SEMINAR 3
AUTOMATED VULNERABILITY SCANNING TOOLS

Finding vulnerabilities made easy

JOSÉ MANUEL REDONDO LÓPEZ *"S-81 ISAAC PERAL"* PROJECT V3.0

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

INDEX

< Go to Index

Source: zona-militar.com

Introduction

Understanding these tools

Introduction

José Manuel
Redondo López

- **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

José Manuel
Redondo López

- **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

José Manuel
Redondo López

- **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

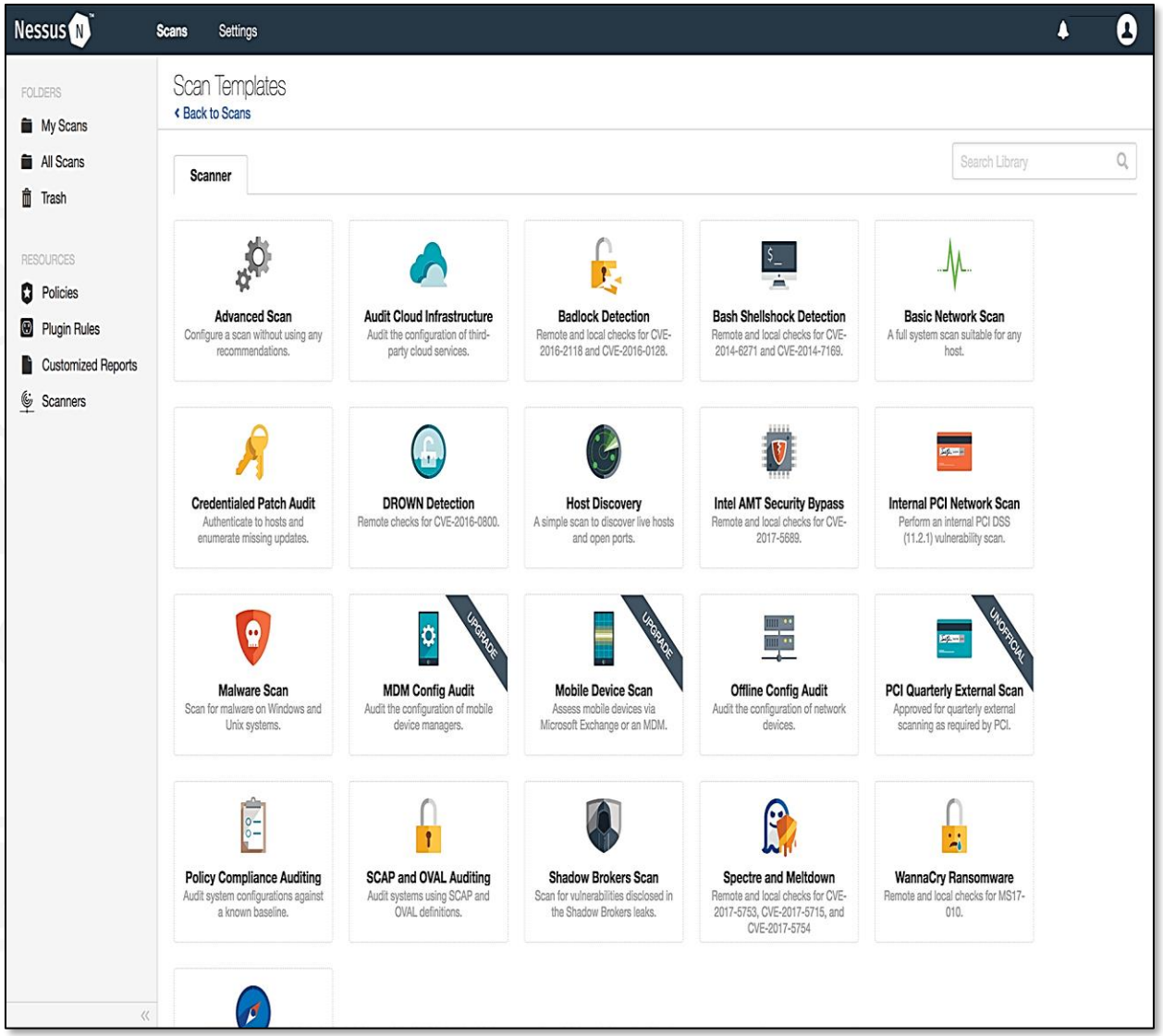
Source: zona-militar.com

NESSUS

http://www.tenable.com/products/nessus

José Manuel
Redondo López

- **One of the most used tools of this type**
  - Allows in-depth analysis of a compute
  - 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



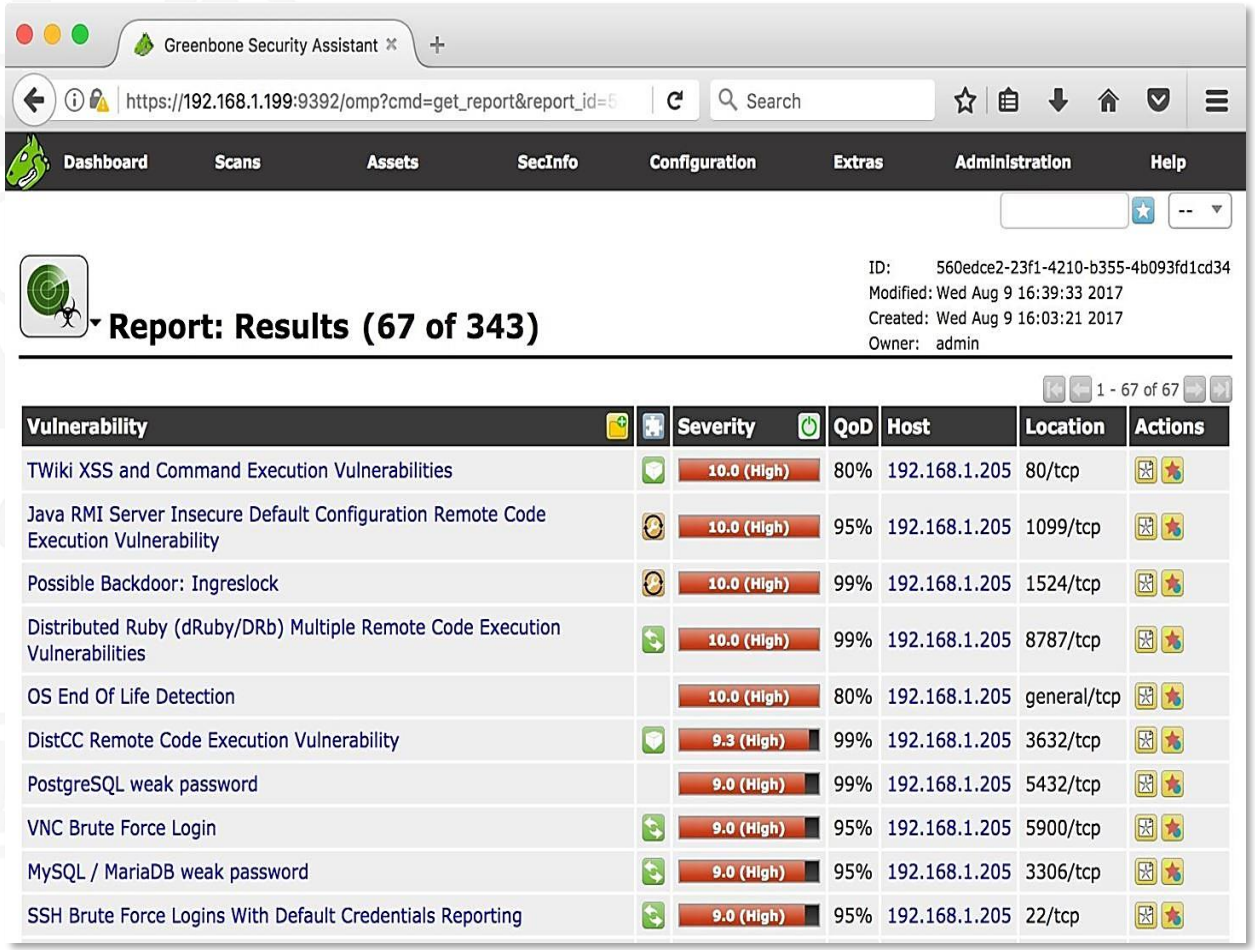
OpenVAS

http://www.openvas.org

José Manuel
Redondo López

- **Part of their 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-scapdata-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/

