Abstract

The vulnerability that I encountered is Denial of Service (DoS) it ´s consist in saturating a system with multiple request simultaneous until that the recurses available they run out and the service leaves of responding. In the context current, it ´s vulnerability in critic because affect directly the availability of web application, a pilar fundamental of the security according to the model CIA (Confidentiality, Integrity and Availability).

In its demonstration it was used OWASP ZAP for launch multiple requests concurrently against the application Mutillidae installed in a Virtual Machine. The result evidence that the increment the threads of scan and execute fuzzing massive, the server Apache began to consume high levels of CPU and memory, degrading the performance until it causes the service to be interrupted. Its exercise sample like an attacker can blow the lack of mechanisms of protection for affect the continuity operative of the organization.

That ´s why is necessary carry out a studding about of the possible vulnerability they can have after of put in production.

Introduction and contextualization

Defined of the problem: The vulnerability selected is Denial of Service it is a series of the request to a service or web application for saturate the service.

Classification OWASP: Its related with the OWASP Top 10 Software and Data Integrity Failures and Mishandling of exceptional Conditions that include failures of availability.

Impact of business: An company affected for DoS losses availability of services, interrupts operations critics, affect the experience of client, damaged your reputation and can suffer losses economics but its depend of the attack and time that last.

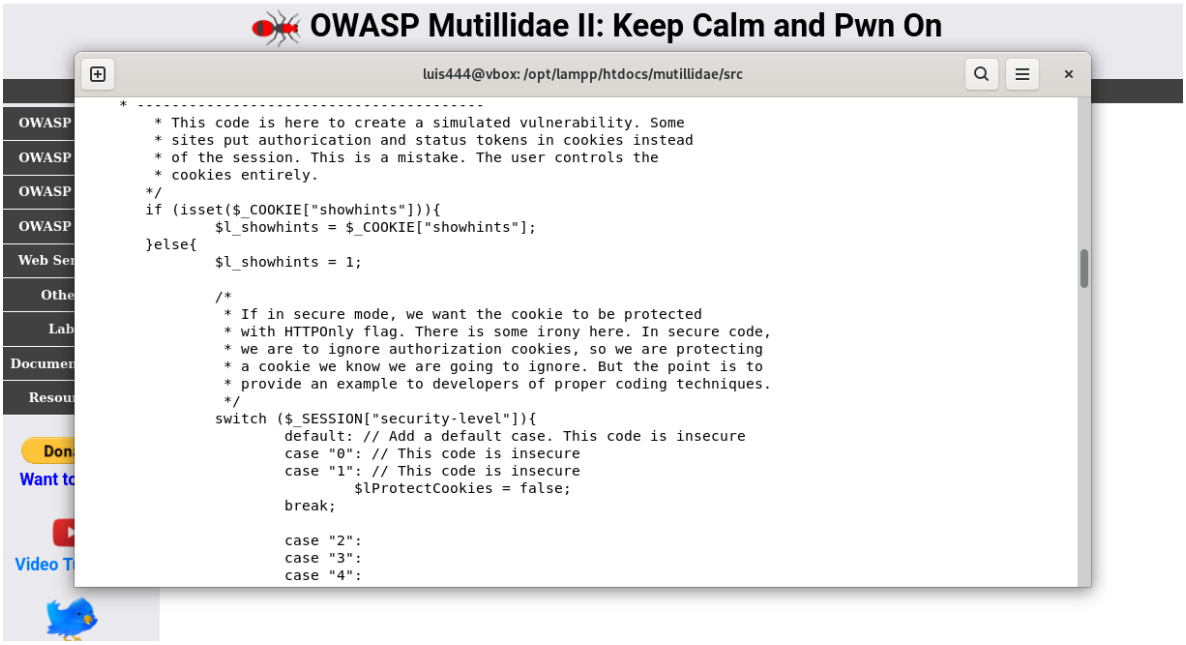
Analysis Technic of the Vulnerability

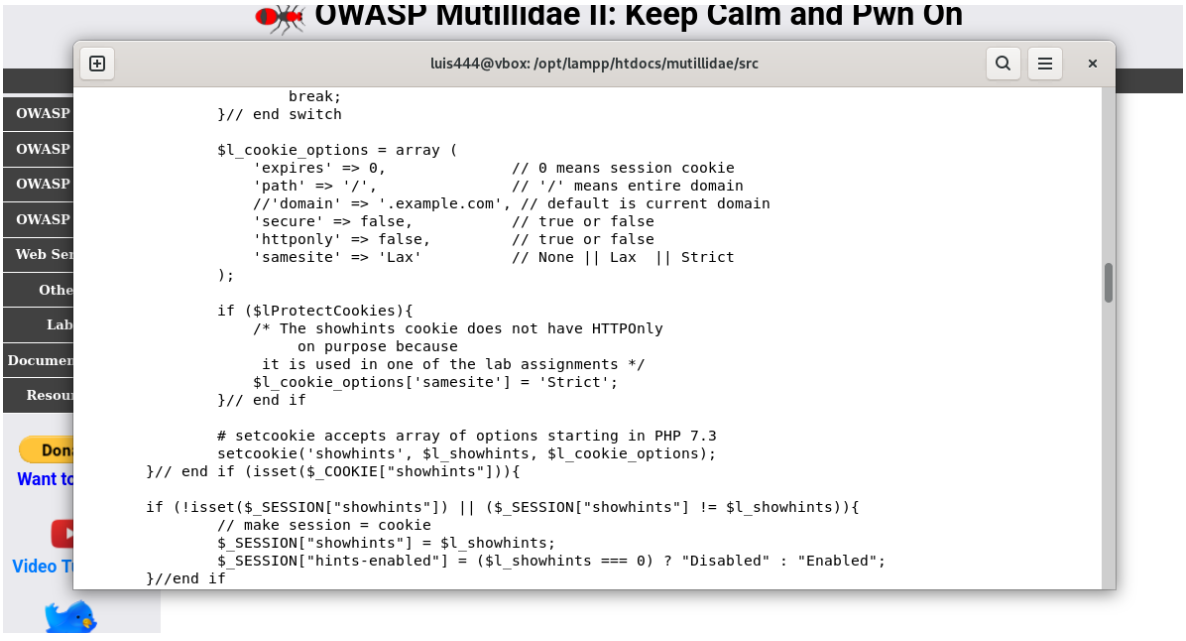
Mechanisms of exploitation

1. The attack identify an endpoint vulnerability
2. Config OWASP ZAP for launch multiple request concurrent through scan automatized and fuzzing
3. The server receives thousands of request simultaneous and starts to saturates
4. The service it degrades until leave of responding

Analysis of code vulnerability

The conde vulnerability its in the next screenshot because the app trust in the value of the cookie showhints send for the client and its value is copied directly of the session but the cookies are controlled for the user, an attack can modify in you browser and alter the behavior of the application.





Vectors of attack

- Scan automatized repeat
- Fuzzing massive about parameters such as page, user, etc.
- Request concurrent without limitation of rate

Demonstration environment

Technologies:

- Language: PHP
- Databases: MySQL
- Server Web: Apache Debian

Tool of Pentesting

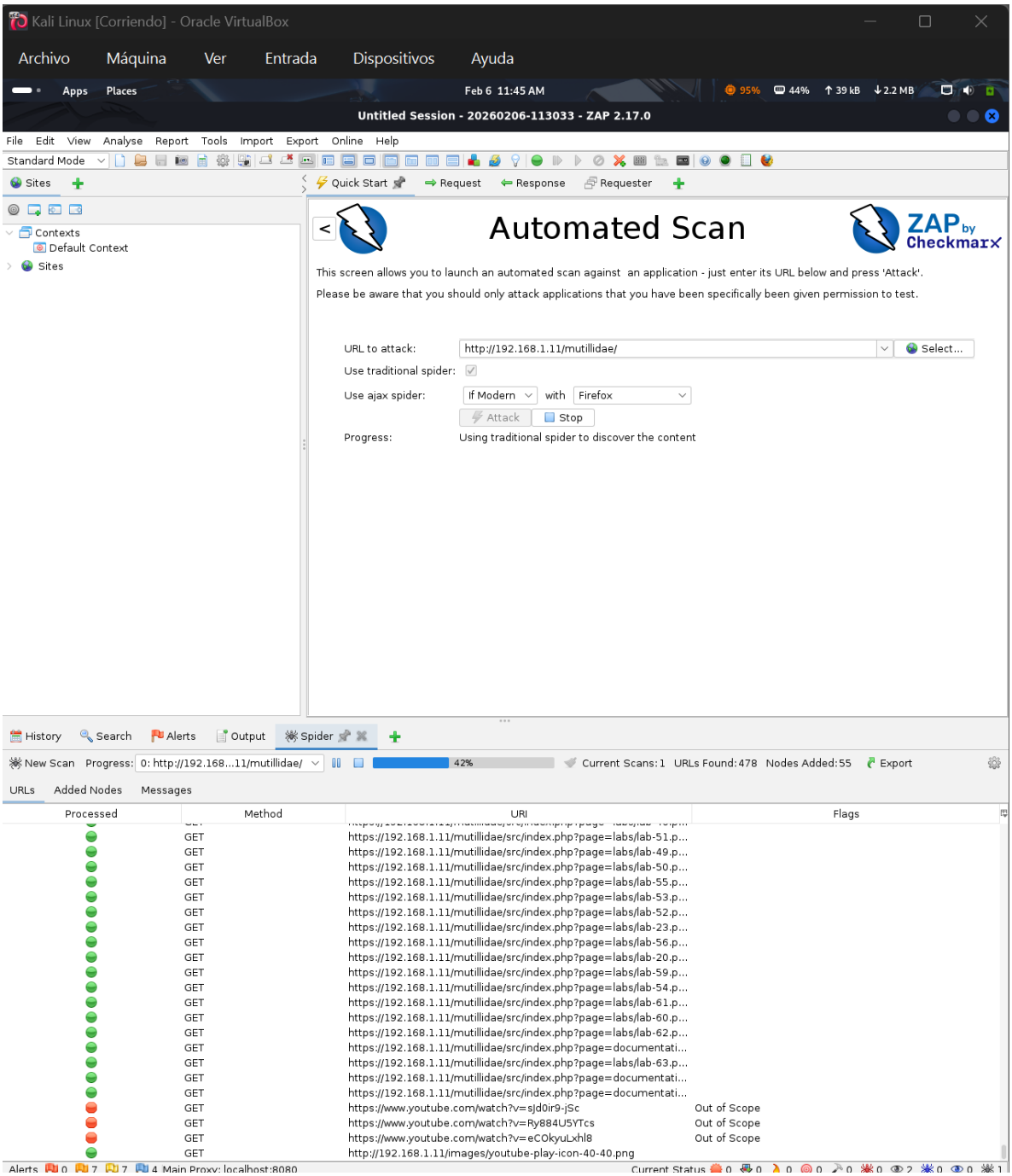
- OWASP ZAP for the scan automatized and fuzzing
- Kali Linux as an attack environment

