

SEMINAR 3

AUTOMATED VULNERABILITY SCANNING TOOLS



Finding vulnerabilities made easy



JOSÉ MANUEL REDONDO LÓPEZ "S-81 ISAAC PERAL" PROJECT V4.0



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

Logo: @creative_vanesa (Instagram)



INDEX

- ▶ Introduction
- ▶ Automated scanning tools for servers
- ▶ Complementary automated scanning tools for the web

[< Go to Index](#)

INTRODUCTION

Understanding the purpose these tools



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

- **Is there a quick way to test if a system have vulnerabilities?**
 - Yes, although it is not perfect: **automatic vulnerability discovery tools**
- **We will review a couple of them in this seminar**
- **They allow us to obtain a clear summary of the most evident vulnerabilities a system may have, saving us time**
 - **They DO NOT substitute (just complement) the work of a proper security audit**
- **These tools just perform vulnerability scans**
 - **NEVER** to be confused with a pentesting or with the work of a Red Team
 - Some companies call using one of these tools “pentesting”: this is deceiving and **WRONG**

INTRODUCTION: THE IMPORTANCE OF THESE TOOLS

- They are **professional and very powerful** programs that automatically discover vulnerabilities on any machine
 - Windows, Linux, MacOS, web server or not, ...
- They might save us a LOT of time
 - And could do better work than us detecting vulnerabilities manually in certain cases
 - We can try to combine the results of multiple ones to increase result reliability
- If all the problems detected by these tools are fixed, the target machine will be significantly less vulnerable
 - Therefore, they are necessary tools for every security engineer...
 - ... but we shouldn't just use them for a full analysis and do nothing more
- Every tool generates a substantial amount of network traffic
 - And may require a high number of resources from the target
 - Therefore, we **NEVER** have to launch them without proper authorization from the owner!

INTRODUCTION: OTHER TOOLS



Computer Security

● We will review some of these tools

- But we can find additional ones that allow us to explore the target considering different criteria or vulnerabilities to find

● Some are

- Invicti (previously Netsparker): <https://www.invicti.com/>
- Acunetix: <https://www.acunetix.com/>
- Core Impact: <https://www.coresecurity.com/products/core-impact>
- Probely: <https://probely.com/>
- Indusface WAS Free Website Security Check: <https://www.indusface.com/website-security-scan.php>
- Dradis Reporting and Collaboration tools for security professionals (**not really a vulnerability scanner**, but very useful to communicate their results): <https://dradisframework.com/ce/>

● More information

- <https://www.softwaretestinghelp.com/penetration-testing-tools/>

[< Go to Index](#)

AUTOMATED VULNERABILITY SCANNING TOOLS

Automatic scanning for machines



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

● One of the most used tools of this type

- Allows in-depth analysis of a computer
- Performing a detailed audit of its services
- Covering a great amount of potential security issue vectors
- Analyzes configurations, patches, webs, networks, systems, data and applications...

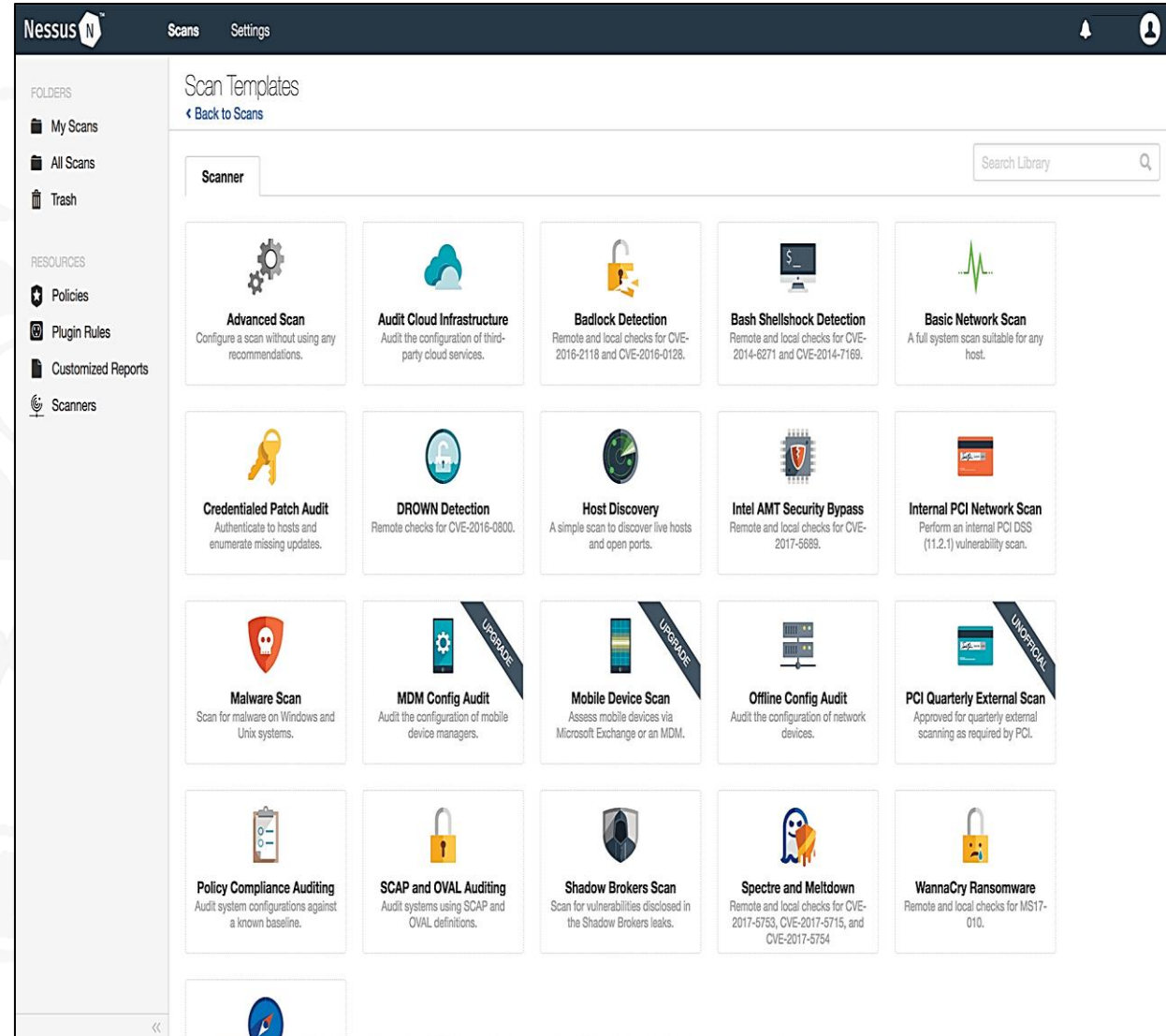
● Requires 4+ Gb RAM (just for the app)

● Detects more than 100,000 potential vulnerabilities (frequently updated)

- The free version (Nessus Home Feed) detects less vulnerabilities than the commercial one
- And is limited to 16 different IPs

● Tutorial

- http://www.reydes.com/d/?q=Instalacion_de_Nessus_en_Kali_Linux



- Part of the commercial vulnerability management product family "Greenbone Security Manager" (GSM)