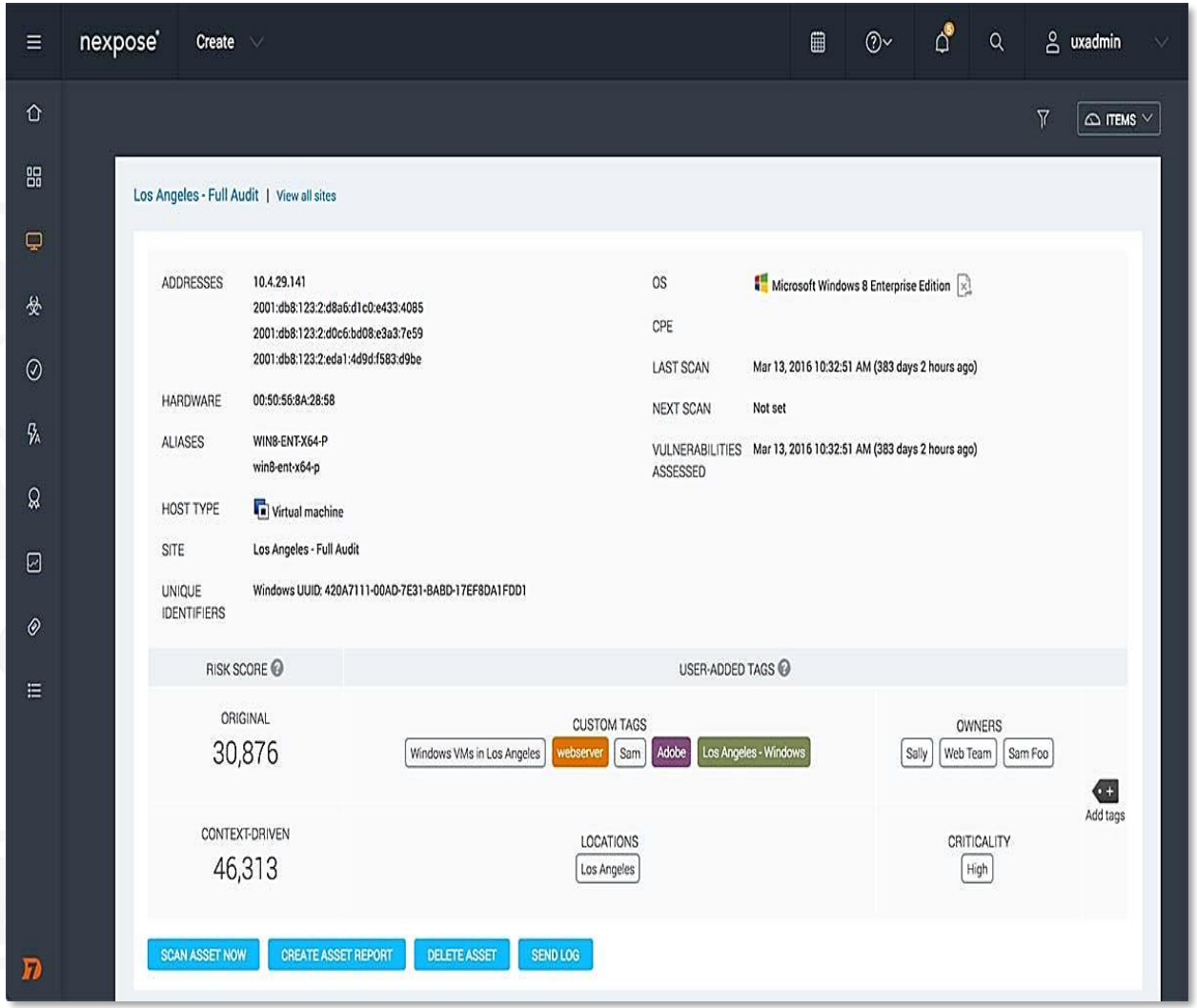


NEXPOSE

https://www.rapid7.com/products/nexpose/

José Manuel
Redondo López

- **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



José Manuel
Redondo López

(1) Analyzing a sample OpenVAS / Nessus output

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.

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

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

Source: zona-militar.com

Complementary automated web vulnerability scanning tools

Automatic scanning for the web (additional tools)

Why a separate category of tools?

José Manuel
Redondo López

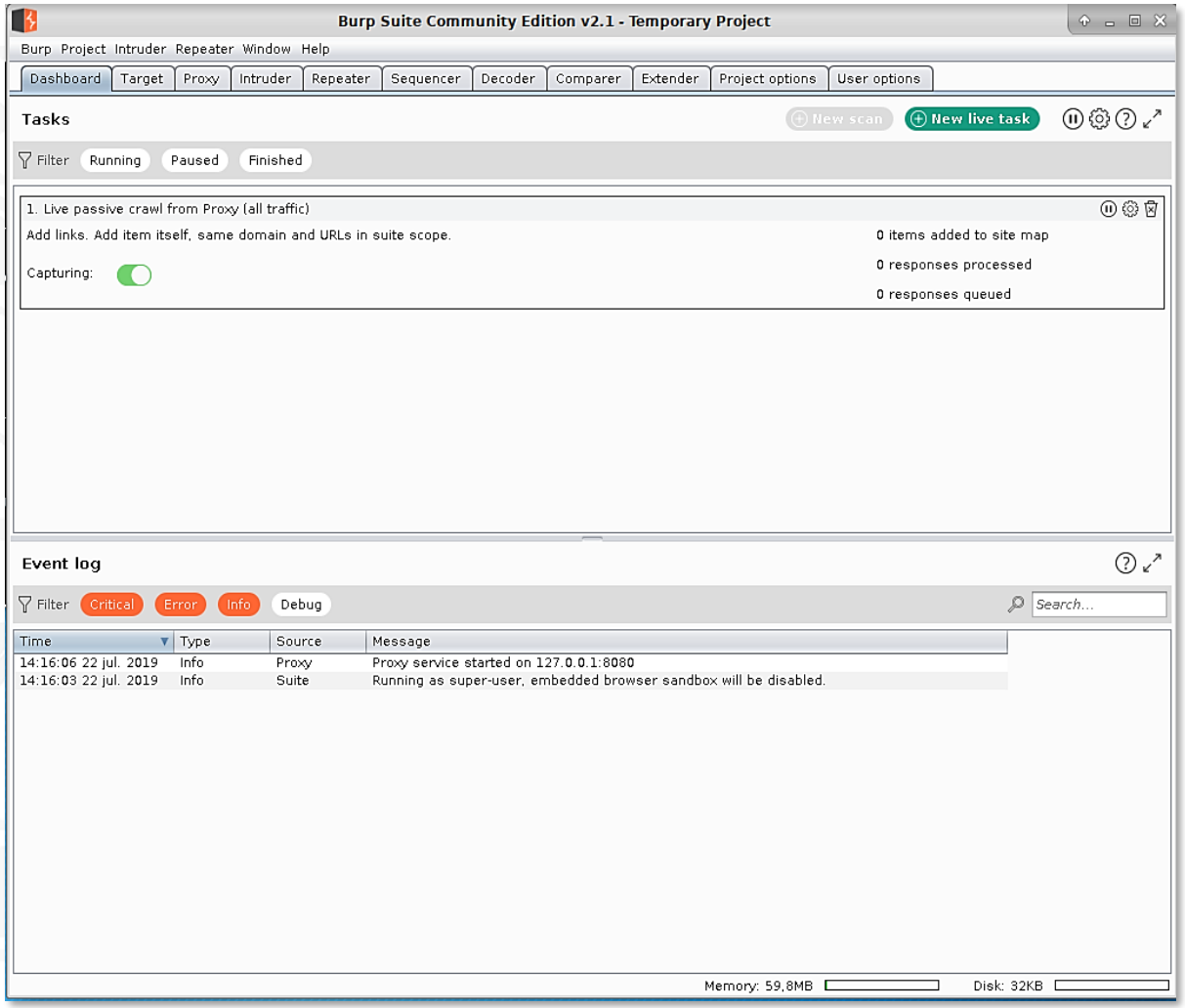
- **Web-based applications are everywhere nowadays, and have their own type of specific vulnerabilities**
- **The previous tools may also detect them**
  - But the scope of these tools is too broad and require a lot of time to complete the scan
  - Maybe they report things we are not interested in if 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, **discovering vulnerabilities faster**
- **Therefore, they are a complement of the previous ones and those shown in other course parts**

BURP SUITE

http://portswigger.net/burp/

José Manuel
Redondo López

- **Burp Suite is a lot of things in one**
  - **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



BURP SUITE

José Manuel
Redondo López

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 their functionality

- List of most useful extensions: https://github.com/snoopysecurity/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

José Manuel
Redondo López

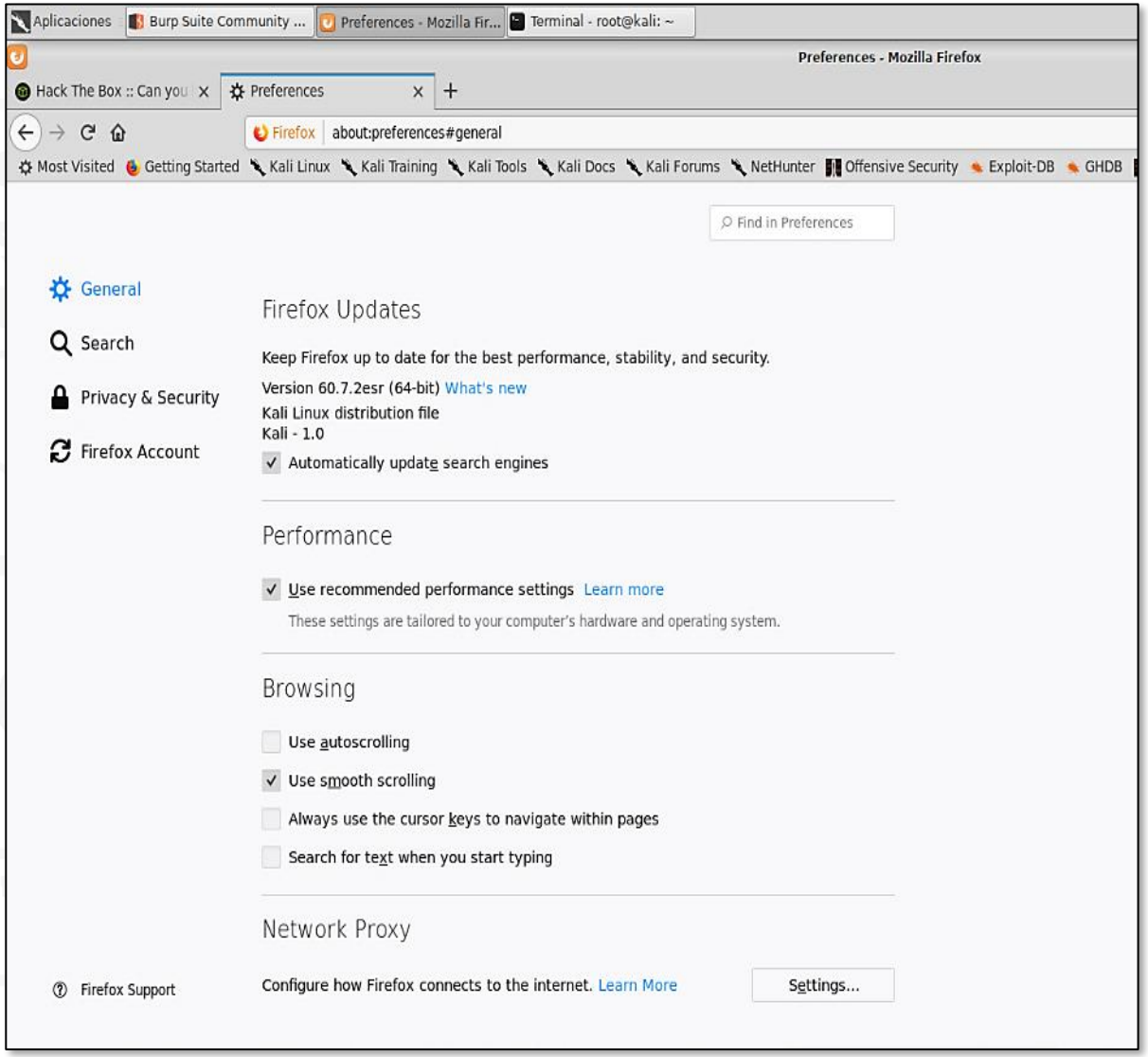
- **When we say we can bypass client-side validation we mean that some pages really rely on it thinking that it is a real security measure**
  - This is an error, and **it has a great cost**
  - Things like this check the input values of the client…
  - But once they reach **Burp** you can modify them, 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|\bselect\s+.*\bfrom\b|\bupdate\b|\bdelete\s+.*|\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

José Manuel
Redondo López

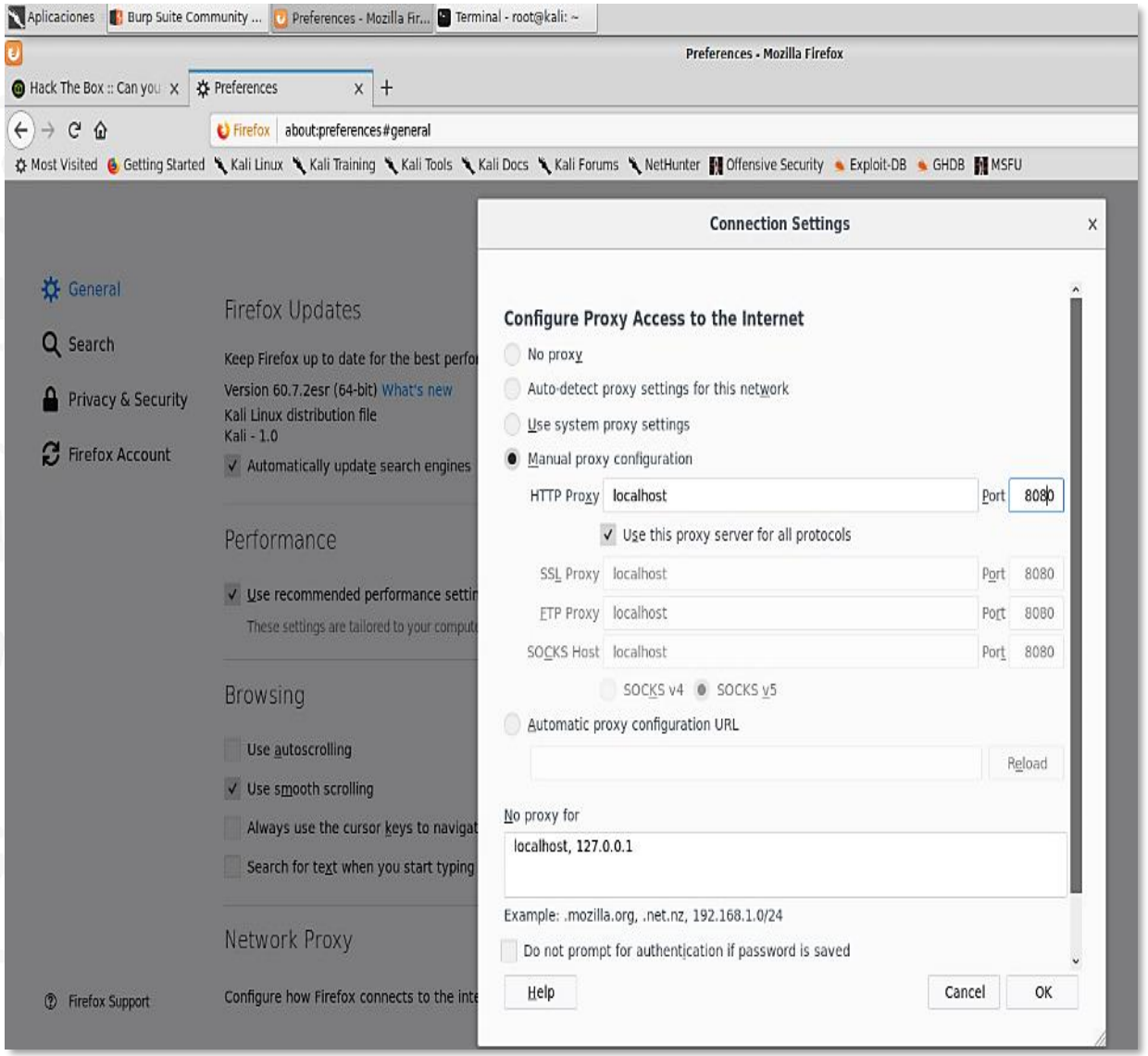
- To use Burp proxy, it is necessary to tell the browser that we will use it to send requests
- We must use the option to set up a proxy that every browser has
- In **Firefox** we can go to **General – Network Proxy**



Burp HTTP proxy

José Manuel
Redondo López

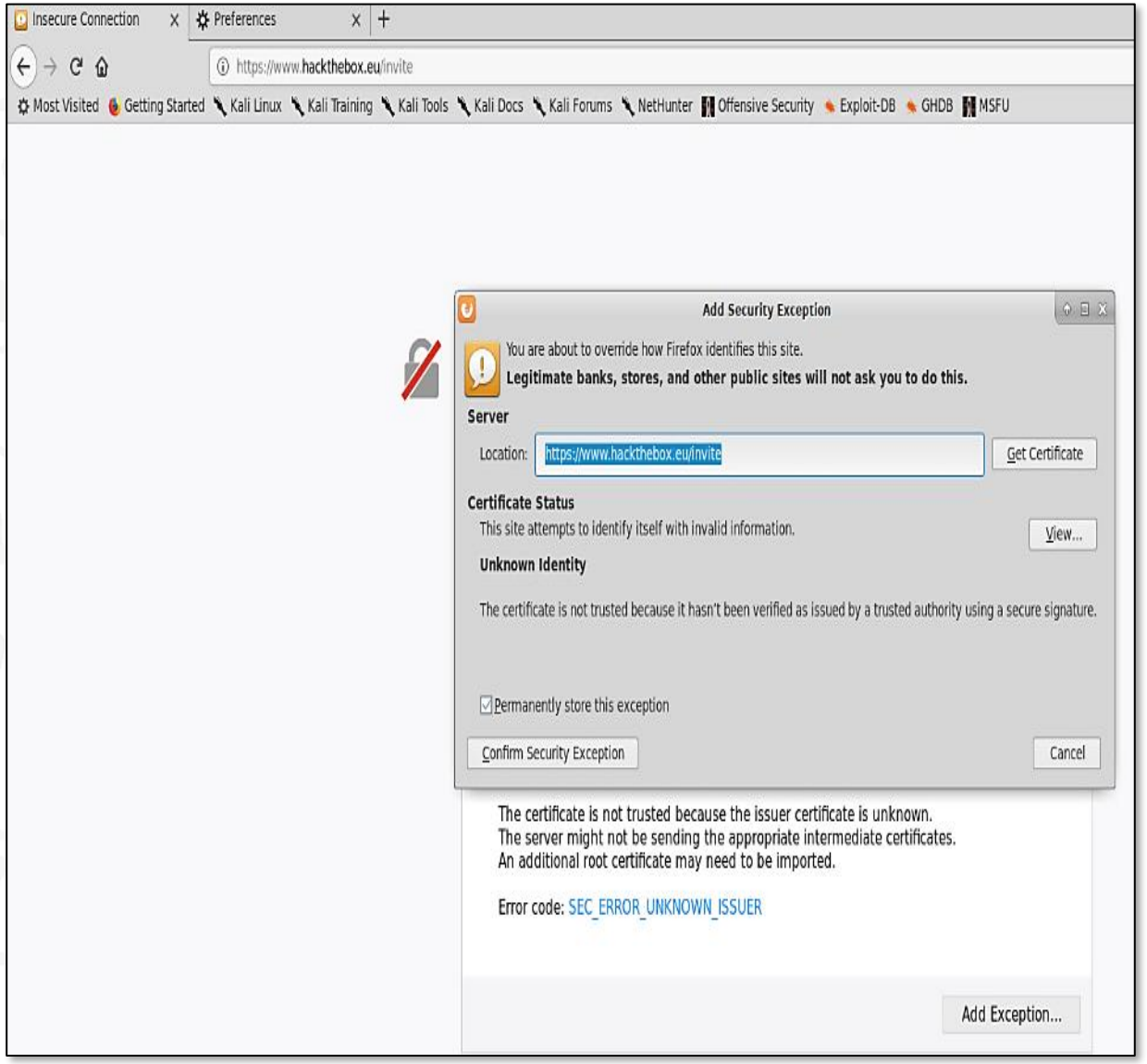
- Once Burp starts, it remains listening on localhost, port 8080
- So, we must indicate this address to use Burp as a proxy for everything
- Now we can "intercept" all the HTTP traffic we generate!
- Both requests and their responses



Burp HTTP proxy: Inspecting

José Manuel
Redondo López

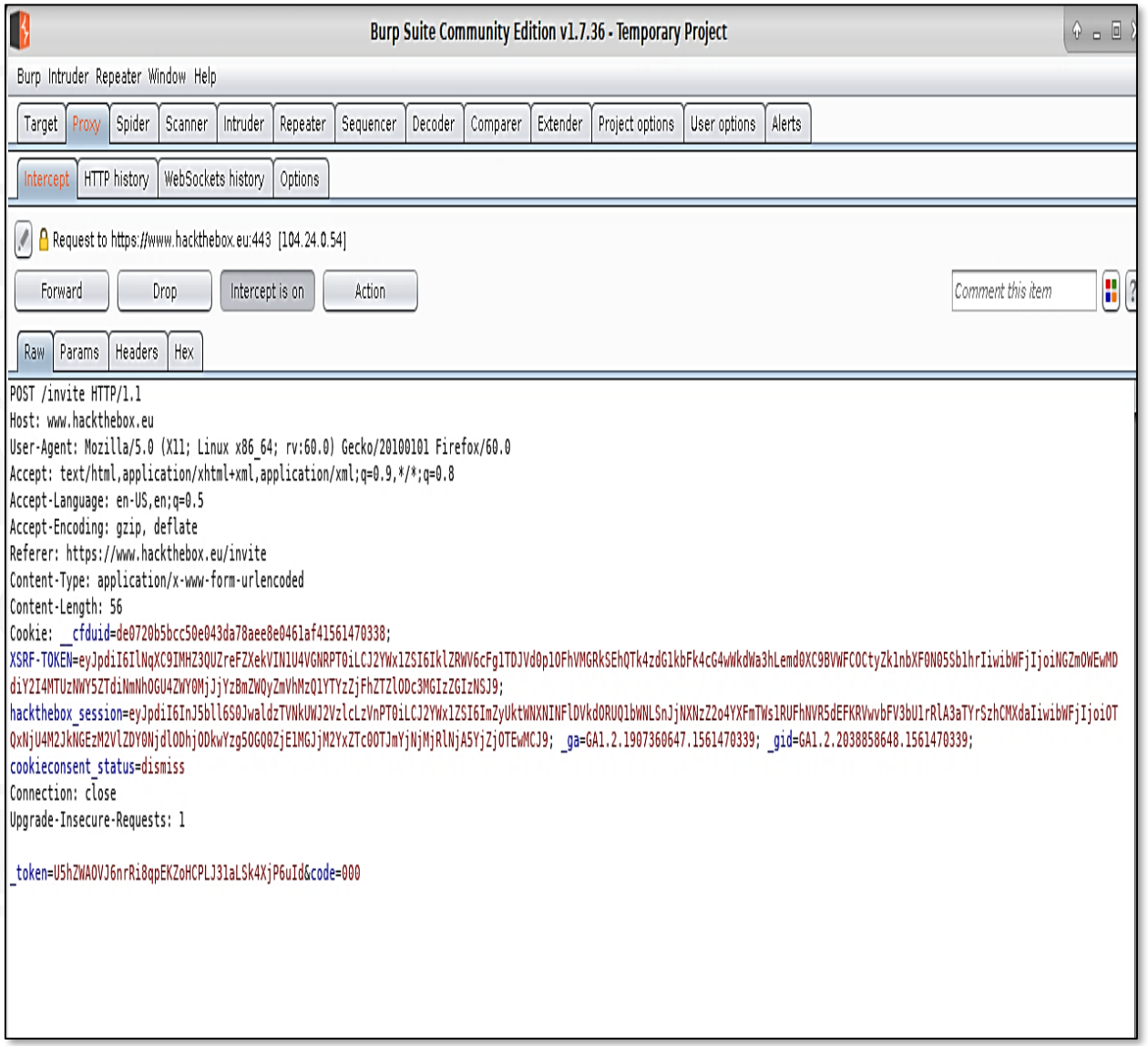
- **Sometimes the browser shows errors!**
- **When using HTTPs, using a proxy may cause the browser to show a potential AitM warning**
  - There's an intermediary intercepting a supposedly secure connection!
  - In this case we can add an exception, as we indeed are doing it!
- **But if this happens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



Burp HTTP proxy: Inspecting

José Manuel
Redondo López

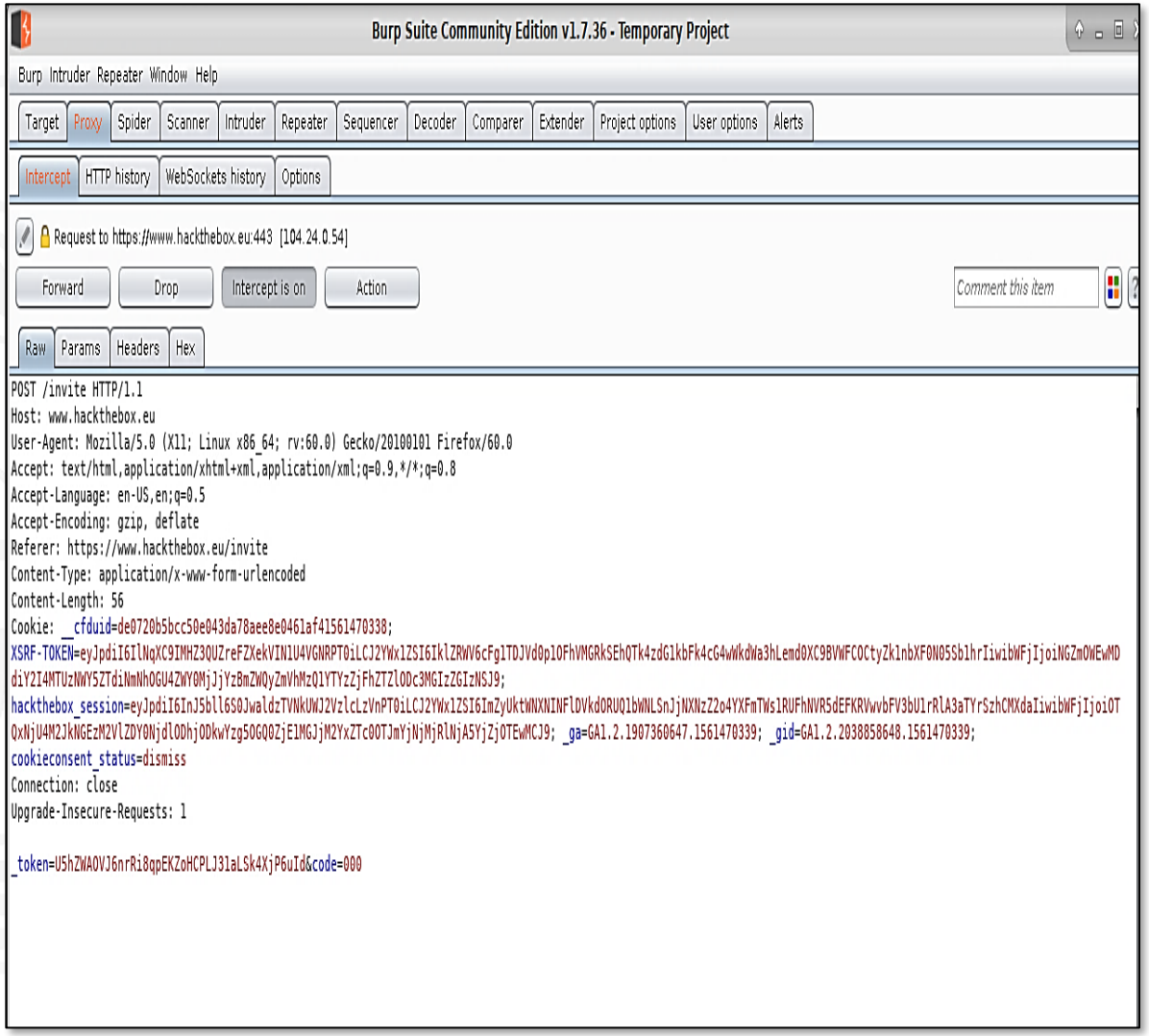
- **To examine HTTP traffic, we can**
  - **Click "Forward"**: Sends one request and re-intercept the corresponding response
    - Or, if this request generates requests to other URLs, intercept the next request
  - **Disable interception**: the browser behaves normally
    - No request/response is stopped, and no data is captured
- **What kind of data can we expect?**



Burp HTTP proxy: Inspecting

José Manuel
Redondo López

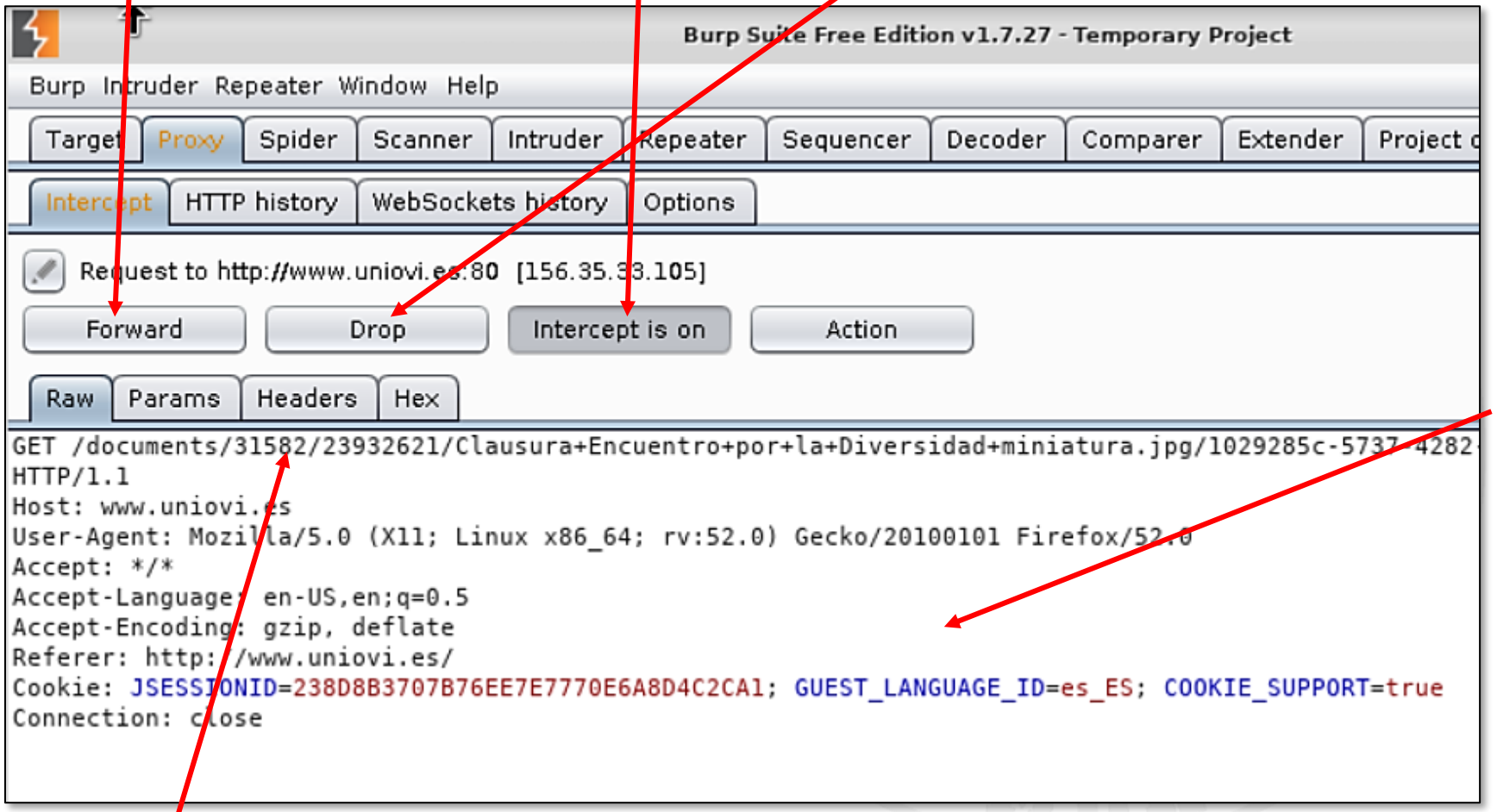
- **The HTTP request header**
  - In this case it has nothing worth mentioning
- **A `SessionID` cookie: in this case is truly random, not predictable**
  - We cannot impersonate other users easily
  - We could only do that if we steal a valid one
- **`__cfuid`: session ID that indicates that the service is behind CloudFlare**
  - It is “shielded” against a great deal of attacks
- **We know how to view and modify any HTTP traffic at will**
  - Opens lots of possibilities to inspect applications
  - What possibilities? See next slide



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

MODIFY THE BODY OF THE REQUEST AND SEE WHAT HAPPENS ☺ , LIKE:

- **"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 skip any kind of client-side validation the page makes
- The page code is 100% yours!

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

José Manuel
Redondo López

- **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

José Manuel Redondo López

- **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
-nossl: 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)

EXAMPLES

nikto -Display 1234EP -o report.html -Format htm -Tuning 123bde -host 192.168.20.10

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

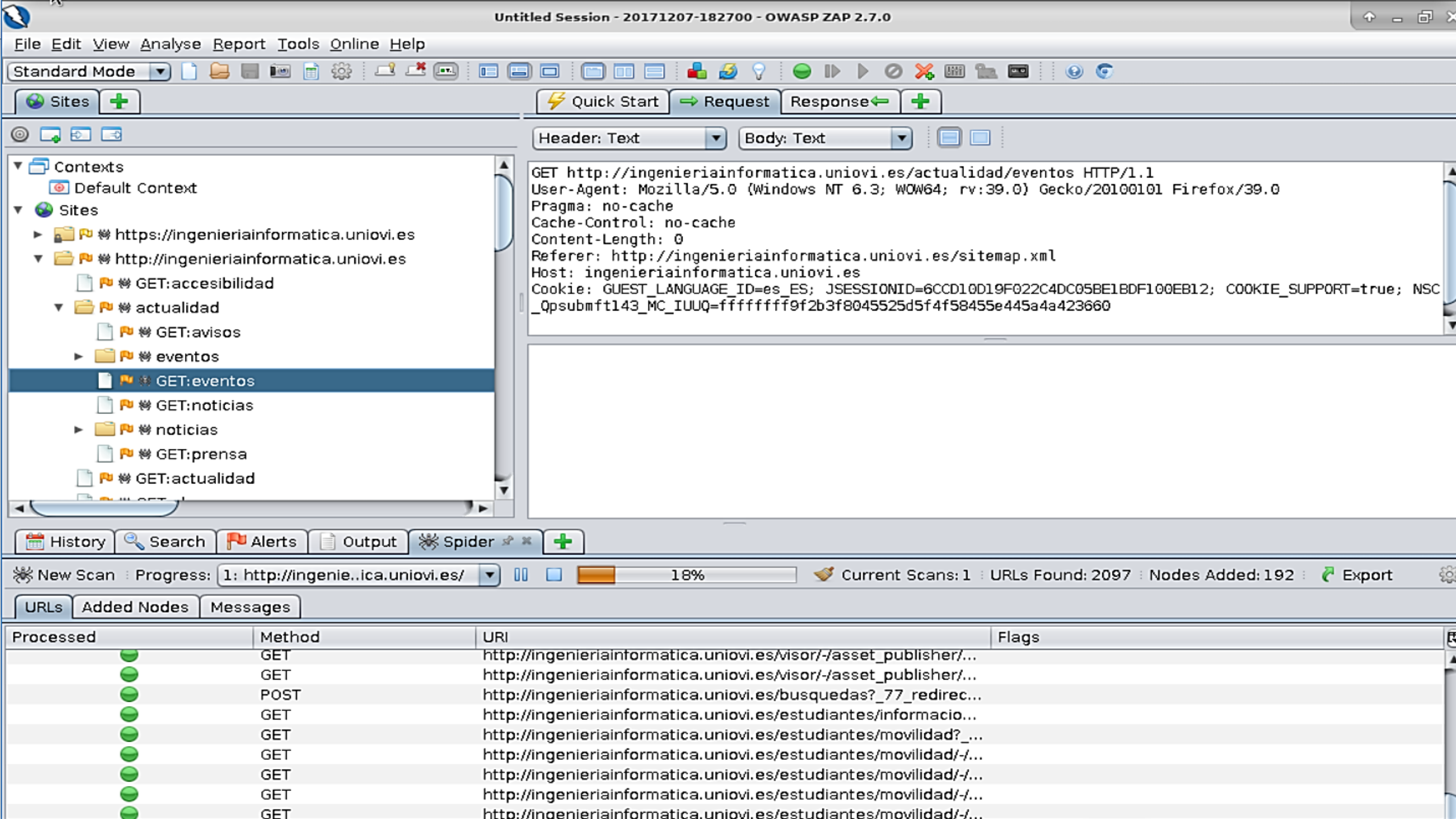
1 Interesting File / Seen in logs
2 Misconfiguration / Default File
3 Information Disclosure
4 Injection (XSS/Script/HTML)
5 Remote File Retrieval - Inside Web Root
6 Denial of Service
7 Remote File Retrieval - Server Wide
8 Command Execution / Remote Shell
9 SQL Injection
0 File Upload
a Authentication Bypass
b Software Identification
c Remote Source Inclusion
d WebService
e Administrative Console
x Reverse Tuning Options (i.e., include all except specified)

ZAP

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

José Manuel
Redondo López

- **Zed Attack Proxy (ZAP) is an 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**
- **Tutorial**
  - https://blog.segu-info.com.ar/2015/09/tutorial-de-uso-owasp-zaproxy.html


Untitled Session - 20171207-182700 - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
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
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
History
Search
Alerts
Output
Spider
New Scan
Progress:
1: http://ingenie..ica.uniovi.es/
18%
Current Scans: 1
URLs Found: 2097
Nodes Added: 192
Export
URLs
Added Nodes
Messages
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/-/...

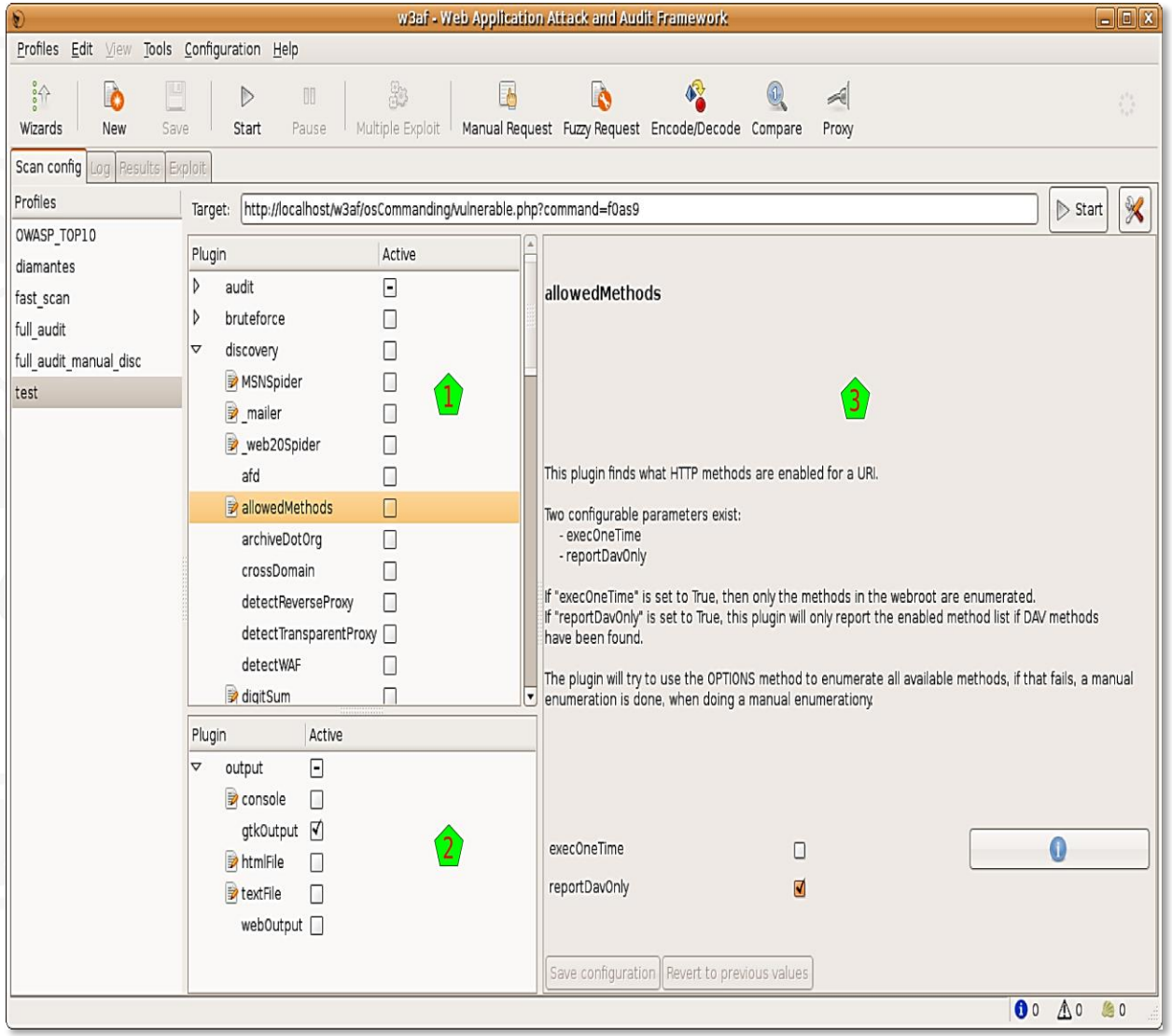
W3AF

http://w3af.org/

José Manuel
Redondo López

- **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



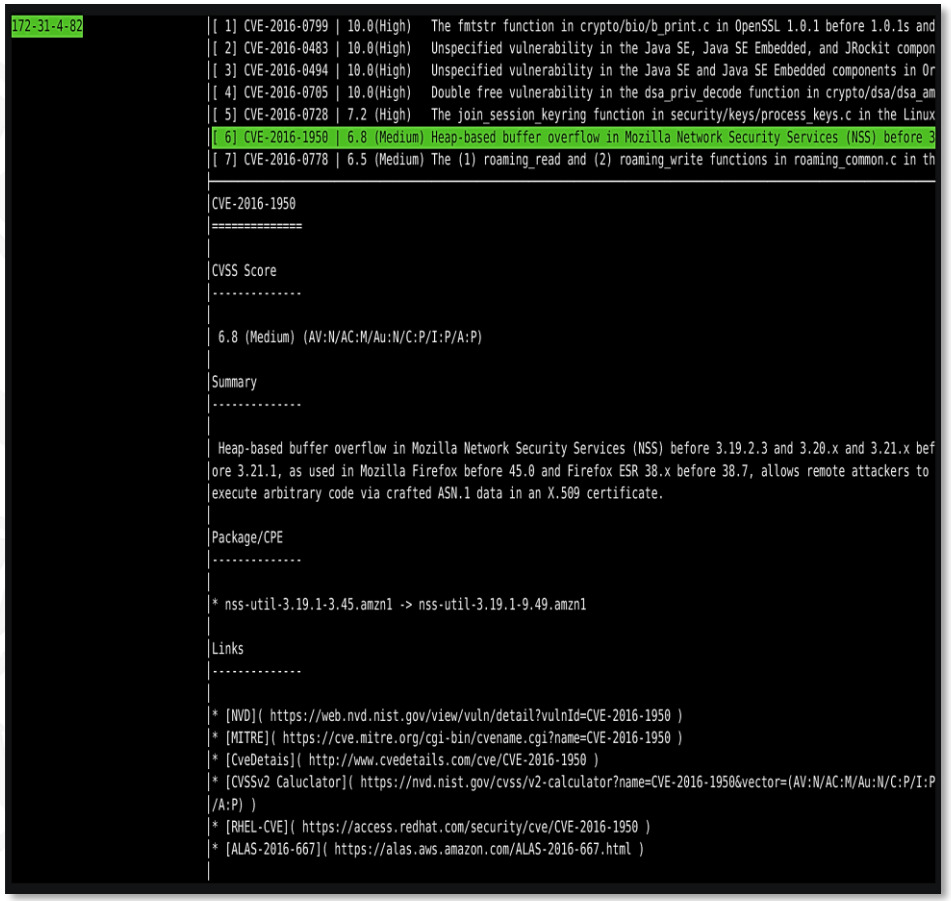
VULS

https://vuls.io/

José Manuel
Redondo López

- **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

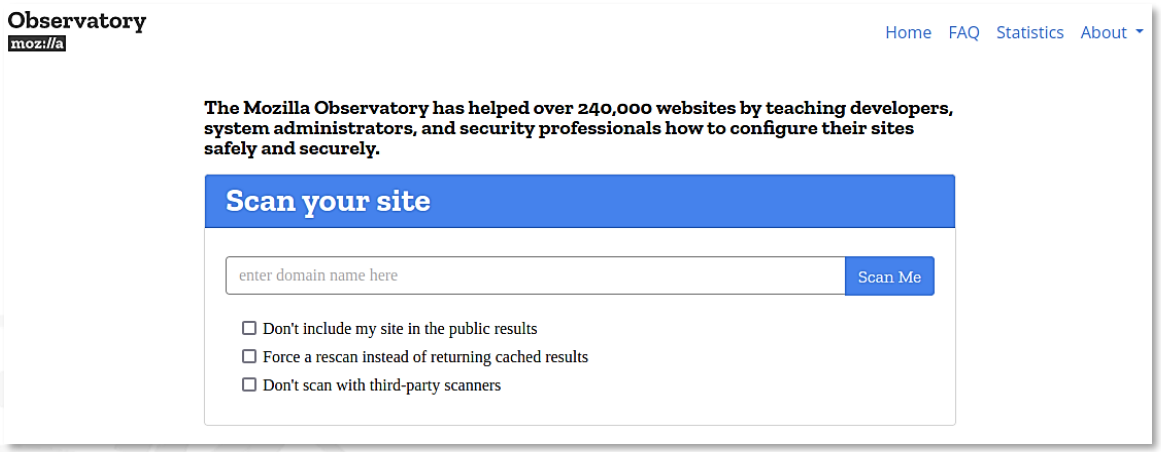


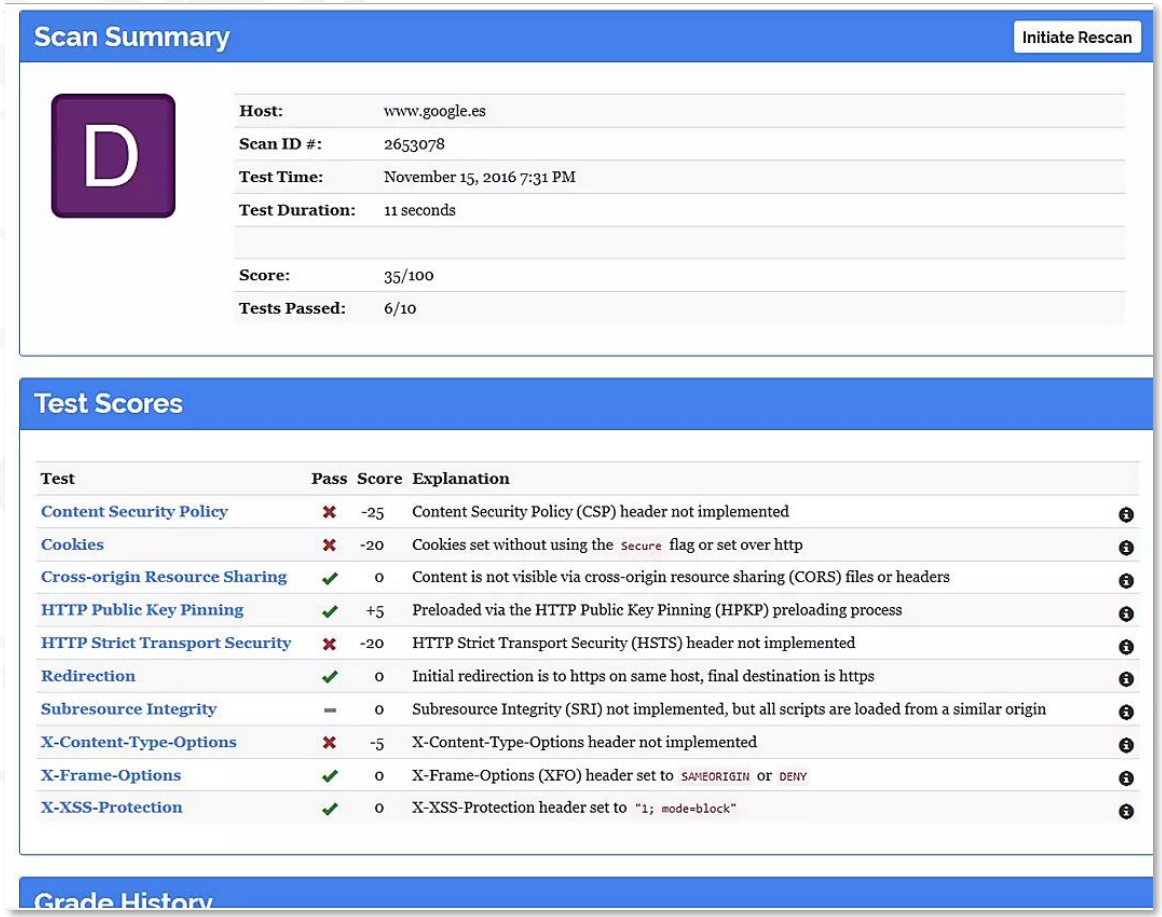
Mozilla Observatory

https://observatory.mozilla.org/

José Manuel
Redondo López

- **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





José Manuel
Redondo López

(1) Using Nikto against a Web Server

NIKTO EXECUTION EXAMPLE

José Manuel
Redondo López

```
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 a
gent 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

José Manuel
Redondo López

- **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 phising 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

Self-evaluation achievement list: Seminar 3

José Manuel
Redondo López

Rank	Concept
	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
	**Automated War Machine**: Be able to effectively use typical automated vulnerability scanners

SEMINAR 3. AUTOMATED VULNERABILITY SCANNING TOOLS

Source: zona-militar.com