Initial State

The application its function normal in /index.php

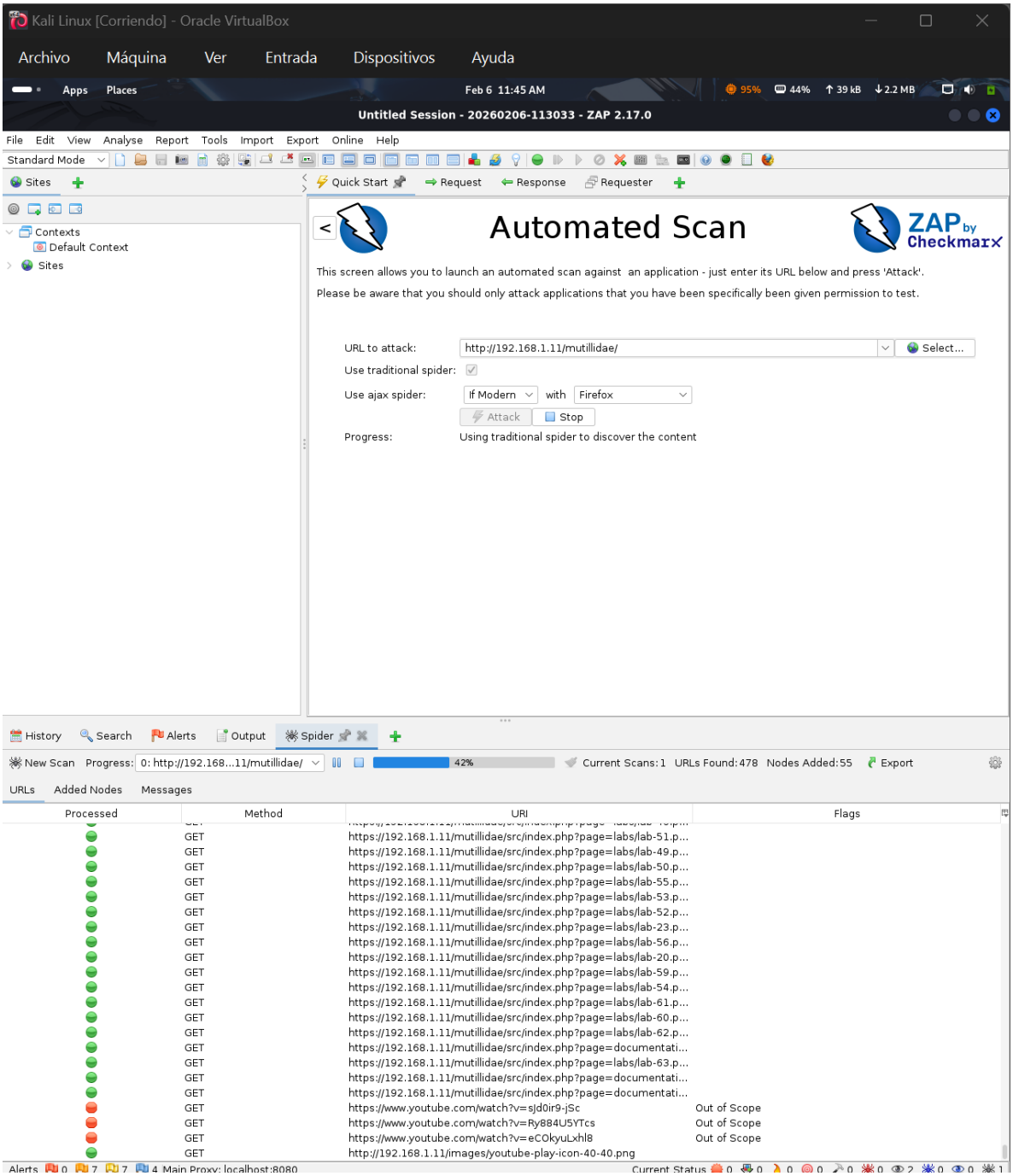
Injection/Exploitation:

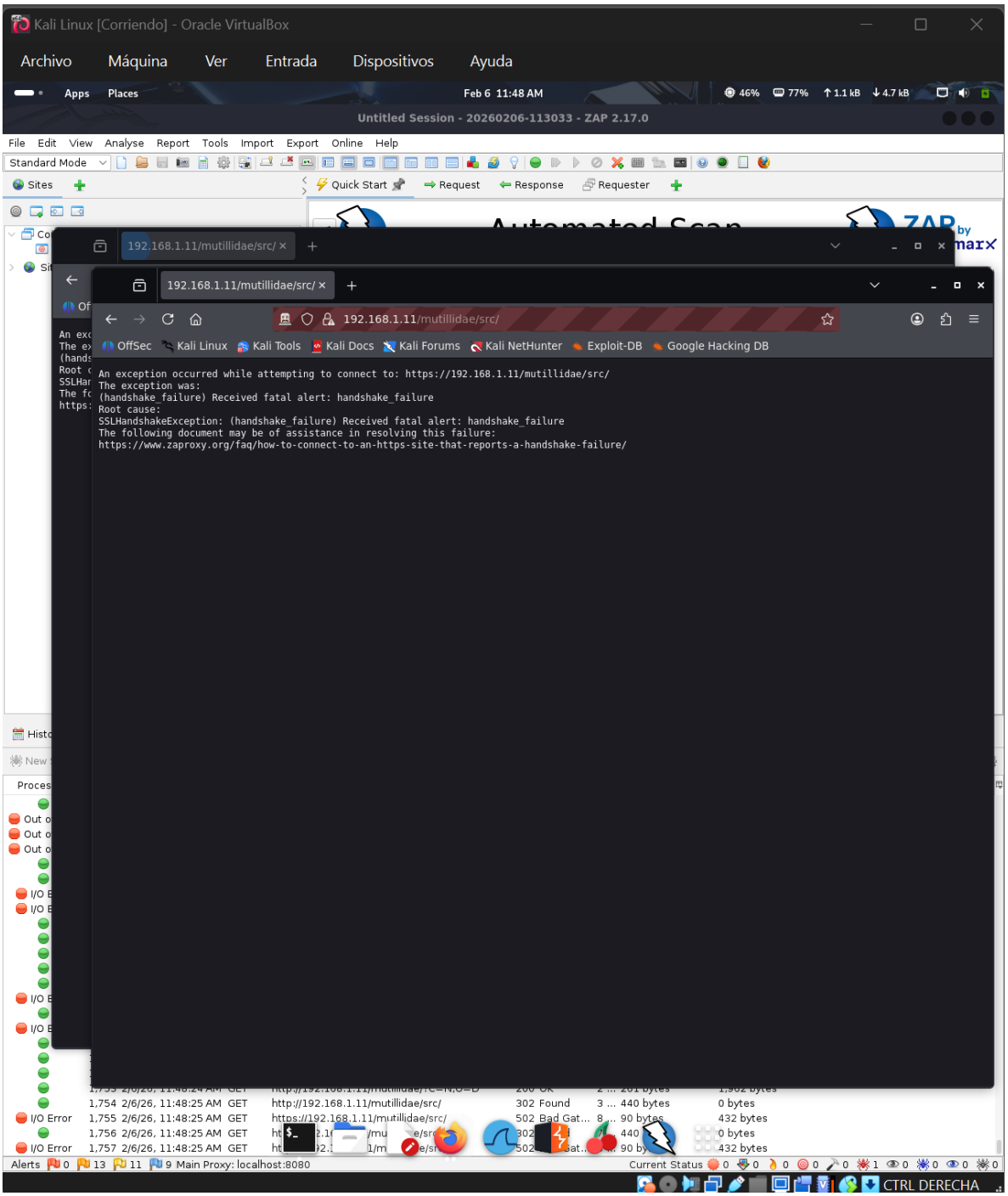
Is configure OWASP ZAP for the attack automatized to http://192.168.1.11/mutillidae/ and click in attack

