Internship Report – Cybersecurity

The Redynox Cybersecurity Team

Report Prepared By : Issa Hassan Youssouf

Company : Redynox

Internship period : June 16 to July 16, 2025

Reporting Manager : *Mr. Ankit Mathur*

Institution : University Institute of the Gulf of Guinea

TABLE OF CONTENTS

Thanks

I would like to warmly thank **Redynox** for giving me the opportunity to welcome me to their team and for allowing me to discover tools such as OWASP ZAP, Wireshark and concrete cybersecurity methodologies.

I would also like to thank my internship supervisor **Mr. Ankit Mathur** for his support, his valuable advice and his availability throughout this experience.

This internship allowed me to strengthen my technical skills, better understand current digital risks and confirm my interest in the field of cybersecurity.

INTRODUCTION

As part of my training, I had the opportunity to do a practical internship at the company Redynox, which specialises in cybersecurity. This internship was an enriching immersion in the world of IT security, especially on technical aspects such as network security, web vulnerability analysis and the use of professional tools such as Wireshark, WebGoat, OWASP ZAP and configure basic security configurations, such as changing default passwords and enabling network encryption (WPA2 or WPA3). I was also encouraged to develop my professional visibility through publications on LinkedIn.

This document is a detailed, step-by-step guide retracing all the tasks I performed during this internship, with the Parrot OS environment as the main support.

I. TASK 1 : INTRODUCTION TO NETWORK SECURITY BASICS

Network security refers to the policies, practices, and technologies used to protect the integrity, confidentiality, and availability of computer networks and data. It involves preventing unauthorized access, misuse, modification, or denial of a network and its accessible resources.

Key Goals of Network Security :

Confidentiality is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes. Methods to ensure confidentiality include data encryption, identity proofing and two factor authentications.

Integrity ensures that system information or processes are protected from intentional or accidental modification. One way to ensure integrity is to use a hash function or checksum.

Availability means that authorized users are able to access systems and data when and where needed and those that do not meet established conditions, are not. This can be achieved by maintaining equipment, performing hardware repairs, keeping operating systems and software up to date, and creating backups.

1) LEARN NETWORK SECURITY CONCEPT

Different types of network threats :

Malware is a type of software designed to cause harm to computer systems, networks, or devices. The term malware is short for malicious software. Malware can be developed in many forms, including viruses, worms, Trojan horses, ransomware, spyware, and adware.

Malware can cause many problems, from disrupting regular system and network operations to stealing sensitive information, such as passwords and business data. Malware can also be used to install hidden remote access, allowing unauthorized access to a system.

Protecting computer systems and devices from malware is essential; keeping software up-to-date, using antivirus software, and practicing safe browsing habits all help. In addition, be vigilant and cautious when downloading software or opening email attachments, as these can be common vectors for malware infection.

Virus :

A virus is a type of malicious software that replicates itself and infects other programs or files on a computer. A virus typically spreads by attaching itself to a legitimate program or file. It can then spread to other computers when that file is shared or when the infected program runs on another computer.

A virus can cause many problems, including slowing computer performance, stealing sensitive information, and even destroying data. Some viruses can also be used as a tool for more extensive cyberattacks, such as distributed denial-of-service (DDoS) attacks.

Damage from viruses includes :

- Corrupting files,
- Computer slowdown,
- Taking over essential functions of the operating system.

Worm

A computer worm is an independent malware program that reproduces itself to infect other computers. It can spread to other computers without attaching to an existing program and can damage the network.

Damage from worms includes :

- Bandwidth consumption,
- Stopping active anti-malware service,
- Immobilizing Safe Mode,
- Hindering operating systems auto-update.

Worms can :

- Cause significant damage by consuming network bandwidth, slowing computer performance, and compromising the security of sensitive information,
- Spread rapidly and cause widespread infections, making them a significant threat to computer security,
- Exploit vulnerabilities in operating systems or software, allowing attackers to gain unauthorized access to computer systems.

Protect against worms by :

- Keeping software up-to-date,
- Using firewalls,
- Practicing safe browsing habits.

Using antivirus software and intrusion detection systems help to detect and respond to worm infections.

Phishing

Phishing is a cyberattack that tricks individuals into sharing sensitive information through fake emails or directed to websites that appear legitimate. The cybercriminals who use phishing scams masquerade as real:

- Prominent companies,
- Banks and financial institutions,
- Government offices,
- Credit card businesses,
- Charities and nonprofits.

They are looking for sensitive information such as passwords and financial information.

Phishing attacks take advantage of communication tools that people use every day and can happen in various ways: email, text messages, phone calls, or instant messages.

Features of a phishing scam will include one or more of the following.

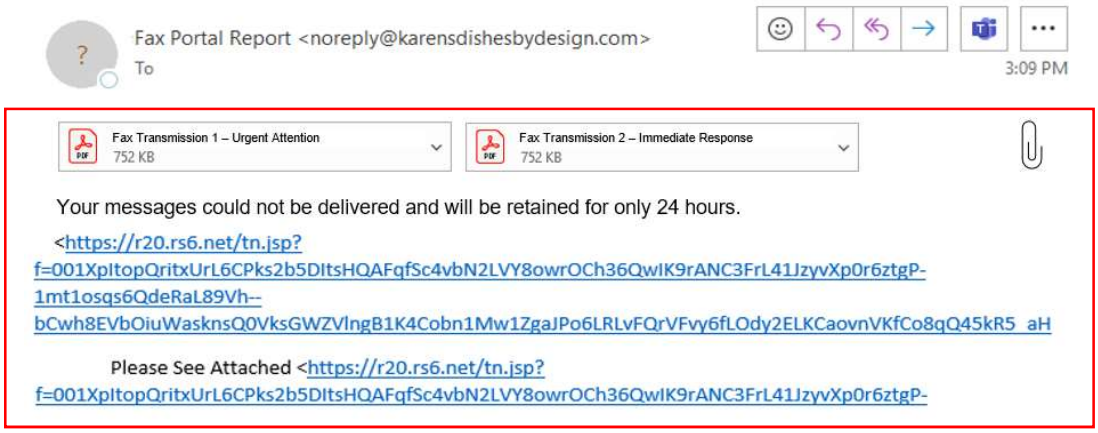
Request for immediate action and urgent offers

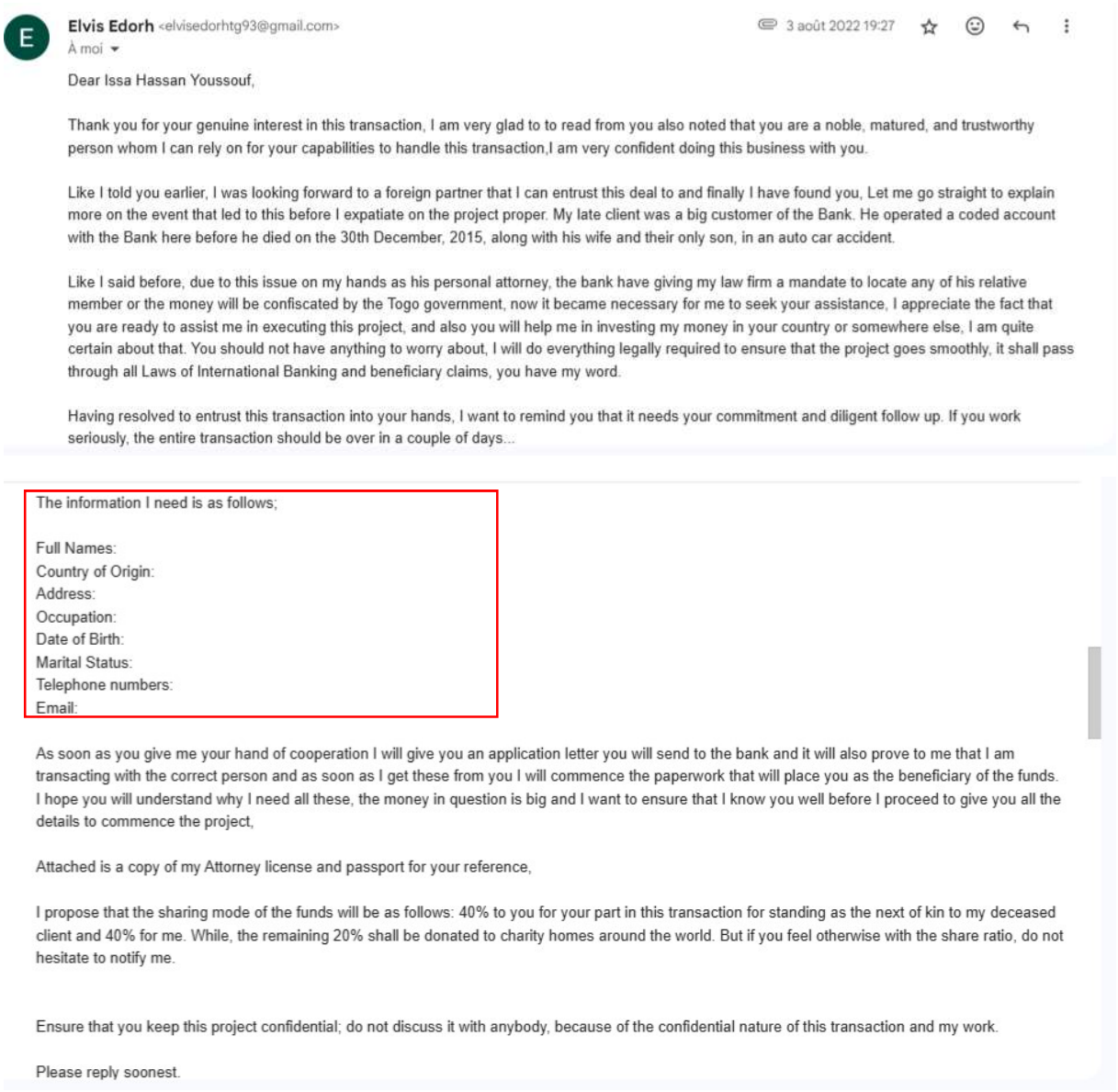
- Claim that there's a problem with your account or password,
- Request to confirm your password or account information,
- Say that there's been suspicious activity on your account,
- Notify you of a failed or missed payment,
- Offer you a free coupon or gift, or say that you're eligible for a refund

Digital Communication (Email, Text, Messaging)

- Generic information to the sender and from an unknown sender,
- Unrequested invoice or message attachment or invoice,
- Mismatched subject and contents,
- Spelling errors and basic punctuation mistakes,
- Similar characters for numbers and vice versa. For example, the number 1 instead of capital I,
- Ask you to click on a link or provide information for a new security update,
- A hyperlink to what seems to be a legitimate website,
- Virus warnings.

In the examples below, can you recognize at least 14 phishing scam items.





Elvis Edorh <elvisedorhtg93@gmail.com>
À moi

3 août 2022 19:27

Dear Issa Hassan Youssouf,

Thank you for your genuine interest in this transaction, I am very glad to to read from you also noted that you are a noble, matured, and trustworthy person whom I can rely on for your capabilities to handle this transaction,I am very confident doing this business with you.

Like I told you earlier, I was looking forward to a foreign partner that I can entrust this deal to and finally I have found you, Let me go straight to explain more on the event that led to this before I expatiate on the project proper. My late client was a big customer of the Bank. He operated a coded account with the Bank here before he died on the 30th December, 2015, along with his wife and their only son, in an auto car accident.

Like I said before, due to this issue on my hands as his personal attorney, the bank have giving my law firm a mandate to locate any of his relative member or the money will be confiscated by the Togo government, now it became necessary for me to seek your assistance, I appreciate the fact that you are ready to assist me in executing this project, and also you will help me in investing my money in your country or somewhere else, I am quite certain about that. You should not have anything to worry about, I will do everything legally required to ensure that the project goes smoothly, it shall pass through all Laws of International Banking and beneficiary claims, you have my word.

Having resolved to entrust this transaction into your hands, I want to remind you that it needs your commitment and diligent follow up. If you work seriously, the entire transaction should be over in a couple of days...

The information I need is as follows;

Full Names:
Country of Origin:
Address:
Occupation:
Date of Birth:
Marital Status:
Telephone numbers:
Email:

As soon as you give me your hand of cooperation I will give you an application letter you will send to the bank and it will also prove to me that I am transacting with the correct person and as soon as I get these from you I will commence the paperwork that will place you as the beneficiary of the funds. I hope you will understand why I need all these, the money in question is big and I want to ensure that I know you well before I proceed to give you all the details to commence the project,

Attached is a copy of my Attorney license and passport for your reference,

I propose that the sharing mode of the funds will be as follows: 40% to you for your part in this transaction for standing as the next of kin to my deceased client and 40% for me. While, the remaining 20% shall be donated to charity homes around the world. But if you feel otherwise with the share ratio, do not hesitate to notify me.

Ensure that you keep this project confidential; do not discuss it with anybody, because of the confidential nature of this transaction and my work.

Please reply soonest.

Watch out for words and phrases such as :

1. We suspect unauthorized use or transactions on your account.
2. We will lock or close your account if you do not immediately confirm your identity.
3. Click the link to verify your account is not compromised

Trojan

A Trojan Horse is a type of malware that disguises itself as a legitimate program or file. Unlike a virus, which typically replicates itself and infects other programs or files, a Trojan horse operates by hiding itself within a seemingly harmless program or file.

Once a Trojan horse is installed on a computer, it can carry out many malicious activities including :

- Stealing sensitive information,
- Installing other malware,
- Taking control of the infected computer,
- Create backdoors to get information the system,
- Allowing other attackers to gain unauthorized access to a system.

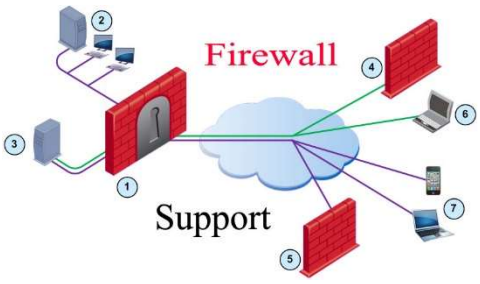
Damage from Trojan Horse includes :

- Crashing the computer,
- Deleting files,
- Corrupting data,
- Logging keystrokes.

Basic security concepts :

Firewall

A firewall is a network security device that acts as a barrier between a trusted internal network and untrusted external networks, such as the Internet. It monitors and controls incoming and outgoing network traffic based on predefined security rules. Its main role is to protect networks and systems from unauthorized access, malicious activities, and potential threats.



Operation and Importance :

- Traffic Filtering: Firewalls inspect network data packets and enforce security policies to either allow or block traffic.
- Threat Protection : They serve as a first line of defense against viruses, hackers,
- DDoS attacks, and unauthorized access attempts, according to Fortinet.
- Types of Firewalls : Firewalls can come in the form of hardware, software, Software-as-a-Service (SaaS), or virtual (cloud-based) solutions. There are also different categories, such as stateless, stateful, application-level, next-generation firewalls (NGFW), and personal firewalls.

In summary, a firewall is a critical component of cybersecurity, acting as a gatekeeper to secure networks by controlling and filtering data traffic.

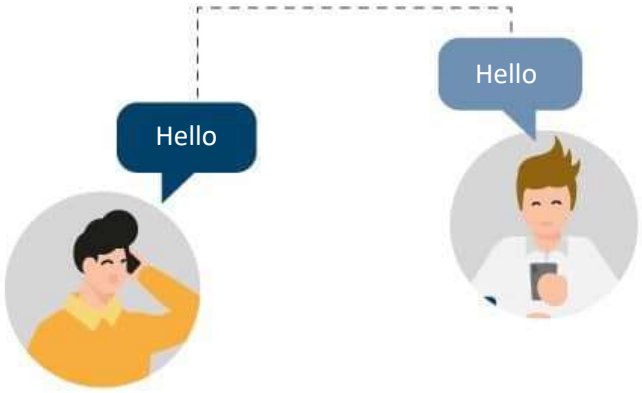
Encryption

Let's begin our exploration of cryptography with encryption.

Encryption is the process of protecting data by rendering it unintelligible. Our focus will primarily be on ensuring data confidentiality.

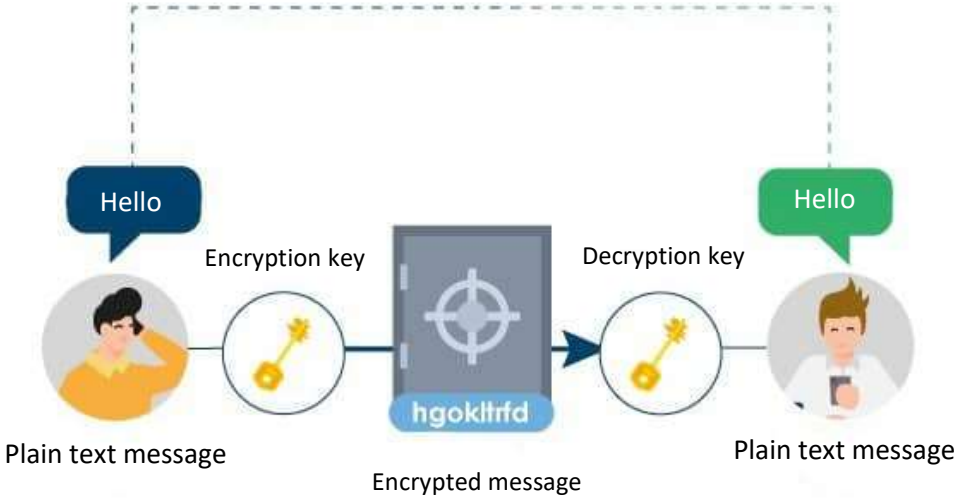
The reverse operation, decryption, is only possible if one possesses a secret element known as the key

By convention, the original message to be protected is referred to as the plaintext, and the result of encryption is called the ciphertext.



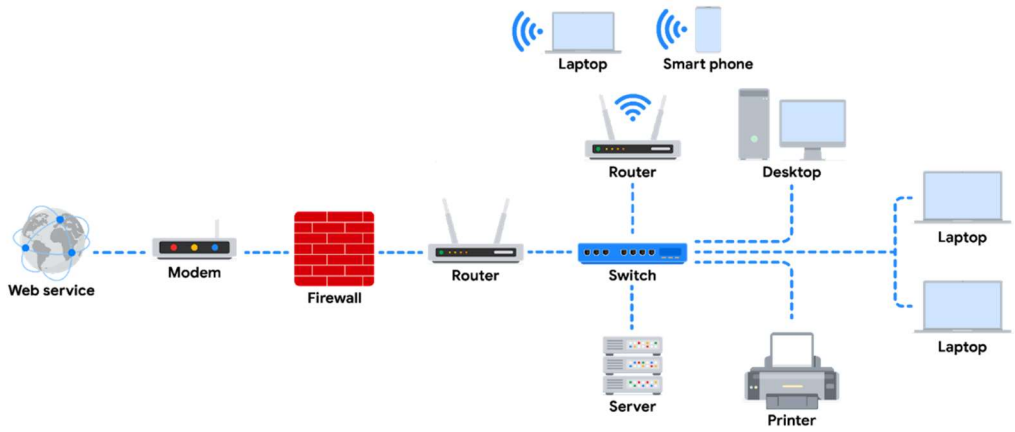
In other words, encryption is the process of transforming plaintext into ciphertext using a (unique) key, so that it can only be understood by those who possess that key.

This allows secure transmission of a message to a recipient over an otherwise untrusted medium—meaning a channel where the data in transit could potentially be intercepted or altered



Secure network configurations

Secure network configurations involve implementing security measures to protect the confidentiality, integrity, and availability of data and network resources from unauthorized access and cyberattacks. This includes using robust security protocols, properly configuring firewalls, enforcing strong authentication, and proactively monitoring the network.



Key Elements of Secure Network Configurations :

- Robust Security Protocols :

Utilize encryption protocols such as IPsec, SSL/TLS, and DTLS, as well as solutions like VPNs (Virtual Private Networks) to secure communications. For Wi-Fi networks, prioritize the use of WPA3 or WPA2/WPA3 Transitional modes.

- Firewalls :

Configure hardware or software firewalls with custom rules to block unsecured traffic and vulnerable ports (such as port 445, which is associated with WannaCry).

- Access Control and Authentication :

Implement strong authentication mechanisms, including multi-factor authentication (MFA) and the use of strong, complex passwords.

- Application and Service Configuration :

Harden application configurations, including setting trusted certificate authorities (or using custom ones), and disabling unnecessary plaintext protocols (such as Telnet).

- Network Monitoring and Anomaly Detection :

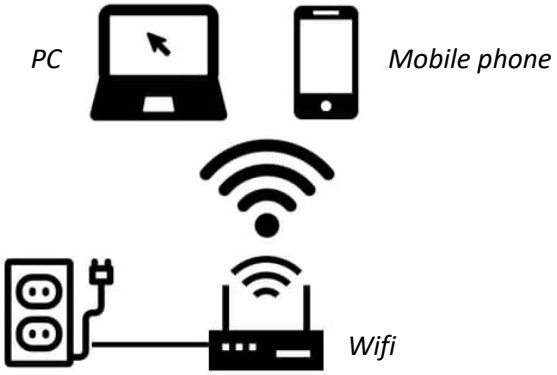
Actively monitor network traffic and activity to detect any suspicious or unauthorized behavior in real time, allowing for quick response to potential threats.

- Configuration Management :

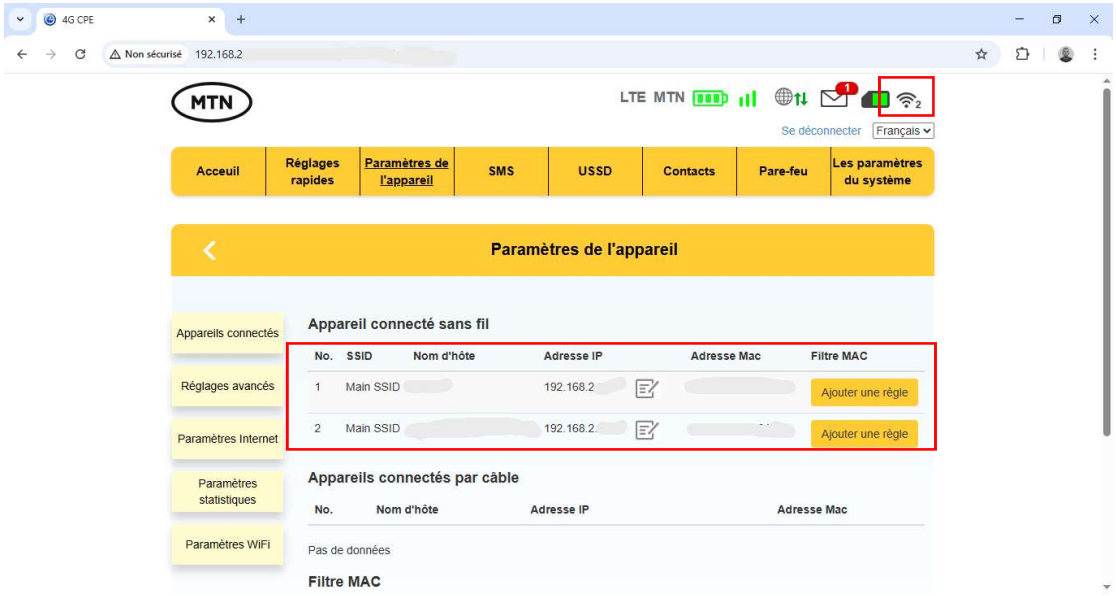
Regularly audit the configurations of network devices and services to ensure they remain secure and aligned with best practices.

2) Implement basic measures

Set up a simple network environment



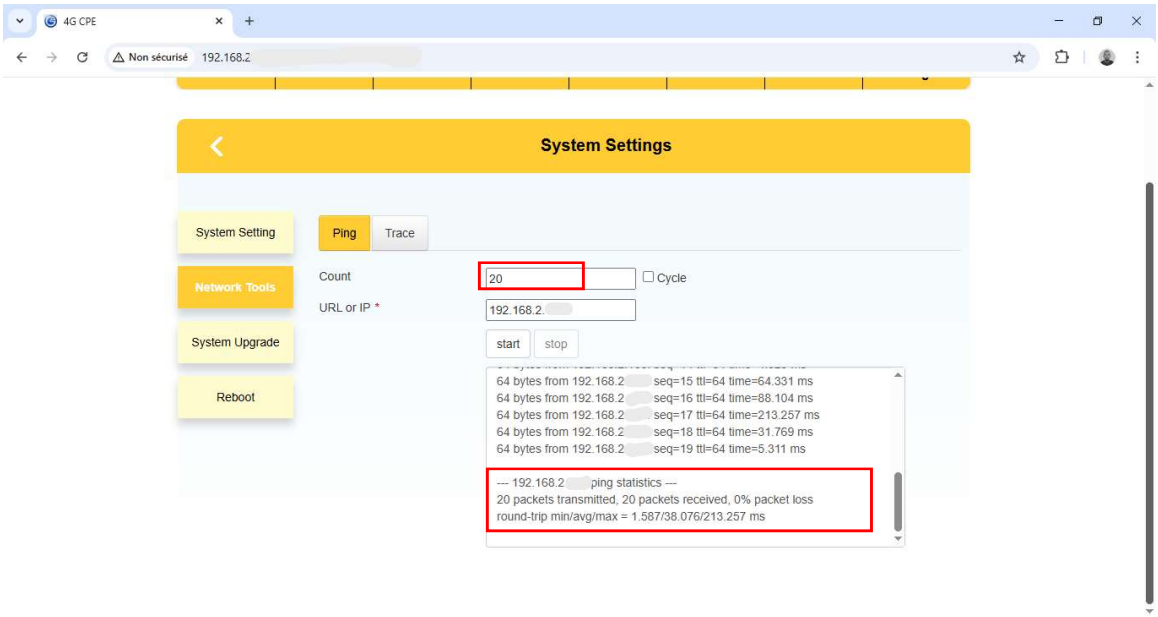
The architecture of my home network is composed of a PC, a mobile phone, and a Wifi Box from MTN.



Here are the equipment connected to the Wifi Box: 1 and 2.

Now let's try the Ping to see the connectivity :

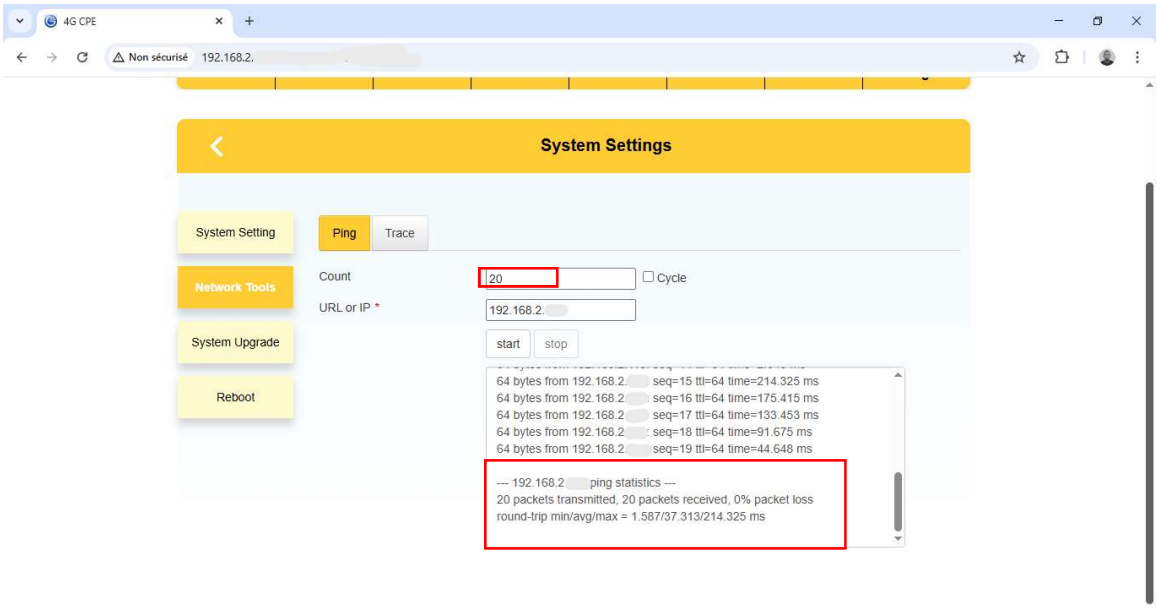
- The interface of the **Wifi Box** to the **PC**



Result: ---192.168.2.*** Ping Statistics----

20 packets transmitted, 20 packets received, 0% packets loss

- The interface from the **Wifi Box** to **the mobile phone**



Result: ---192.168.2.*** Ping Statistics----

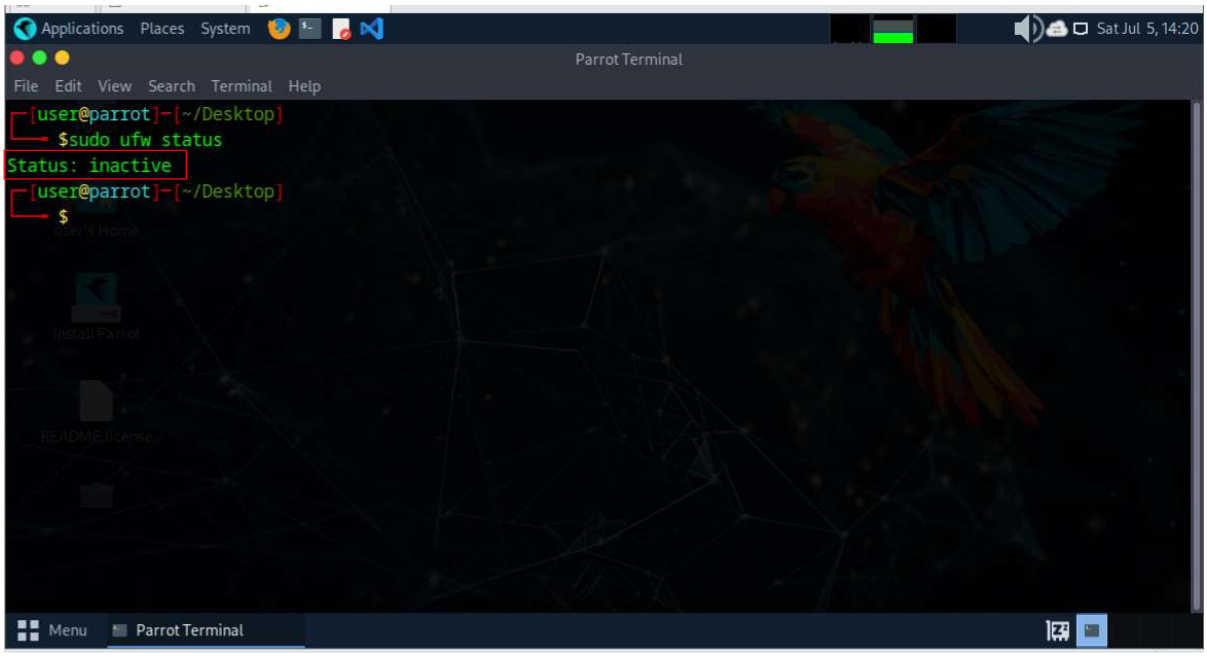
20 packets transmitted, 20 packets received, 0% packets loss

Enable and configure a basic firewall

Configuring ufw (Uncomplicated Firewall) on a Debian system with the Parrot OS GUI:

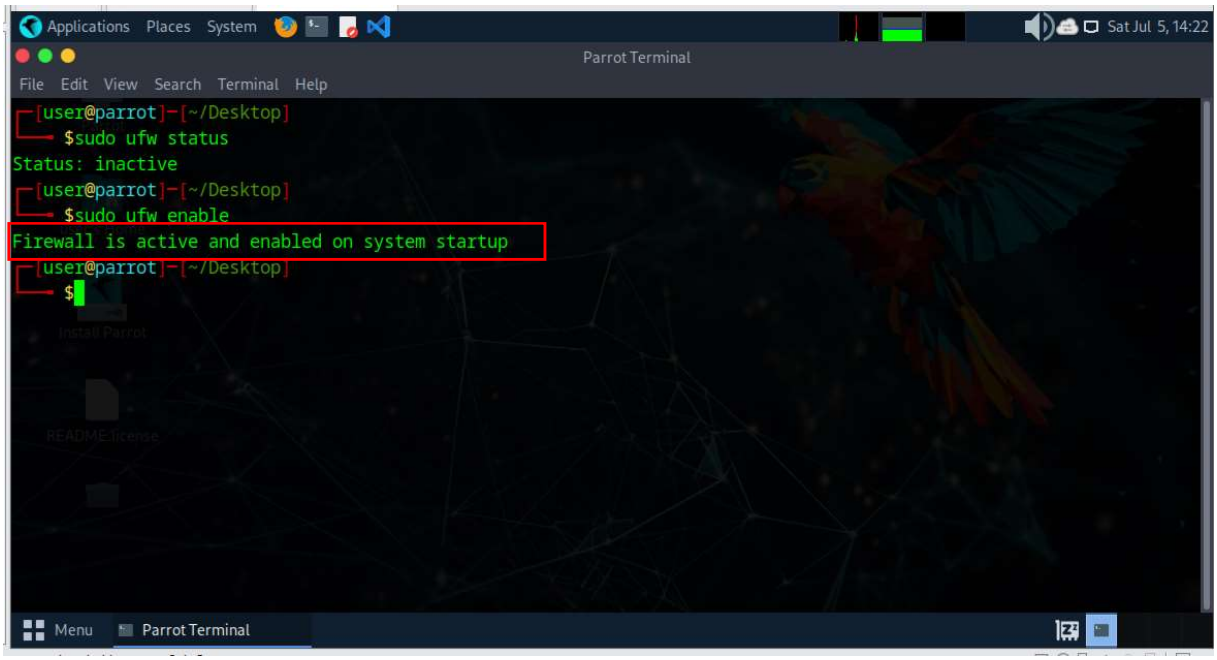
Enable and configure the UFW Firewall

- Open the terminal.
- Tape : `sudo ufw status` to check Firewall.



Status : Inactive,

- Tape : `sudo ufw enable`



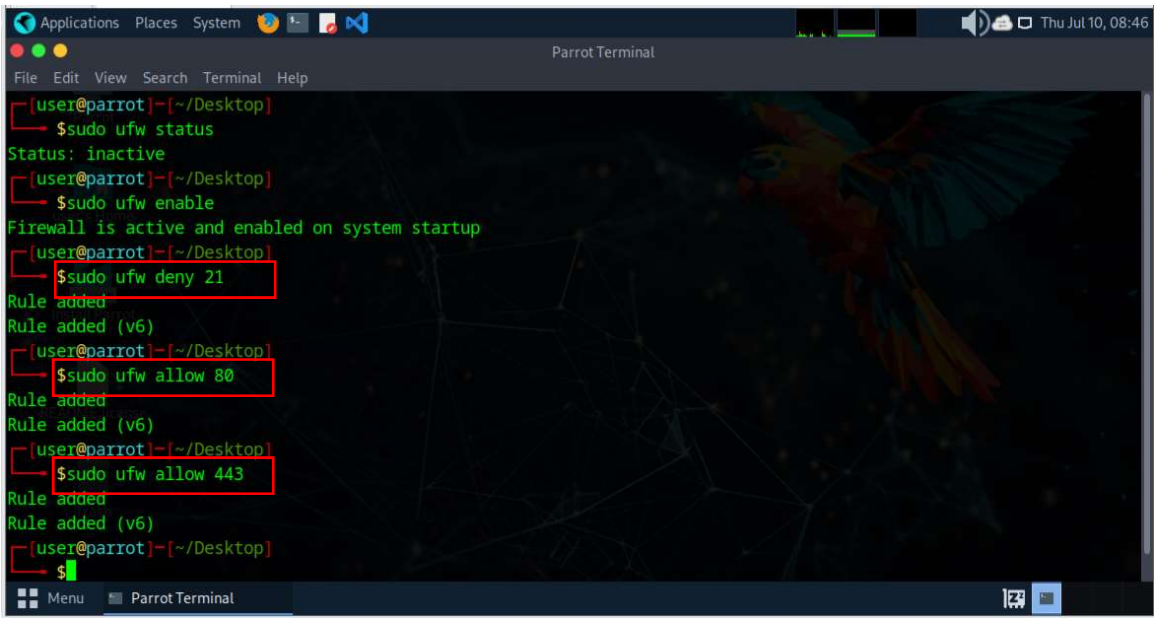
Firewall is active and enabled on system startup.

- Block an FTP port : `sudo ufw deny 21`
- Allows web traffic :
  `sudo ufw allow 80`

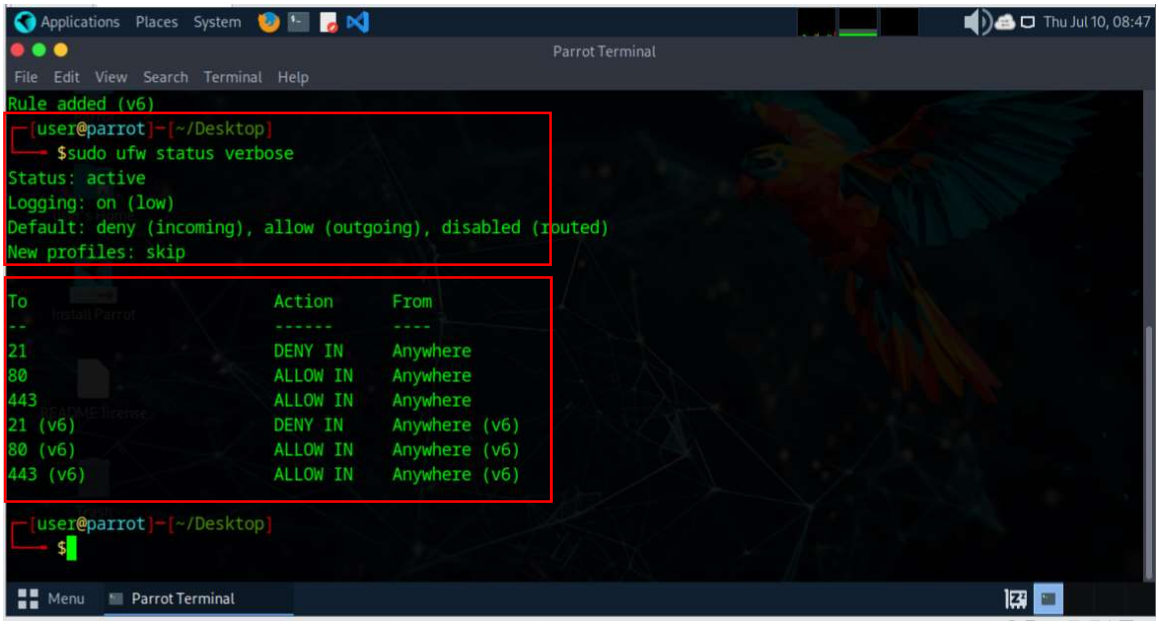
Allows inbound traffic on port 80 (HTTP).

`sudo ufw allow 443`

Allows inbound traffic on port 443 (HTTPS).



Tape : `sudo ufw status verbose` to view the current status of the firewall with details.

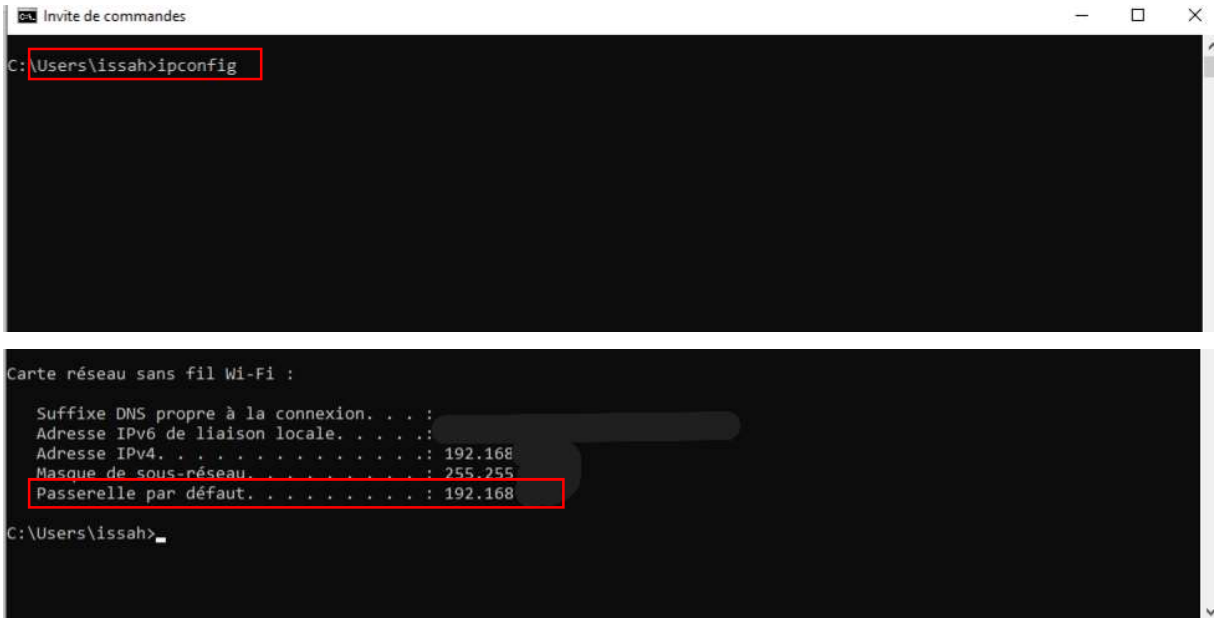


ACTIVE RULES:

Port	Action	From
21	DENY IN	Anywhere
80	ALLOW IN	Anywhere
433	ALLOW IN	Anywhere
21 (v6)	DENY IN	Anywhere (v6)
80 v6)	ALLOW IN	Anywhere (v6)
443 (v6)	ALLOW IN	Anywhere (v6)

Basic security configurations, such as changing default passwords.

To change the default password, we choose the network of the MTN Box that was configured previously. With the address of the default gateway of the network, we will go to the Chrome browser on Windows 10 home and before going to the browser, let's launch the terminal on Windows with the `ipconfig` command to identify the address of the default gateway, here is the step as follows :



Here are the details about the Wi-Fi wireless network card :

Connection-specific DNS suffix…..... :

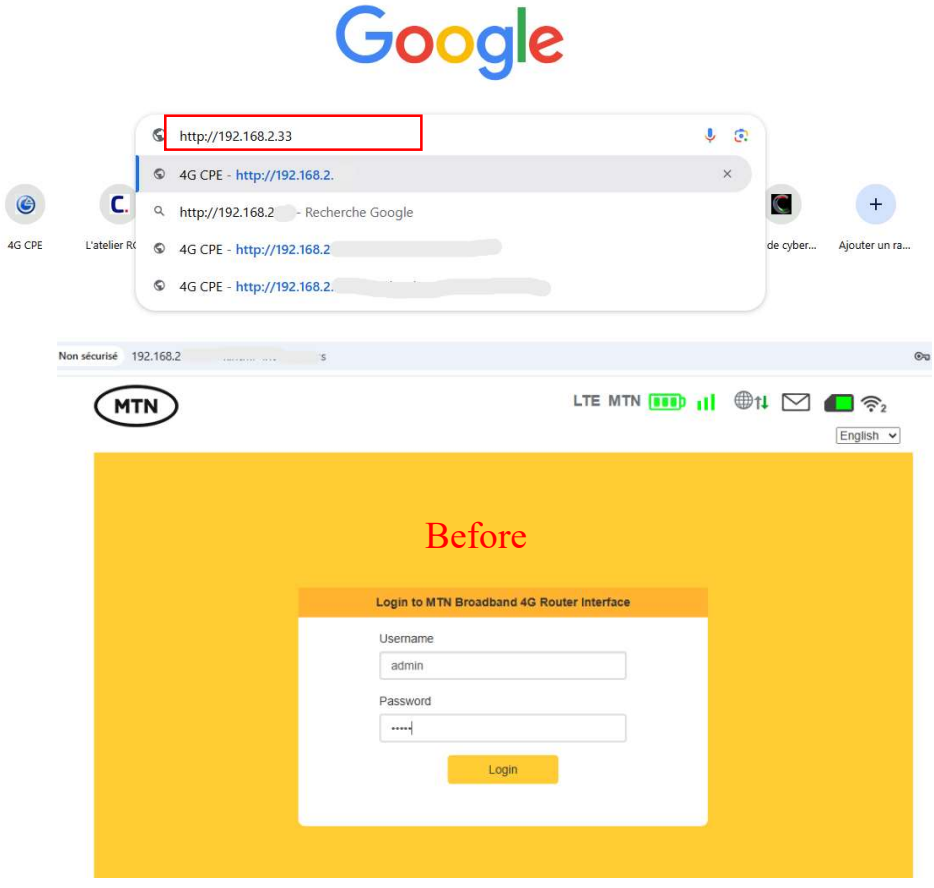
IPv6 address of the local link……. : **********

IPv4 address……: 192.168.***

Subnet mask…….... : 255.255.***

Default gateway……..: 192.168.***

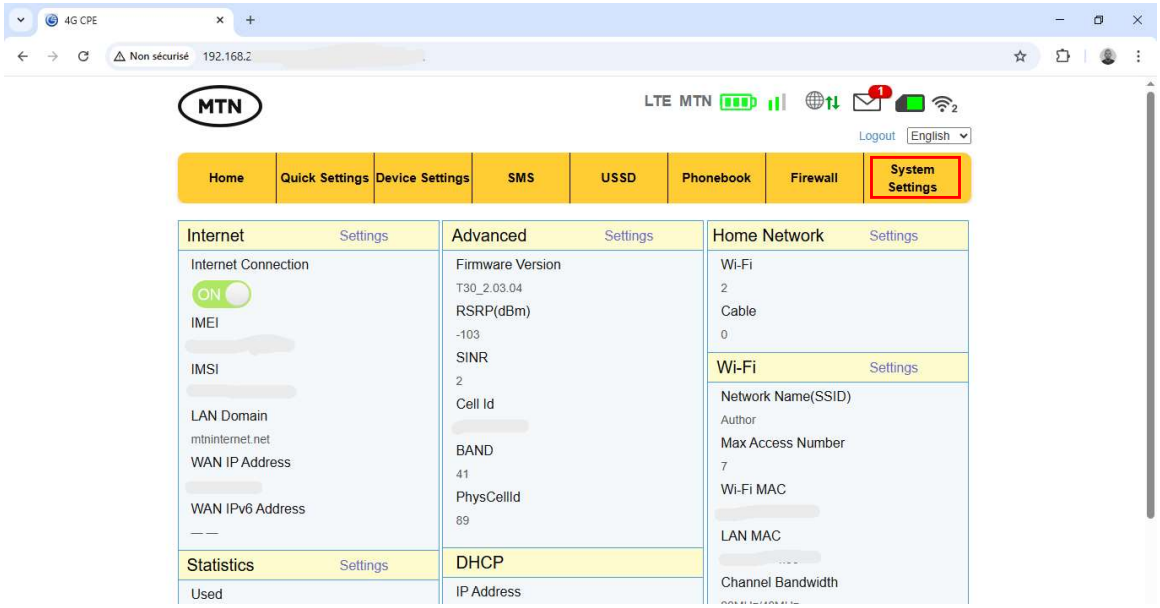
With the default gateway, go to the Chrome browser : http://192.168.***



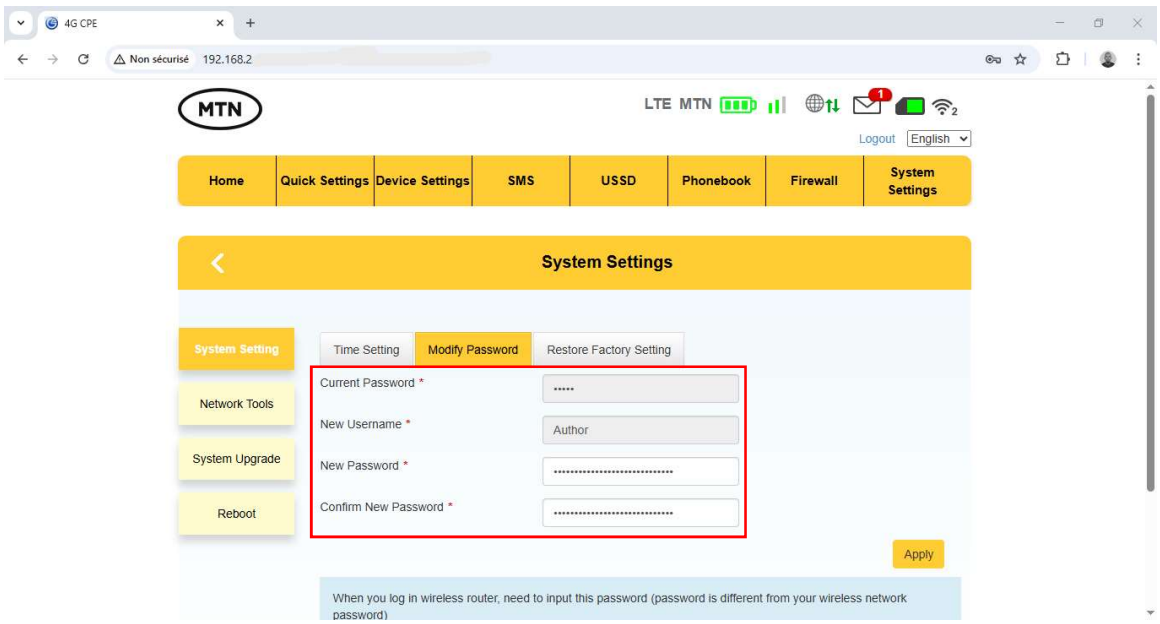
When displaying this interface above, the username and password are the default for each network device:

Username : admin

Password : admin



Under the system settings tab, you can change the default password.



The step continues as follows and choose a strong password consisting of uppercase and lowercase letters and the end of numbers and special characters.

