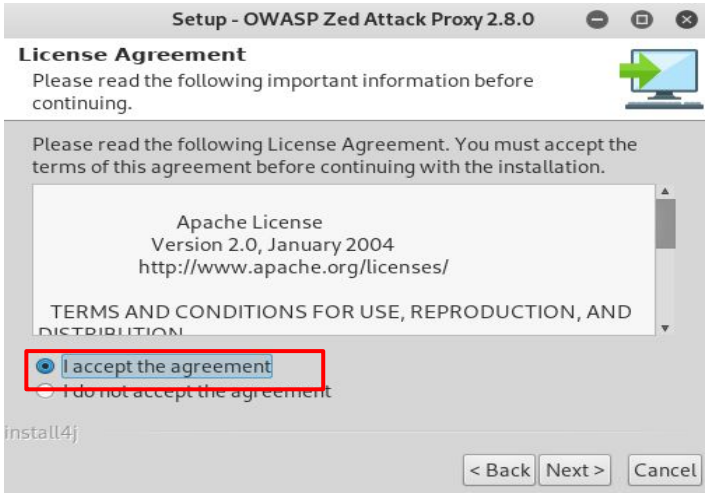
https://github.com/zaproxy/zaproxy/wiki/Downloads
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

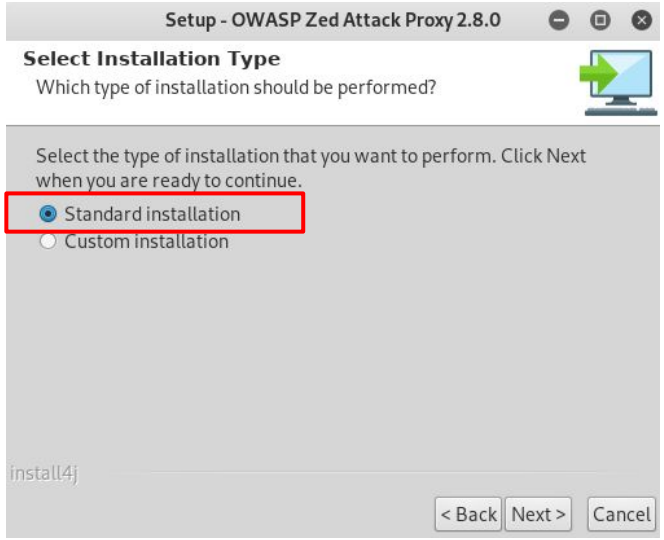


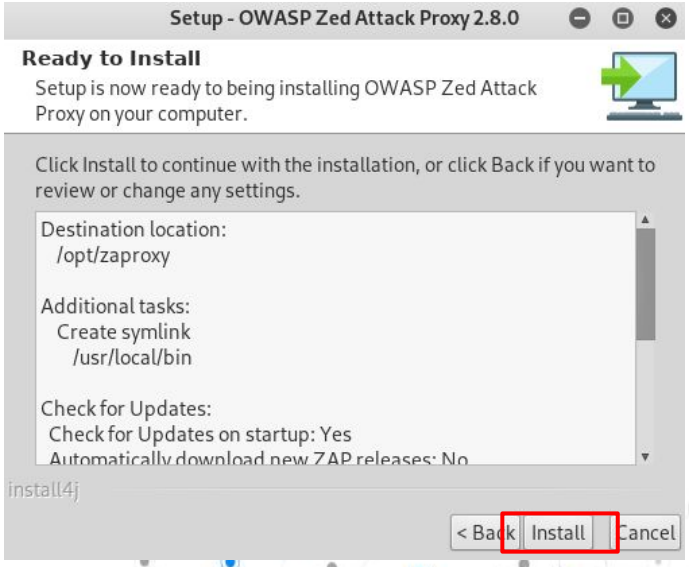

```
root@kali:~/Downloads# ls
UserDatabase.mv.db                webgoat-container-7.1-exec.jar  ZAPGettingStartedGuide-2.8.pdf
webgoat-container-7.0.1-war-exec.jar  ZAP_2_8_0_unix.sh
root@kali:~/Downloads# sh ZAP_2_8_0_unix.sh
```

ZAP


Setup - OWASP Zed Attack Proxy 2.8.0
Welcome to the OWASP Zed Attack Proxy Setup Wizard
This will install OWASP Zed Attack Proxy on your computer. The wizard will lead you step by step through the installation.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel


Setup - OWASP Zed Attack Proxy 2.8.0
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND
I accept the agreement
I do not accept the agreement
install4j
< Back
Next >
Cancel

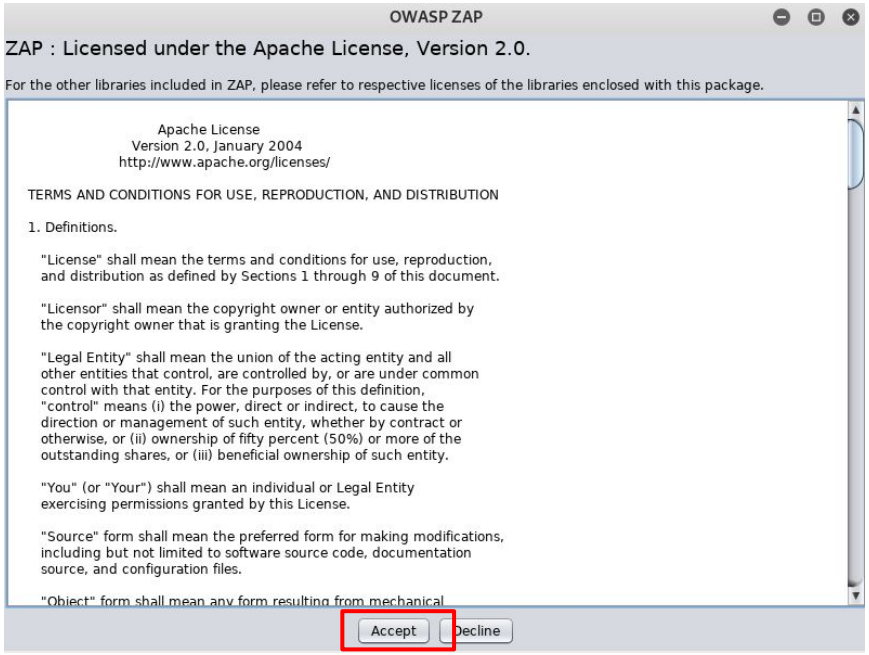

Setup - OWASP Zed Attack Proxy 2.8.0
Select Installation Type
Which type of installation should be performed?
Select the type of installation that you want to perform. Click Next when you are ready to continue.
Standard installation
Custom installation
install4j
< Back
Next >
Cancel


Setup - OWASP Zed Attack Proxy 2.8.0
Ready to Install
Setup is now ready to being installing OWASP Zed Attack Proxy on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
/opt/zaproxy
Additional tasks:
Create symlink
/usr/local/bin
Check for Updates:
Check for Updates on startup: Yes
install4j
< Back
Install
Cancel