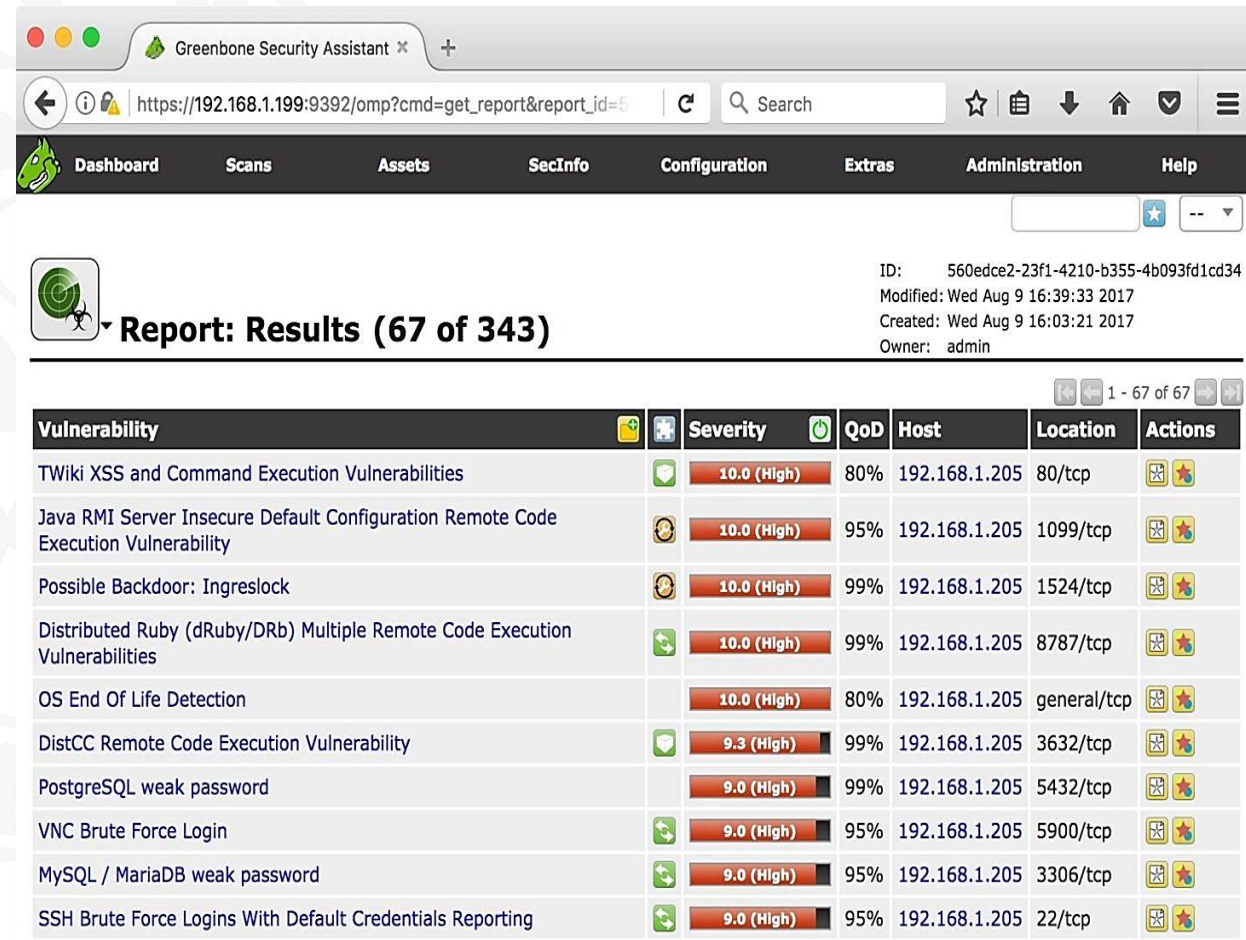
- Allows detailed vulnerability scans

- You can check more than 53,000+ different vulnerabilities, being updated daily
- Requires to update its vulnerability DB periodically to maximize detection
- The process is not straightforward
 - `sudo runuser -u _gvm -- greenbone-nvt-sync`
 - `sudo runuser -u _gvm -- greenbone-scadata-sync`
 - `sudo runuser -u _gvm -- greenbone-certdata-sync`
- Also requires 4+ Gb RAM just for the app

- Tutorials

- <https://blog.ehcgroup.io/index.php/2018/06/21/escaneo-de-vulnerabilidades-con-openvas-9-parte-1-instalacion-y-configuracion/>
- <https://blog.ehcgroup.io/index.php/2018/06/21/escaneo-de-vulnerabilidades-con-openvas-9-parte-2-escaneo-de-vulnerabilidades/>

Source: <https://null-byte.wonderhowto.com/how-to/perform-large-scale-network-security-audit-with-openvass-gsa-0179340/>



The screenshot shows the OpenVAS Greenbone Security Assistant (GSA) web interface. The browser address bar displays the URL: `https://192.168.1.199:9392/omp?cmd=get_report&report_id=5`. The interface includes a navigation menu with options: Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area displays a report titled "Report: Results (67 of 343)". The report details include: ID: 560edce2-23f1-4210-b355-4b093fd1cd34, Modified: Wed Aug 9 16:39:33 2017, Created: Wed Aug 9 16:03:21 2017, and Owner: admin. Below the report header is a table of vulnerabilities.

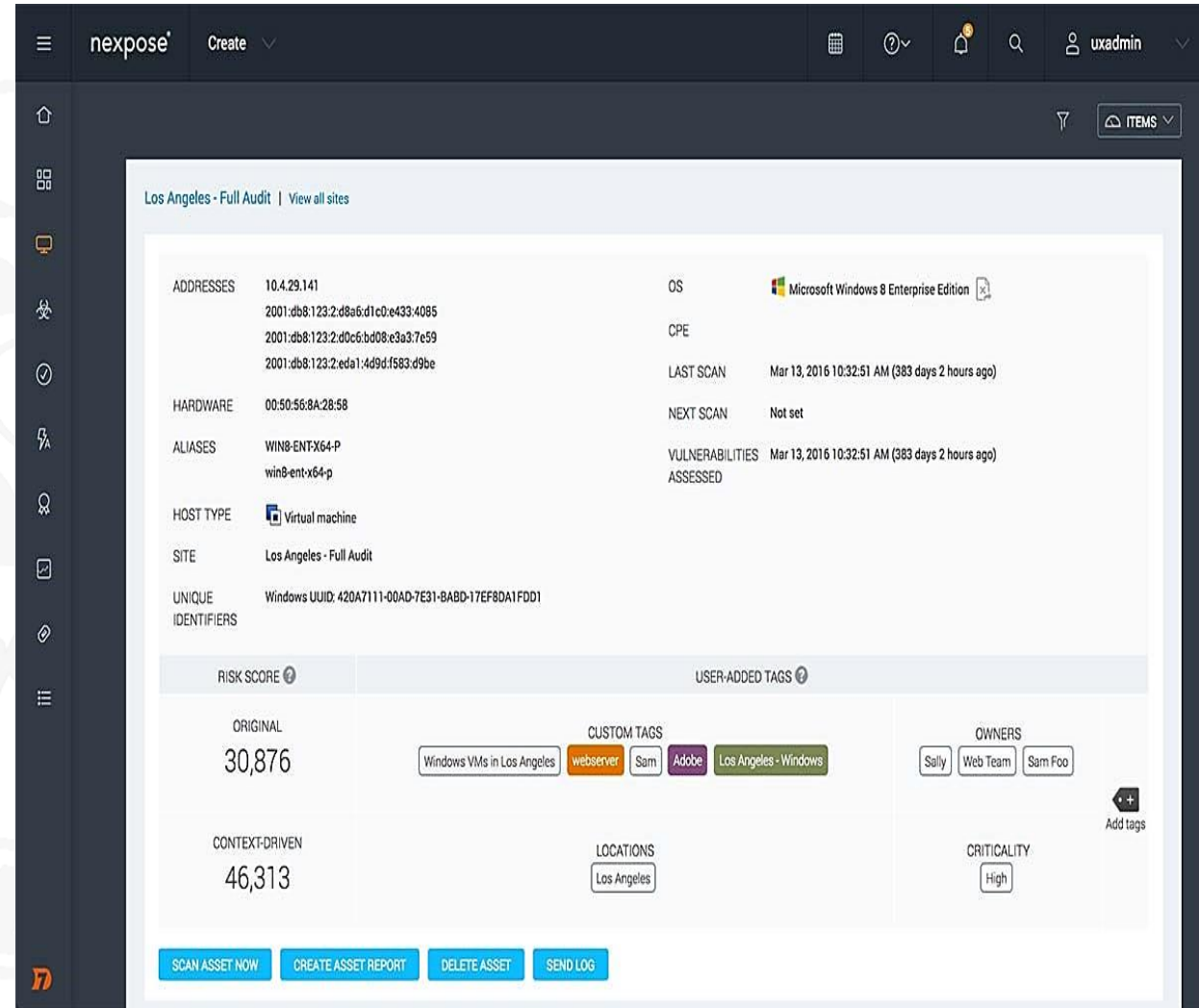
Vulnerability	Severity	QoD	Host	Location	Actions
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.1.205	80/tcp	[Icons]
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.1.205	1099/tcp	[Icons]
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.205	1524/tcp	[Icons]
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.1.205	8787/tcp	[Icons]
OS End Of Life Detection	10.0 (High)	80%	192.168.1.205	general/tcp	[Icons]
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.205	3632/tcp	[Icons]
PostgreSQL weak password	9.0 (High)	99%	192.168.1.205	5432/tcp	[Icons]
VNC Brute Force Login	9.0 (High)	95%	192.168.1.205	5900/tcp	[Icons]
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.1.205	3306/tcp	[Icons]
SSH Brute Force Logins With Default Credentials Reporting	9.0 (High)	95%	192.168.1.205	22/tcp	[Icons]

● Considered the most powerful automatic vulnerability discovery tool

- Complete vulnerability management platform
 - Risks, vulnerability tracking, vulnerabilities on containers...
- Discovers vulnerabilities and shows their possible exploits
- But it can use more exploits than other similar tools that we will see (Metasploit)
- Shows more vulnerabilities and works on a larger scale than other similar tools
- Unfortunately, it is not free (30-day trial only)