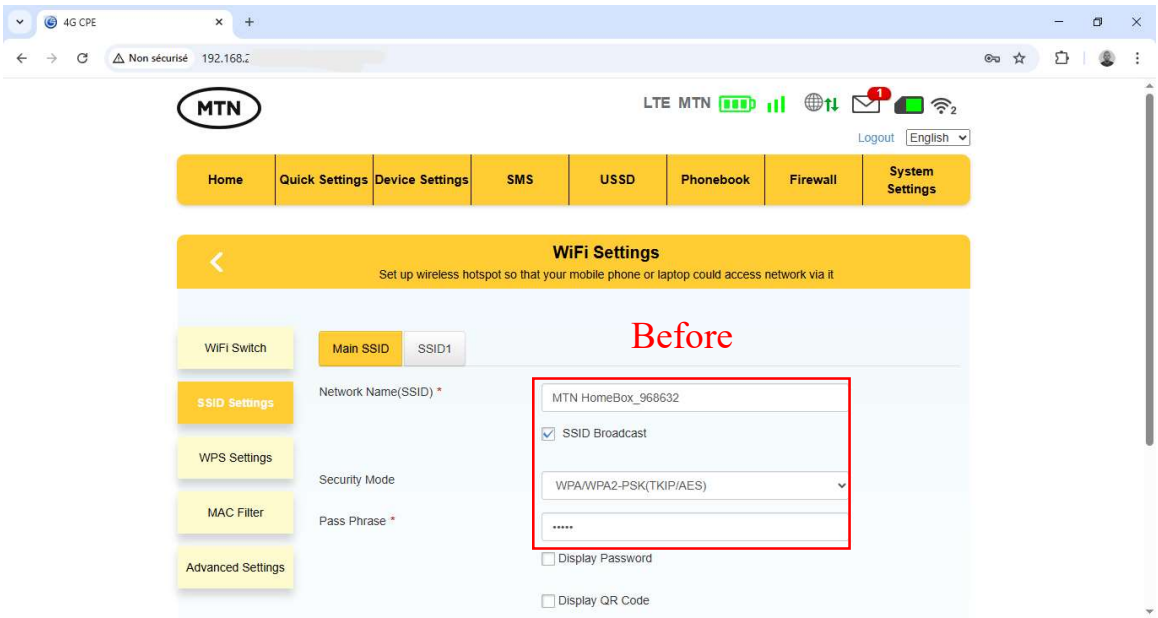
Current Password : admin
New Username : Author
New Password : ****************************
Comfirm New Password : ********************

L'activation du chiffrement réseau (WPA2 ou WPA3)

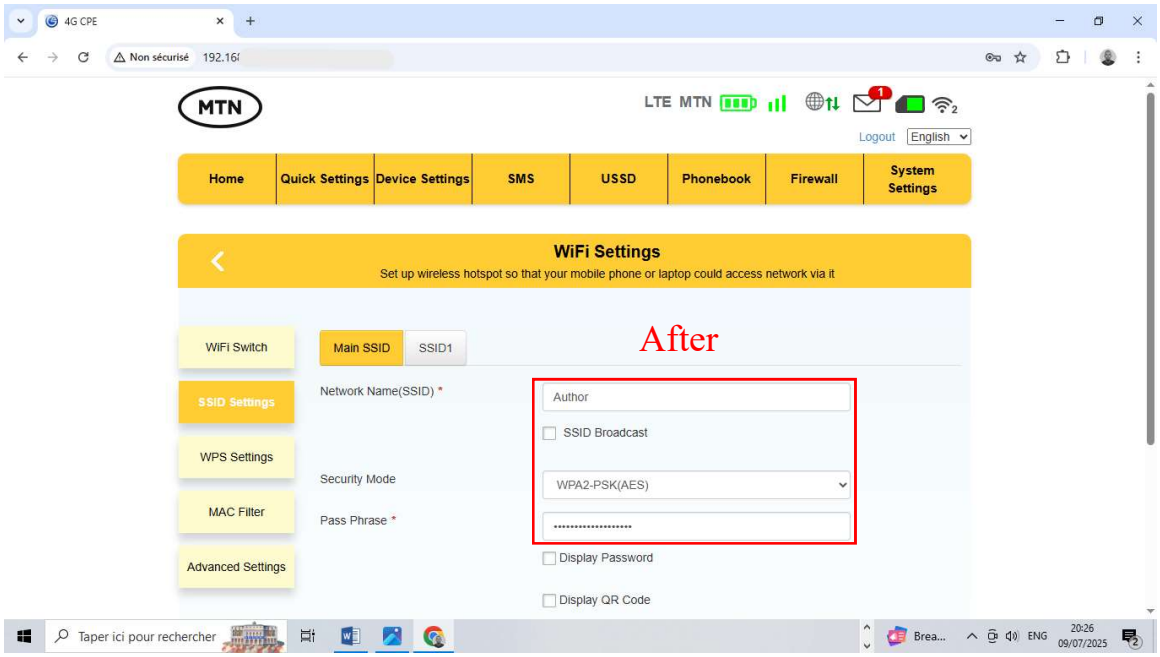
Click on the Wifi settings tab to change the default setting to enable network encryption for the interception of messages or resources that will be shared with attackers such as the man-in-the-middle attack.

Here is the default setting :

Some devices offer and even recommend this option in mixed mode. This option enables both WPA and WPA2, with TKIP and AES. This provides maximum compatibility with any older devices you may have, but it also allows an attacker to break into your network by cracking the most vulnerable WPA and TKIP protocols.

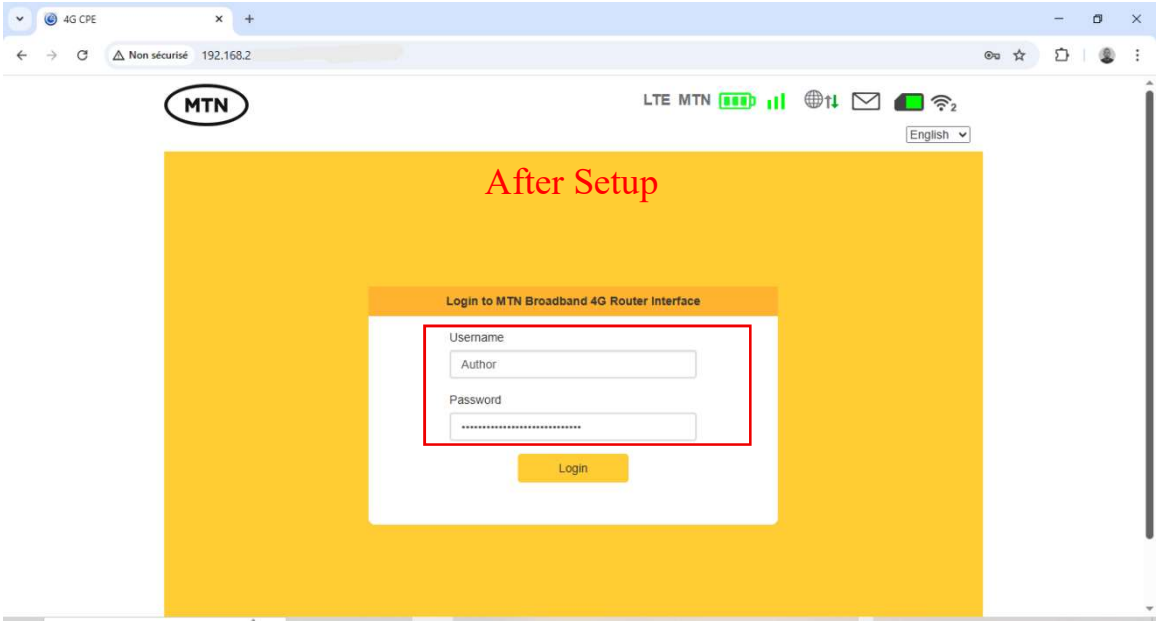


After setup, mixed encryption with more secure encryption.



This is the most secure option (outside of the new WPA3). It uses WPA2, the latest Wi-Fi encryption standard, and the latest AES encryption protocol. We need to use this option unless our Box supports WPA3 and then use it instead. On some devices, we'll only see the WPA2 or WPA2-PSK option. If we do, it will probably just use AES, as it is a common sense choice.

Final results after strengthening network security :



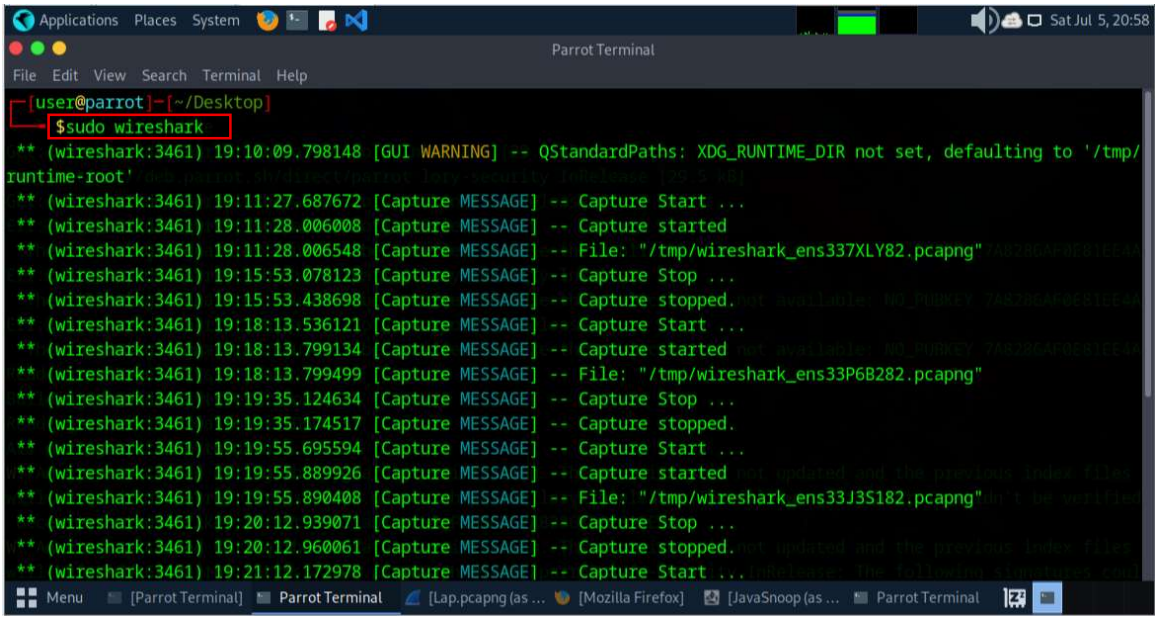
3) Monitor Network Traffic

Wireshark to capture and analyse network traffic

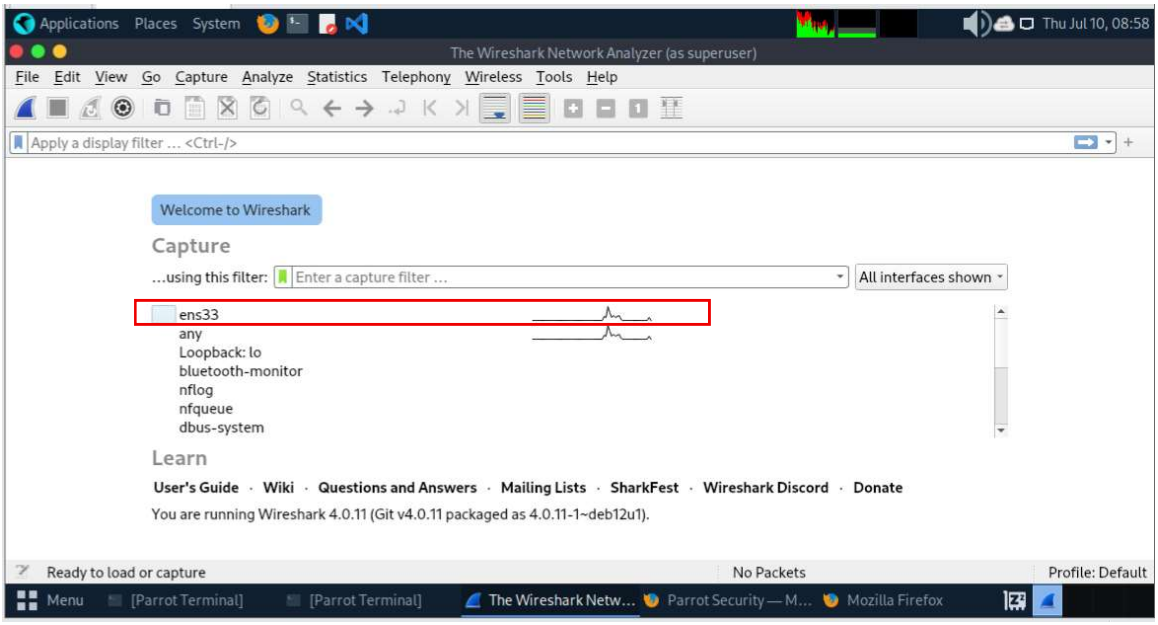
Wireshark is a free and open source package analyzer. It is used in computer network troubleshooting and analysis, protocol development, education, and reverse engineering.

Wireshark uses the Qt software library for its UI implementation and pcap for package capture; it works on many Unix-compatible environments such as GNU/Linux, FreeBSD, NetBSD, OpenBSD or Mac OSX, but also on Microsoft Windows. There is also a command-line version called TShark. These programs are distributed free of charge under the GNU General Public License.

Open Terminal : `sudo wireshark`



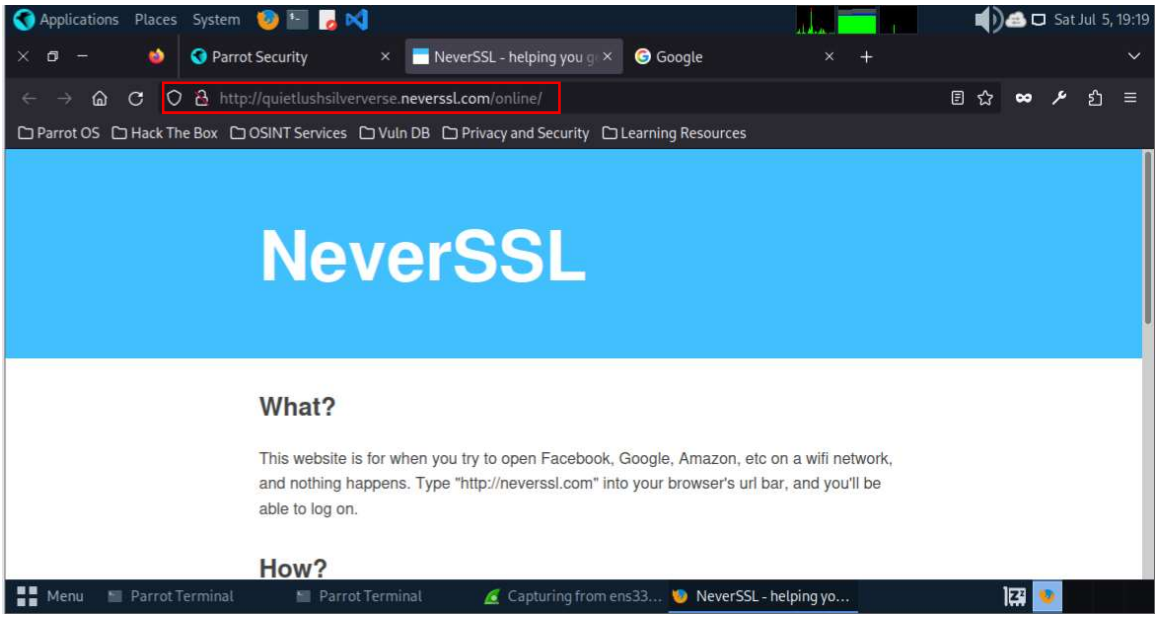
Once on the GUI, let's choose the interface for ens33 to start the analysis.

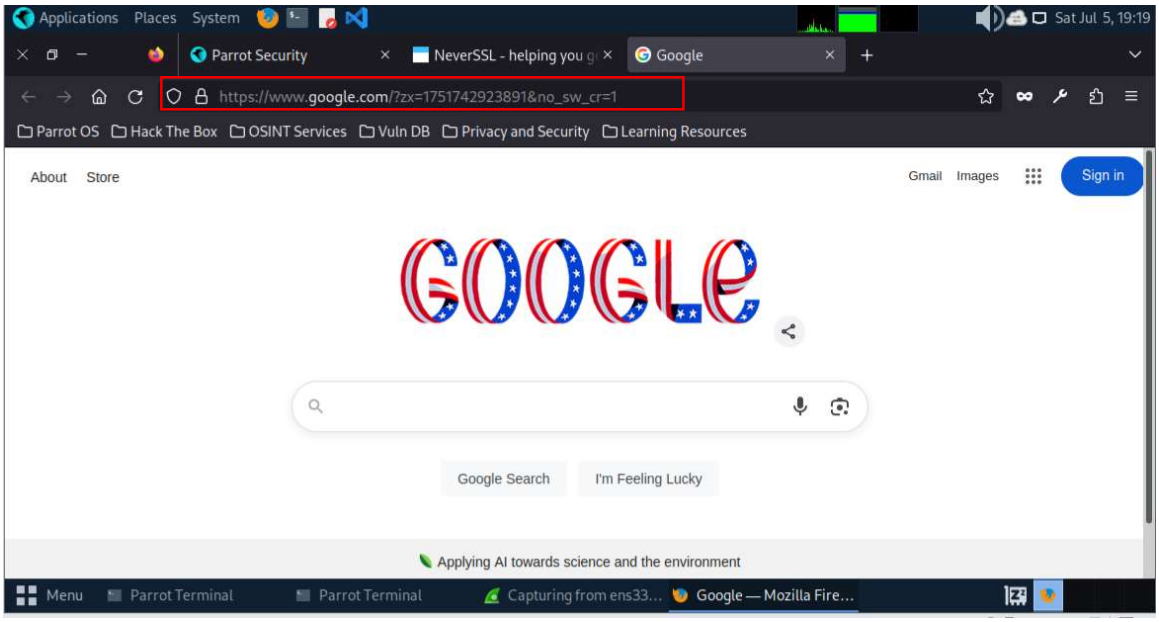


After choosing the ens33 interface, click start and then let's open Firefox, visit :

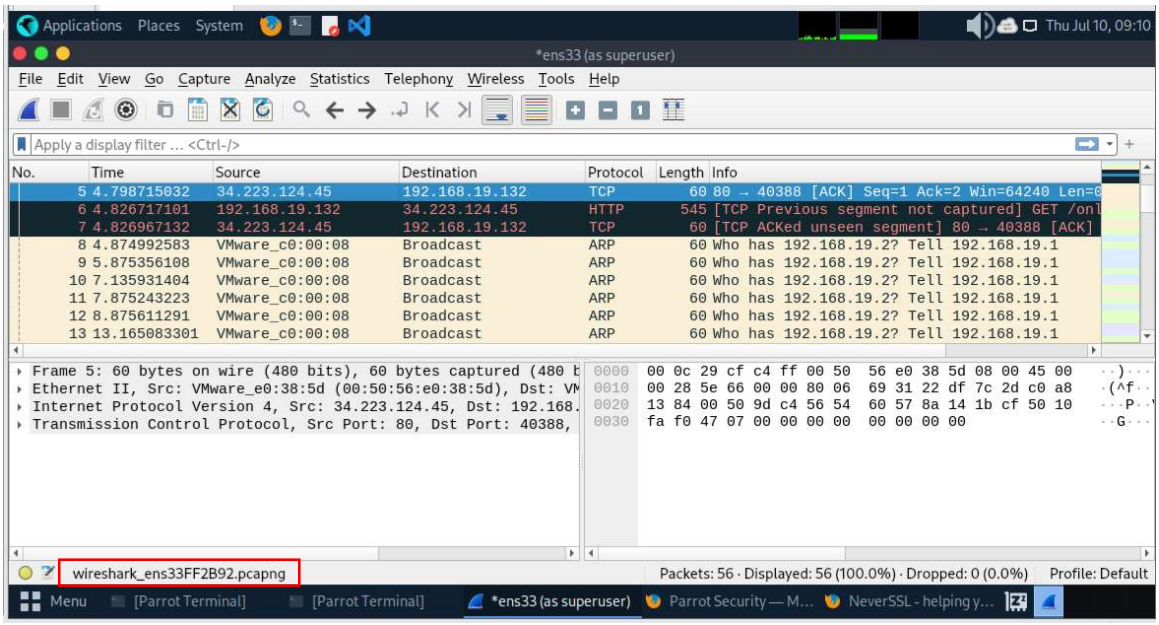
http://neverssl.com

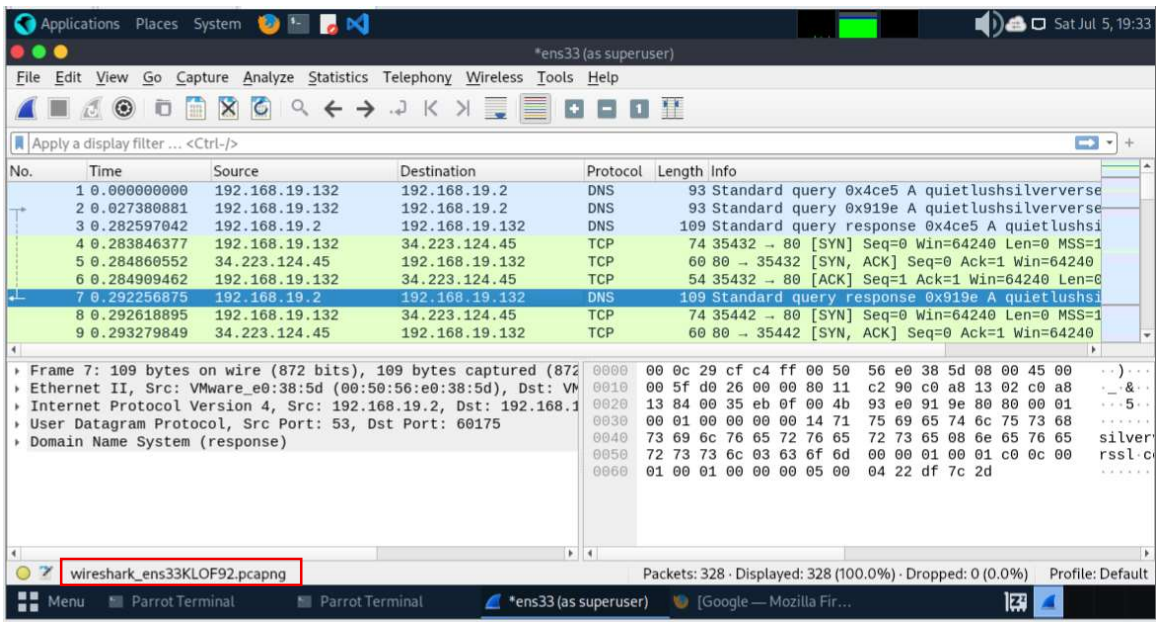
https://google.com

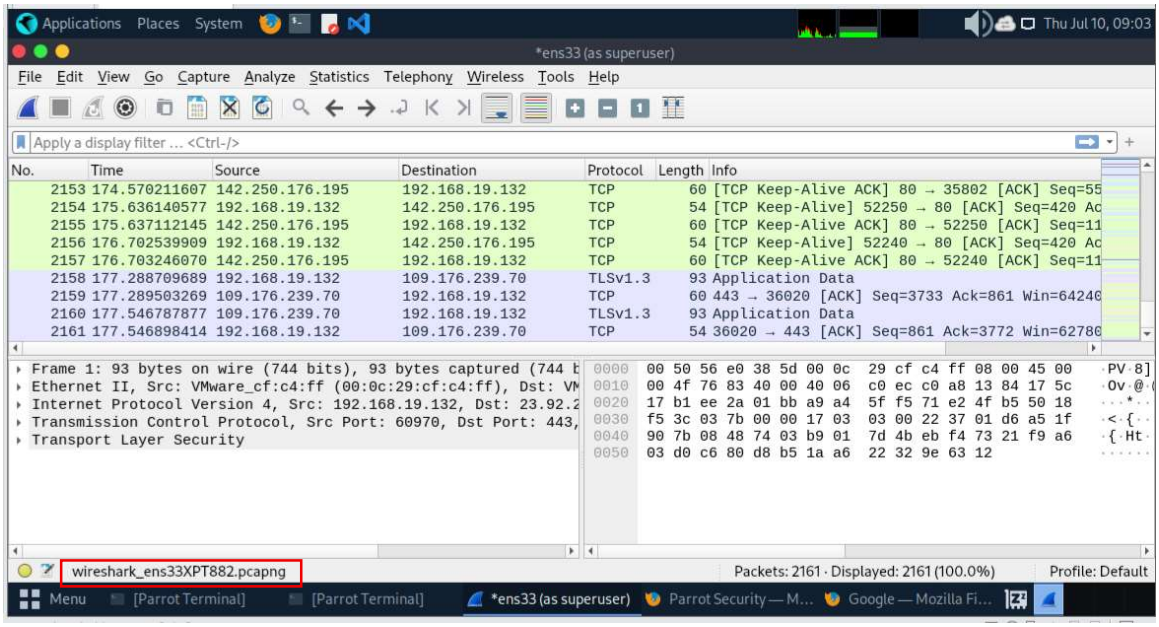




Let's go back into Wireshark, click stop to see the network traffic.







Identify different types of traffic, such as HTTP, DNS, and others, and understand what they mean

Based on the three Wireshark captures, several essential network protocols were observed:

- DNS (Domain Name System) – Port 53/UDP

Role : Resolves domain names to IP addresses.

Observed example : Requests to `quietlushsilverssl.com`, uncommon domain.

Note : Multiple DNS swaps in the ***ens33KLOF92.pcapng*** capture, showing a query followed by a response.

- HTTP (HyperText Transfer Protocol) – Port 80/TCP

Role: Unencrypted web communication (port 80).

Observed example: An HTTP `GET /onl` request was sent to the public IP address `34.223.124.45`, hosted on AWS

Problem: Insecure request (lack of TLS), i.e. the traffic is in the clear without encryption, potentially exposing sensitive data to sniffing or MITM attacks.

- TCP (Transmission Control Protocol)

Role: Establish a reliable connection between two hosts.

Observation: Full TCP handshake (`SYN`, `SYN-ACK`, `ACK`) captured. Other packets show anomalies such as :

`TCP Previous segment not captured`

`TCP ACKed unseen segment`

Hypothesis: This could be packet loss or malicious fragmentation used to bypass detection.

- TLSv1.3 (Transport Layer Security) – Port 443/TCP

Role : Encrypts HTTPS communications.

Example observed : Active sessions in ***ens33XPT882.pcapng capture*** with *Application Data* visible (encrypted content).

Security : This type of traffic is legitimate, but cannot be analyzed without decryption.

- ARP (Address Resolution Protocol)

Role: Associates IP addresses with MAC addresses.

Observation : Frequent ARP queries (Who has `192.168.19.27` ?).

Possible Issue : A high frequency of ARP requests may signal an attempt to network reconnoitre, spoofing, or ARP scanning.

Detection of Suspicious or Anomalous Traffic

Suspicious behaviors detected:

TYPE OF TRAFFIC	ANOMALIE DETECTEE	POTENTIAL RISK
DNS	Unknown domain (`quietlushsilverssl.com`)	Malware C2
HTTP	Unencrypted request	Data leakage, interception
TCP	Missing or unseen segments	Evasion via fragmentation
ARP	High request frequency	Network reconnaissance or spoofing

Main Threats Identified :

Communication with Suspicious Domain

- `quietlushsilverssl.com` may be DGA-generated by malware.
- Possibly used for Command & Control (C2) communication.

Use of HTTP Instead of HTTPS

- Plaintext requests expose sensitive data.
- Enables attacks like session hijacking or MITM.

Anomalous TCP Packets

- Indicates potential for malicious packet manipulation.
- Could be used to hide payloads from IDS/IPS systems.