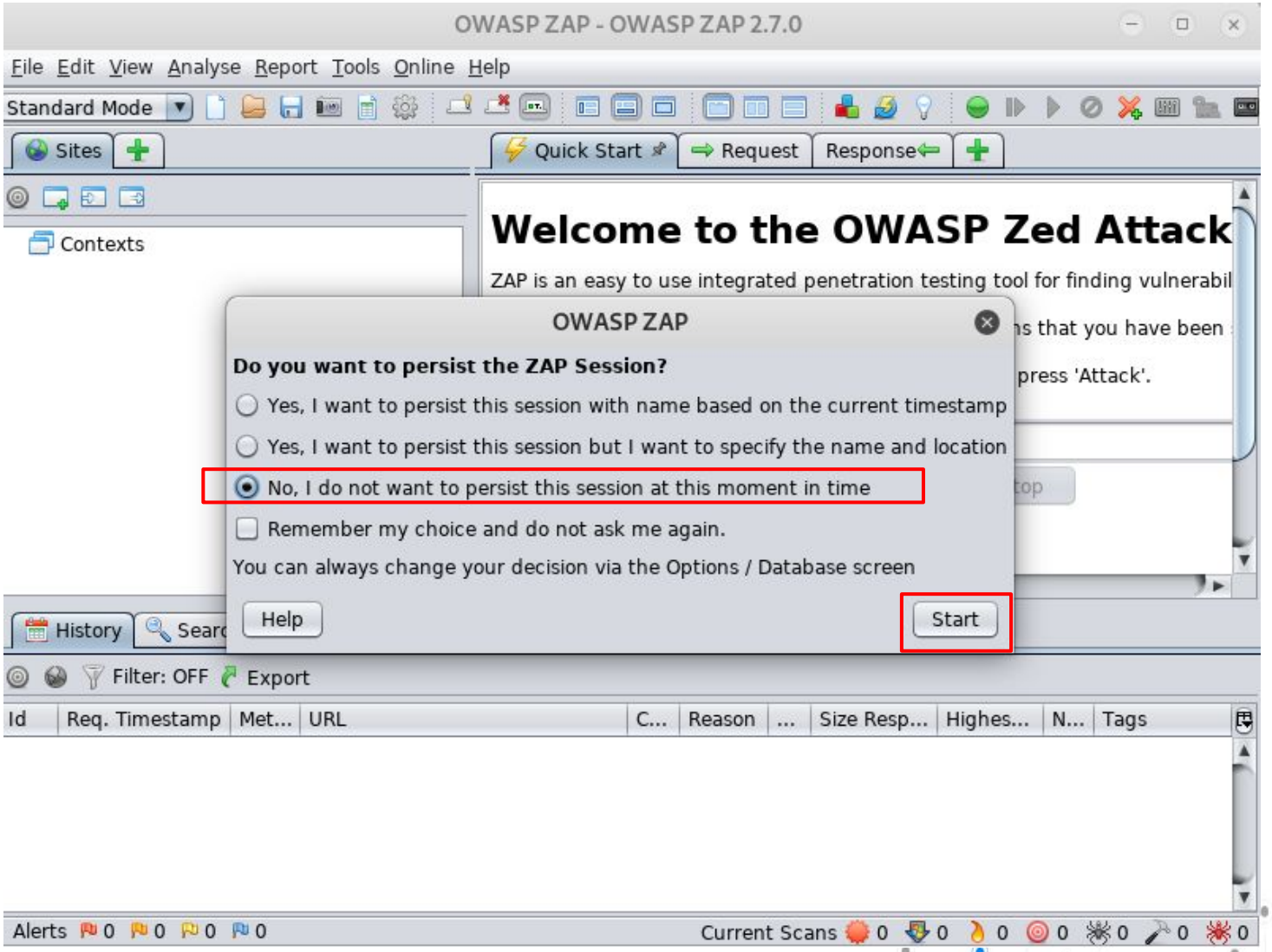
ZAP

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

```
root@kali:~/Downloads# owasp-zap
Found Java version 1.8.0_171
Available memory: 1996 MB
Setting jvm heap size: -Xmx499m
640 [main] INFO org.zaproxy.zap.GuiBootstrap - OWASP ZAP 2.7.0 started 20/10/19 23:25:58 with home /root/.ZAP/
```

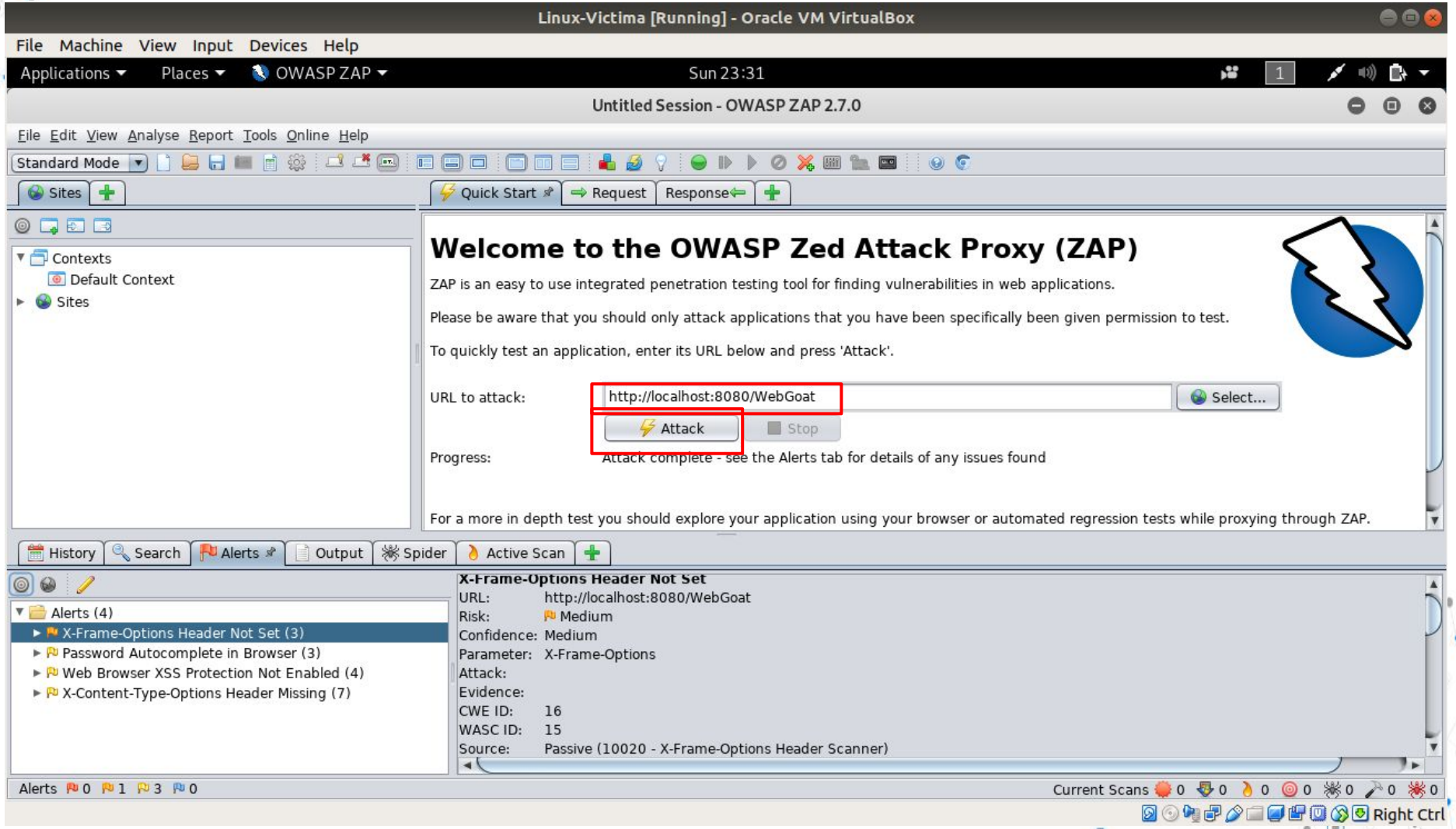


ZAP


OWASP ZAP - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Welcome to the OWASP Zed Attack
ZAP is an easy to use integrated penetration testing tool for finding vulnerabil
ns that you have been
press 'Attack'.
OWASP ZAP
Do you want to persist the ZAP Session?
Yes, I want to persist this session with name based on the current timestamp
Yes, I want to persist this session but I want to specify the name and location
No, I do not want to persist this session at this moment in time
Remember my choice and do not ask me again.
You can always change your decision via the Options / Database screen
Help
Start
History
Filter: OFF
Export
Id
Req. Timestamp
Met...
URL
C...
Reason
...
Size Resp...
Highes...
N...
Tags
Alerts
Current Scans