● Tutorial

- <https://www.javatpoint.com/ethical-hacking-installing-nexpose>



The screenshot displays the Nexpose web interface for an asset named 'Los Angeles - Full Audit'. The interface is divided into several sections:

- Metadata:** Includes ADDRESSES (10.4.29.141, 2001:db8:123:2:d8a6:d1c0:e433:4085, 2001:db8:123:2:d0c6:bd08:e3a3:7e59, 2001:db8:123:2:eda1:4d9d:f583:d9be), OS (Microsoft Windows 8 Enterprise Edition), CPE, LAST SCAN (Mar 13, 2016 10:32:51 AM (383 days 2 hours ago)), NEXT SCAN (Not set), VULNERABILITIES ASSESSED (Mar 13, 2016 10:32:51 AM (383 days 2 hours ago)), HARDWARE (00:50:56:8A:28:58), ALIASES (WIN8-ENTX64-P, win8-ent-x64-p), HOST TYPE (Virtual machine), SITE (Los Angeles - Full Audit), and UNIQUE IDENTIFIERS (Windows UUID: 420A7111-00AD-7E31-BABD-17EF8DA1FDD1).
- RISK SCORE:** Shows an ORIGINAL score of 30,876 and a CONTEXT-DRIVEN score of 46,313.
- CUSTOM TAGS:** Includes 'Windows VMs in Los Angeles', 'webserver', 'Sam', 'Adobe', and 'Los Angeles - Windows'.
- OWNERS:** Lists 'Sally', 'Web Team', and 'Sam Foo'.
- LOCATIONS:** Shows 'Los Angeles'.
- CRITICALITY:** Set to 'High'.

At the bottom, there are four buttons: 'SCAN ASSET NOW', 'CREATE ASSET REPORT', 'DELETE ASSET', and 'SEND LOG'.

(1) Analyzing a sample OpenVAS / Nessus output

Medium (CVSS: 4.3)

NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

cpe:/a:jquery:jquery:1.7.1

Detected by jQuery Detection (OID: 1.3.6.1.4.1.25623.1.0.141622)

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

Installed version: 1.7.1

Fixed version: 1.9.0

Solution

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: jQuery < 1.9.0 XSS Vulnerability

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: \$Revision: 12183 \$

Product Detection Result

Product: cpe:/a:jquery:jquery:1.7.1

Method: jQuery Detection

OID: 1.3.6.1.4.1.25623.1.0.141622)

References

CVE: CVE-2012-6708

Other:

URL:https://bugs.jquery.com/ticket/11290

1 Result Overview

Host	High	Medium	Low	Log	False Positive
[REDACTED]uniovi.es	0	9	0	28	0
Total: 1	0	9	0	28	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

This report contains all 37 results selected by the filtering described above. Before filtering there were 37 results.

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

81777 - MongoDB Service Without Authentication Detection

Synopsis

The remote host is running a database system that does not have authentication enabled.

Description

MongoDB, a document-oriented database system, is listening on the remote port, and it is configured to allow connections without any authentication. A remote attacker can therefore connect to the database system in order to create, read, update, and delete documents, collections, and databases.

See Also

<https://www.mongodb.com/>

Solution

Enable authentication or restrict access to the MongoDB service.

Risk Factor

Medium

[< Go to Index](#)

COMPLEMENTARY AUTOMATED WEB VULNERABILITY SCANNING TOOLS

Automatic scanning for the web (additional tools)



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo



WHY A SEPARATE CATEGORY OF TOOLS?

- **Web-based applications are everywhere nowadays, and have their own type of specific vulnerabilities**
- **The previous tools may also detect them**
 - But the scope of these tools is very broad and require a lot of time to complete the scan
 - Maybe they report things we are not interested in if we only need to handle web vulnerabilities
 - Web vulnerabilities depend on the technologies / frameworks used to build them
 - These tools focus only on the web and allow us to perform specialized scans more efficiently
 - **Therefore, they discover web vulnerabilities faster** (and with less resource requirements)
- **Therefore, they are a complement of the previous ones and those shown in other course parts**

BURP SUITE

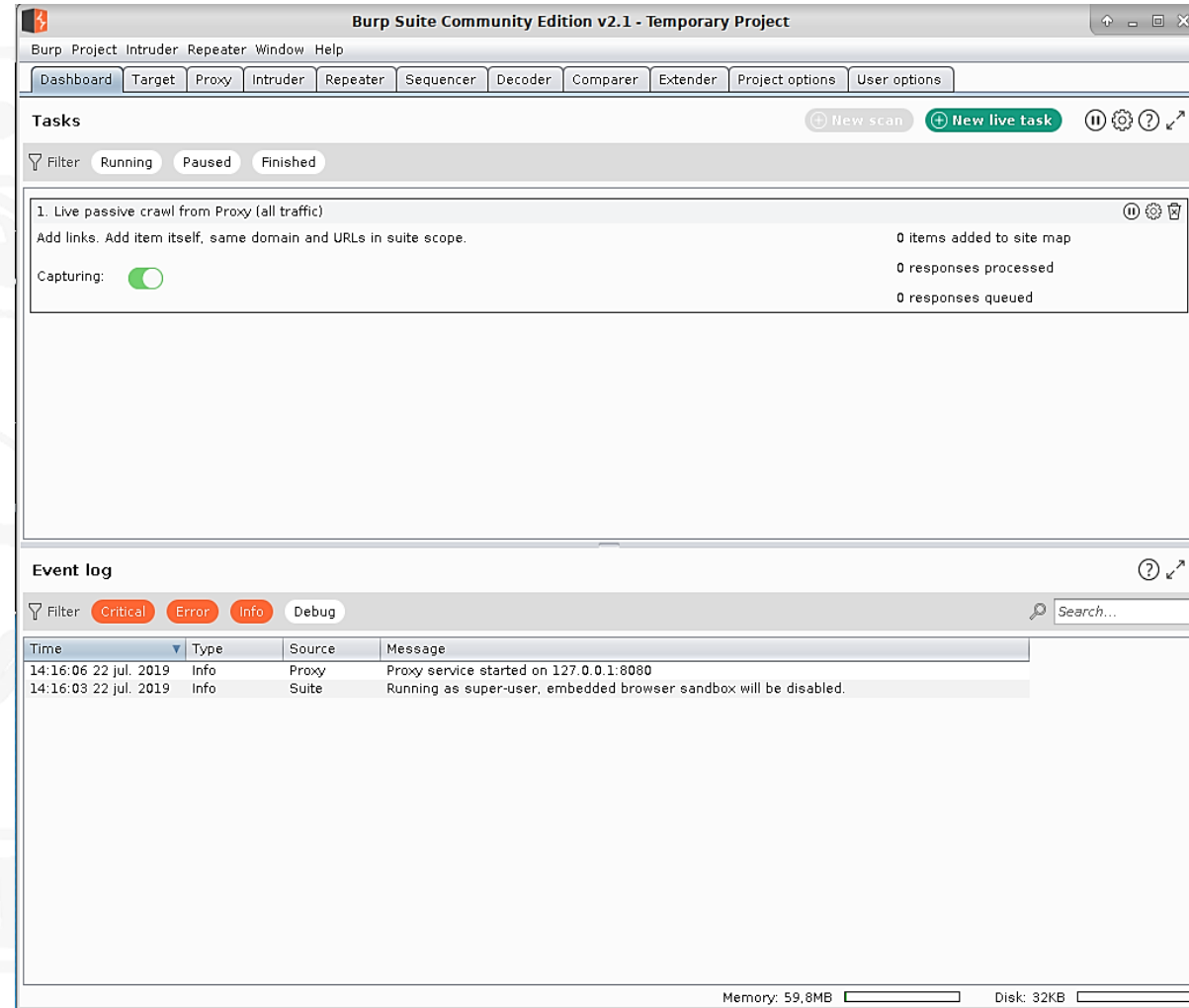
<http://portswigger.net/burp/>



Computer Security

● It is a multipurpose tool

- **Proxy interceptor**: allows you to inspect and modify traffic between browser and applications
- **Spider**: automatic / manual website inspection
 - A manual spider collects information from a website as we browse it
 - It doesn't have the limitations of automatic ones
- **Scanner**: detecting various types of vulnerabilities in web applications
- An **intrusion module** to find and exploit vulnerabilities
- A **request repetition** module
- Analysis of the **session token strength**
- Some of these features are only for the non-free version



● Usages of the free version

- Observing **GET**, **POST** parameters of any web request and its responses
- “Freeze” the request before it goes to the server, and allow you to modify **ANY PART OF IT**
 - Headers, parameters, parameter values, cookies...
 - Once all the client validation has been executed (JavaScript)
 - Therefore, with tools like this, **client-side validation is not effective** (can be easily bypassed)
- Allows to **fully transform** the information sent from clients to servers
 - Causing errors that would not be possible otherwise...

● Admits **extensions** that greatly improve its functionality

- List of most useful extensions: <https://github.com/snoopyscurity/awesome-burp-extensions>
- Extension to rotate the IP on each request: <https://www.kitploit.com/2019/08/iprotate-extension-for-burp-suite-which.html>
- Extension to find XSS vulnerabilities: <https://github.com/wish-i-was/femida>

● There are other similar applications

- Zap: <https://owasp.org/www-project-zap/>
- WebScarab: https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- **More:** https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

CLIENT-SIDE VALIDATION



- When we say we can bypass client-side validation we mean that some pages really rely on it thinking that it is a real security measure
 - This is an error, and it has a great cost
 - Things like this check the input values of the client... (**NOTE:** This script is from a real website)
 - But once they reach Burp you can modify them, **rendering all this code useless!**

```
//comprobacion SQL injection
function chequear_sql(elmFORM)
{
    var mensaje, patron;
    var token_trobat = new Array();
    var cnjFORM = document.getElementById(elmFORM);

    patron = /\binsert\s+.*into\b|\bselect\s+.*\bfrom\b|\bupdate\b|\bdelete\s+.*\b|\bdistinct\b|\btruncate\b|\breplace\b|\bexists\b|\bprocedure\b|\border\s+by\b|\bgroup\s+by\b|\balter\s+(table|clus

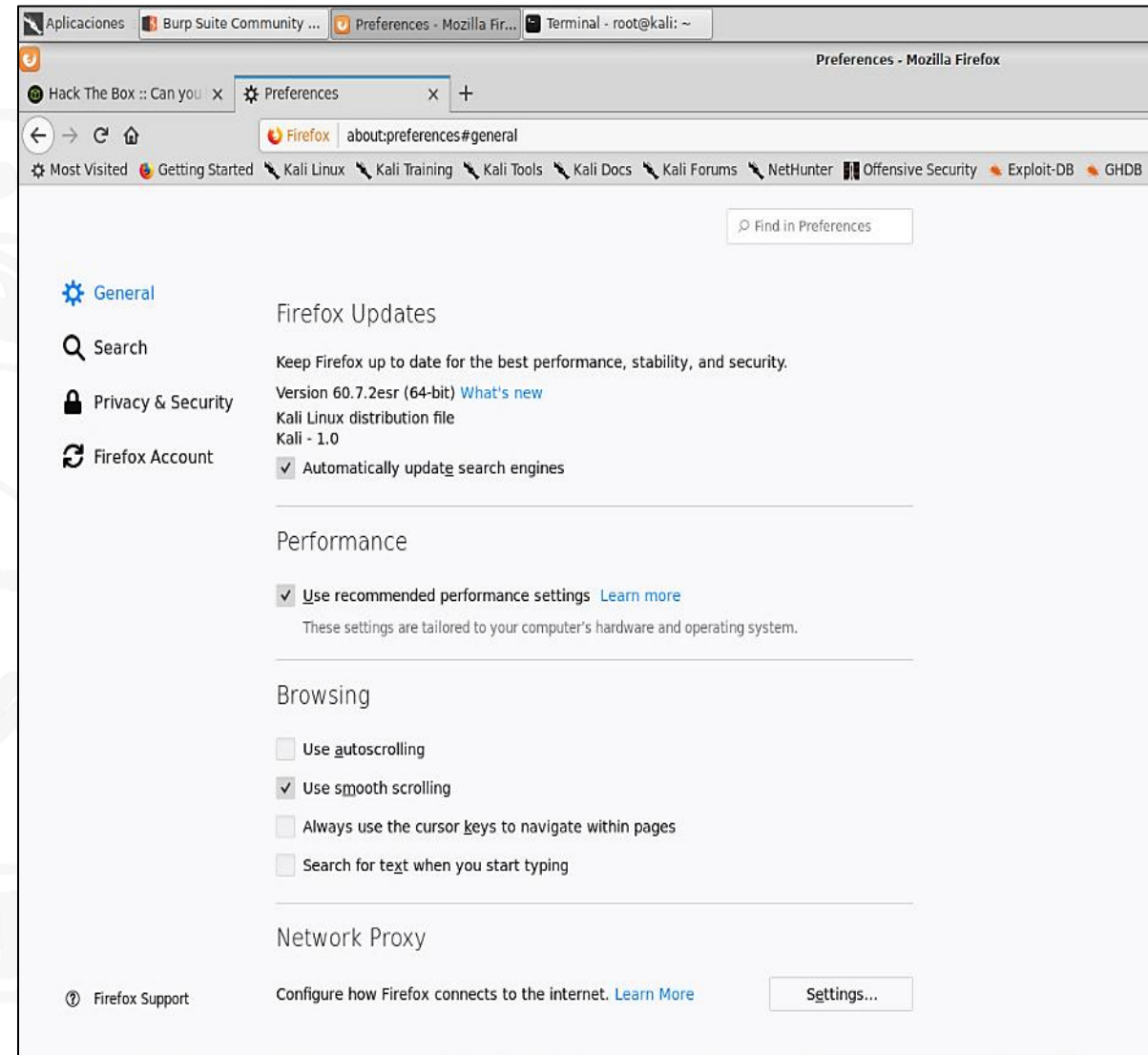
    for (var i=0; i<cnjFORM.length; i++)
    {
        token_trobat = patron.exec(cnjFORM[i].value);
        if ((cnjFORM[i].type != 'hidden') && (token_trobat != null))
        {
            mensaje = MENSAJES[6000]+token_trobat[0].toUpperCase();
            alert_generico(mensaje, cnjFORM[i].id , true);
            return false;
        }
    }
    return true;
}
```

BURP HTTP PROXY



Computer Security

- To use Burp proxy, it is necessary to tell the browser that we will use a proxy to send requests
- We must use the option to set up a proxy that every browser has
- In **Firefox** we can go to **General – Network Proxy**

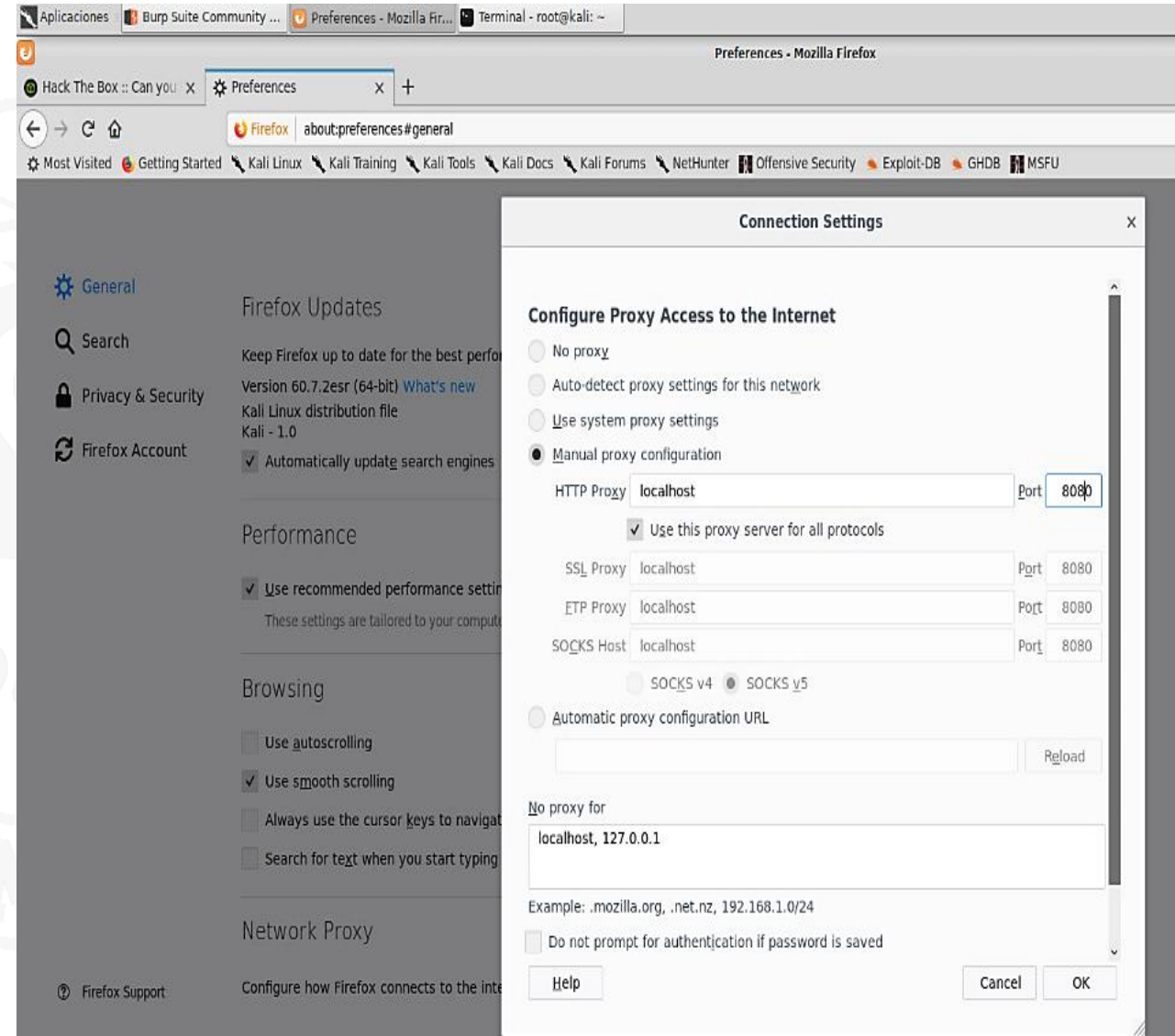


BURP HTTP PROXY



Computer Security

- Once Burp starts, it remains listening on localhost, port 8080
- So, we must indicate this address to use Burp as a proxy for everything
- Now we can "intercept" all the HTTP traffic we generate!
- Both requests and their responses

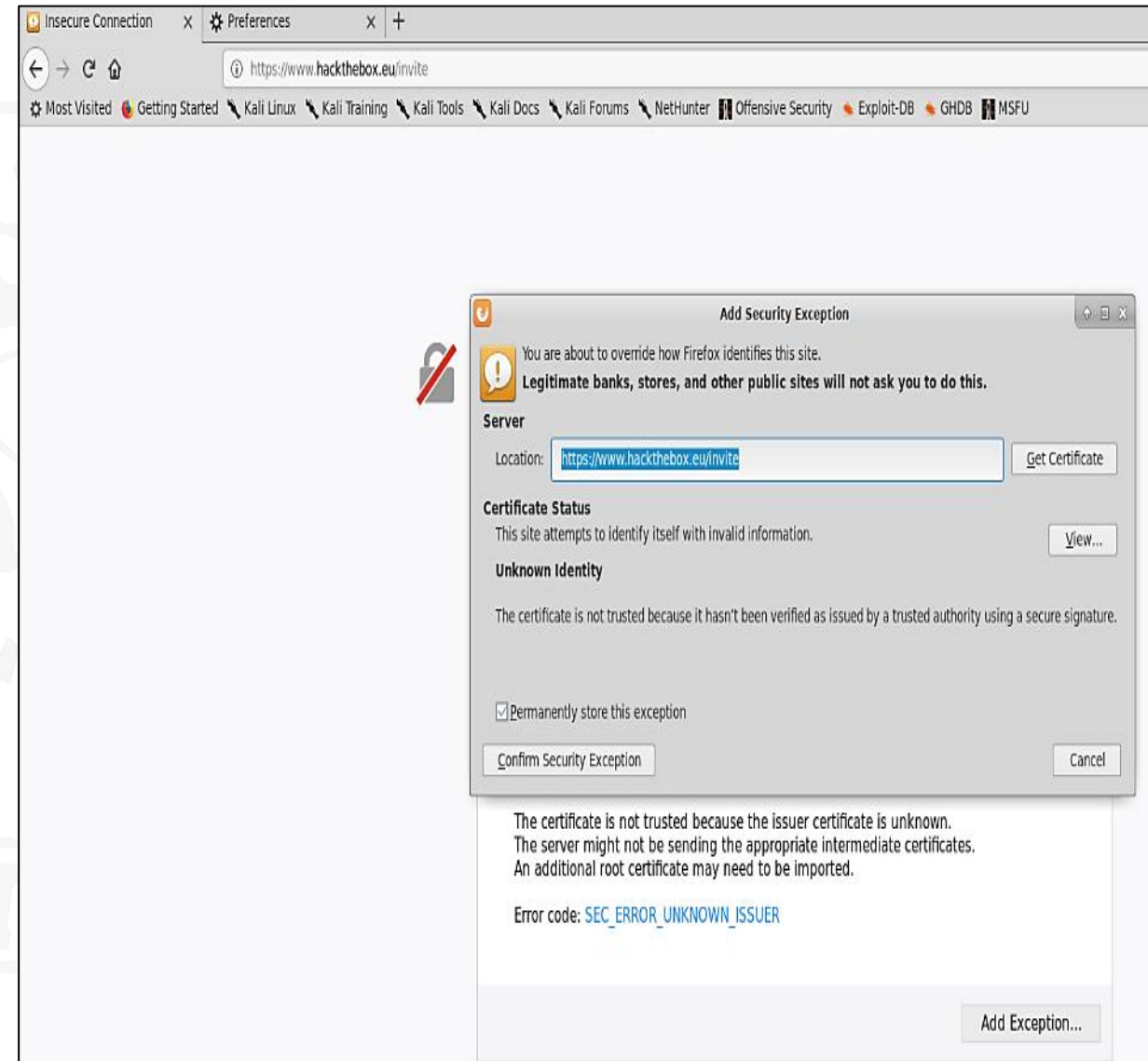


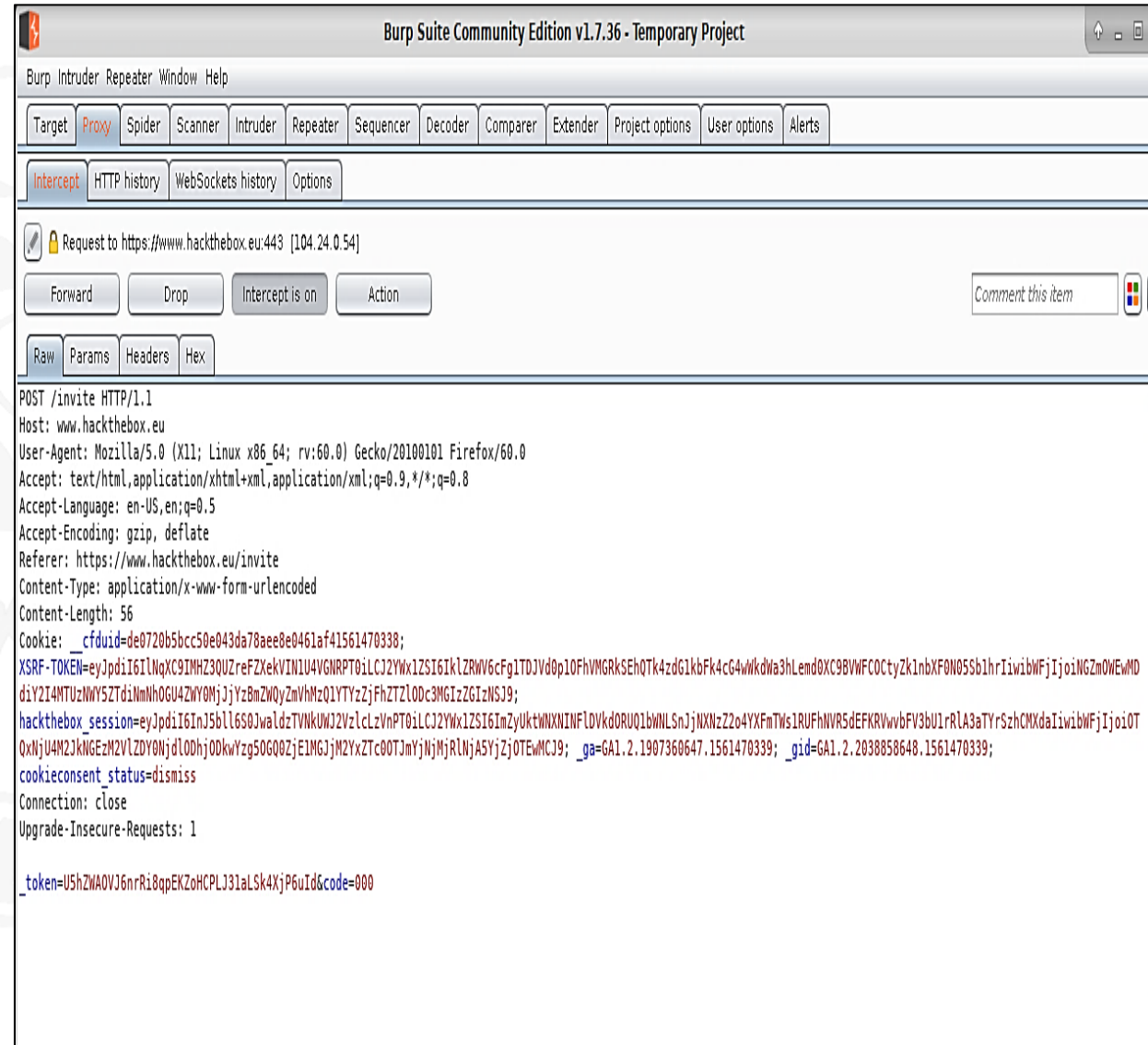
BURP HTTP PROXY: INSPECTING



Computer Security

- Sometimes the browser shows errors!
- When using HTTPs, using a proxy may cause the browser to show a potential AitM warning
 - There's an intermediary intercepting a supposedly secure connection!
 - In this case we can add an exception, as we indeed are doing it!
- But if this happens in real life, with a website that never had such problems
 - It may be exactly that!
 - Either the administrator has renewed the website certificates wrongly
 - Or somebody is doing an Attacker-in-the-Middle (AitM) attack to steal our data, **watch out!**





● The HTTP request header

- **A cookie with a session ID: in this case is truly random, not predictable**

- **__cfuid**: session ID that showing that the service is behind CloudFlare

- **We know how to view and modify any HTTP traffic at will**

- The screenshot displays the Burp Suite Community Edition v1.7.36 interface. The top menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". Below the menu is a toolbar with buttons for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. A secondary toolbar shows Intercept (highlighted), HTTP history, WebSockets history, and Options.

The main window shows a captured request from https://www.hackthebox.eu:443 [104.24.0.54]. The status bar indicates "Request is on". Action buttons include Forward, Drop, Intercept is on, and Action. A comment field contains "Comment this item".

The raw view of the request is shown below:

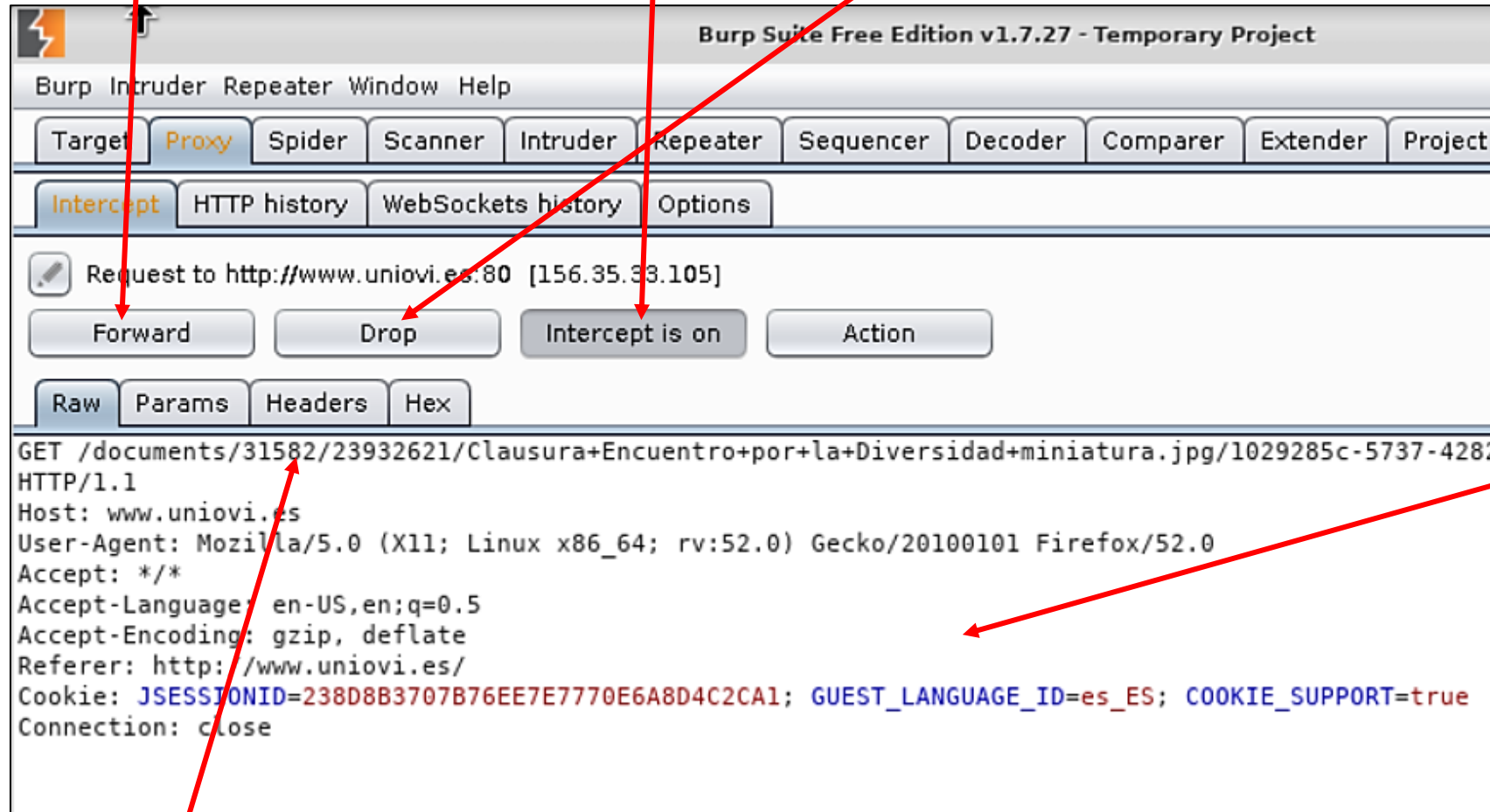
```
POST /invite HTTP/1.1
Host: www.hackthebox.eu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.hackthebox.eu/invite
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Cookie: cfduid=de0720b5bc50e043da78ae8e0461af41561470338;
XSRF-TOKEN=eypJpdIi6lInQKXC9IMH3QUZreFZXekVINIU4VGNRPT0iLCJ2YWx1ZSI6Ik1ZRWV6cFg1TDJvD0p1OFhVNGRKSUhQTk4zdG1kbFk4cG4wWkdwa3hLemd0XC9BWFcoCTYzklbnhXFN05SblhrIiwibWFiIjoiaWZmOWEwMDdiY2I4MTUzMWY5ZTdiNmNoGU4ZWYOMjJjYzBmZWQyZmVhMzQ1YTZzZjFhZTZlODc3MGZzZGIzNSJ9;
hackthebox_session=eypJpdIi6lInQKXC9IMH3QUZreFZXekVINIU4VGNRPT0iLCJ2YWx1ZSI6ImZyUktWNXNINWFldvdkORUQ1bWMLSnJjNXNzZ2o4YXFmTWsIRUFhNVRSdEFKRvwvbFV3bu1rLA3aTYrSzChCMXdaIiwibWFiIjoioTOTQwNjU4M2JlNGEzM2VlZDYONjdlODhjODkwYzg5OGQ0ZjElMGcjM2YxZTc0OTJmYjRlNjA5YjZjOTEwMCJ9; _ga=GA1.2.1907360647.1561470339; _gid=GA1.2.2038858648.1561470339;
cookieconsent_status=dismiss
Connection: close
Upgrade-Insecure-Requests: 1

_token=UShZWA0VJ6nrRi8qpEKZoHCPLJ3laLSk4XkjP6uId&code=000
```

Send the modified request to the server

This stops and shows us every request we make from the browser

This request will not reach the server!



Modify the URL parameters and see what happens

You can modify the body of the request and see what happens

☺ . E. g.:

- “New” HTTP methods: JET Instead of GET ☺
- Non-existent or wrong **versions** of HTTP
- **Host** or **Referer** set to different pages
- Changes in the **Cookie**: Another session ID...
- There are **many options**: The request is at our mercy, and with this tool we can skip any kind of client-side validation the page makes
- The client-side page code is 100% yours!

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

```
java.lang.NullPointerException
    com.mojo.blog.web.servlet.DemoErrorServlet.getNullPointerException(DemoErrorServlet.java:58)
    com.mojo.blog.web.servlet.DemoErrorServlet.processPage(DemoErrorServlet.java:34)
    com.mojo.blog.web.servlet.DemoErrorServlet.doGet(DemoErrorServlet.java:22)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:689)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
```

note The full stack trace of the root cause is available in the Apache Tomcat/5.5.9 logs.

Apache Tomcat/5.5.9

What if we use it to provoke errors?
Enumeration!

Technology used to make the page!

Server type and version!



Type and versions of software and operating system!

ADDITIONAL ENUMERATION TOOLS OF BURP SUITE

- **Apart from request manipulation, there are two additional Burp tools that are very useful in enumeration processes**
 - **Burp Repeater**: tool for manually manipulating and reissuing individual HTTP and WebSocket messages, analyzing the application's responses
 - It can be used to change parameter values to test for input-based vulnerabilities
 - Issuing requests in a specific sequence to test for logic flaws
 - Reissuing these requests from Burp Scanner
 - ...
 - **Tutorial**: <https://portswigger.net/burp/documentation/desktop/tools/repeater/using>
 - **Burp Spider**: Automatic crawler of all website pages
 - We can download the whole site and analyze its contents locally in detail
 - **Tutorial**: <https://fwhibbit.es/burp-suite-ii-construyendo-un-objetivo-sitemap-spider>

NIKTO2 / WIKTO

<http://www.cirt.net/nikto2/>, <http://research.sensepost.com/tools/web/wikto>



Computer Security

● GPL web server scanner

● Run a comprehensive test set to any web server looking for

- 6500+ dangerous files or CGIs
- Old server versions
- Known web server configuration issues
- Installed server and running services versions
 - Known vulnerabilities/issues with these versions

● Wikto (Nikto for Windows) adds some extra features, making it more powerful

● Consumes few resources, especially if compared to OpenVAS or Nessus

● Tutorial

- <https://www.securityartwork.es/2014/02/27/intro-al-escaner-de-web-nikto-ii/>

Nikto 2.1.6 Cheatsheet (ingenieriainformatica.uniovi.es)	
Lightweight web server vulnerability scanner	
https://cirt.net/Nikto2	
GENERAL USAGE	
nikto -host <url> [options]	
NOTES	
+ means that the option requires a value	
Options in stronger bold font are detailed in separate tables	
OPTIONS	
-config+ : Use this config file	
-dbcheck : check database and other key files for syntax errors	
-Display+ : Turn on/off display outputs	
-evasion : Encoding technique to use to avoid WAFs, etc.	
-Format+ : save file (-o) format	
-Help : Extended help information	
-host+ : target host/URL	
-id+ : Host authentication to use, format is id:pass or id:pass:realm	
-list-plugins : List all available plugins	
-mutate : Guess additional file names	
-no404 : Disables 404 checks	
-noss1 : Disables using SSL	
-output+ : Write output to this file	
-Plugins+ : List of plugins to run (default: ALL)	
-port+ : Port to use (default 80)	
-root+ : Prepend root value to all requests, format is /directory	
-ssl : Force ssl mode on port	
-timeout+ : Timeout for requests (default 10 seconds)	
-Tuning+ : Scan tuning	
-update : Update databases and plugins from CIRT.net	
-Version : Print plugin and database versions	
-vhost+ : Virtual host (for Host header)	
EVASION OPTIONS	
1	Random URI encoding (non-UTF8)
2	Directory self-reference (./)
3	Premature URL ending
4	Prepend long random string
5	Fake parameter
6	TAB as request spacer
7	Change the case of the URL
8	Use Windows directory separator (\)
A	Use a carriage return (0x0d) as a request spacer
B	Use binary value 0x0b as a request spacer
MUTATE OPTIONS	
1	Test all files with all root directories
2	Guess for password file names
3	Enumerate user names via Apache (/~user type requests)
4	Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests)
5	Attempt to brute force sub-domain names, assume that the host name is the parent domain
6	Attempt to guess directory names from the supplied dictionary file
TUNING OPTIONS	
1	Interesting File / Seen in Logs
2	Misconfiguration / Default File
3	Information Disclosure
4	Injection (XSS/Script/HTML)
5	Remote File Retrieval - Inside Web Root
6	Denial of Service
7	Remote File Retrieval - Server Wide
8	Command Execution / Remote Shell
9	SQL Injection
0	File Upload
a	Authentication Bypass
b	Software Identification
c	Remote Source Inclusion
d	WebService
e	Administrative Console
x	Reverse Tuning Options (i.e., include all except specified)
EXAMPLES	
nikto -Display 1234EP -o report.html -Format htm -Tuning 123bde -host 192.168.20.10	

ZED ATTACK PROXY (ZAP)

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



Computer Security

- **Open-source web security scanner used as a professional tool for penetration testing**
 - One of the most famous and used tools for these purposes
- **When used as a proxy server, allows users to manipulate all traffic that passes through it, including HTTPS, as Burp does**
- **It also includes several passive and/or active security scans that allow you to find vulnerabilities in scanned webs**
 - Including **fuzzing** and **brute force** techniques
- **It has several plugins that improve its functionality**
- **We'll also use it in **Lab 10** as a DAST tool (**Topic 6**)**
- **Tutorial**
 - <https://blog.segu-info.com.ar/2015/09/tutorial-de-uso-owasp-zaproxy.html>

FileEditViewAnalyseReportToolsOnlineHelp

Standard Mode

Sites

Quick StartRequestResponse

Header: TextBody: Text

Contexts

Default Context

Sites

https://ingenieriainformatica.uniovi.es

http://ingenieriainformatica.uniovi.es

GET:accesibilidad

actualidad

GET:avisos

eventos

GET:eventos

GET:noticias

noticias

GET:prensa

GET:actualidad

GET http://ingenieriainformatica.uniovi.es/actualidad/eventos HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://ingenieriainformatica.uniovi.es/sitemap.xml
Host: ingenieriainformatica.uniovi.es
Cookie: GUEST_LANGUAGE_ID=es_ES; JSESSIONID=6CCD10D19F022C4DC05BE1BDF100EB12; COOKIE_SUPPORT=true; NSC_Qpsubmft143_MC_IUUQ=ffffffff9f2b3f8045525d5f4f58455e445a4a423660

HistorySearchAlertsOutputSpider

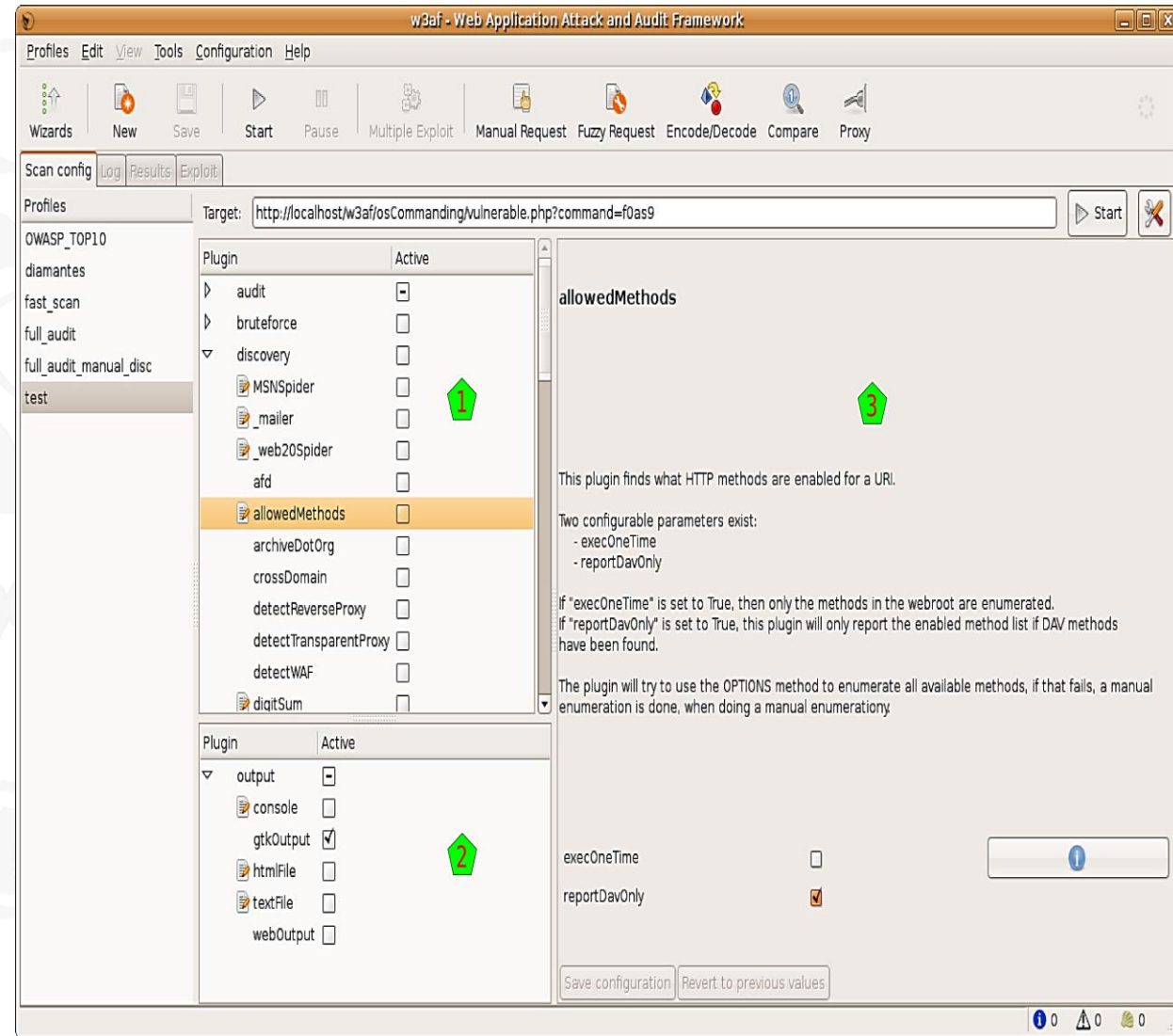
New Scan : Progress: 1: http://ingenie...ica.uniovi.es/ 18% Current Scans: 1 : URLs Found: 2097 : Nodes Added: 192 : Export

URLsAdded NodesMessages

Processed	Method	URI	Flags
●	GET	http://ingenieriainformatica.uniovi.es/visor/-/asset_publisher/...	
●	GET	http://ingenieriainformatica.uniovi.es/visor/-/asset_publisher/...	
●	POST	http://ingenieriainformatica.uniovi.es/busquedas?_77_redirec...	
●	GET	http://ingenieriainformatica.uniovi.es/estudiantes/informacio...	
●	GET	http://ingenieriainformatica.uniovi.es/estudiantes/movilidad?_...	
●	GET	http://ingenieriainformatica.uniovi.es/estudiantes/movilidad/-/...	
●	GET	http://ingenieriainformatica.uniovi.es/estudiantes/movilidad/-/...	
●	GET	http://ingenieriainformatica.uniovi.es/estudiantes/movilidad/-/...	
●	GET	http://ingenieriainformatica.uniovi.es/estudiantes/movilidad/-/...	

- A web application audit and attack framework
- Allows finding and exploiting vulnerabilities
- It contains many known web vulnerabilities
 - Including those of the OWASP Top 10 (seen on theory topic 6)
 - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Tutorial
 - <http://docs.w3af.org/en/latest/basic-ui.html>

Source: <http://docs.w3af.org/en/latest/gui/scanning.html>



- **Uses multiple DDBB (NVD, JVN, OVAL, RHSA / ALAS / ELSA / FreeBSD-SA...) to detect vulnerabilities**

- This might enable it to detect vulnerabilities that have no patches published

- **Allow remote (via SSH) and local scans and implements two scan modes**

- **Fast scan:** scans without `root` privileges, no internet access, almost no load on the scan target
- **Deep scan** mode

- **Detect known vulnerabilities in non-OS packages**

- User-compiled executables, language libraries and frameworks, etc.

- **Installation and tutorial**

- <https://www.howtoforge.com/tutorial/how-to-install-and-use-vuls-vulnerability-scanner-on-ubuntu/>
- <https://vuls.io/docs/en/tutorial.html>

Source: <https://github.com/future-architect/vuls>

```
172-31-4-82 [ 1] CVE-2016-0799 | 10.0(High) The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and
[ 2] CVE-2016-0483 | 10.0(High) Unspecified vulnerability in the Java SE, Java SE Embedded, and JRockit compon
[ 3] CVE-2016-0494 | 10.0(High) Unspecified vulnerability in the Java SE and Java SE Embedded components in Or
[ 4] CVE-2016-0705 | 10.0(High) Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_am
[ 5] CVE-2016-0728 | 7.2 (High) The join_session_keyring function in security/keys/process_keys.c in the Linux
[ 6] CVE-2016-1950 | 6.8 (Medium) Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3
[ 7] CVE-2016-0778 | 6.5 (Medium) The (1) roaming_read and (2) roaming_write functions in roaming_common.c in th

CVE-2016-1950
=====

CVSS Score
-----

6.8 (Medium) (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Summary
-----

Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x bef
ore 3.21.1, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to
execute arbitrary code via crafted ASN.1 data in an X.509 certificate.

Package/CPE
-----

* nss-util-3.19.1-3.45.amzn1 -> nss-util-3.19.1-9.49.amzn1

Links
-----

* [NVD]( https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1950 )
* [MITRE]( https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1950 )
* [CveDetails]( http://www.cvedetails.com/cve/CVE-2016-1950 )
* [CVSSv2 Calculator]( https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2016-1950&vector=(AV:N/AC:M/Au:N/C:P/I:P/A:P) )
* [RHEL-CVE]( https://access.redhat.com/security/cve/CVE-2016-1950 )
* [ALAS-2016-667]( https://alas.aws.amazon.com/ALAS-2016-667.html )
```

MOZILLA OBSERVATORY

<https://observatory.mozilla.org/>



- Online tool to scan websites and check for potential known problems
- It does not discover vulnerabilities per se
 - But configuration problems that can cause them
- It is a good practice to use it against our own websites
 - To ensure we did not forget something important

Observatory
mozilla

[Home](#) [FAQ](#) [Statistics](#) [About](#)

The Mozilla Observatory has helped over 240,000 websites by teaching developers, system administrators, and security professionals how to configure their sites safely and securely.

Scan your site

enter domain name here

Scan Me

- ☐ Don't include my site in the public results
- ☐ Force a rescan instead of returning cached results
- ☐ Don't scan with third-party scanners

Scan Summary

Initiate Rescan



Host: www.google.es
Scan ID #: 2653078
Test Time: November 15, 2016 7:31 PM
Test Duration: 11 seconds
Score: 35/100
Tests Passed: 6/10

Test Scores

Test	Pass	Score	Explanation	
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	?
Cookies	✗	-20	Cookies set without using the <code>Secure</code> flag or set over http	?
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	?
HTTP Public Key Pinning	✓	+5	Preloaded via the HTTP Public Key Pinning (HPKP) preloading process	?
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	?
Redirection	✓	0	Initial redirection is to https on same host, final destination is https	?
Subresource Integrity	—	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	?
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	?
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to <code>SAMEORIGIN</code> or <code>DENY</code>	?
X-XSS-Protection	✓	0	X-XSS-Protection header set to <code>"1; mode=block"</code>	?

Grade History

(1) Using Nikto against a Web Server



NIKTO EXECUTION EXAMPLE



```
root@kali:~# nikto -url www.ingenieriainformatica.uniovi.es
- Nikto v2.1.6
-----
+ Target IP:          156.35.33.143
+ Target Hostname:    www.ingenieriainformatica.uniovi.es
+ Target Port:       80
+ Start Time:        2019-10-22 17:52:01 (GMT2)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://ingenieriainformatica.uniovi.es/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Cookie JSESSIONID created without the httponly flag
+ 7984 requests: 13 error(s) and 4 item(s) reported on remote host
+ End Time:          2019-10-22 17:52:58 (GMT2) (57 seconds)
-----
+ 1 host(s) tested
```

BOTNETS



Computer Security

- Compromised hardware is used for a variety of malicious purposes
- One of the most common is to be integrated into a botnet
 - These networks of compromised machines can be used for different crimes
 - DDoS, send phishing messages, host fake shops...
- We can **check** if our hardware has been detected as part of a botnet with an OSI service
 - <https://www.osi.es/es/servicio-antibotnet>
 - If this service detects a compromised machine, it offers tools to solve the problem

The screenshot shows the OSI website's 'Servicio AntiBotnet' page. At the top, there's a navigation bar with links like 'Quiénes somos?', 'Encuesta de valoración', 'Contacto', and 'Boletines'. Below this is a search bar and a menu with options like 'Ponte al día', 'Campañas', 'Protégete', 'Recursos', 'Soporte técnico', 'Juegos educativos', and 'IS4K'. The main content area is titled 'Servicio AntiBotnet' and explains that the service helps identify security incidents related to botnets. It lists two ways to use the service: through internet service providers or online. Two large orange buttons are present: 'Consulta tu código' (with a download icon) and 'Chequea tu conexión' (with a checkmark icon). Below these are links for '¿Cómo funciona el servicio de notificación de códigos?' and '¿Cómo funciona el servicio de chequeo?'. At the bottom, it mentions collaboration with Telefonica and includes a download link for a browser plugin.

SELF-EVALUATION ACHIEVEMENT LIST: SEMINAR 3



- Understand the advantages and disadvantages of automated vulnerability scanning tools
- Understand the legal implications of using these tools
- Understand the usefulness of automatic vulnerability discovery tools for web sites
- Know how to launch an OpenVAS scan against a target
- Know how to launch a Nikto vulnerability scan against a web target
- Know a series of automatic scanning tools that complement the theory contents
- Know an “arsenal” of tools able to discover vulnerabilities automatically

SEMINAR 3

AUTOMATED VULNERABILITY SCANNING TOOLS