Frequent ARP Requests

- May signal internal ARP spoofing, MITM, or host discovery scan.

Security Measures Implemented :

SECURITY MEASURE	JUSTIFICATION
UFW Firewall	Block incoming/outgoing traffic to suspicious Ips.
Block unused ports	Reduce network attack surface.
DNS filtering (Pi-hole / DoH)	Prevent requests to malicious domains.
ARP monitoring (DAI)	Detect and block ARP spoofing attempts.
Enforce HTTPS	Secure data transmission and prevent eavesdropping.
Regular Wireshark analysis	Early detection of anomalies or potential threats.

How These Measures Help Protect the Network

These measures allow us to:

- Quickly identify non-compliant or dangerous traffic (unknown DNS requests).
- Block communication to external malicious domains or servers.
- Prevent internal attacks, such as ARP spoofing or scanning.
- Ensure data confidentiality through enforced encryption.
- Mitigate TCP-based attacks and recognize fragmentation/evasion techniques.

4) REFLECT ON SECURITY BEST PRACTICES

Cybersecurity awareness is understanding the potential dangers posed by technology and the knowledge of how to use technology securely and safely to protect individuals, organizations, and societies. It encompasses the understanding of the importance of protecting sensitive data and systems from cyberattacks, the recognition of potential cyber threats, and the adoption of safe practices to prevent or mitigate such threats. Cybersecurity Awareness is essential for individuals and organizations to stay protected in today's digital age.

The rapid development of technology and the methods we use to communicate and share information with friends, family, and colleagues has increased the possibility of cybersecurity breaches.

Opportunities to steal data from personal and work devices are easier for online criminals when we do not safeguard networks, devices, and applications. Cybercriminals take advantage of stealing information from a wide variety of sources including (but not limited to) social media posts, email, and online business transactions conducted at the local coffee shop or gas station.

Using strong passwords to prevent threats against the privacy and security of the data associated with your information, your company, and your customers are necessary to achieve password security and, thus, information security

MFA is a way of authenticating an individual's identity using two components before they gain access. The idea behind this process is that although an imposter has one piece of the victim's identifying information, they most likely don't have two.

Instead of merely protecting your account with a username and password, you also obtain verification through phone, email, text, or specialized PIN numbers. Even if someone gets your password, they still won't be able to access the account without having access to your MFA information.

Examples of information that can be used for authentication purposes include:

- SMS code
- Text code
- Key
- Password
- Fingerprint
- Token
- Voice recognition

Public Wi-Fi networks are less secure and more vulnerable to attack than private Wi-Fi. Never enter private data when using public Wi-Fi.

- Use a secure virtual private network (VPN) in public areas to protect information
- Remember to shield your screen from shoulder surfers when entering sensitive information
- Use the best practices to increase your safety when in a café, hotel, or other public space

You can use alternatives to public Wi-Fi if the networks available to you feel unsafe. Consider the following public Wi-Fi alternatives:

Personal hotspot :
A personal hotspot is your own private, secure network connection. You can often connect to your phone's hotspot using cellular data and battery. Or you can buy a separate mobile device to connect to your hotspot.

Cellular network :
You can also use your phone to connect to the Internet directly through your cellular network. In general, cellular data is safer than an unsecured Wi-Fi connection.

The more detail we share online, the easier it is to hack into someone's digital profile.

The more we reuse passwords on multiple platforms, the faster our identity can be stolen.

Think of this as leaving a key to your home with an address everywhere you visit.

Standard disclosures we share should not include the following:

- Date of birth
- City of birth
- Have you invited people to any activities at your home that includes specific details about where you live?
- Phone number or email address
- Social Security, passport, or driver's license numbers
- Bank, loan, or credit card information
- School, family, or work information
- Car information

The first step in Cybersecurity Awareness is to protect your PII.

Think about your Facebook or related social media profile. Have you ever manually changed *Settings* to minimize public disclosure of PII?

- Only volunteer information that is vital for social media use
- Never post about your birthdate and turn off social reminders
- Never post your home address. Sometimes cybercriminals work with physical thieves that target homes, workplaces, and cars and watch movements like stalkers
- Minimize the information you can see if the viewer is not a connection
- Do not provide check ins of your whereabouts during business or personal trips

And finally, updating equipment and the use of anti-virus software is essential to maintain the system against threats and avoid the theft of sensitive information.

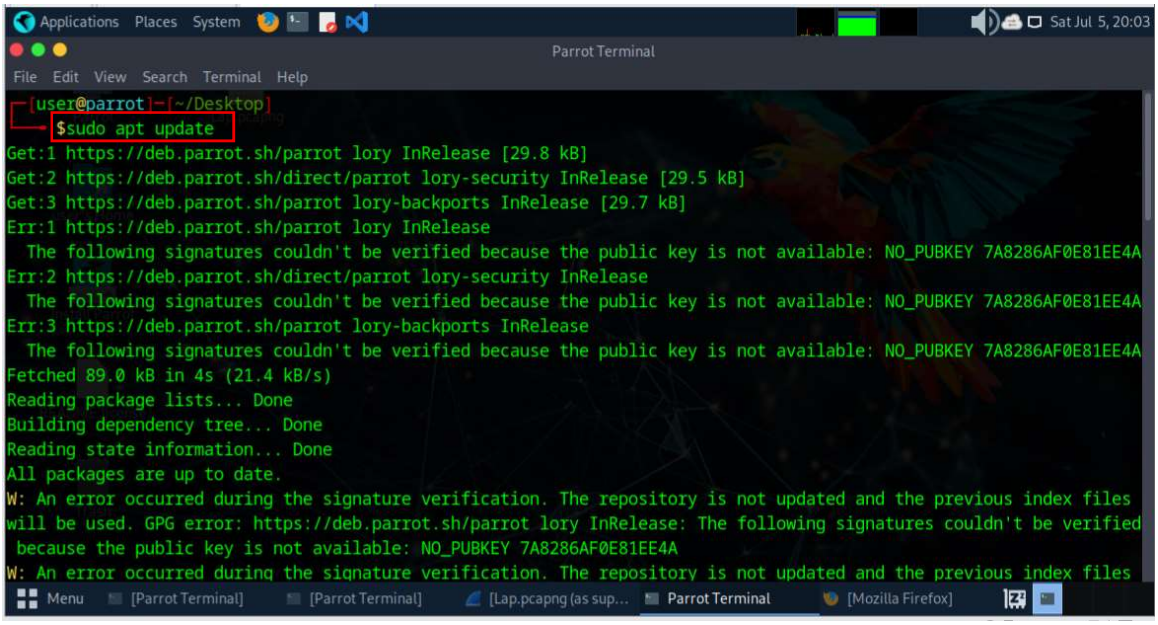
II. TASK 2 : INTRODUCTION TO WEB APPLICATION SECURITY

1) Setup

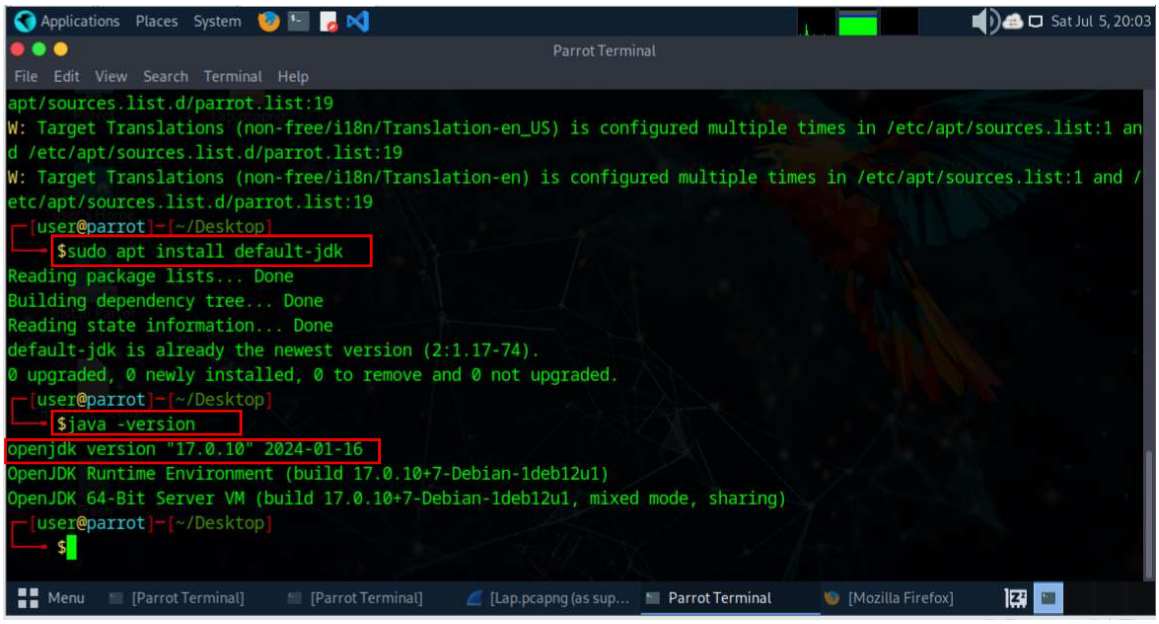
Install and set up WebGoat and Java

Install Java under Parrot, open the terminal:

```
sudo apt update
```



`sudo apt install default-jdk`

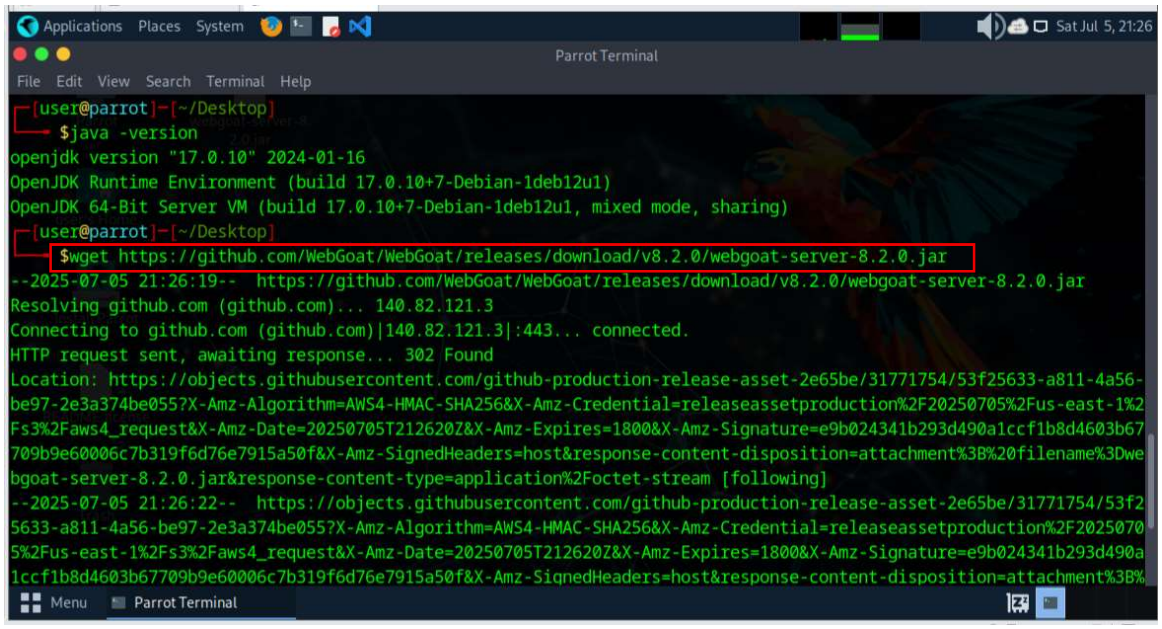


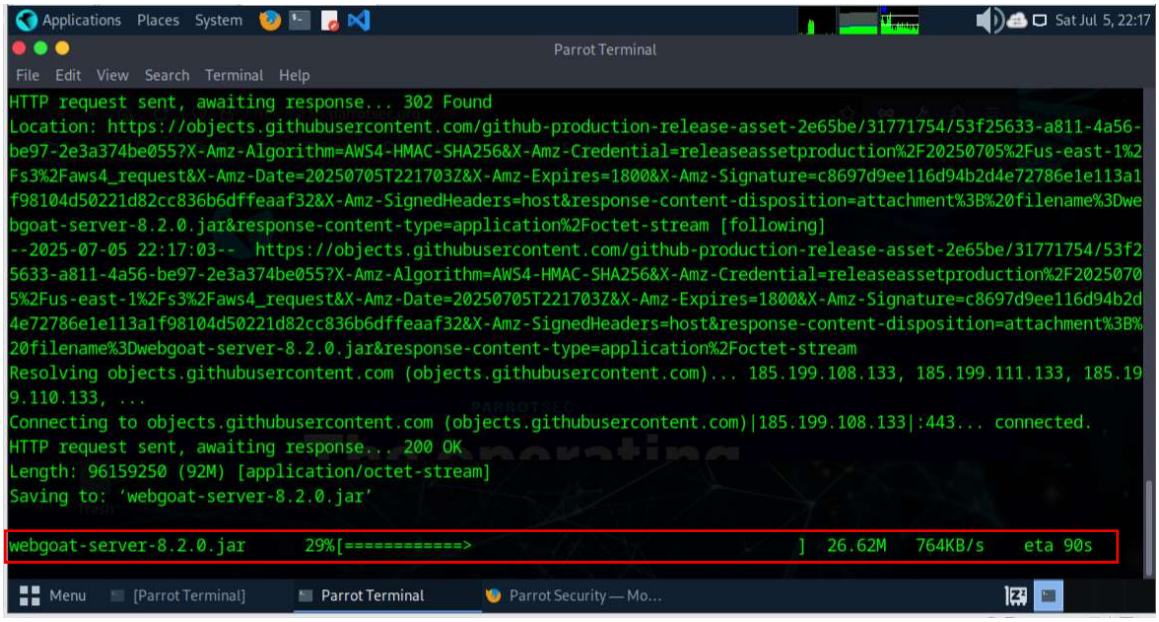
Verify installation : `java -version`

Result : `openjdk version "17.0.10" 2024-01-16`

Download WebGoat on the Parrot terminal :

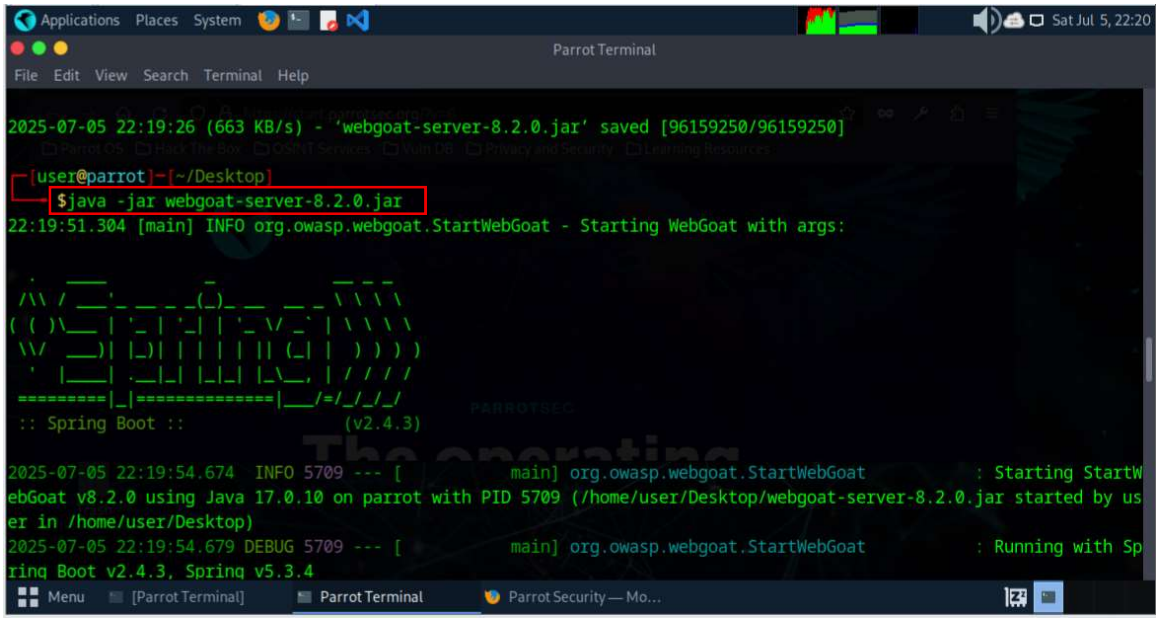
`Wget`https://github.com/WebGoat/WebGoat/releases/download/v8.2.0/webgoat-server-8.2.0.jar



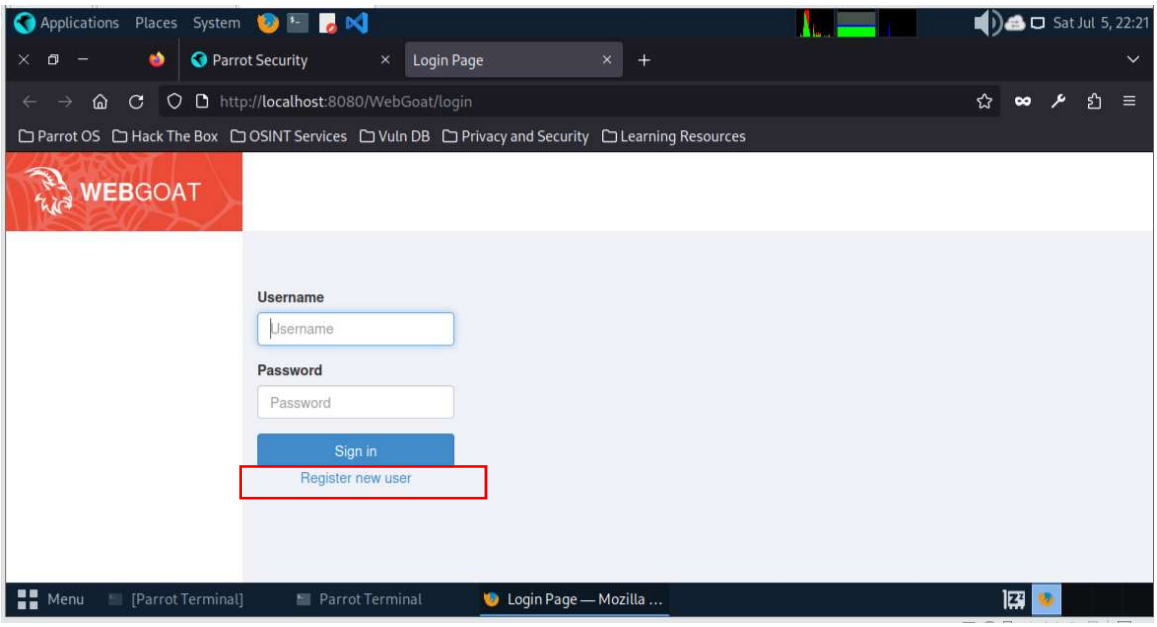


Let's launch WebGoat :

```
java -jar webgoat-server-8.2.0.jar
```



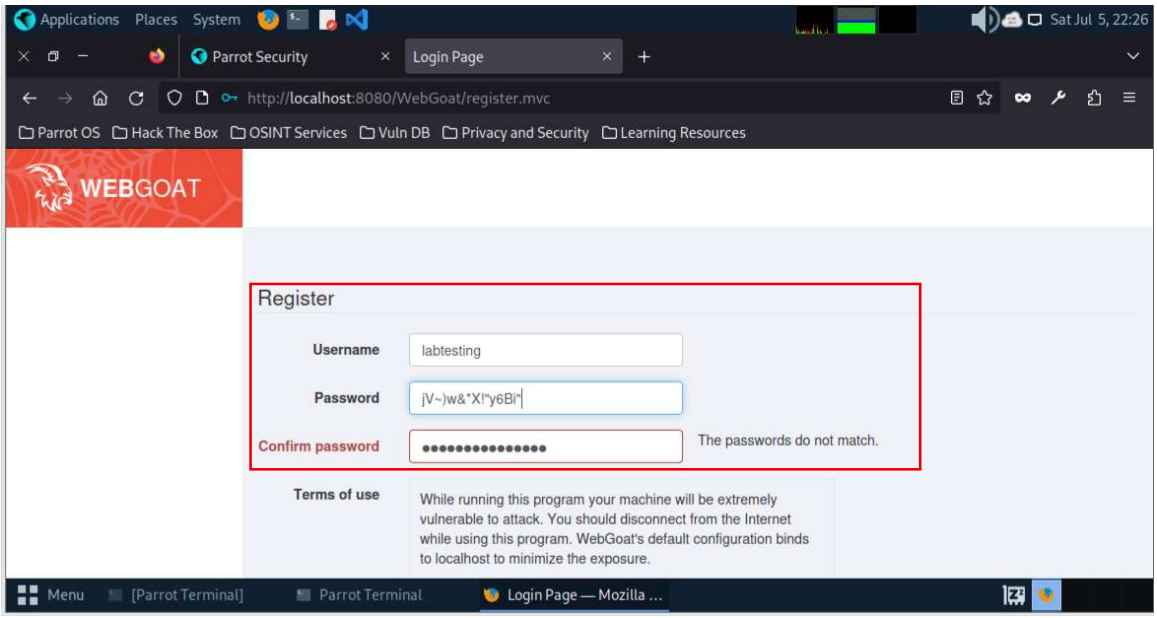
Accède via Firefox à : http://localhost:8080/WebGoat



Register :

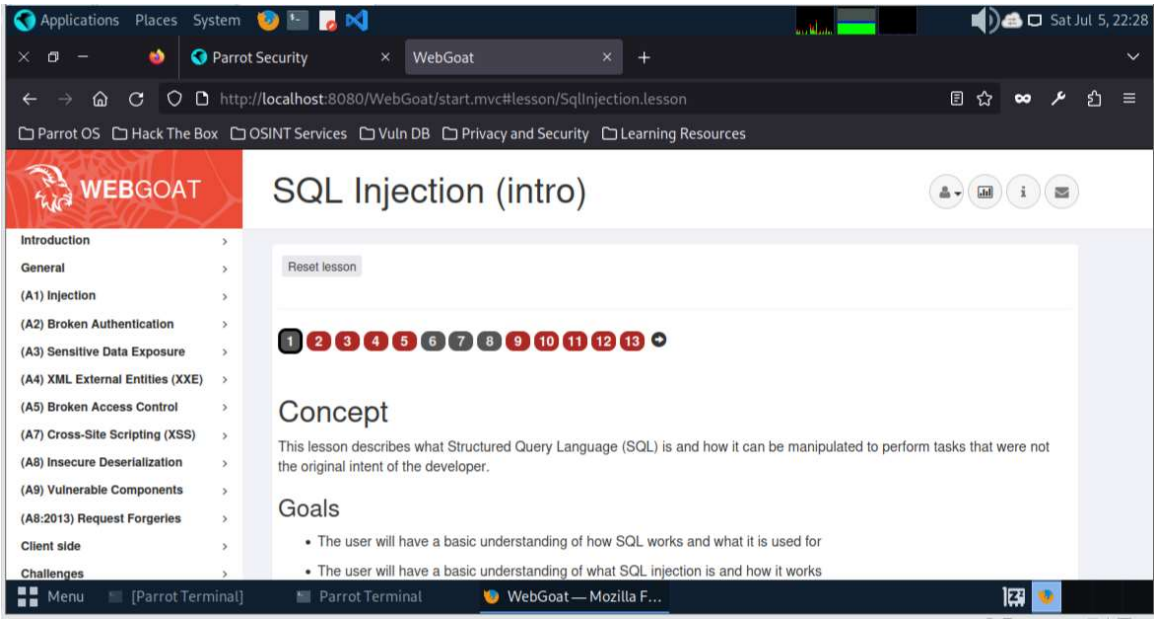
Username : labtesting

Password : jV-)w&*X!''y6Bi''

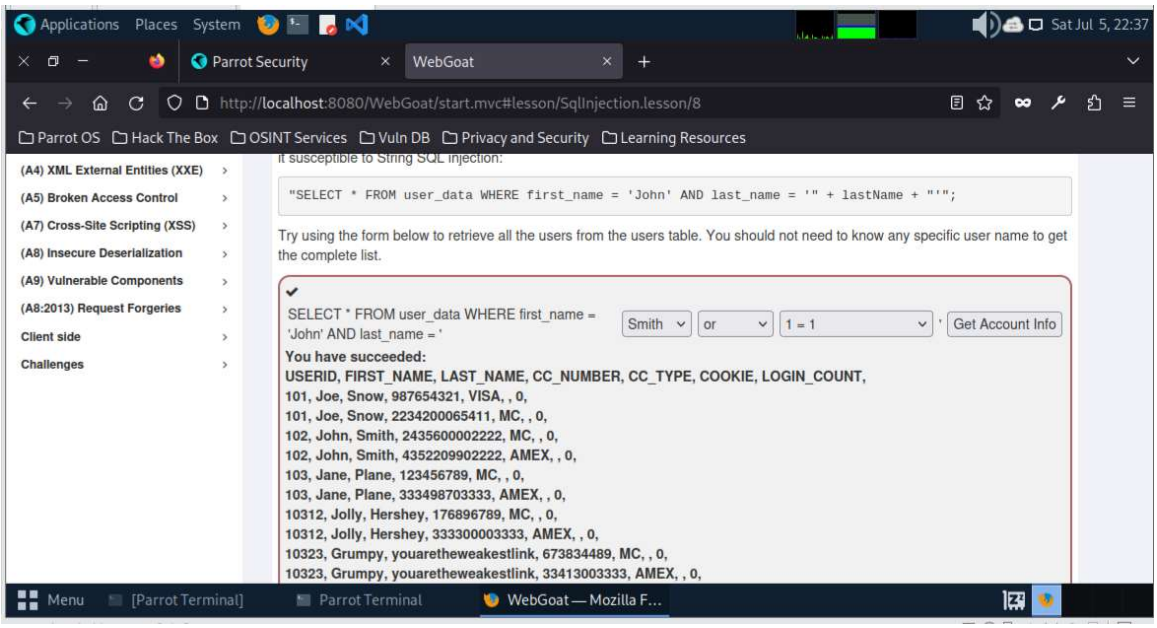


SOL Injection :

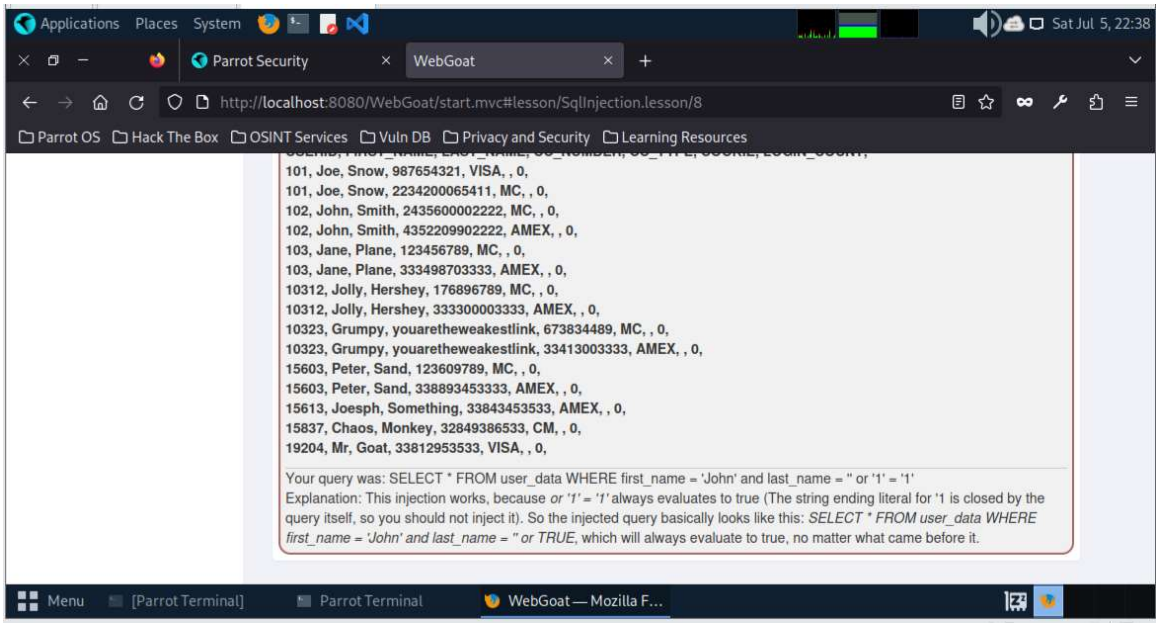
SQL is a standardized (ANSI in 1986, ISO in 1987) programming language which is used for managing relational databases and performing various operations on the data in them. A database is a collection of data. The data is organized into rows, columns and tables, and indexed to make finding relevant information more efficient.

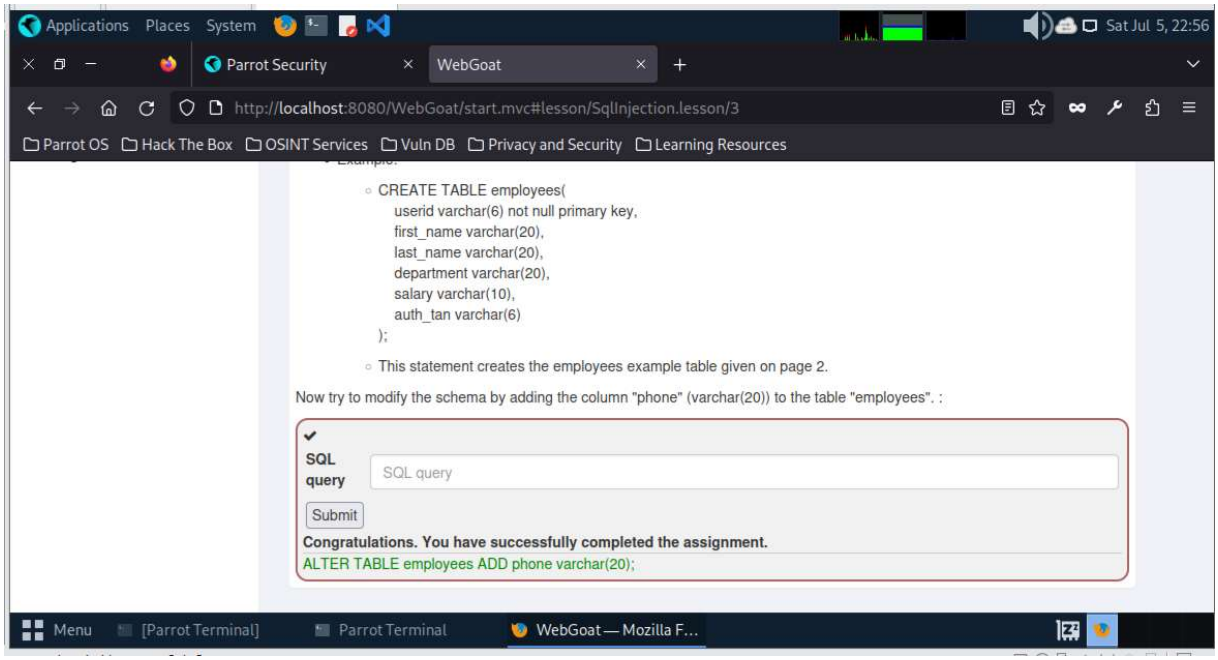


Injecting a SQL command via form (' OR '1'='1).

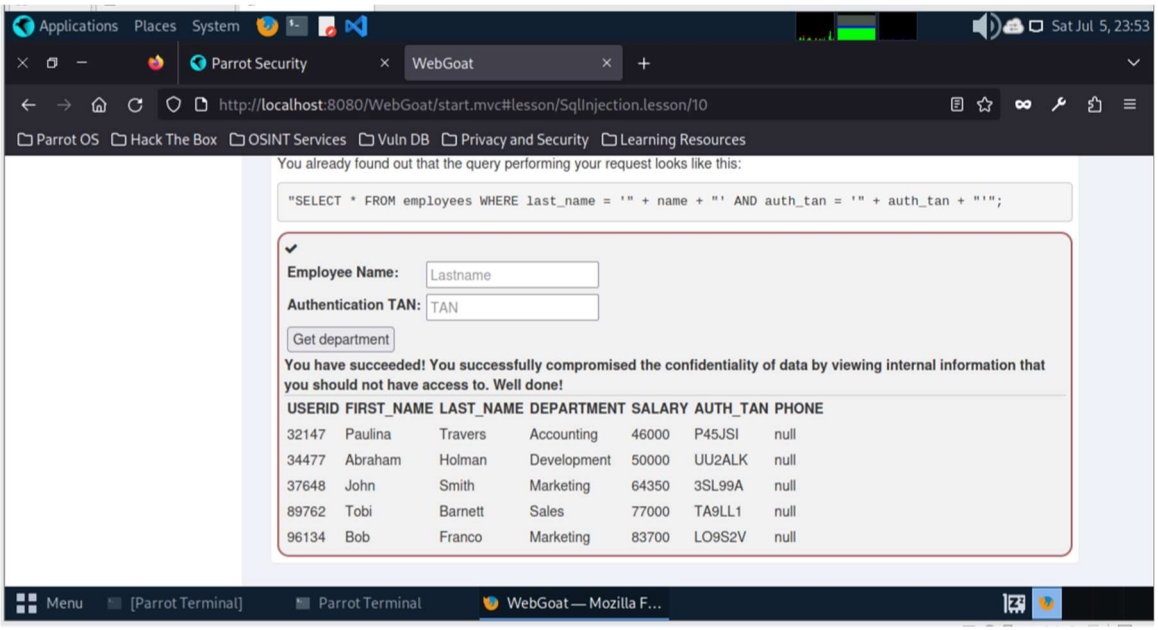


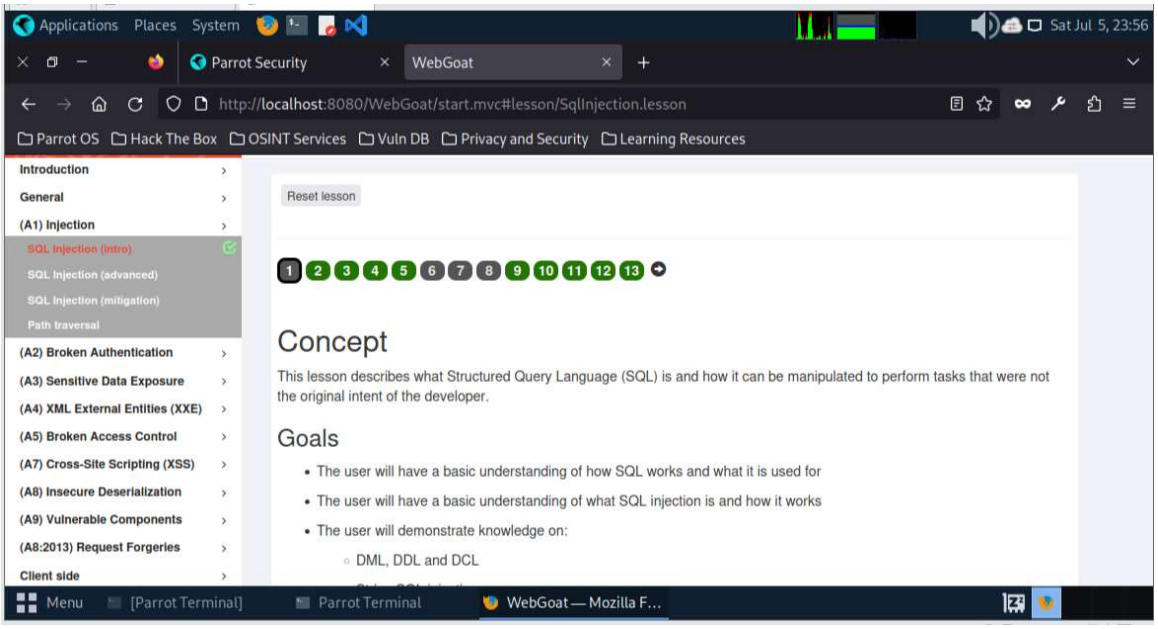
The continuation of the previous form :





SQL query : ALTER TABLE employees ADD phone varchar(20);





What is XSS?

Cross-Site Scripting (also commonly known as XSS) is a vulnerability/flaw that combines the allowance of html/script tags as input that are rendered into a browser without encoding or sanitization.

Cross-Site Scripting (XSS) is the most prevalent and pernicious web application security issue

While there is a simple well-known defense for this attack, there are still many instances of it on the web. In terms of fixing it, coverage of fixes also tends to be a problem. We will talk more about the defense in a little bit.

XSS has significant impact :

Especially as 'Rich Internet Applications' are more and more commonplace, privileged function calls linked to via JavaScript may be compromised. And if not properly protected, sensitive data (such as your authentication cookies) can be stolen and used for someone else's purpose.

Quick examples:

From the JavaScript console in the developer tools of the browser (Chrome, Firefox)

alert("XSS Test");

alert(document.cookie);

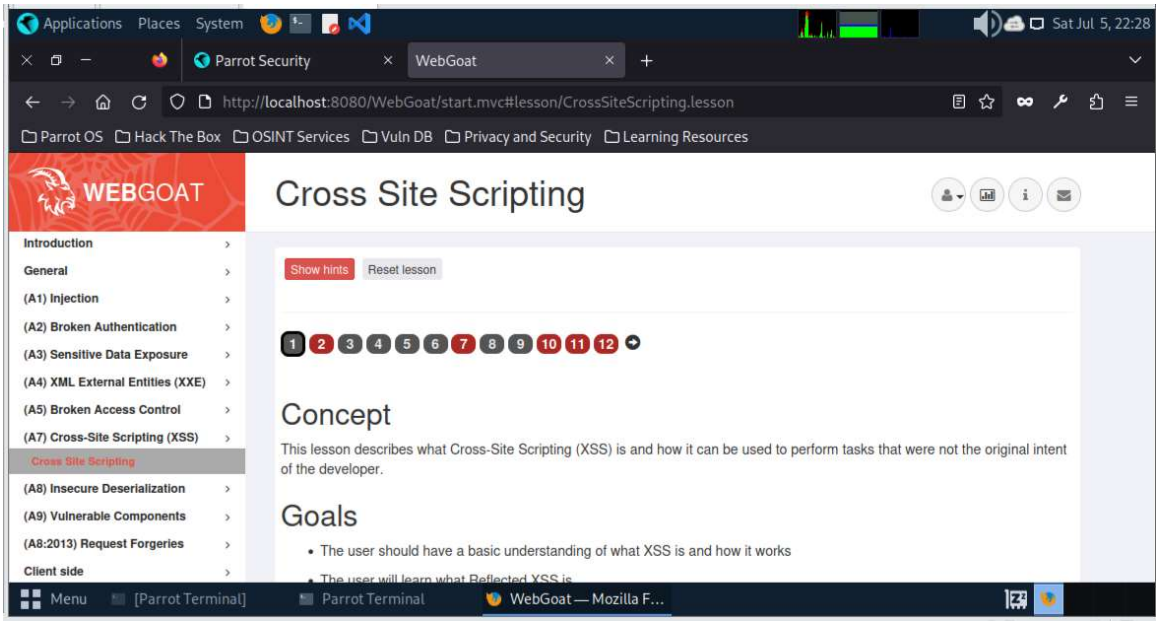
Any data field that is returned to the client is potentially injectable

<script>alert("XSS Test")</script>

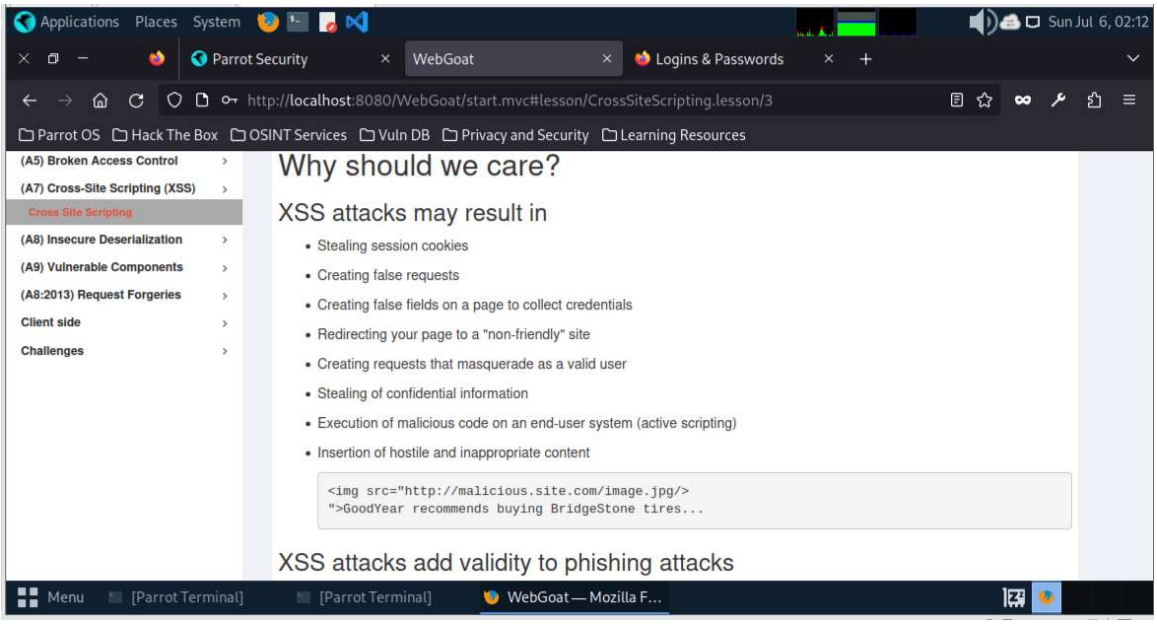
Try It! Using Chrome or Firefox

Open a second tab and use the same url as this page you are currently on (or any url within this instance of WebGoat)

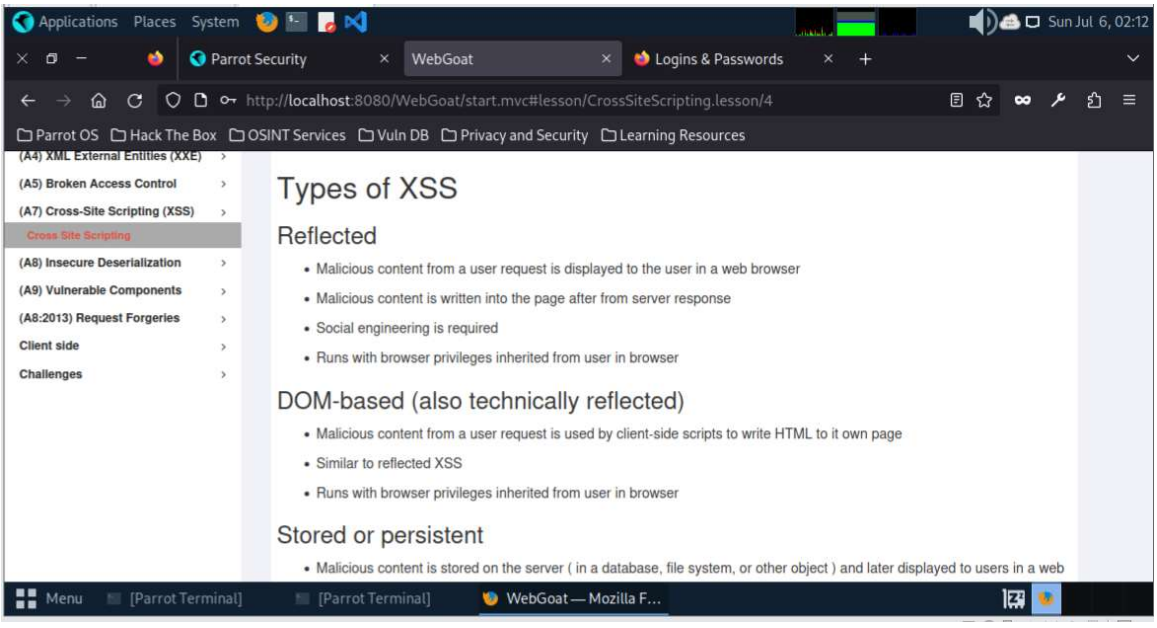
Then, on that second that open the browser developer tools and open the javascript console. And type: alert(document.cookie); .



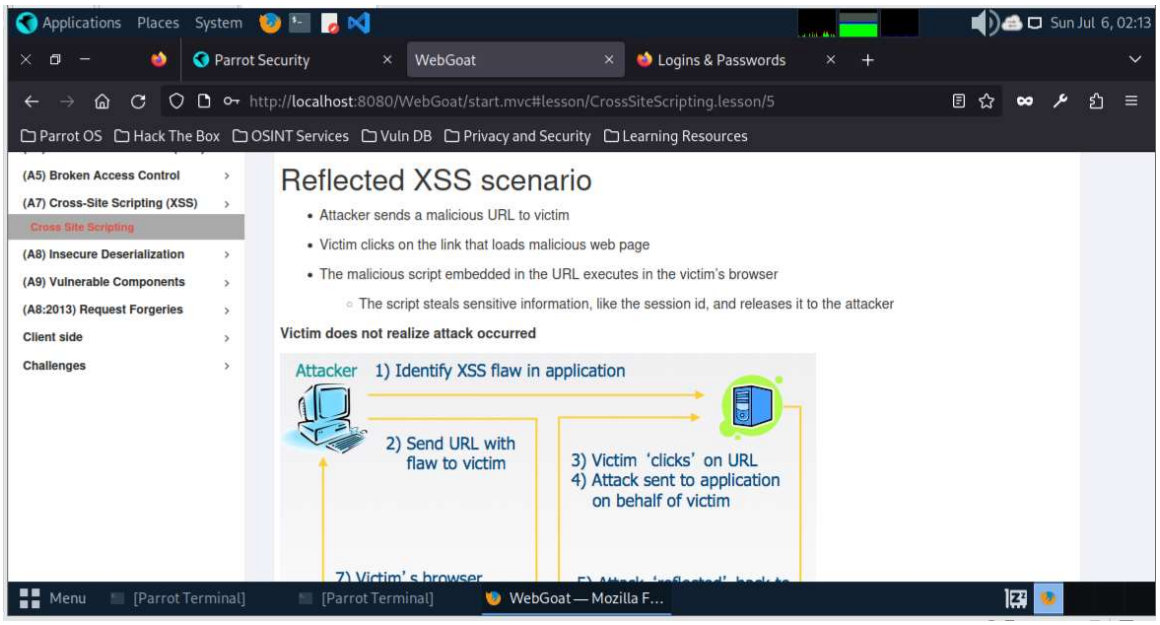
Why should we care ?

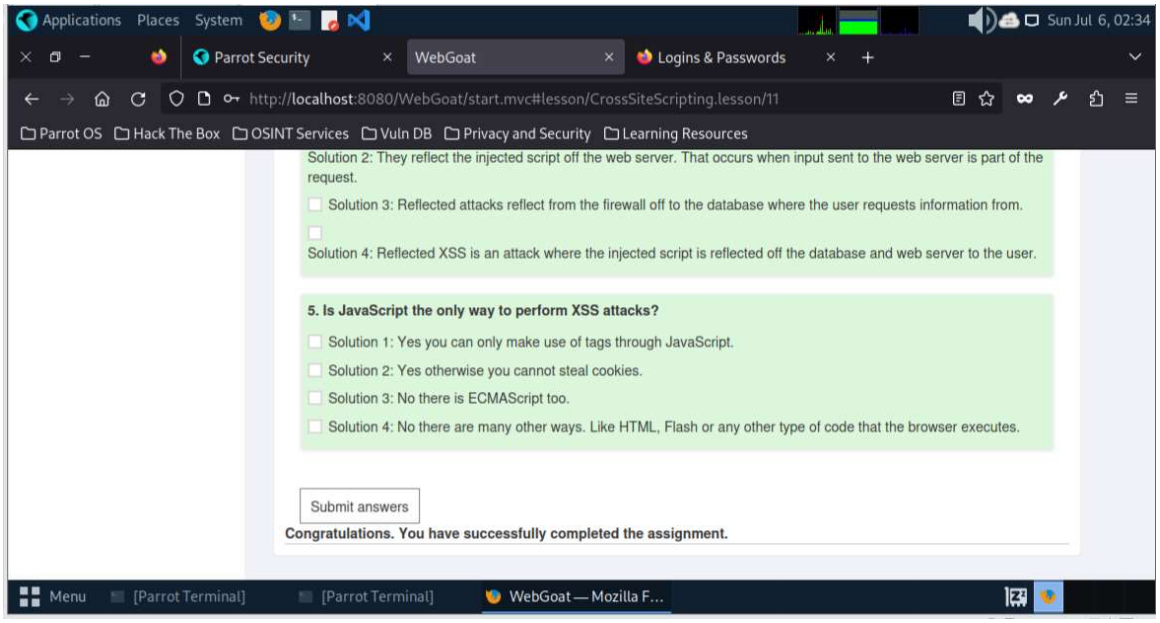


Type of XSS :



Reflected XSS scenario :





2) Perform Basic Vulnerability Analysis

Install and use OWASP ZAP (version 2.16.1) to scan for vulnerabilities.

Open a terminal :

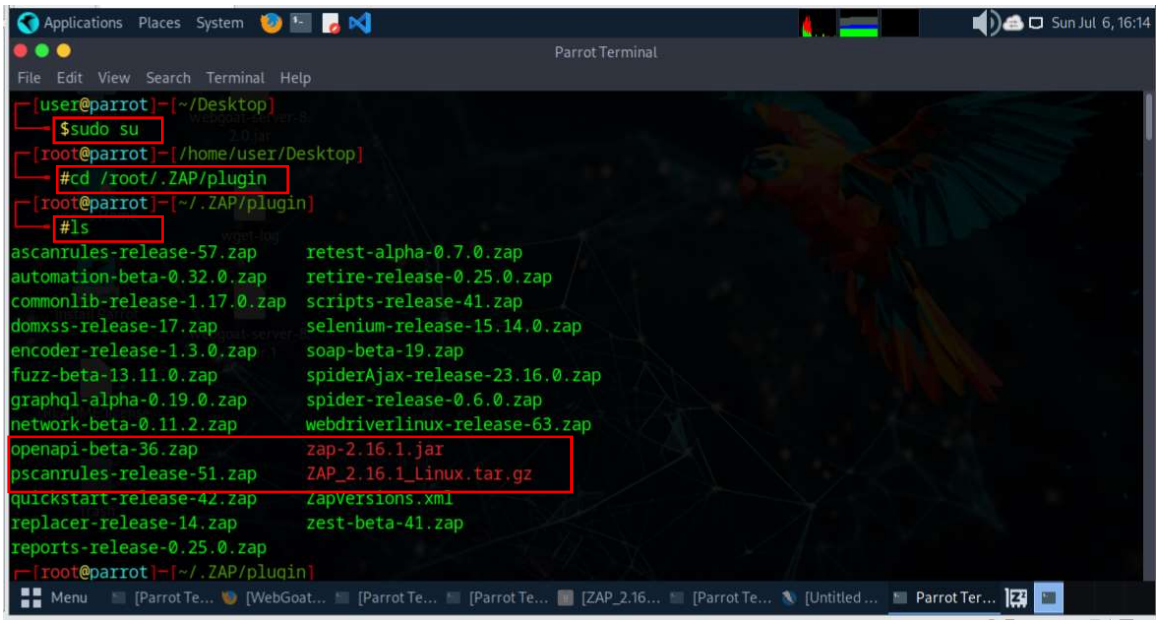
```
sudo su
```

```
cd /root/.ZAP/plugin
```

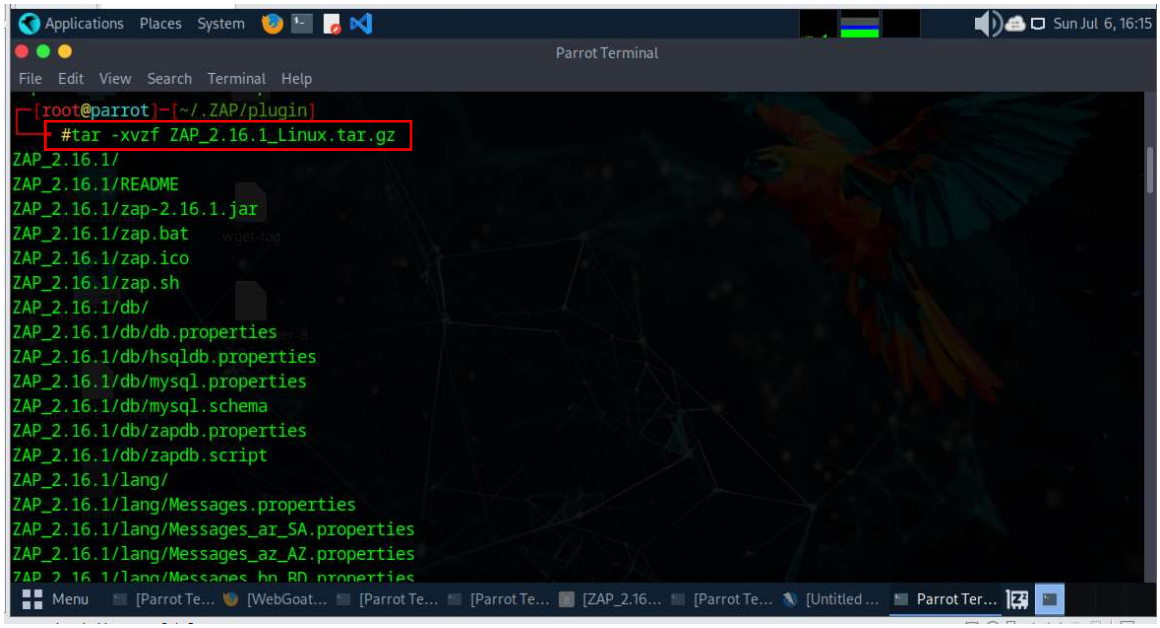
Verify that the file exists :

```
ls
```

After verification the file exists : `ZAP_2.16.1_Linux.tar.gz`



Extract the archive : `tar -xvzf ZAP_2.16.1_Linux.tar.gz`



Go to the extracted folder:

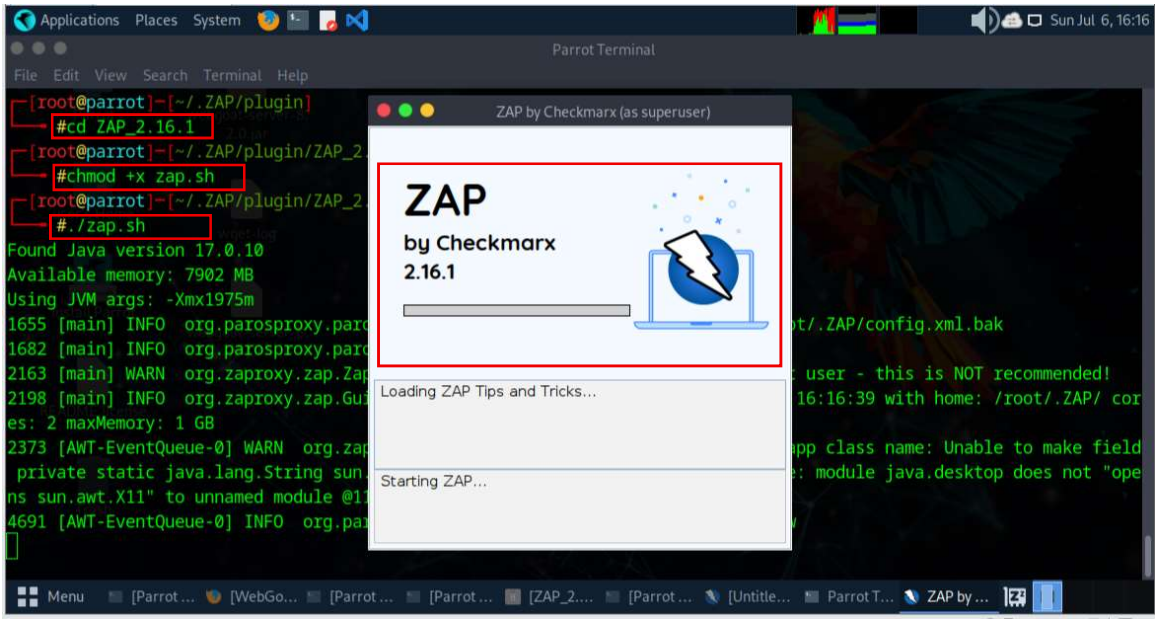
```
cd ZAP_2.16.1
```

Make the script executable :

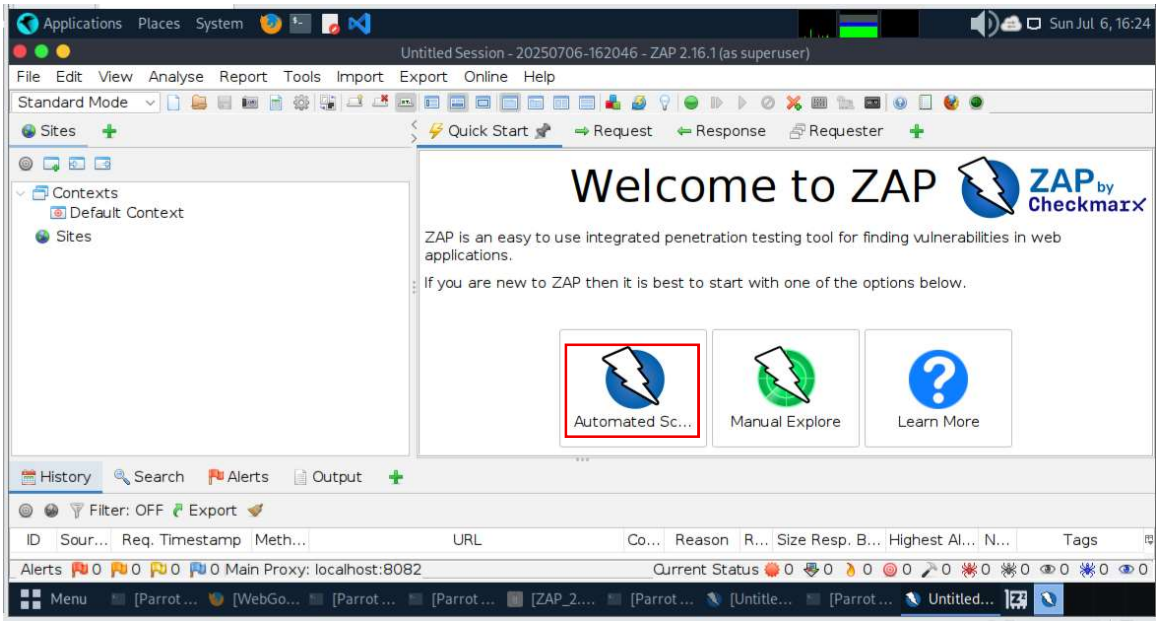
```
chmod +x zap.sh
```

Launch ZAP :

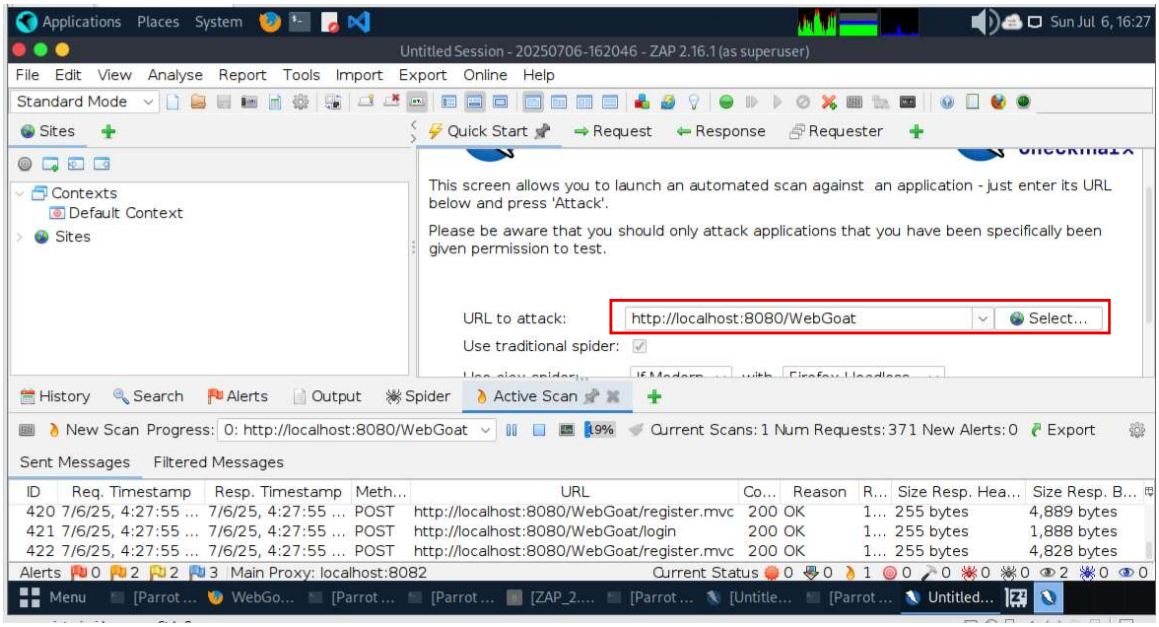
```
./zap.sh
```



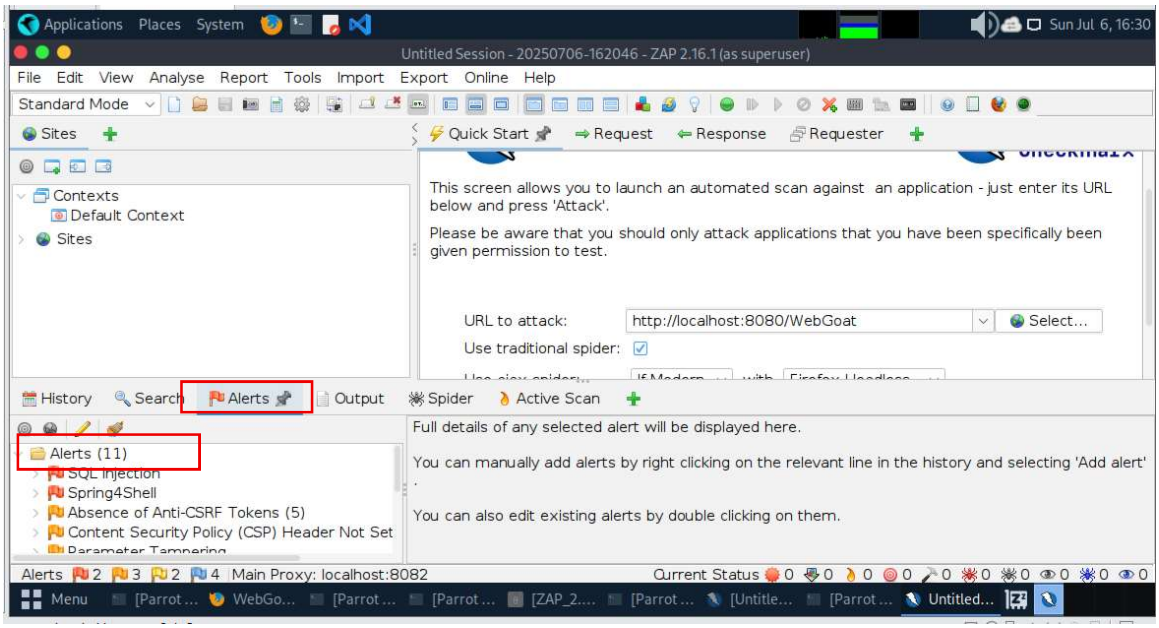
Once ZAP is launched, click on Start a **Automated Scan** :



Dans le champ URL to attack, entre : `http://localhost:8080/WebGoat`



Click on each alert to read the details and proposed solutions.

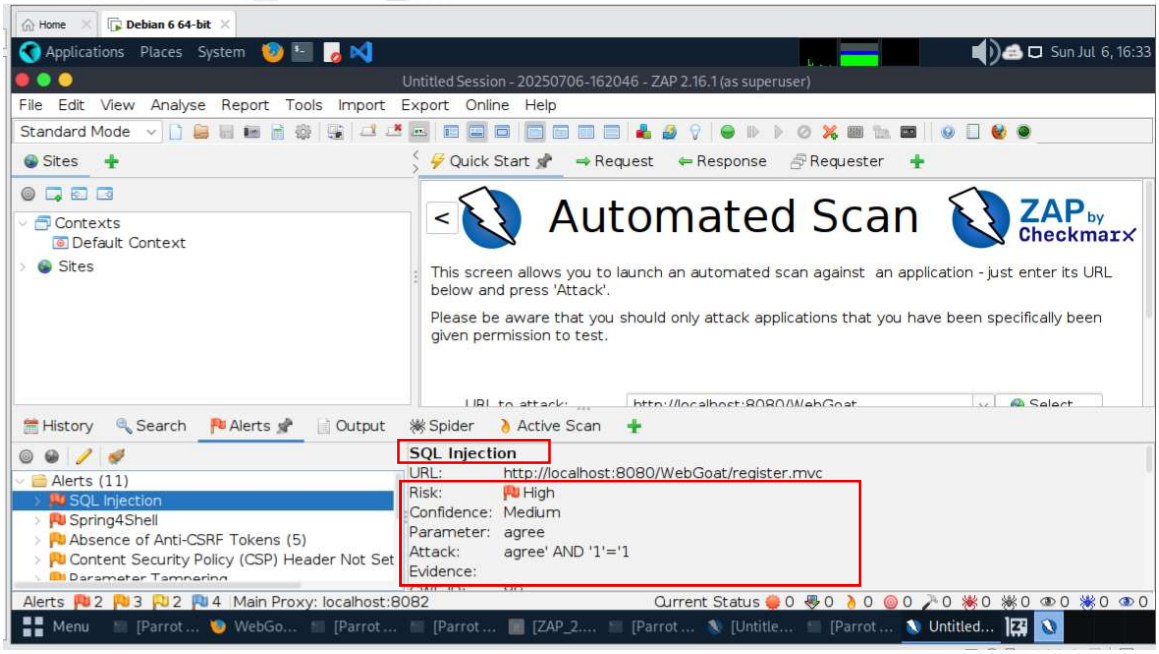


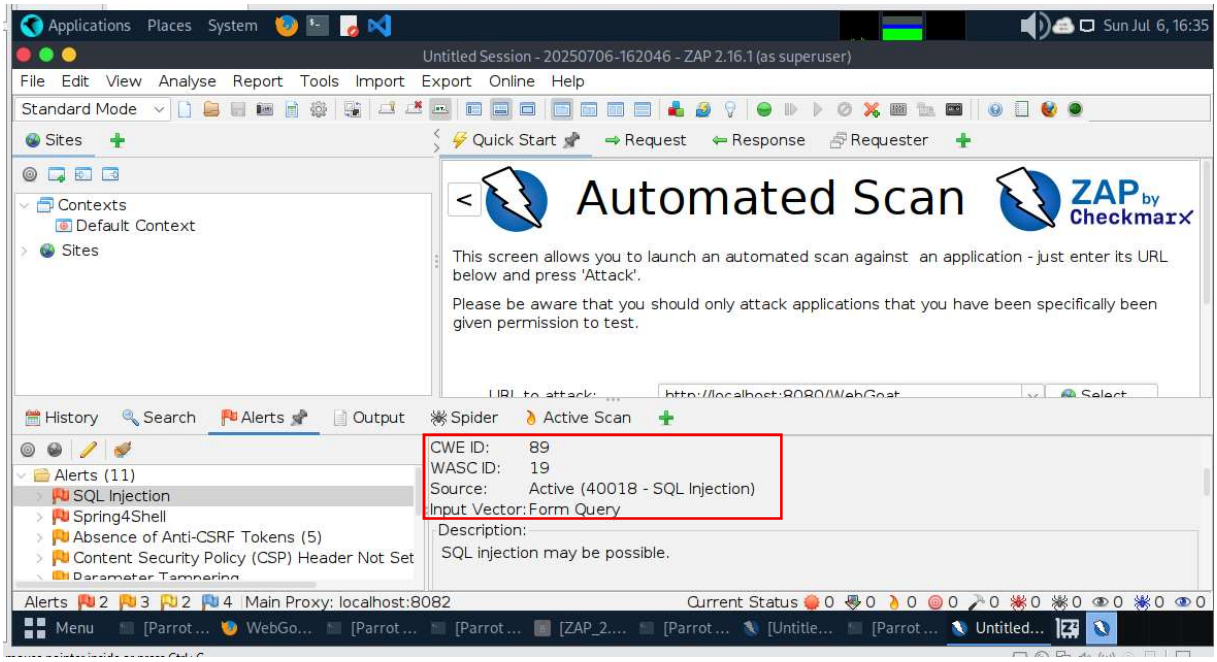
After the vulnerability scan, the alert tells us 11 vulnerabilities :

SQL Injection, Spring4Shell, Absence of Anti-CSRF Tokens (5), content Security Policy (CSP) Header Not Set, Parameter Tampering, Cookie No HttpOnly Flag, Cookie without SameSite Attribute, Authentication Request Identified, Session Management Reponse Identified, User Agent Fuzzer (91), User Controllable HTML Element Attribute (Potential XSS).

3) Explore Vulnerabilities

SQL Injection :





Other informations :

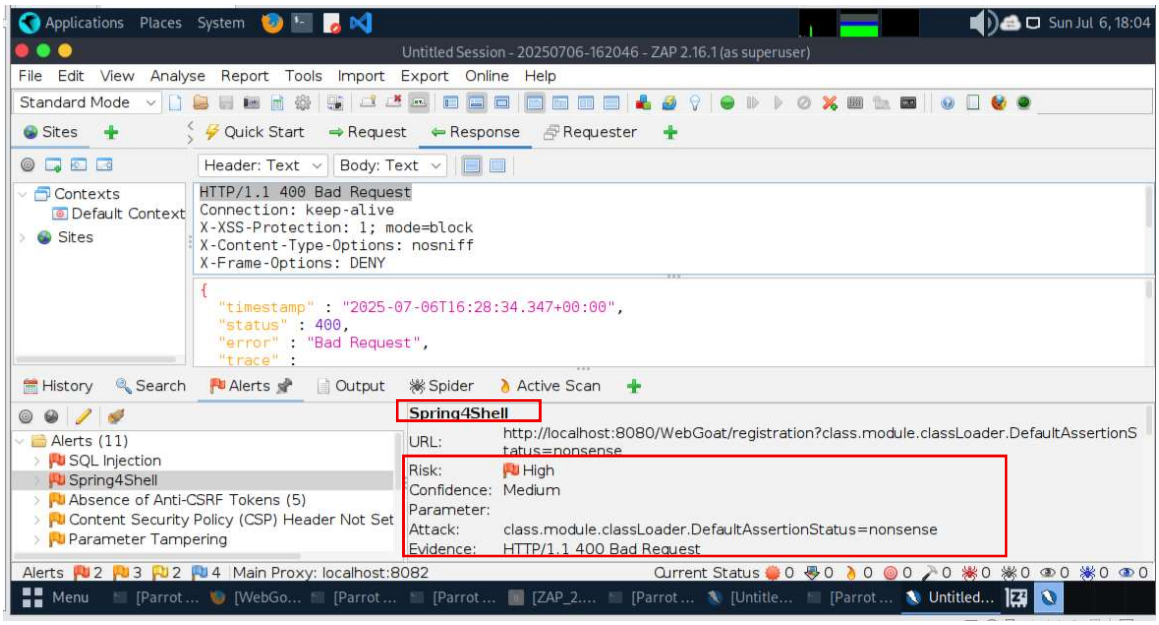
- The page results were successfully manipulated using the boolean conditions [agree' AND '1'='1] and [agree' AND '1'='2]
- The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison.

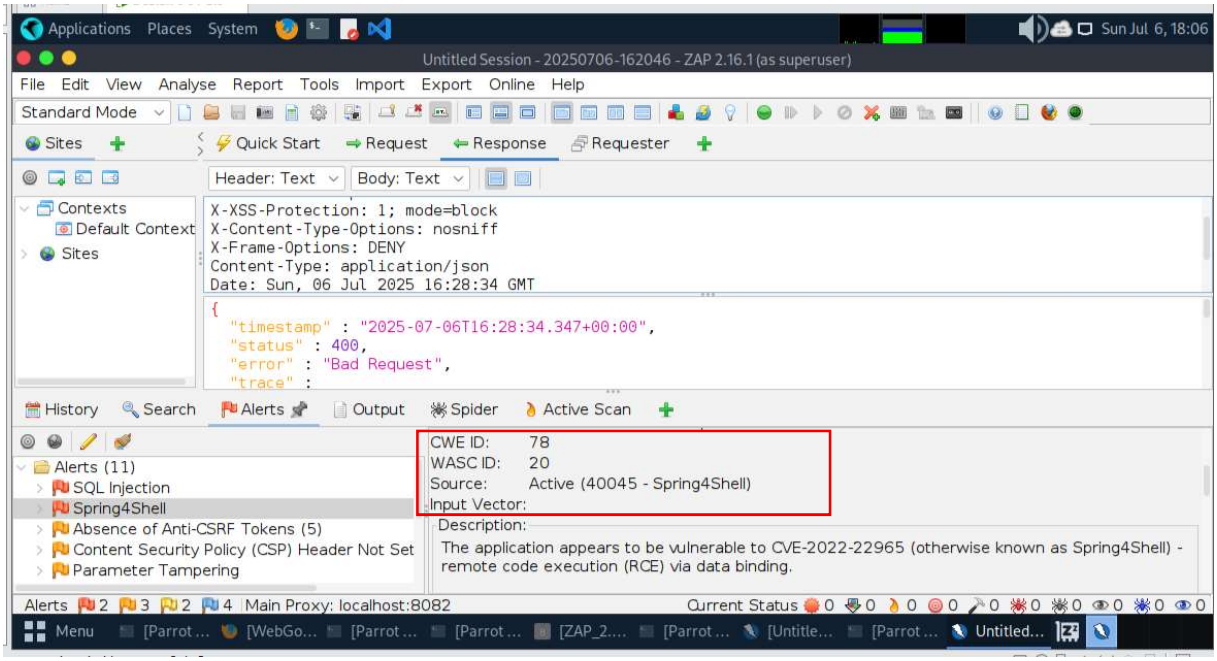
- Data was returned for the original parameter.
- The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.

Solution :

- Do not trust client side input, even if there is client side validation in place.
- In general, type check all data on the server side.
- If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'
- If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.
- If database Stored Procedures can be used, use them.
- Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!
- Do not create dynamic SQL queries using simple string concatenation.
- Escape all data received from the client.
- Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.
- Apply the principle of least privilege by using the least privileged database user possible.
- In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.
- Grant the minimum database access that is necessary for the application.

Spring4Shell :





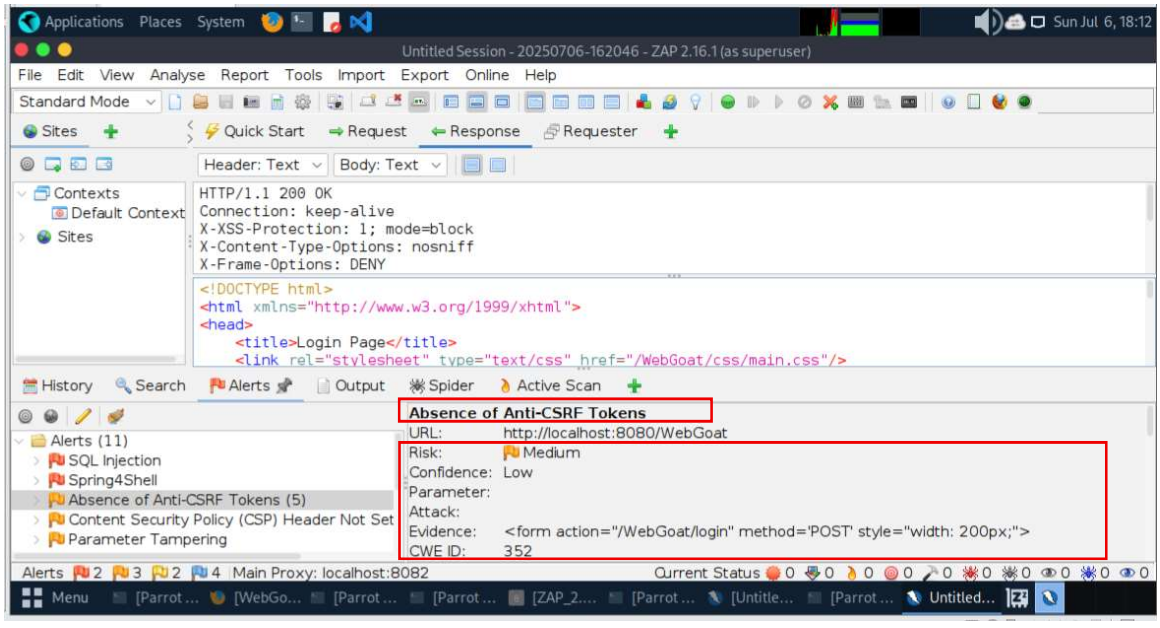
Description :

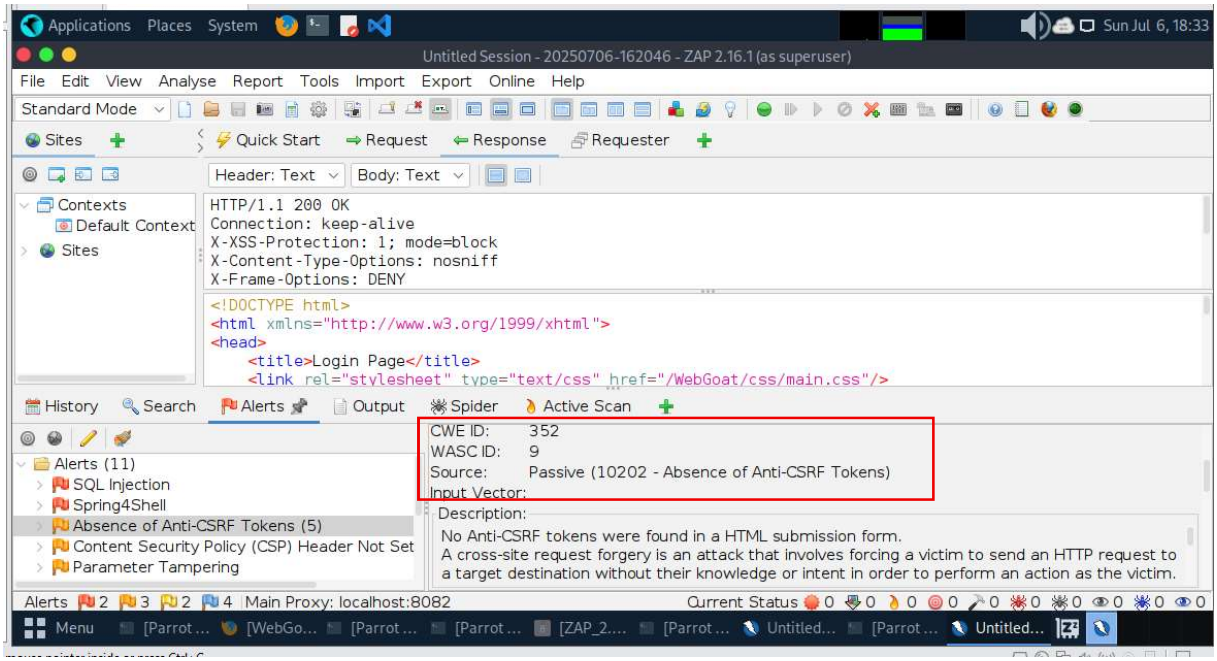
The application appears to be vulnerable to CVE-2022-22965 (otherwise known as Spring4Shell) - remote code execution (RCE) via data binding.

Solution :

Upgrade Spring Framework to versions 5.3.18, 5.2.20, or newer.

Absence of Anti-CSRF Tokens





Description :

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- The victim has an active session on the target site.
- The victim is authenticated via HTTP auth on the target site.
- The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Other Information :

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "exampleInputEmail1" "exampleInputPassword1"].

Solution :

- Phase : Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

- Phase : Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

- Phase : Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

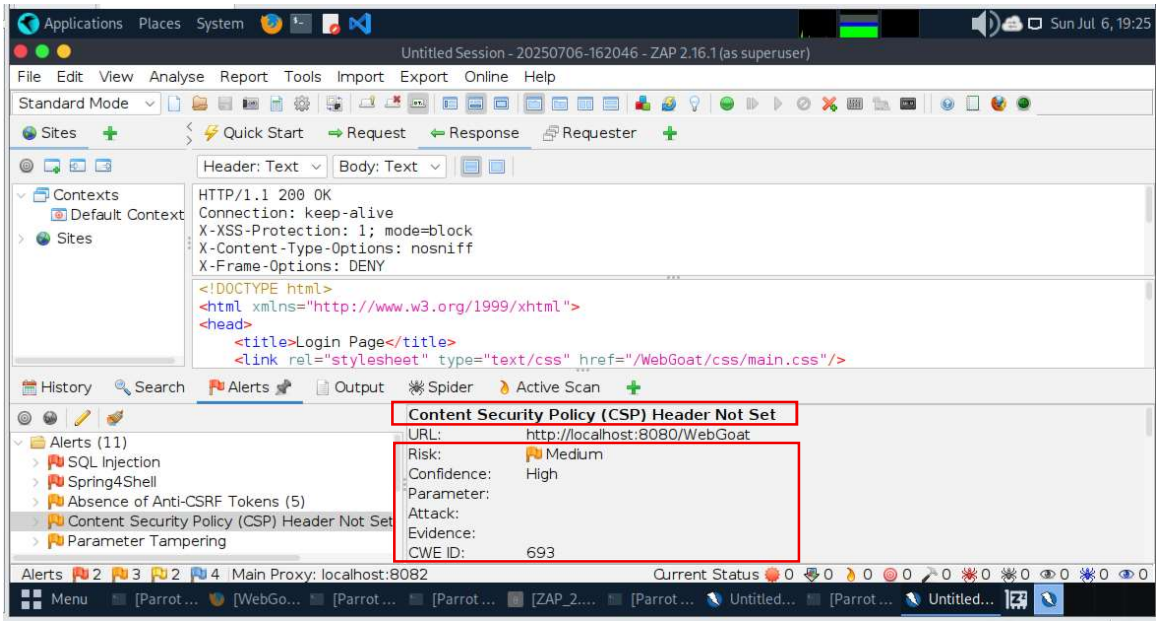
This control includes a component for CSRF.

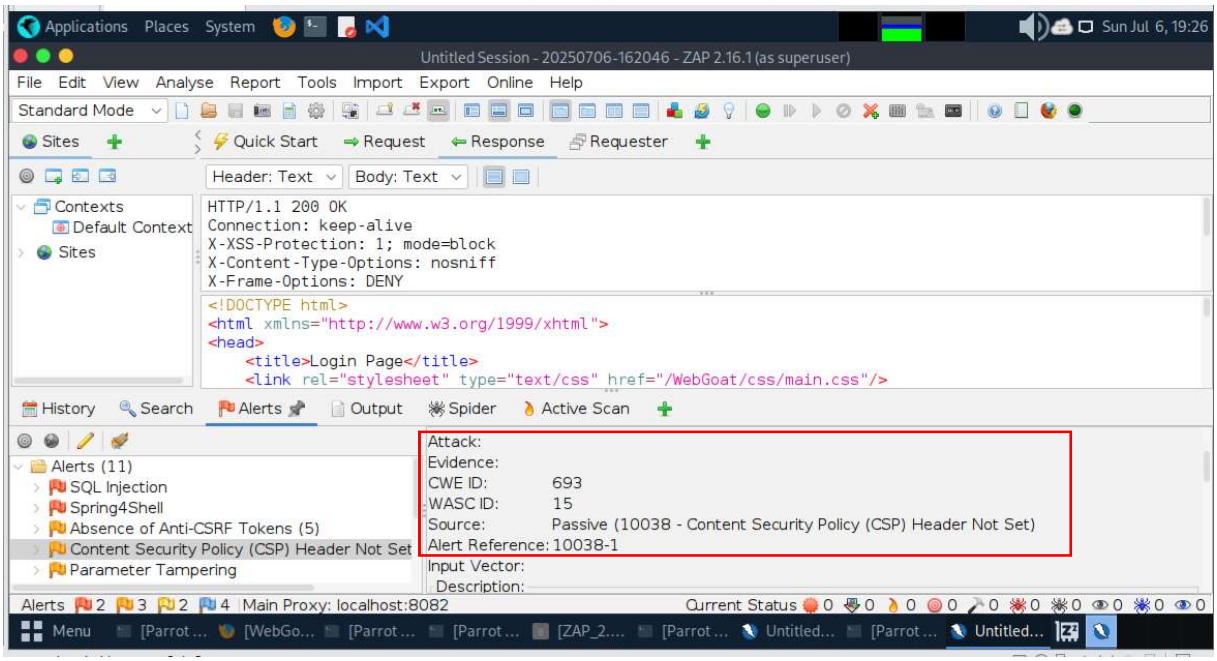
Do not use the GET method for any request that triggers a state change.

- Phase : Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Content Security Policy (CSP) Header Not Set





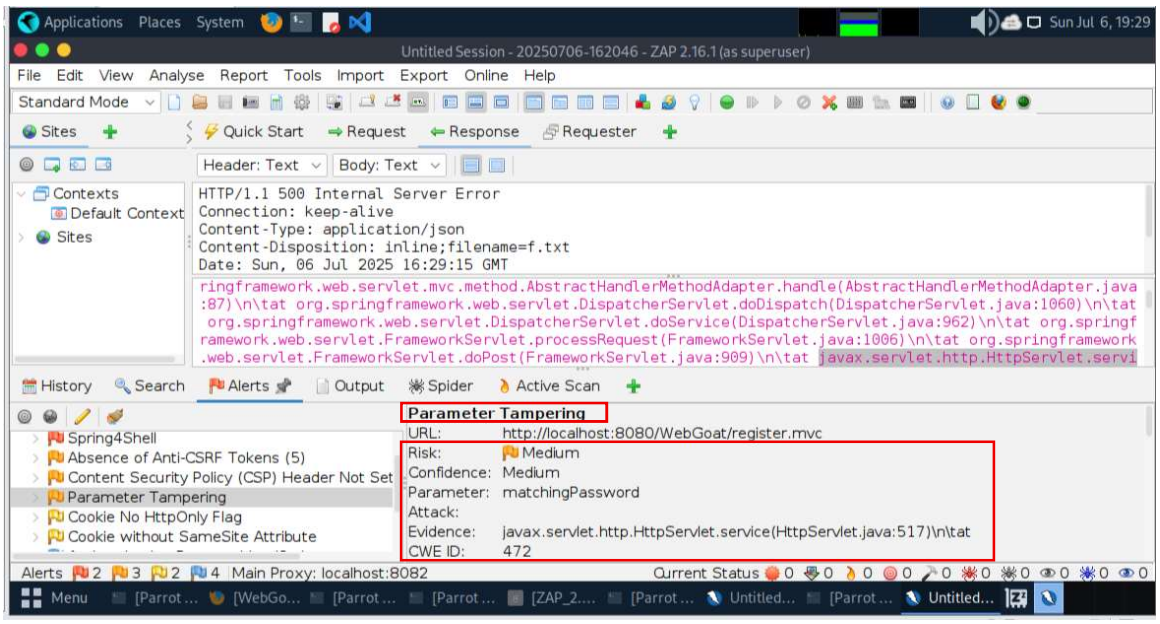
Description :

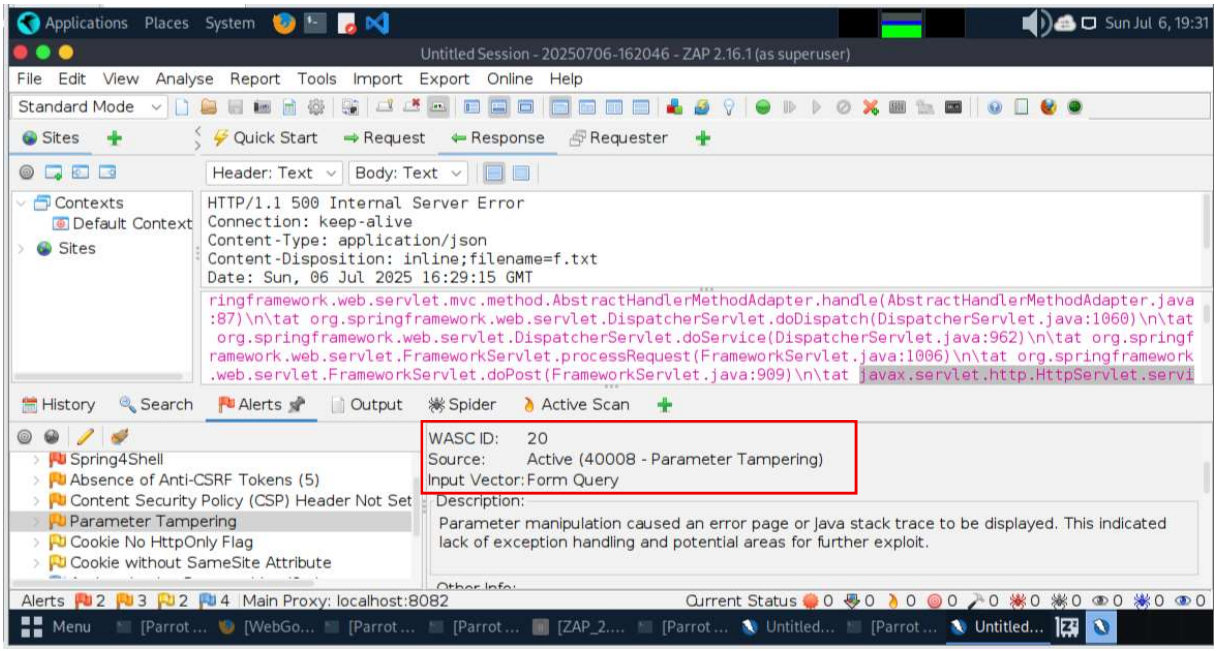
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution :

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Parameter Tampering





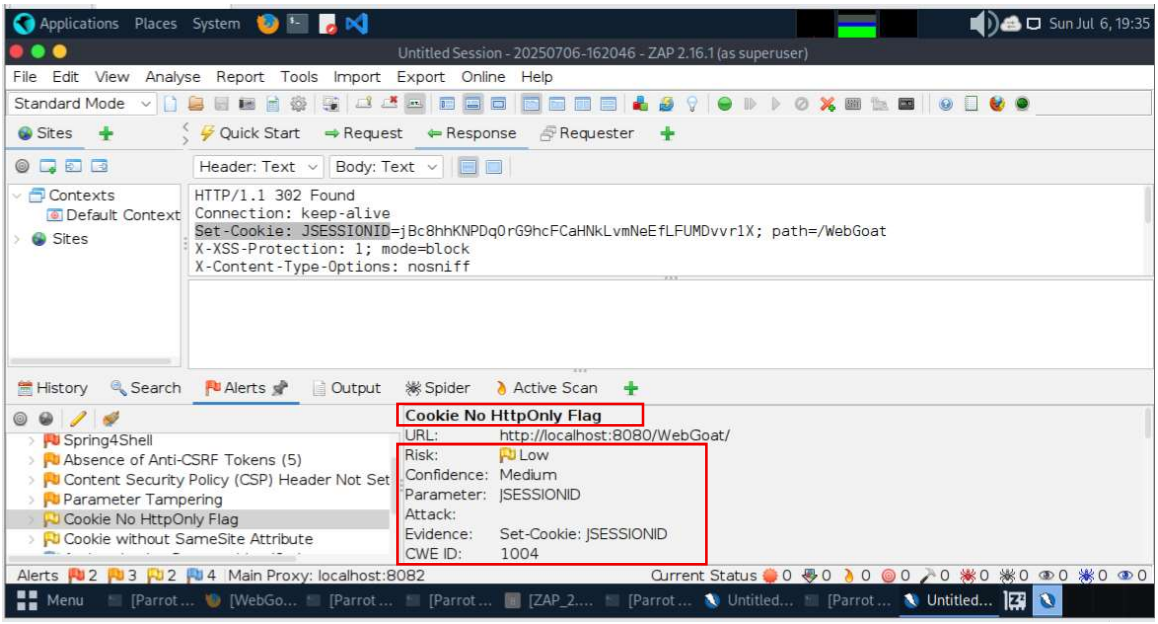
Description :

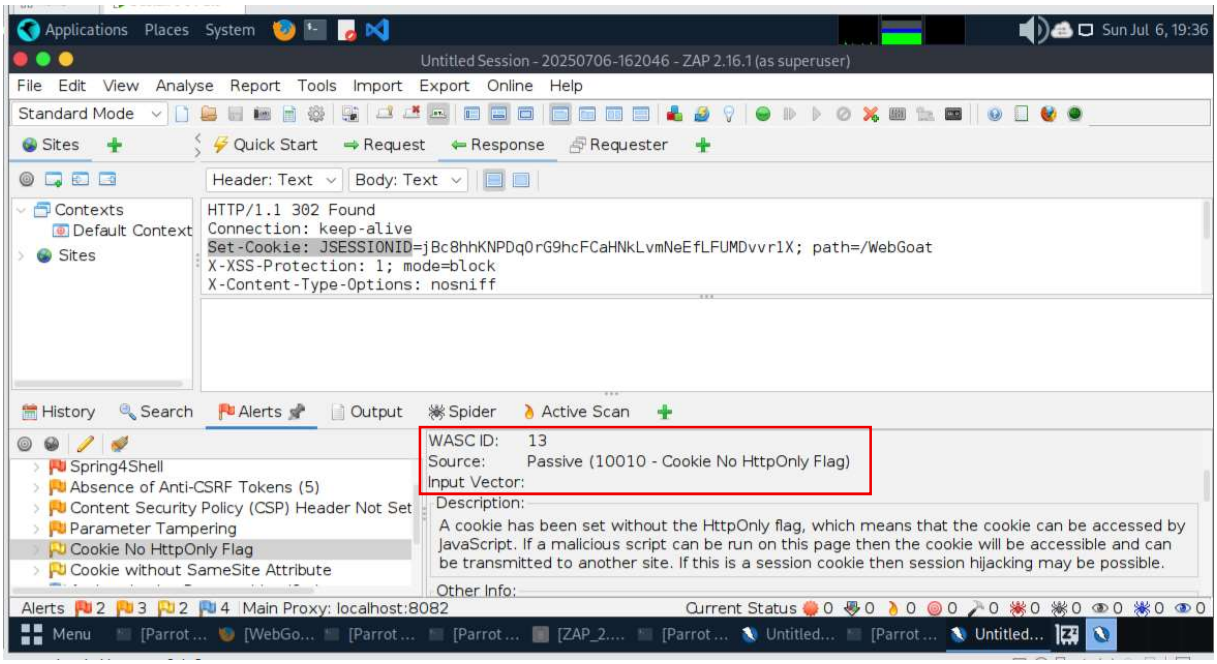
Parameter manipulation caused an error page or Java stack trace to be displayed. This indicated lack of exception handling and potential areas for further exploit.

Solution :

Identify the cause of the error and fix it. Do not trust client side input and enforce a tight check in the server side. Besides, catch the exception properly. Use a generic 500 error page for internal server error.

Cookie No HttpOnly Flag





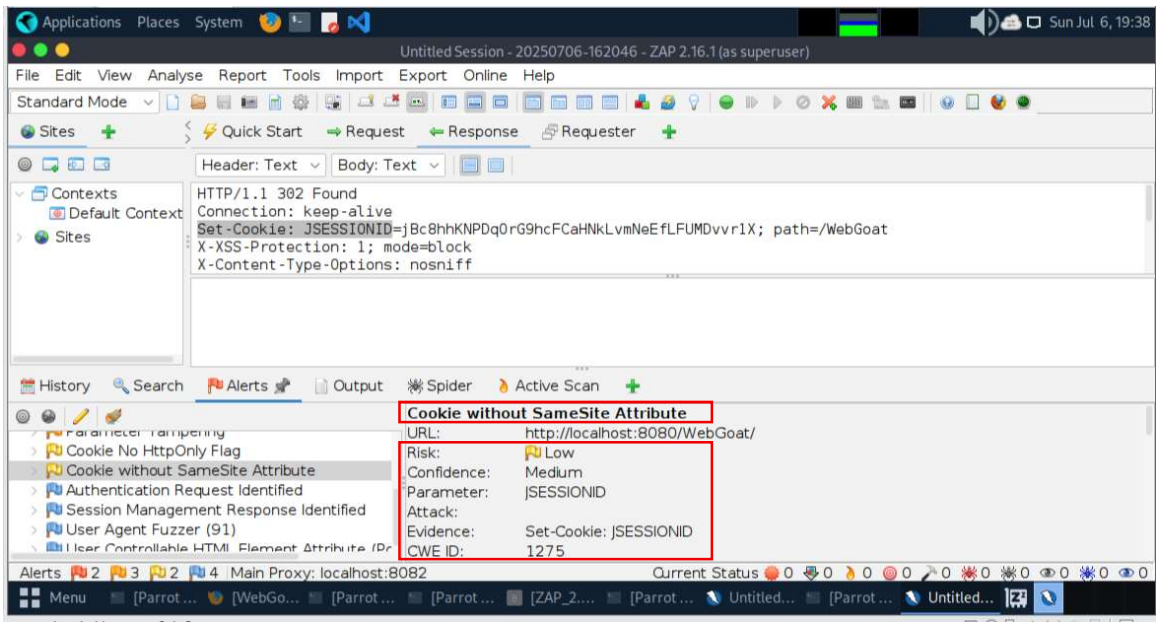
Description :

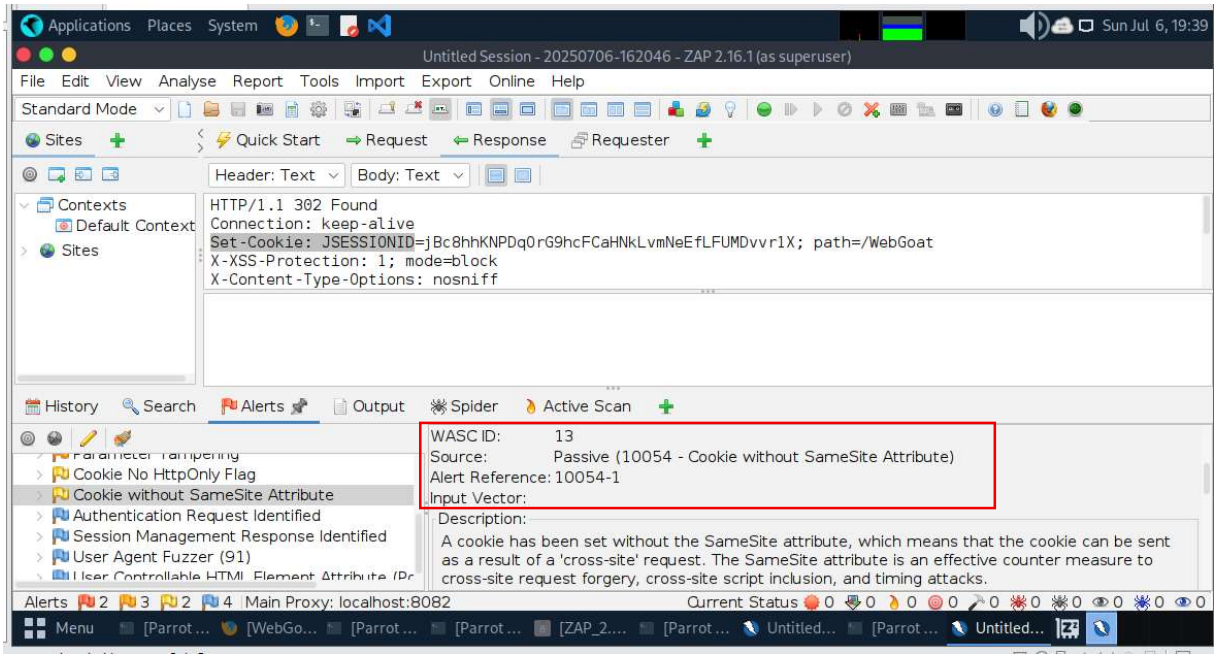
A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

Solution:

Ensure that the HttpOnly flag is set for all cookies.

Cookie without SameSite Attribute





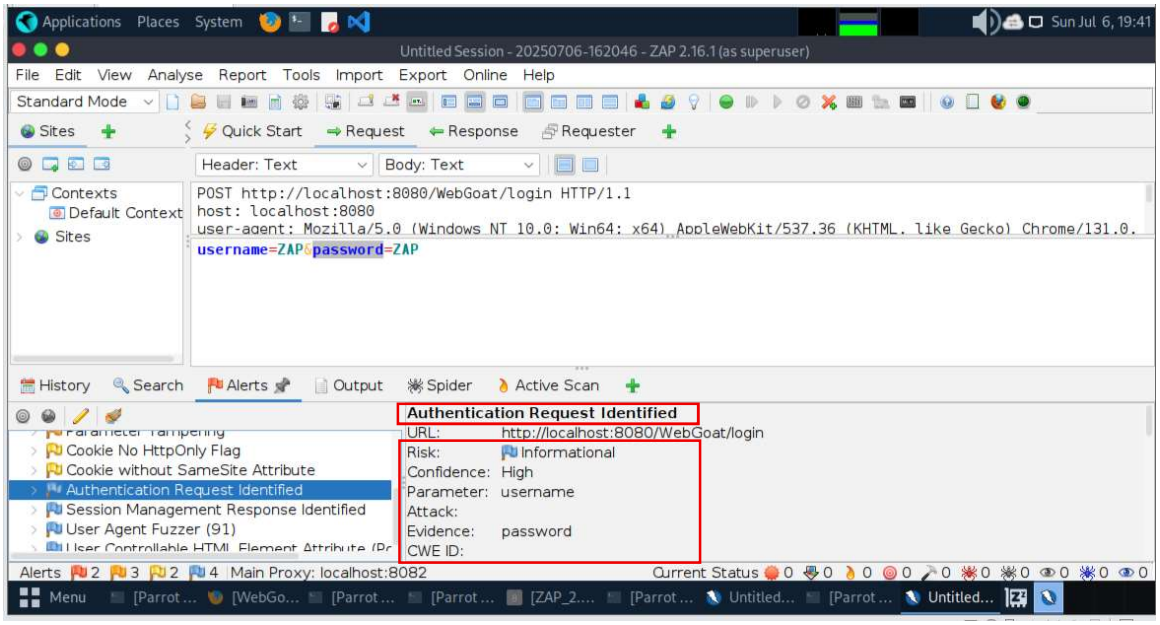
Description :

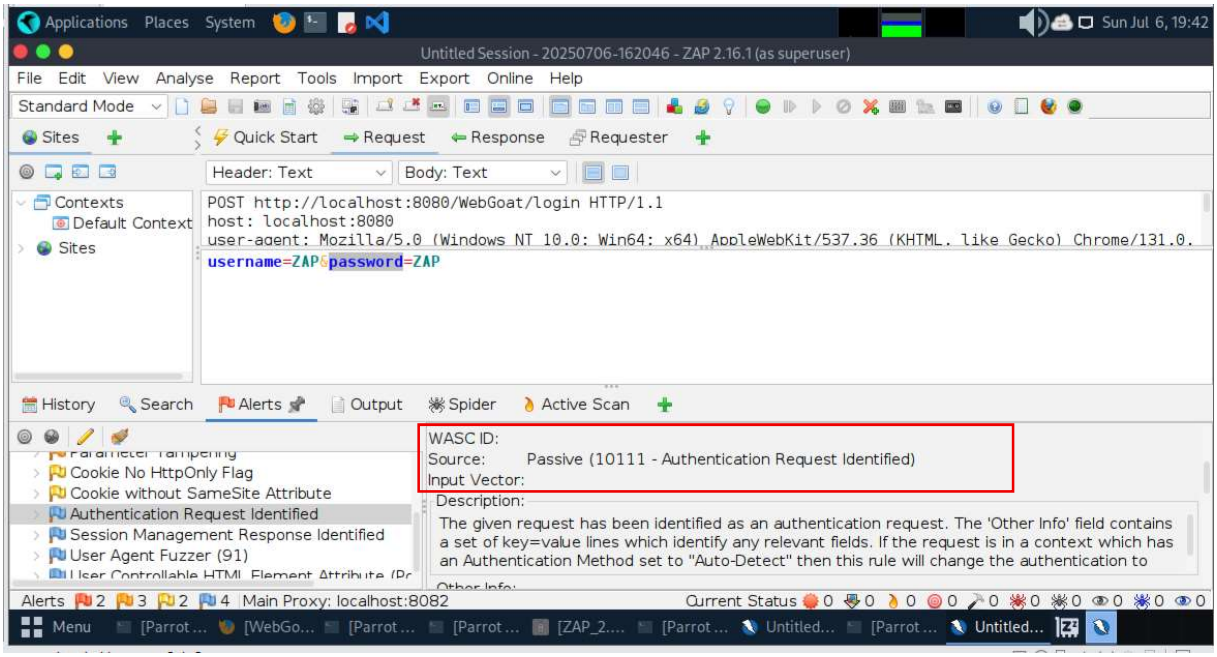
A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution :

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Authentication Request Identified





Description :

The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.

Other Info:

userParam=username

userValue=ZAP

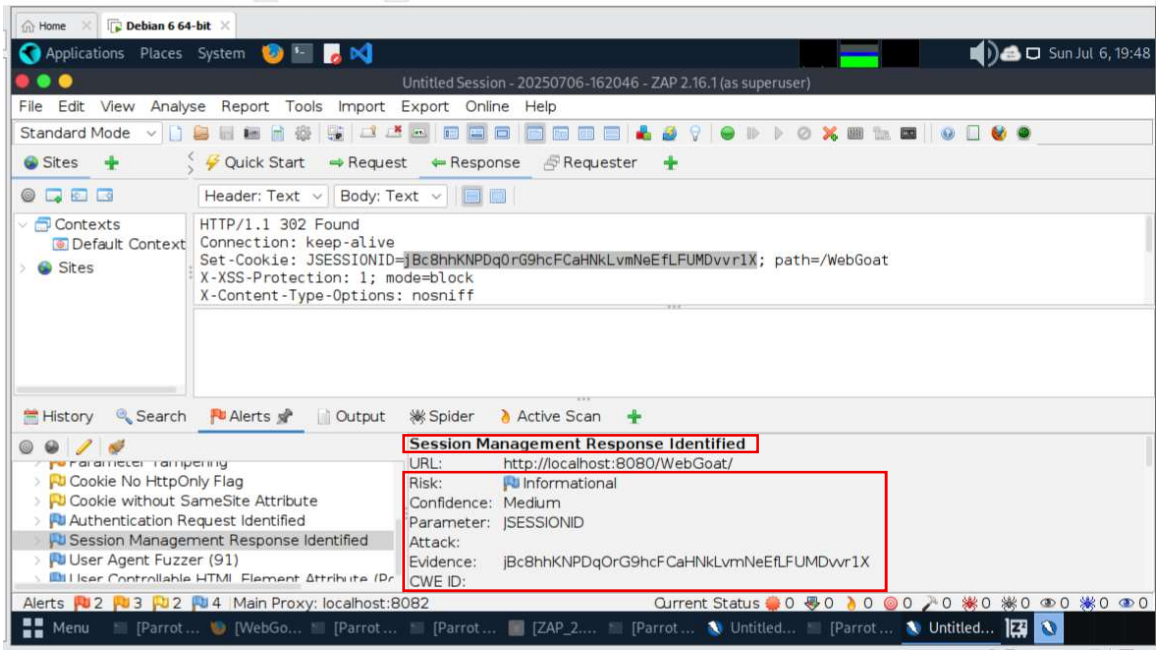
passwordParam=password

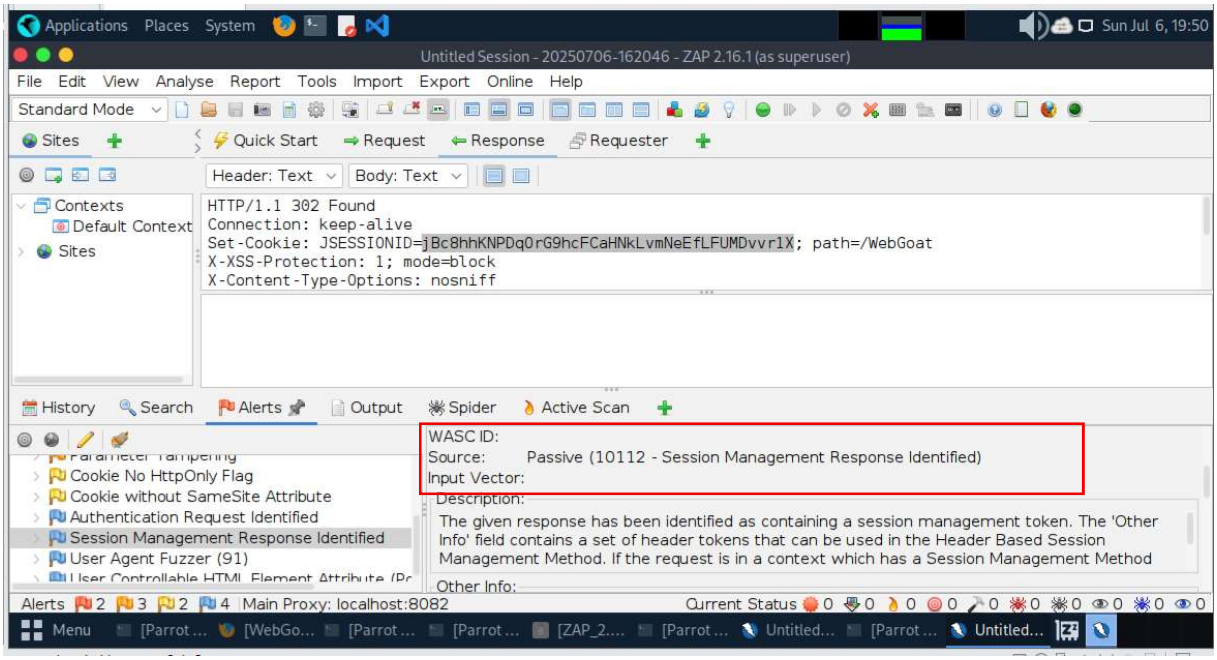
referer=http://localhost:8080/WebGoat/login

Solution :

This is an informational alert rather than a vulnerability and so there is nothing to fix.

Session Management Response Identified





Description :

The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

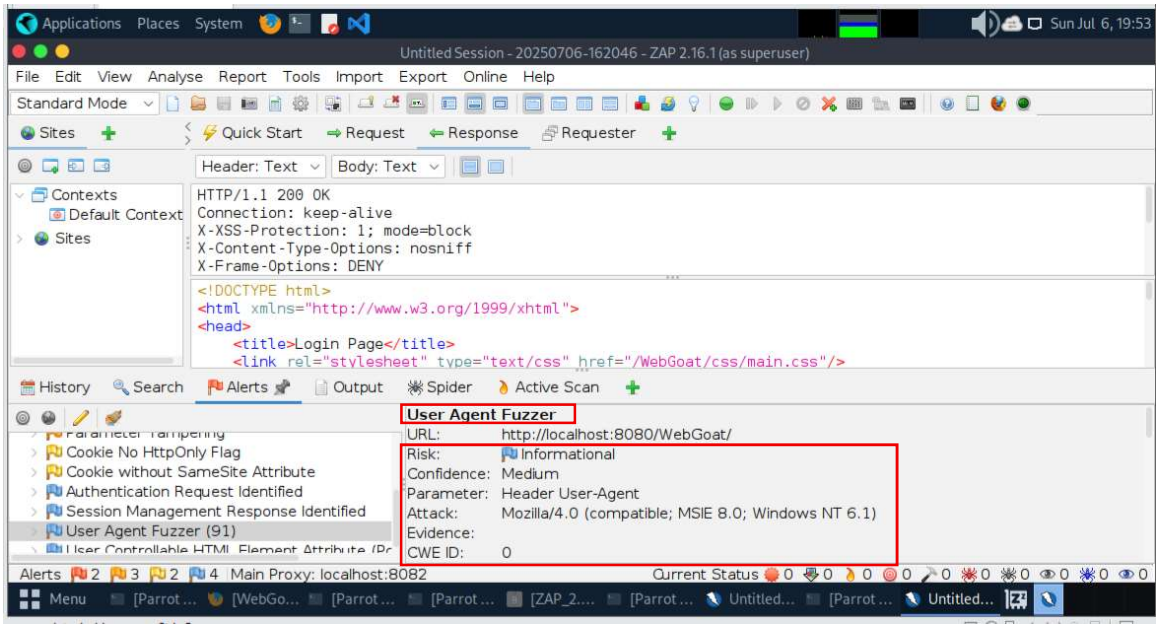
Other :

Cookie : JSESSIONID

Solution :

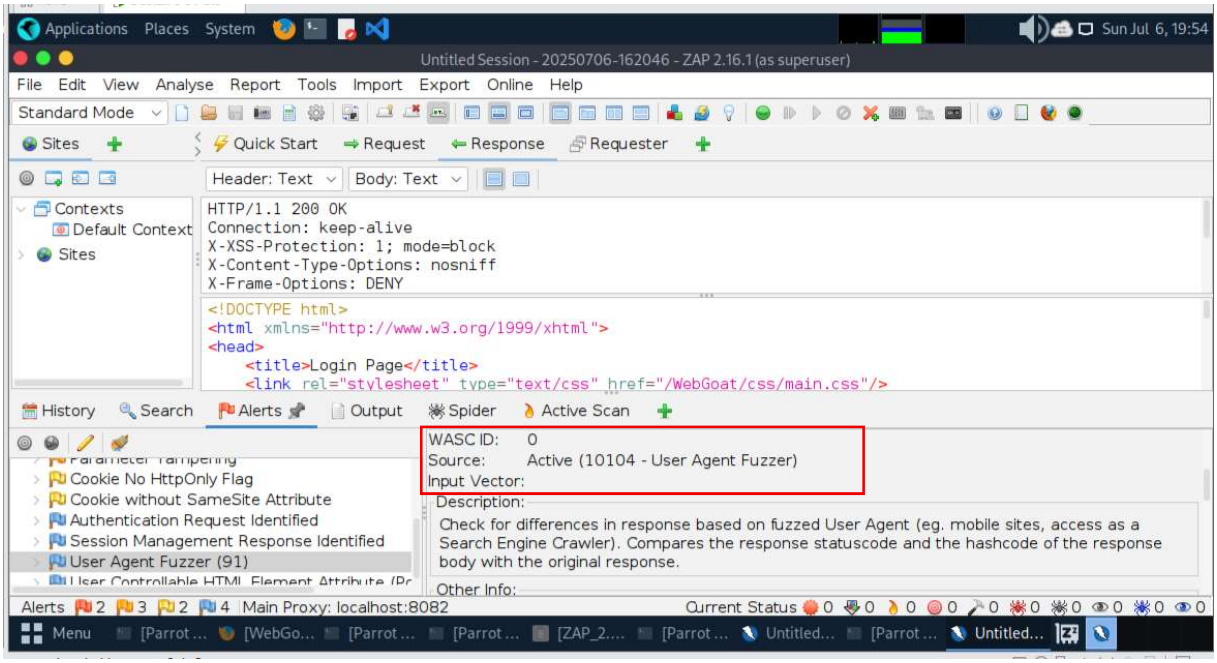
This is an informational alert rather than a vulnerability and so there is nothing to fix.

User Agent Fuzzer (91)

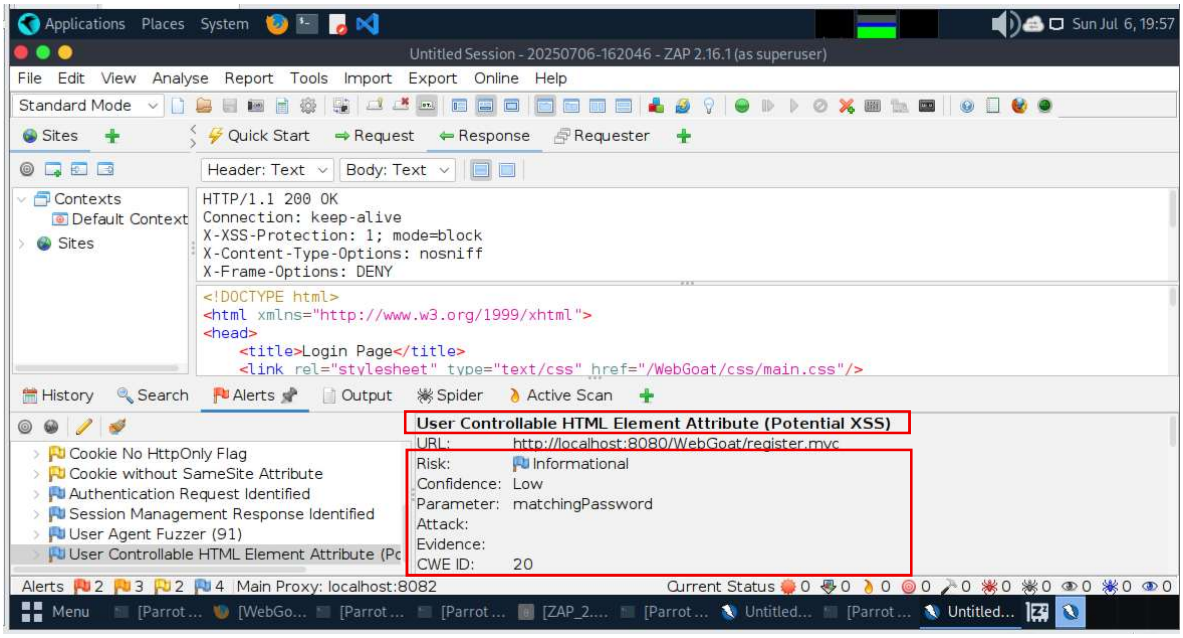


Description :

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.



User Controllable HTML Element Attribute (Potential XSS)



Description :

This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.

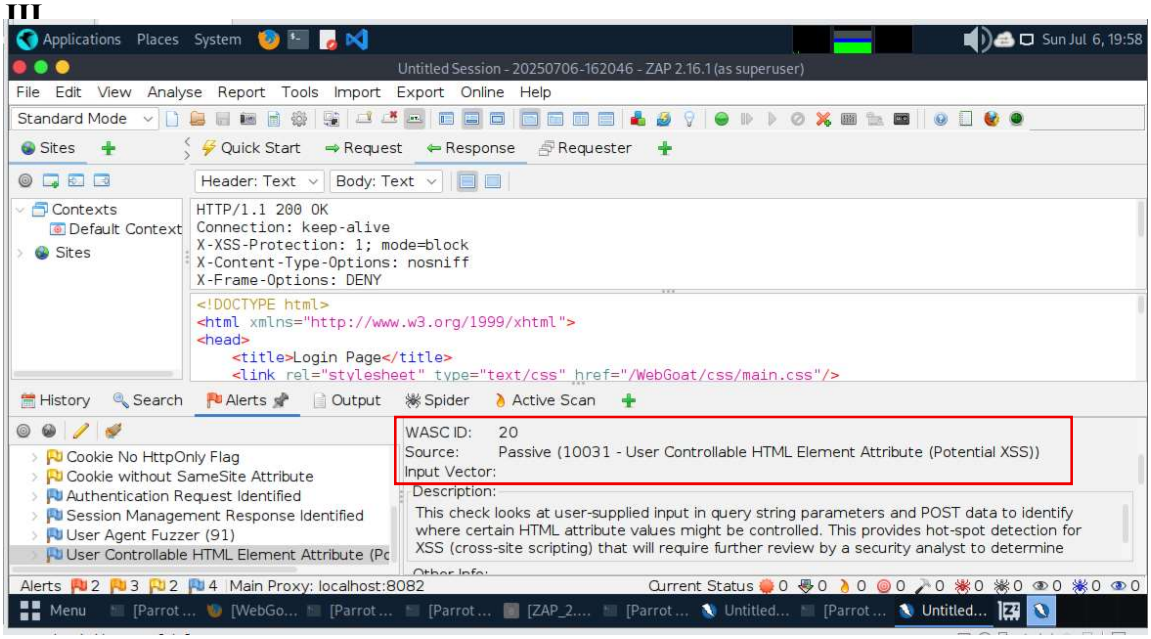
Other :

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

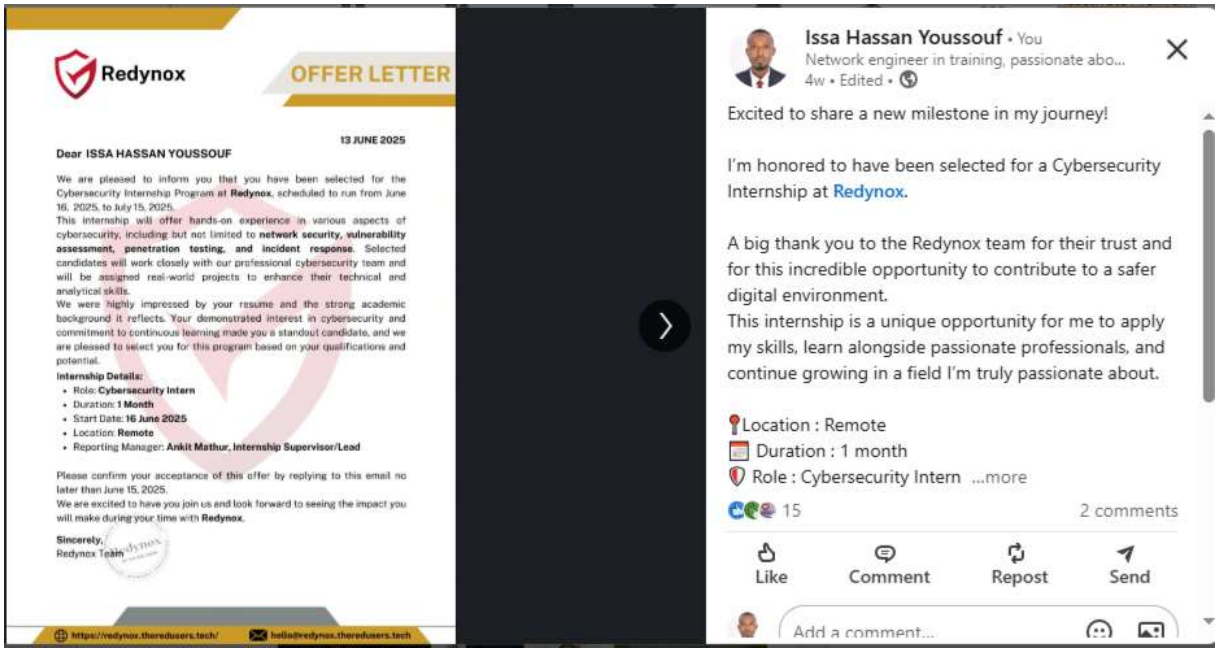
Solution :

Validate all input and sanitize output it before writing to any HTML attributes.

III



TASK 3: LINKEDIN ENGAGEMENT



Redynox

OFFER LETTER

13 JUNE 2025

Dear ISSA HASSAN YOUSSOUF

We are pleased to inform you that you have been selected for the Cybersecurity Internship Program at **Redynox**, scheduled to run from June 16, 2025, to July 15, 2025.
This internship will offer hands-on experience in various aspects of cybersecurity, including but not limited to **network security, vulnerability assessment, penetration testing, and incident response**. Selected candidates will work closely with our professional cybersecurity team and will be assigned real-world projects to enhance their technical and analytical skills.
We were highly impressed by your resume and the strong academic background it reflects. Your demonstrated interest in cybersecurity and commitment to continuous learning made you a standout candidate, and we are pleased to select you for this program based on your qualifications and potential.

Internship Details:

- Role: **Cybersecurity Intern**
- Duration: **1 Month**
- Start Date: **16 June 2025**
- Location: **Remote**
- Reporting Manager: **Ankit Mathur, Internship Supervisor/Lead**

Please confirm your acceptance of this offer by replying to this email no later than June 15, 2025.
We are excited to have you join us and look forward to seeing the impact you will make during your time with **Redynox**.

Sincerely,
Redynox Team

https://redynox.theredusers.tech/ hello@redynox.theredusers.tech

Issa Hassan Youssouf • You
Network engineer in training, passionate abo...
4w • Edited •

Excited to share a new milestone in my journey!

I'm honored to have been selected for a Cybersecurity Internship at Redynox.

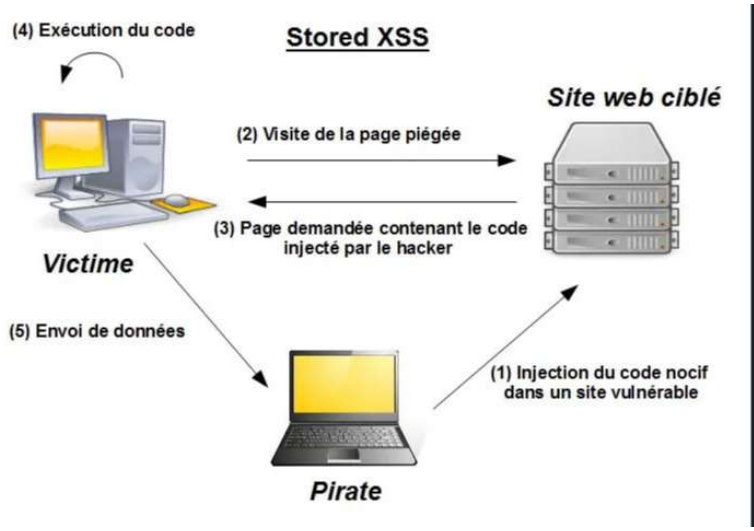
A big thank you to the Redynox team for their trust and for this incredible opportunity to contribute to a safer digital environment.
This internship is a unique opportunity for me to apply my skills, learn alongside passionate professionals, and continue growing in a field I'm truly passionate about.

Location : Remote
Duration : 1 month
Role : Cybersecurity Intern ...more

15 2 comments

Like Comment Repost Send

Add a comment...



Issa Hassan Youssouf • You
Network engineer in training, passionate abo...
2w •

Understanding XSS Attacks : A Key to Web Application Security

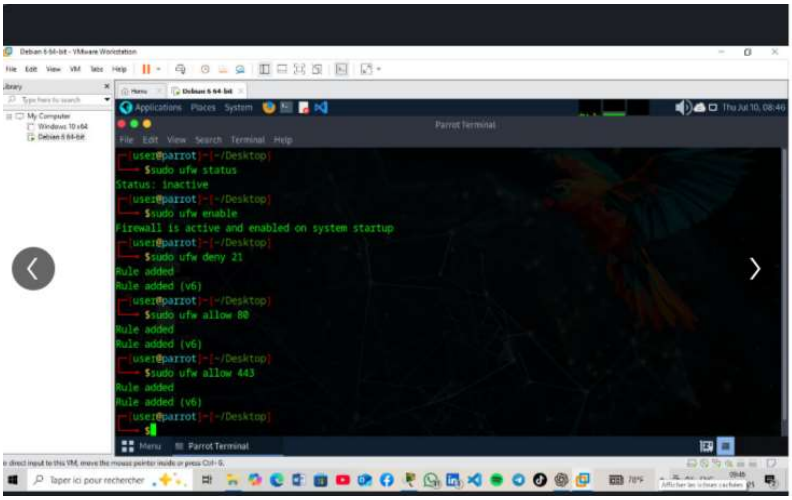
As part of my cybersecurity internship at Redynox, I've been exploring various web vulnerabilities—one of the most impactful being Cross-Site Scripting (XSS). It comes in three main types, each with different characteristics and attack vectors:

1- Stored XSS : Persistent and server-side. The malicious script is saved (e.g., in a database) and executed whenever a user accesses the affected content.
2- Reflected XSS : Non-persistent but also server-side. The attack is delivered via a crafted link and reflected in the server response. ...more

Lydie Ouattara and 4 others

Like Comment Repost Send

Add a comment...



Issa Hassan Youssouf • You
Network engineer in training, passionate abo...
2d • Edited •

Great Journey at Redynox !

I'm proud to share the completion of my cybersecurity internship tasks at Redynox, an experience that was both challenging and enriching.

During this internship, I had the opportunity to:
- Develop a solid understanding of system and network security fundamentals,
- Contribute to the analysis of security vulnerabilities (XSS, SQL injections, etc.) using tools like OWASP® Foundation ZAP and Wireshark Foundation,
- Basic security configurations, such as changing default passwords and enabling network encryption (WPA2 or WPA3), ...more

57 12 comments • 2 reposts

Like Comment Repost Send

CONCLUSION

This internship allowed me to take my first practical steps in the field of cybersecurity. I was able to implement different network security techniques, observe traffic behavior via tools like Wireshark, and understand the importance of securing communications over the Internet such as configuring basic security configurations, such as changing default passwords and enabling network encryption (WPA2 or WPA3) and with the Parrot OS environment as the primary support.

Exploring web vulnerabilities through WebGoat and OWASP ZAP gave me a concrete view of the real attacks that applications can undergo. I learned to identify flaws, understand them, and above all propose effective solutions to correct them.

The professional dimension was also valued through LinkedIn, where I was able to share my experiences and strengthen my presence in the field.

These activities allowed me to consolidate my theoretical knowledge, to discover new professional tools and to develop my technical rigor. I came out of this internship motivated to deepen my cybersecurity skills even more.