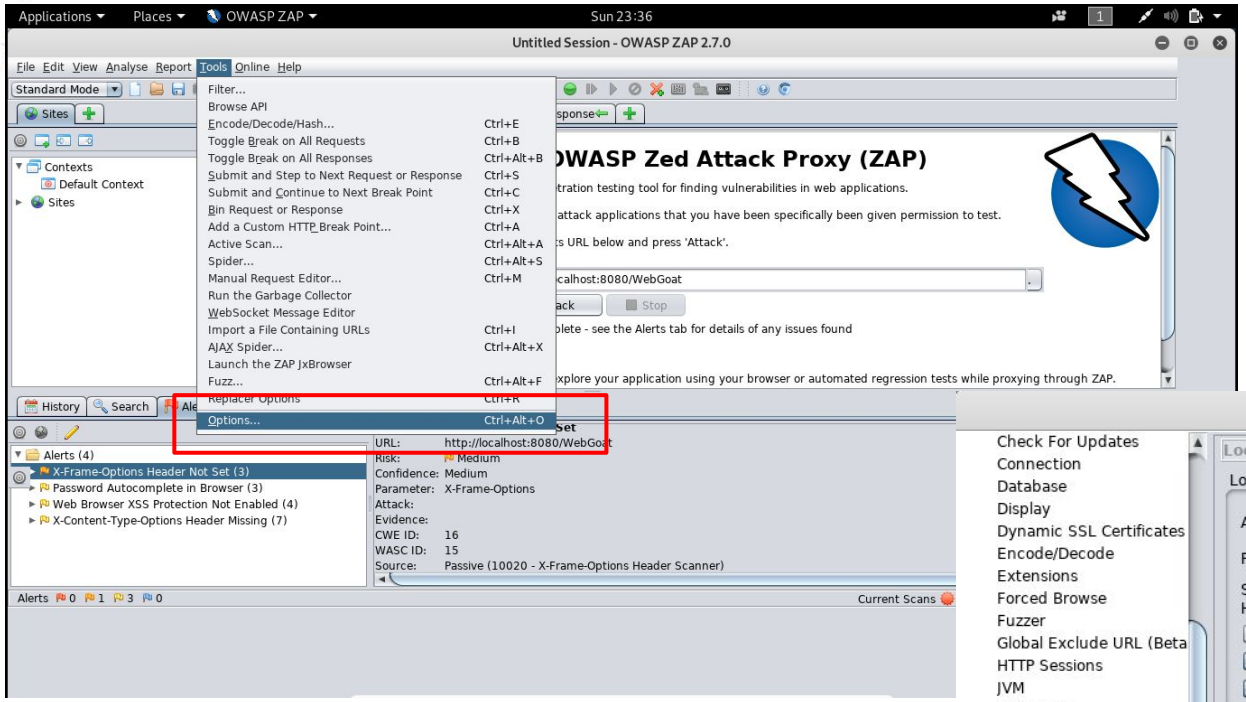
ZAP

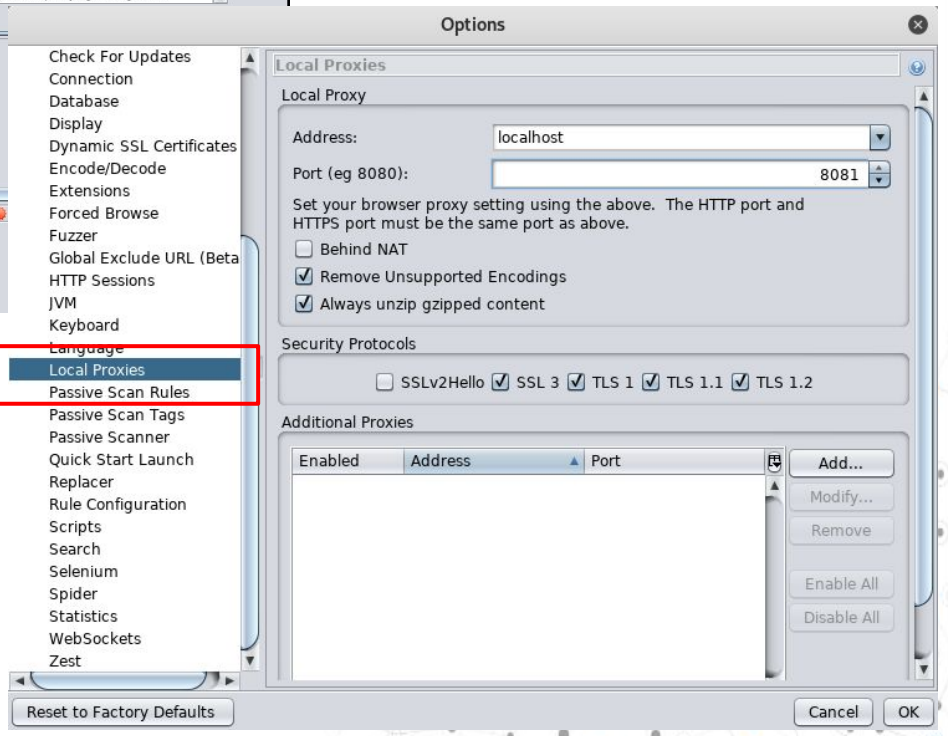
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



ZAP

Para configurar ZAP como proxy, vamos a Tools -> Options -> Local Proxies

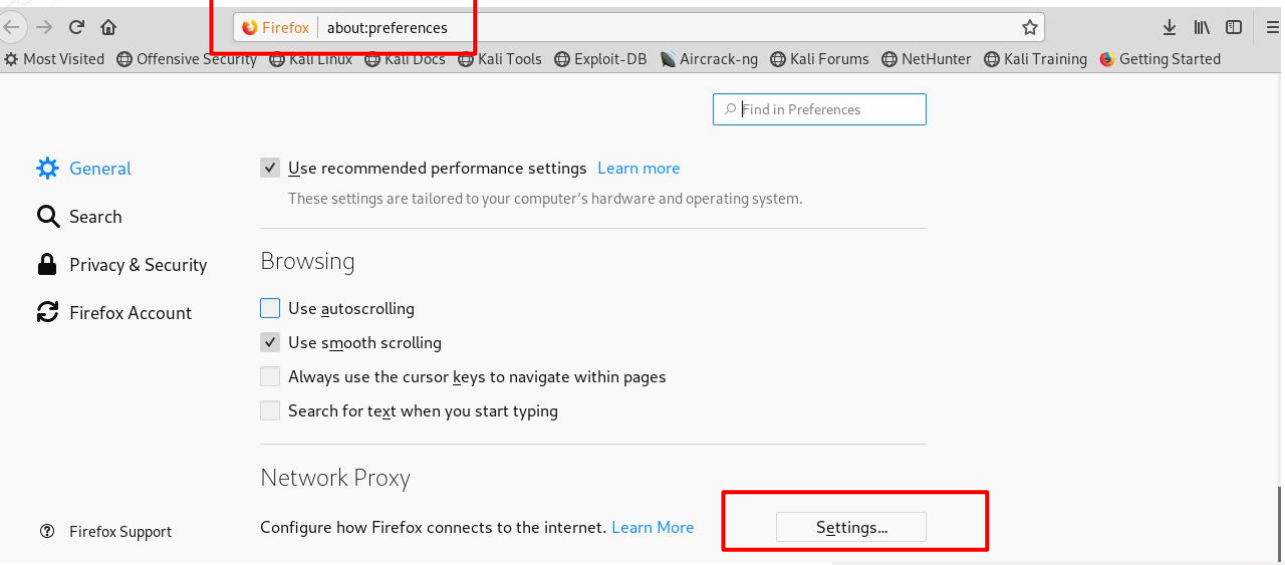


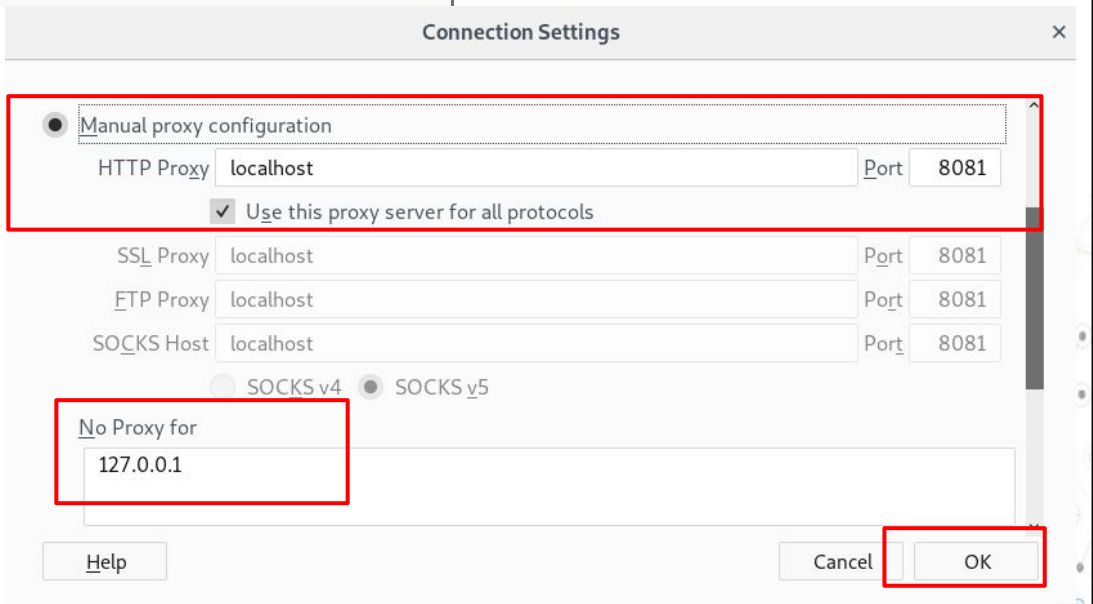


ZAP

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Ahora configuremos que todo el tráfico web vaya primero hacia ZAP



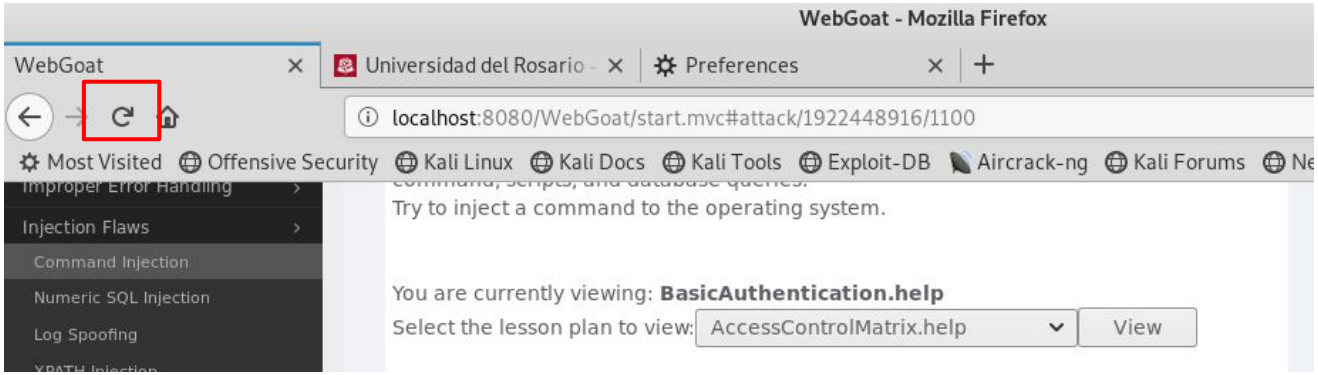


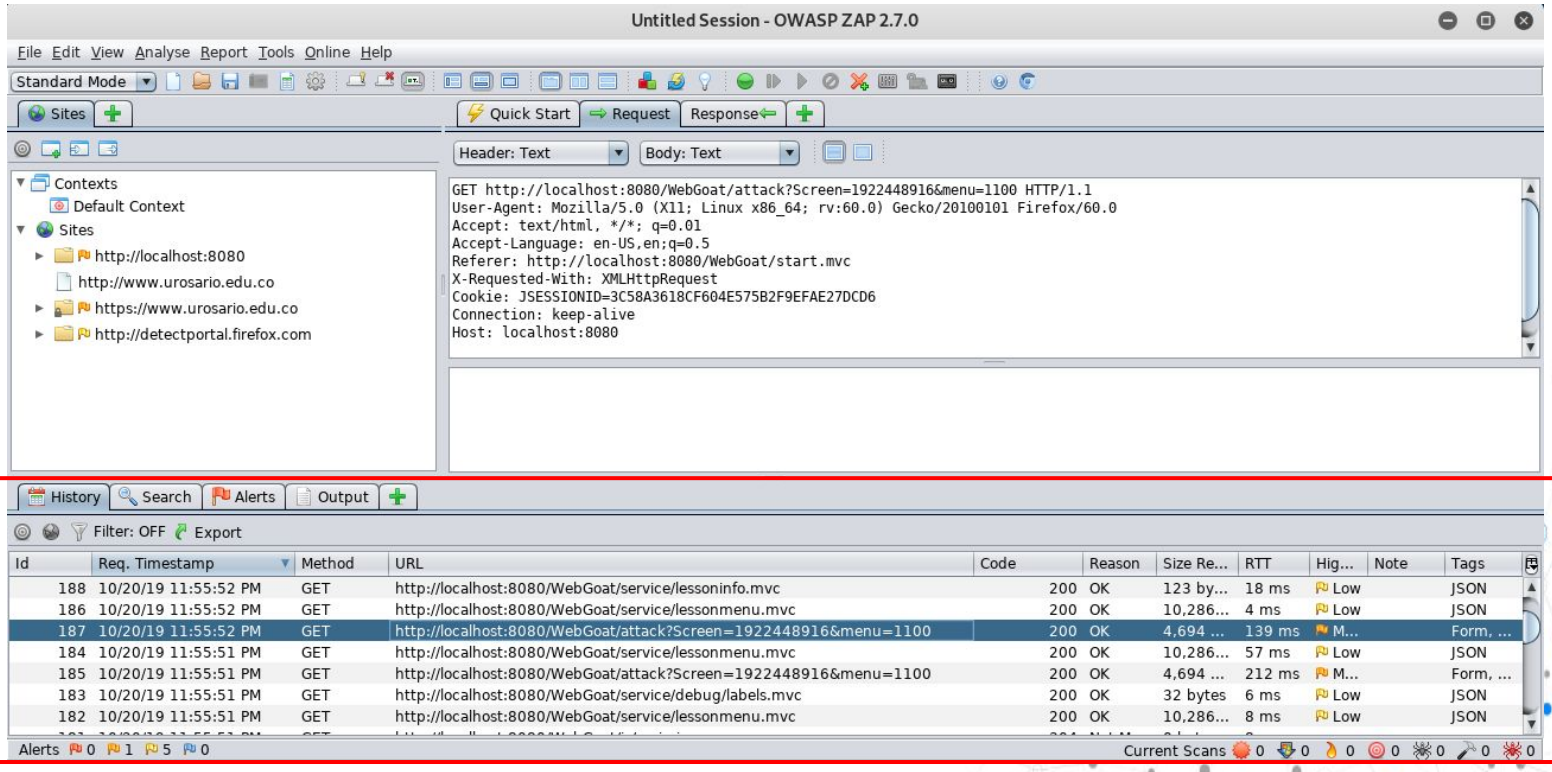
ZAP

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

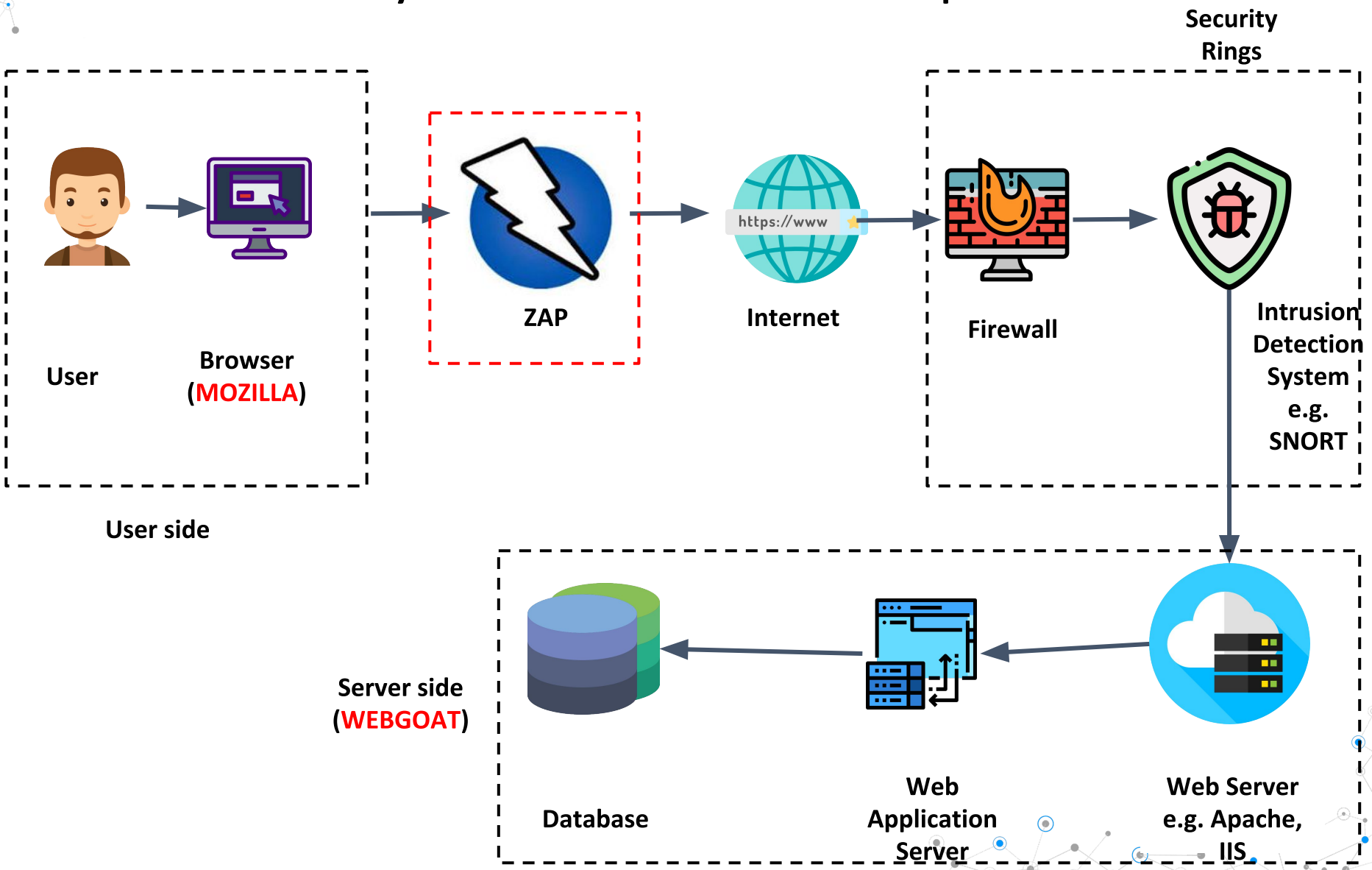
Probemos las capacidades de interceptación de ZAP

Cuando actualizamos una página web, veremos que todas las peticiones y respuestas quedan registradas en ZAP





Ahora ya tenemos nuestro ambiente de prueba



- The ten most critical web application security risks

A1 - Injection – Inyección de código

A2 – Broken authentication and sesion management - Pérdida de Autenticación y Gestión de Sesiones

A3 - Cross-site scripting (XSS) - Secuencia de Comandos en Sitios Cruzados

A4 – Insecure direct object references - Referencia Directa Insegura a Objetos

A5 – Security misconfiguration - Configuración de seguridad Incorrecta

A6 – Sensitive data exposure - Exposición de Datos Sensibles

A7 – Missing function level Access control - Ausencia de Control de Acceso a Funciones

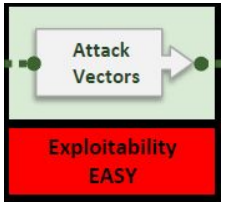
A8 – Cross-Site Request Forgery (CSRF) - Falsificación de Peticiones en Sitios Cruzados

A9 – Components with known vulnerabilities - Uso de Componentes con Vulnerabilidades conocidas

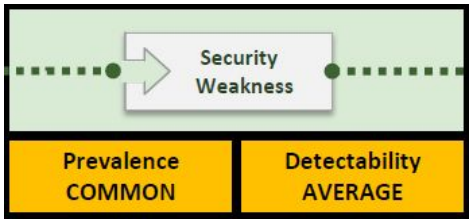
A10- Unvalidated redirects and forwards - Redirecciones y reenvíos no validados

A1- Inyección de Código

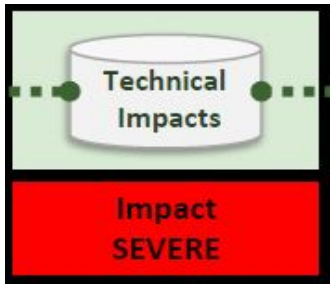
Inyección de Código



- **How?** The intruder sends text-based attacks that exploit the syntax of the application interpreter. Almost any data source (including internal data) can be an attack vector.



- **Why?** It occurs when the data provided by the user are not validated before being processed by the interpreter. Injection can exist in SQL code, LDAP, XPATH, OS Commands, XML parsers, SMTP headers, program arguments, etc.



- **Impact:** Loss of data, modification of data, execution of activities outside of logs, denial of service

Inyección de Código

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

OS COMMAND INJECTION

- Same problem: a command sequence is built using **user input** which is NOT sanitized or validated
- Imagine what would happen if the **OS application account** is not restricted

- **Two types:**

1. The software has a field which is the argument for a single command
2. The software accept an argument which is converted to a command

Flaw

→ The programmer assumes that the input is always trustworthy

→ The programmer assumes that the command will never be used

; /bin/ls -l”

;	%3B
Espace [ ]	%20
“	%22

The command must be codified to URL format

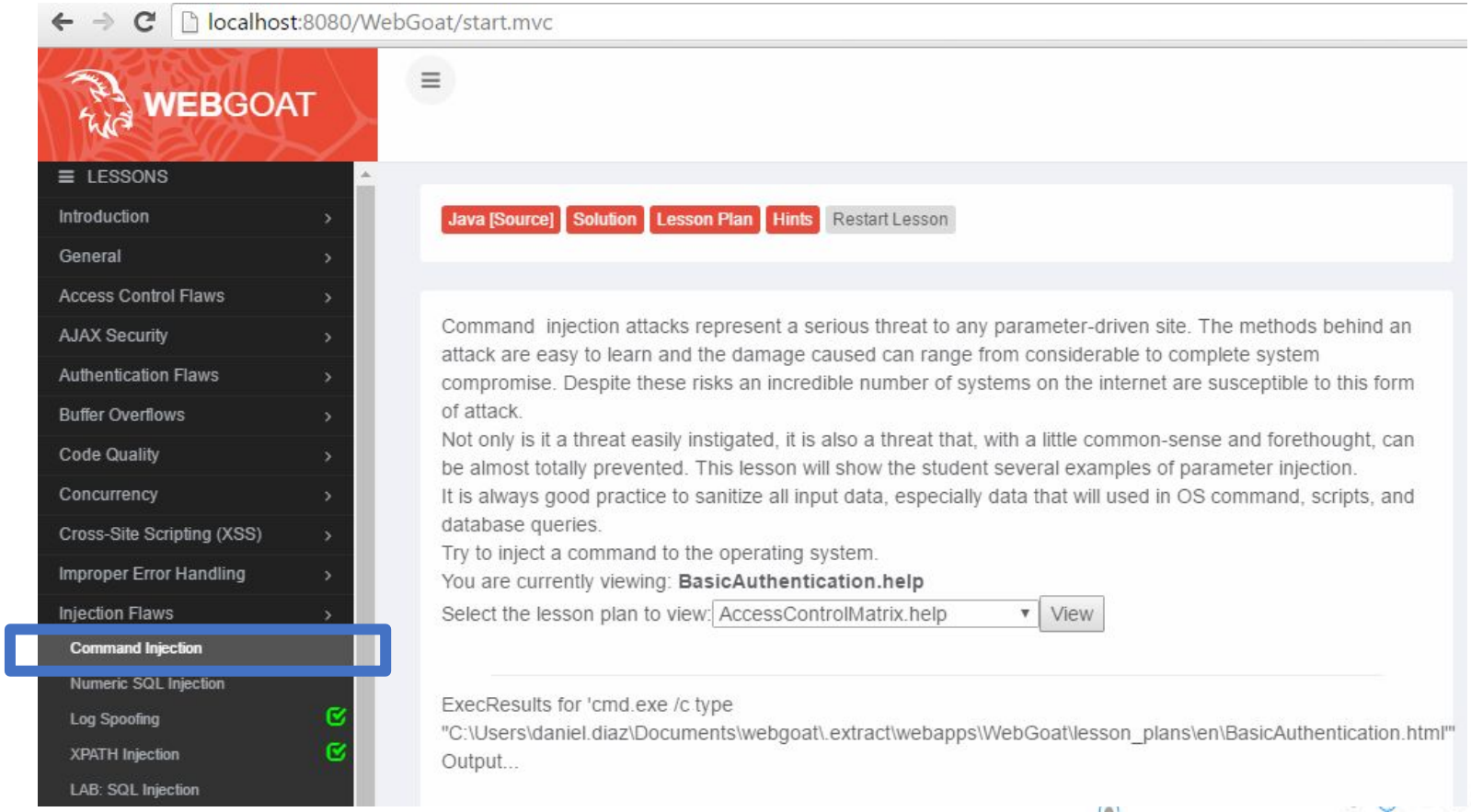
http://www.mycompany.com/sensitive/cgi-bin/userData.pl?doc=%20%3B%20/bin/ls%20-l%22

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

Inyección de Código

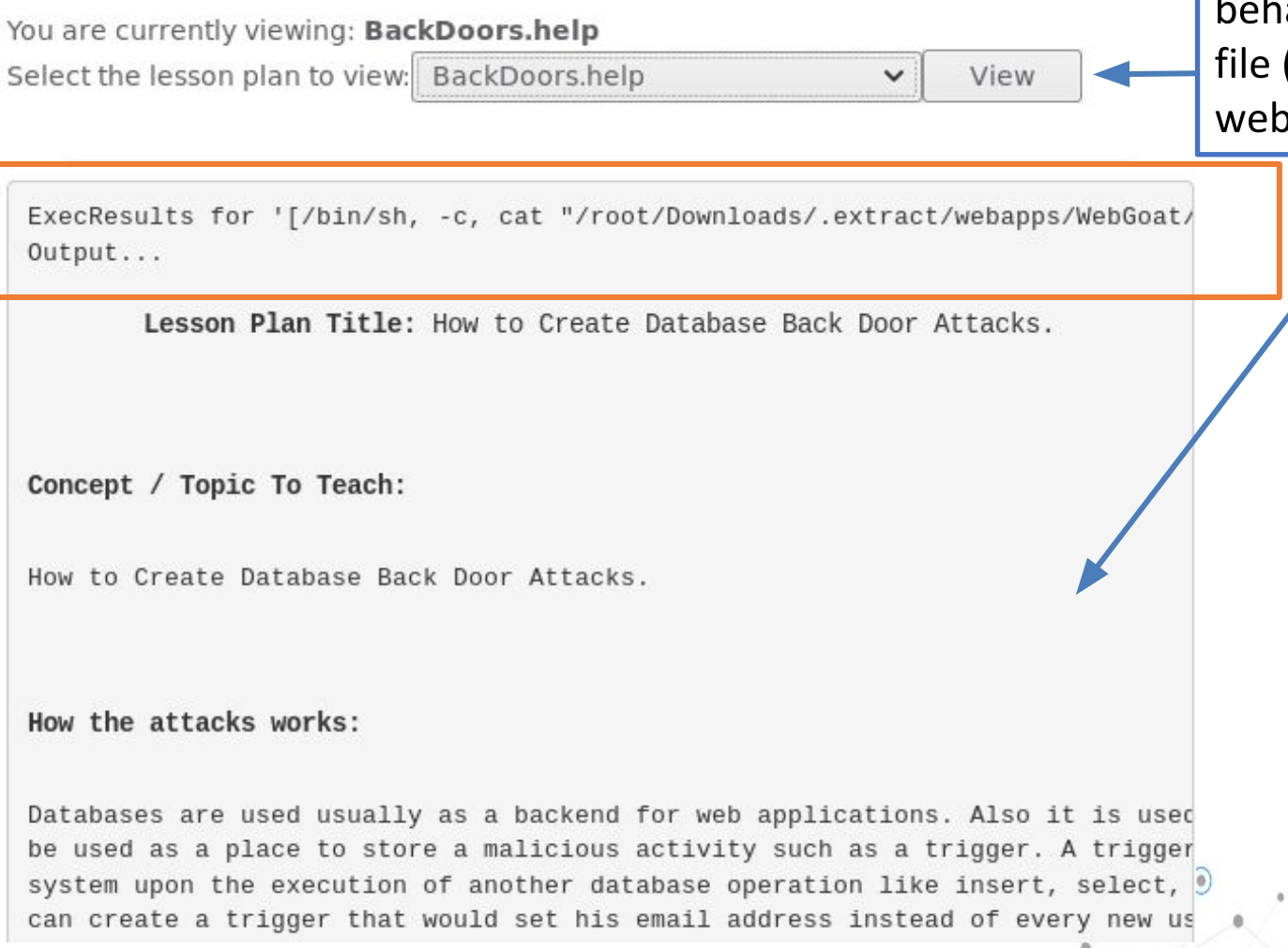
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- Example Command injection in WebGoat



Inyección de Código

- Example Command injection in WebGoat

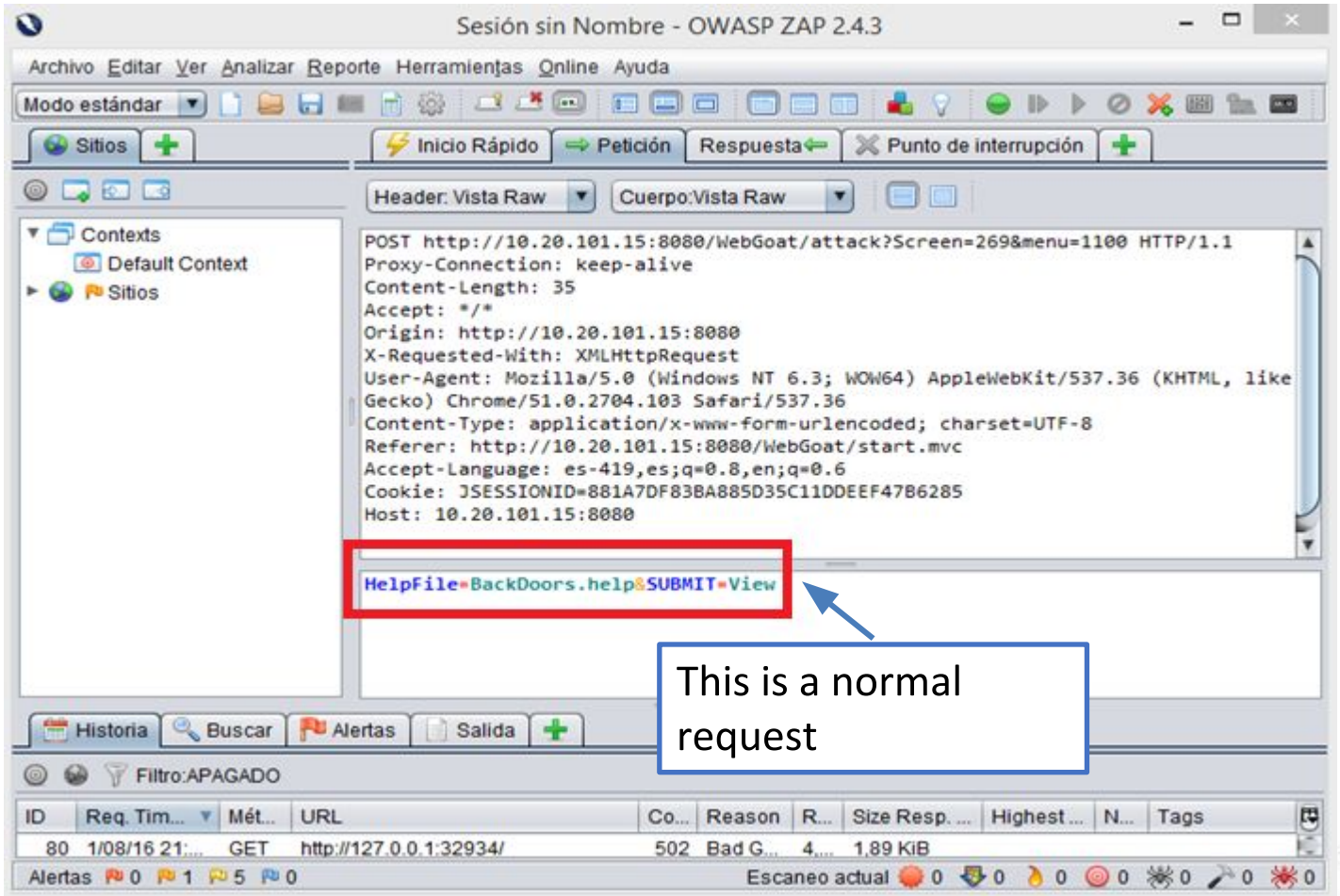


This is the normal behavior: I select a file (lesson) and the web server return it

Inyección de Código

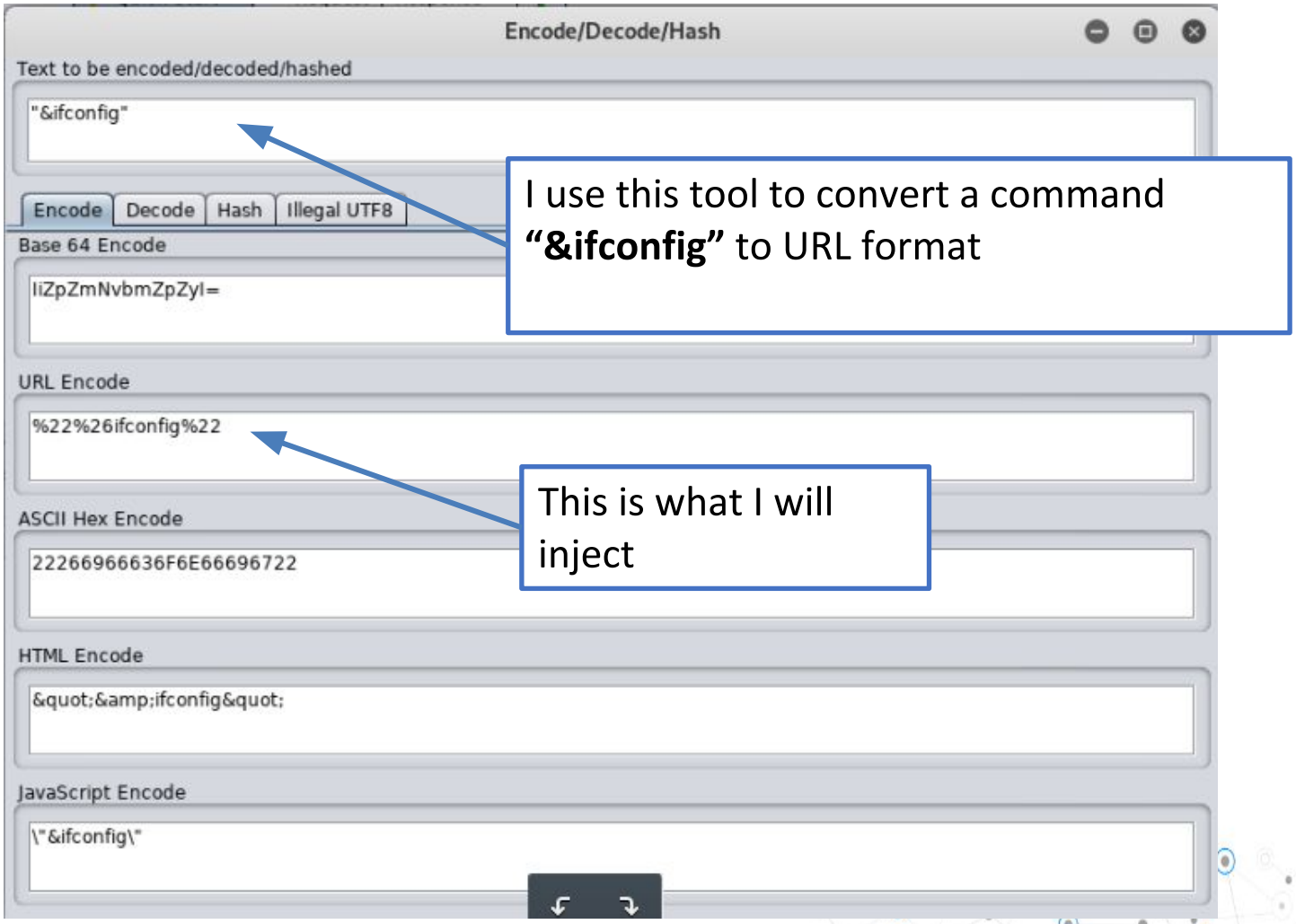
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- Example Command injection in WebGoat



Inyección de Código

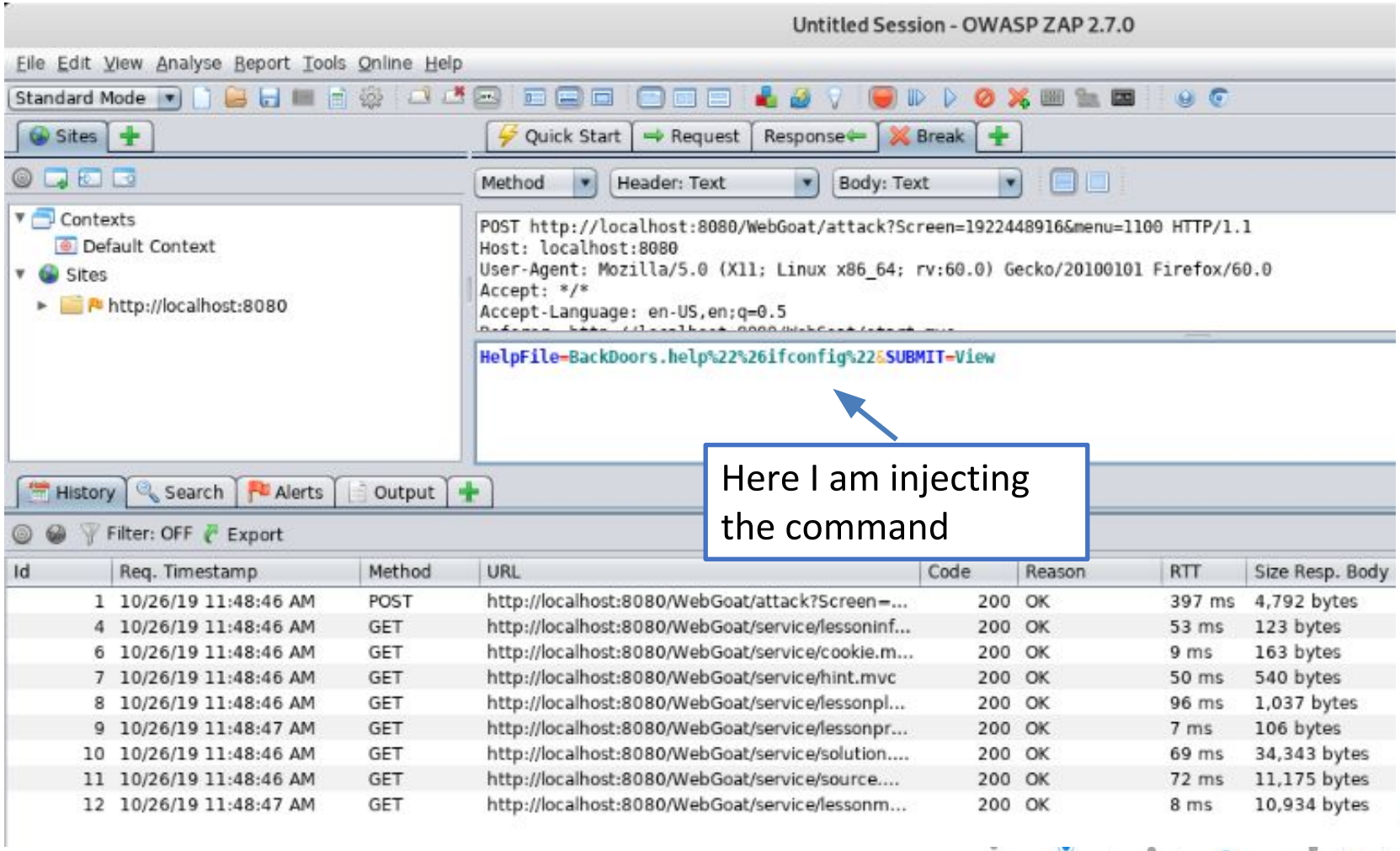
- Example Command injection in WebGoat



Inyección de Código

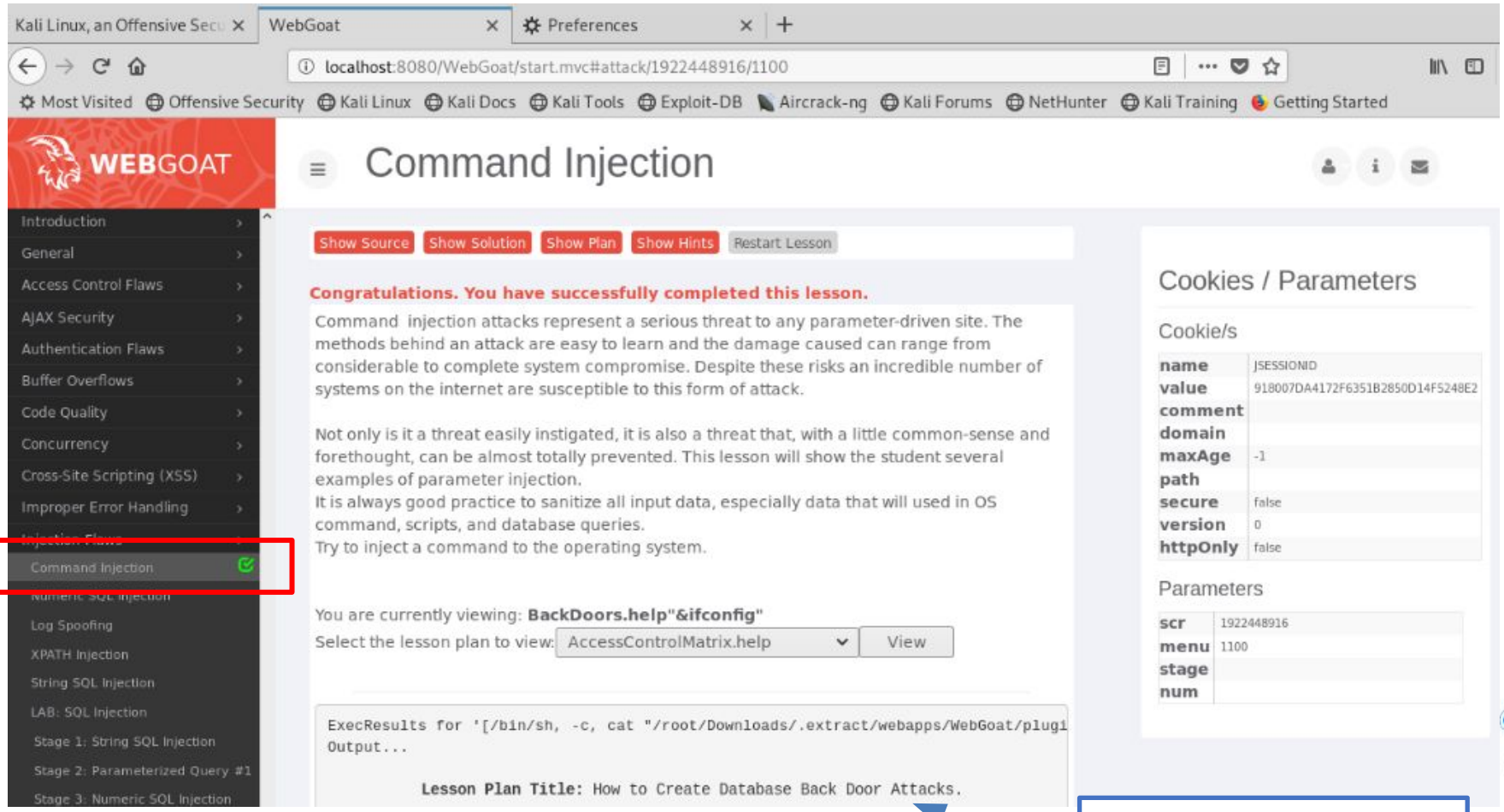
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- Example Command injection in WebGoat



Inyección de Código

- Example Command injection in WebGoat

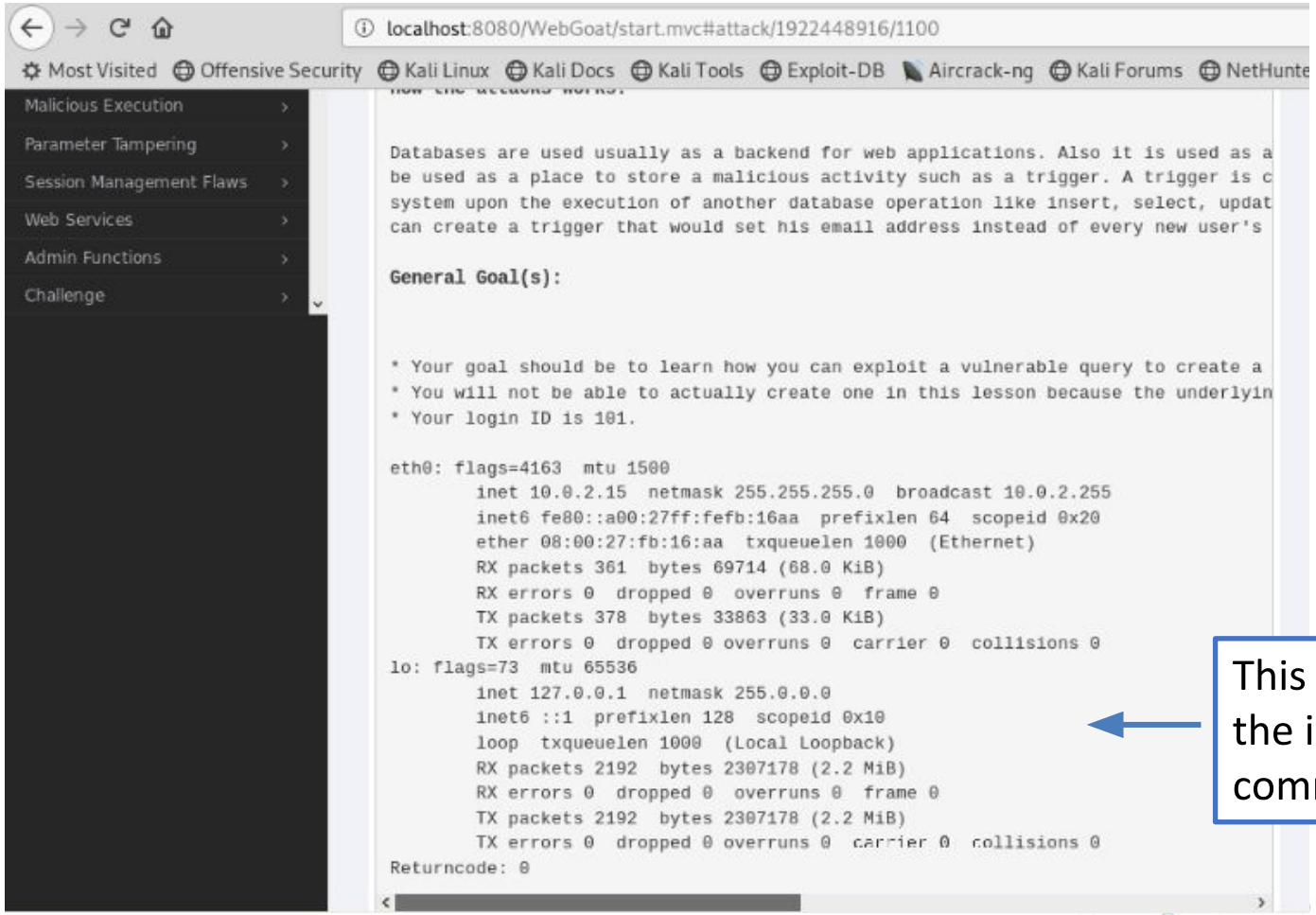


This is the expected answer

Inyección de Código

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

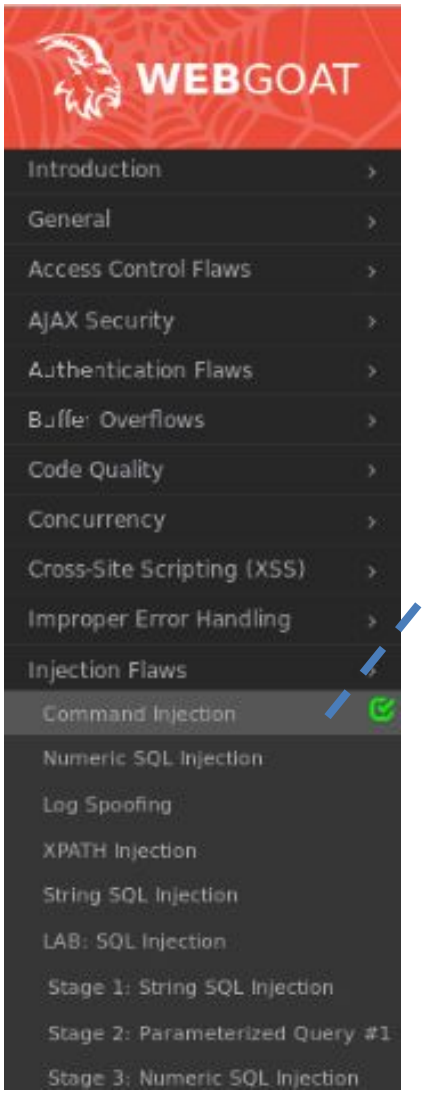
- Example Command injection in WebGoat



Inyección de Código

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Execution on live!



https://www.youtube.com/watch?v=M2wUCSIeeqY&list=PL9HjVcGKtXM305JN2FjKyHNAGIZxZNzNn&index=1

Bibliography

Main resources:

https://www.owasp.org/index.php/Top_10-2017_Top_10
https://www.owasp.org/index.php/Top_10_2013-Top_10

Multimedia resources:

https://www.youtube.com/playlist?list=PL9HjVcGKtXM305JN2FjKyHNAGIZxZNzNn
https://www.youtube.com/playlist?list=PL9HjVcGKtXM2pi1nY2g6SWM9yiyetEB5A

Universidad del Rosario | MACC | HINNT

¡Gracias!