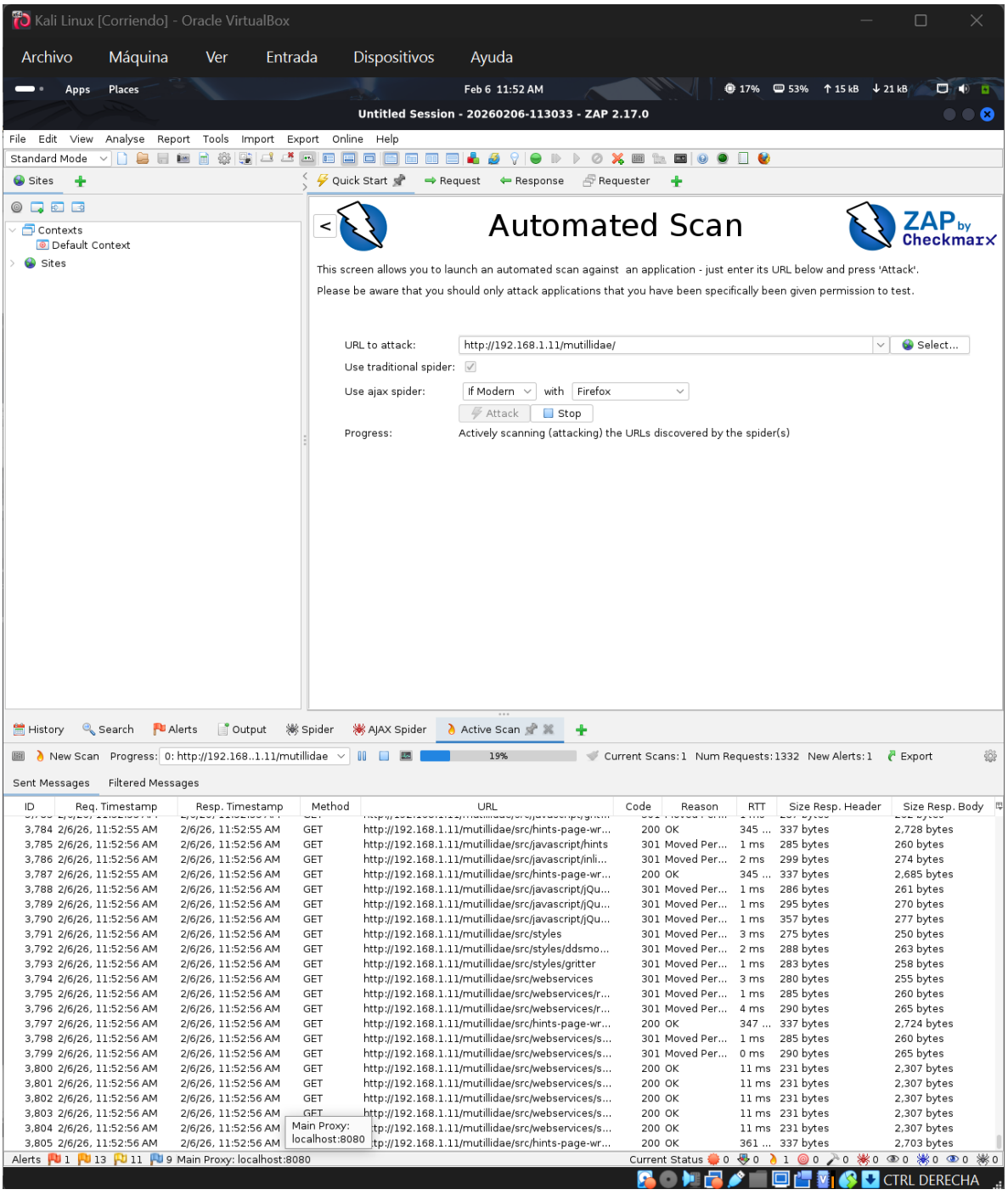


Results:

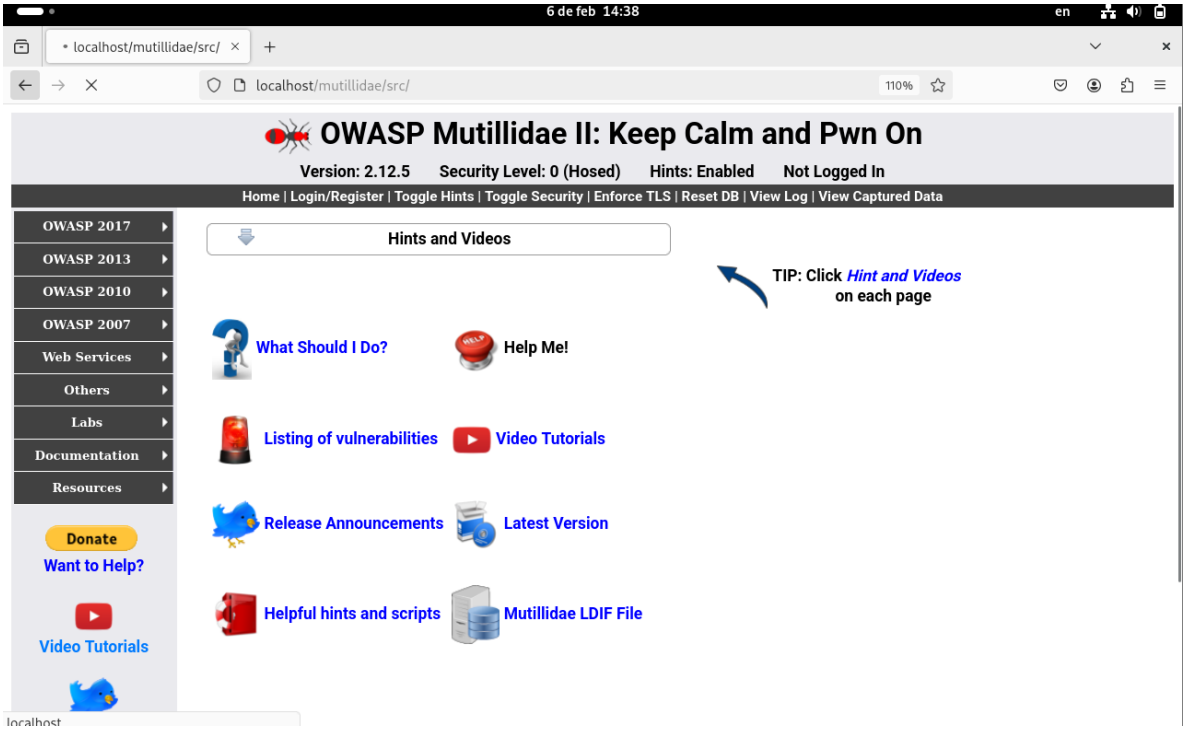
The results are that the application leave of function since I can't stand so many requests

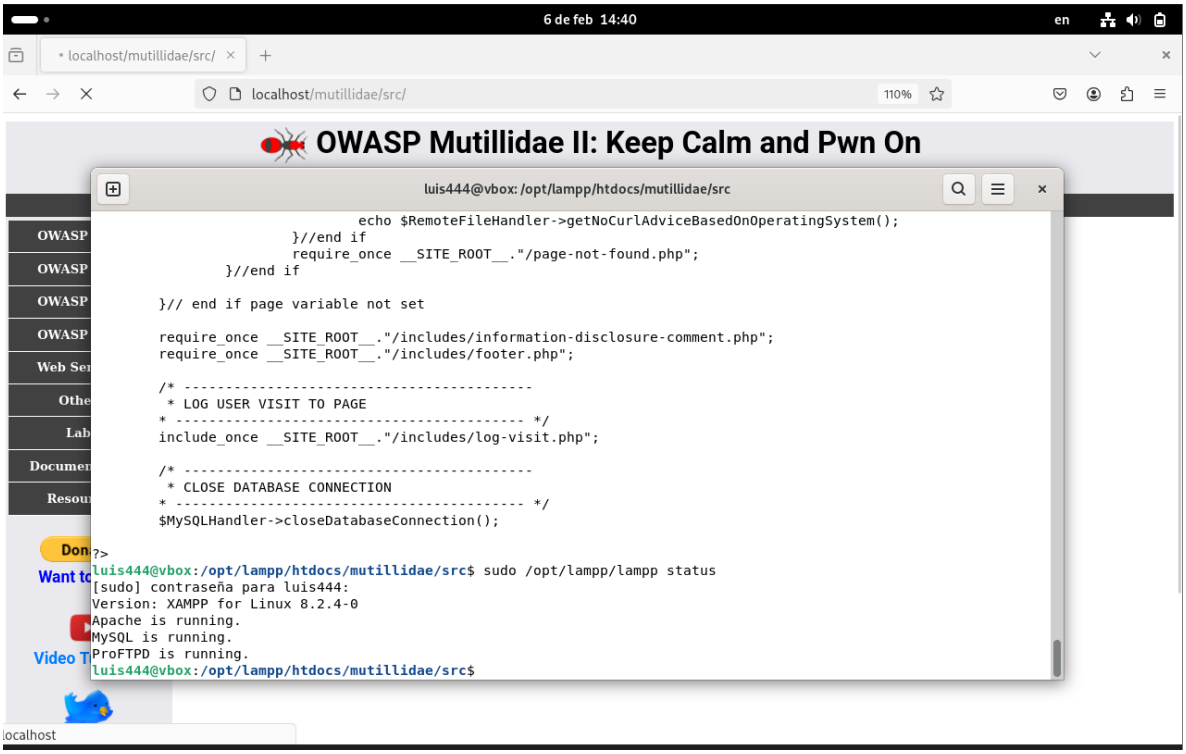



Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Apps Places Feb 6 11:48 AM
Untitled Session - 20260206-113033 - ZAP 2.17.0
192.168.1.11/mutillidae/src/
192.168.1.11/mutillidae/src/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
An exception occurred while attempting to connect to: https://192.168.1.11/mutillidae/src/
The exception was:
(handshake_failure) Received fatal alert: handshake_failure
Root cause:
SSLHandshakeException: (handshake_failure) Received fatal alert: handshake_failure
The following document may be of assistance in resolving this failure:
https://www.zaproxy.org/faq/how-to-connect-to-an-https-site-that-reports-a-handshake-failure/
1,754 2/6/26, 11:48:25 AM GET http://192.168.1.11/mutillidae/src/ 302 Found 440 bytes 0 bytes
1,755 2/6/26, 11:48:25 AM GET https://192.168.1.11/mutillidae/src/ 502 Bad Gat... 90 bytes 432 bytes
1,756 2/6/26, 11:48:25 AM GET 440 0 bytes
1,757 2/6/26, 11:48:25 AM GET 90 bytes 432 bytes
Alerts 0 13 11 9 Main Proxy: localhost:8080
Current Status
CTRL DERECHA


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Apps Places Feb 6 11:52 AM 17% 53% 15 kB 21 kB
Untitled Session - 20260206-113033 - ZAP 2.17.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start Request Response Requester
Contexts
Default Context
Sites
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://192.168.1.11/mutillidae/
Select...
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack Stop
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)
History Search Alerts Output Spider AJAX Spider Active Scan
New Scan Progress: 0: http://192.168..1.11/mutillidae 19% Current Scans: 1 Num Requests: 1332 New Alerts: 1 Export
Sent Messages Filtered Messages
ID Req. Timestamp Resp. Timestamp Method URL Code Reason RTT Size Resp. Header Size Resp. Body
3,784 2/6/26, 11:52:55 AM 2/6/26, 11:52:55 AM GET http://192.168.1.11/mutillidae/src/hints-page-wr... 200 OK 345 ... 337 bytes 2,728 bytes
3,785 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/javascript/hints 301 Moved Per... 1 ms 285 bytes 260 bytes
3,786 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/javascript/inli... 301 Moved Per... 2 ms 299 bytes 274 bytes
3,787 2/6/26, 11:52:55 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/hints-page-wr... 200 OK 345 ... 337 bytes 2,685 bytes
3,788 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/javascript/jQu... 301 Moved Per... 1 ms 286 bytes 261 bytes
3,789 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/javascript/jQu... 301 Moved Per... 1 ms 295 bytes 270 bytes
3,790 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/javascript/jQu... 301 Moved Per... 1 ms 357 bytes 277 bytes
3,791 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/styles 301 Moved Per... 3 ms 275 bytes 250 bytes
3,792 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/styles/ddsmo... 301 Moved Per... 2 ms 288 bytes 263 bytes
3,793 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/styles/gritter 301 Moved Per... 1 ms 283 bytes 258 bytes
3,794 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices 301 Moved Per... 3 ms 280 bytes 255 bytes
3,795 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/r... 301 Moved Per... 1 ms 285 bytes 260 bytes
3,796 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/r... 301 Moved Per... 4 ms 290 bytes 265 bytes
3,797 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/hints-page-wr... 200 OK 347 ... 337 bytes 2,724 bytes
3,798 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/s... 301 Moved Per... 1 ms 285 bytes 260 bytes
3,799 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/s... 301 Moved Per... 0 ms 290 bytes 265 bytes
3,800 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/s... 200 OK 11 ms 231 bytes 2,307 bytes
3,801 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/s... 200 OK 11 ms 231 bytes 2,307 bytes
3,802 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/s... 200 OK 11 ms 231 bytes 2,307 bytes
3,803 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/s... 200 OK 11 ms 231 bytes 2,307 bytes
3,804 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/webservices/s... 200 OK 11 ms 231 bytes 2,307 bytes
3,805 2/6/26, 11:52:56 AM 2/6/26, 11:52:56 AM GET http://192.168.1.11/mutillidae/src/hints-page-wr... 200 OK 361 ... 337 bytes 2,703 bytes
Main Proxy: localhost:8080
Alerts 1 13 11 9 Main Proxy: localhost:8080
Current Status 0 0 1 0 0 0 0 0 0 0
CTRL DERECHA

When I try to access the login page it only loads but does nothing





Mitigation and Remediation Strategies

Solution to level of code:

This would be the corrected code

```
if (!isset($_SESSION["showhints"])) {
   $_SESSION["showhints"] = 1; // valor por defecto
}
```

With this change, the state of the application depends only on the session controlled by the server, eliminating the possibility of manipulation by the client.

Defense in depth

Defending in depth against Denial of Service and cookie tampering attacks involves applying multiple layers of security: using a WAF to filter out anomalous traffic, setting secure session cookies with HttpOnly, Secure, and SameSite attributes, applying CSP policies to reduce risks injection, and maintain the principle of least privilege on servers and databases. Additionally, IDS/IPS monitoring can detect attack patterns and strengthen system availability.

Technical Report: Vulnerability Analysis and Demon Denial of Service

Author: Luis Enrique Islas Acosta

Date: February 10, 2026

Introduction.

The vulnerability called Denial of Service (DoS) happens when a service or web application receives a large number of requests with the intention of exhausting its resources and making it unavailable. It is linked to OWASP categories such as Software and Data Integrity Failures and the improper handling of exceptional conditions, since these weaknesses directly affect system availability. The impact on a company can be considerable: service interruptions can halt critical operations, reduce customer satisfaction, damage reputation, and cause financial losses, depending on the scale and duration of the attack.

Severity: