SEMINARIO 3
HERRAMIENTAS DE ESCANEO AUTOMÁTICO DE VULNERABILIDADES

Encontrar vulnerabilidades de forma sencilla

José Manuel Redondo López Proyecto *"S-81 Isaac Peral"* v4.0

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

ÍNDICE

< Ir al Índice

INTRODUCCIÓN

Entendiendo el propósito de estas herramientas

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Introducción

- ¿Hay una forma rápida de probar si un sistema tiene vulnerabilidades?
  - La hay, aunque no es perfecta: **las herramientas automáticas de descubrimiento de vulnerabilidades**
- En este seminario revisaremos algunas
- Nos permiten obtener un esquema claro de las vulnerabilidades más evidentes que un sistema puede tener, ahorrándonos tiempo
  - **Pero NO sustituyen el trabajo de una auditoria de seguridad bien hecha (la complementan)**
- Estas herramientas hacen escaneo de vulnerabilidades
  - No confundir **NUNCA** con un pentesting o con el trabajo de un Red Team
  - Algunas empresas llaman a esto “pentesting”: esto es engañoso y **ERRÓNEO**

Introducción: La importancia de estas herramientas

- **Son programas profesionales y muy potentes que descubren automáticamente vulnerabilidades en cualquier máquina**
  - Windows, Linux, Mac OS, servidor web o no, ...
- **Nos hacen ahorrar mucho tiempo**
  - Y en ciertos casos pueden hacer un mejor trabajo que nosotros manualmente
  - Podemos combinar los resultados de varias para aumentar la fiabilidad
- **Si se solucionan todos los problemas detectados por estas herramientas, la máquina objetivo será significativamente menos vulnerable**
  - Por lo tanto, son herramientas necesarias para un ingeniero de seguridad...
  - ... pero no deberíamos recurrir únicamente a ellas para un análisis completo
- **Cada herramienta genera una cantidad sustancial de tráfico de red**
  - Y consumir gran cantidad de recursos del objetivo
  - Por lo tanto, **NUNCA tenemos que lanzarlas sin la debida autorización del propietario**

Introducción: Otras herramientas

- **Describiremos algunas de estas herramientas**
  - Pero podemos encontrar otras adicionales que nos permitan explorar el objetivo teniendo en cuenta diferentes criterios o vulnerabilidades a encontrar
- **Algunas son**
  - Invicti (antes 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 (**no son realmente escaneadores de vulnerabilidades,** pero son útiles para comunicar sus resultados): https://dradisframework.com/ce/
- **Más información**
  - https://www.softwaretestinghelp.com/penetration-testing-tools/

< Ir al Índice

Herramientas de escaneo automático de servidores

Escaneo automático para máquinas

Fuente: Bing Chat AI

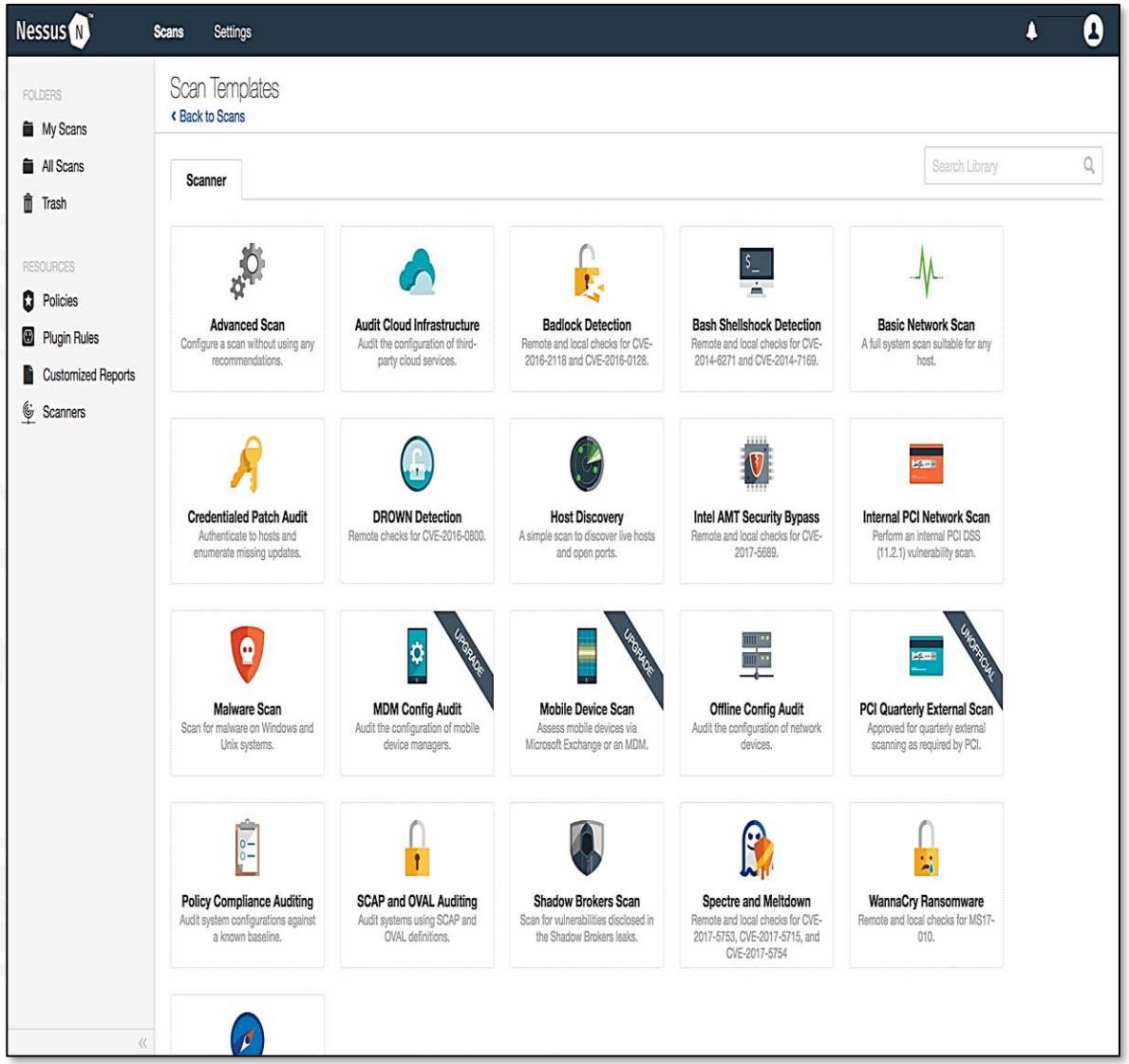
Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

NESSUS

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

- **Una de las herramientas más usadas de este tipo**
  - Permite el análisis en profundidad de un PC
  - Realiza una auditoría detallada de sus servicios
  - Cubriendo gran cantidad de vectores potenciales de problemas de seguridad
  - Analiza configuraciones, parches, aplicaciones web, redes, sistemas, datos y aplicaciones...
- **Requiere 4+ GB RAM (solo la aplicación)**
- **Detecta más de 100.000 vulnerabilidades potenciales y se actualiza con frecuencia**
  - La versión gratuita (Nessus Home Feed) no detecta tantas vulnerabilidades como de pago
  - Y está limitada a 16 IP
- **Tutorial**
  - http://www.reydes.com/d/?q=Instalacion_de_Nessus_en_Kali_Linux

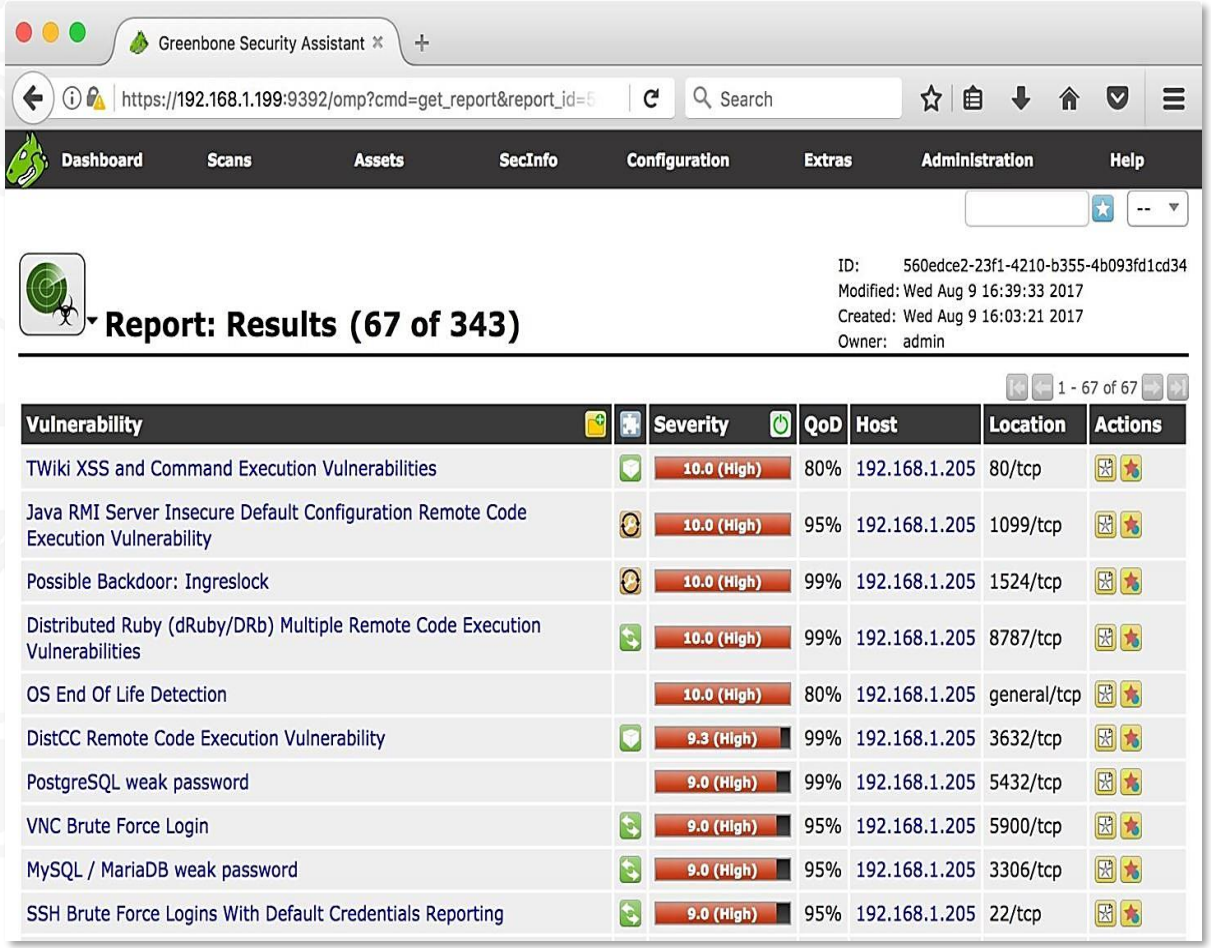


OPENVAS

http://www.openvas.org

- **Parte de la familia de productos "Greenbone Security Manager" (GSM)**
- **Permite análisis en detalle de servidores**
  - Puede comprobar más de 53.000 vulnerabilidades, actualizándose diariamente
  - La actualización de las vulnerabilidades que detecta debe hacerse periódicamente para maximizar la detección
    - `sudo runuser -u _gvm -- greenbone-nvt-sync`
    - `sudo runuser -u _gvm -- greenbone-scapdata-sync`
    - `sudo runuser -u _gvm -- greenbone-certdata-sync`
  - También requiere 4+ Gb RAM solo para la aplicación
- **Tutoriales**
  - 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/

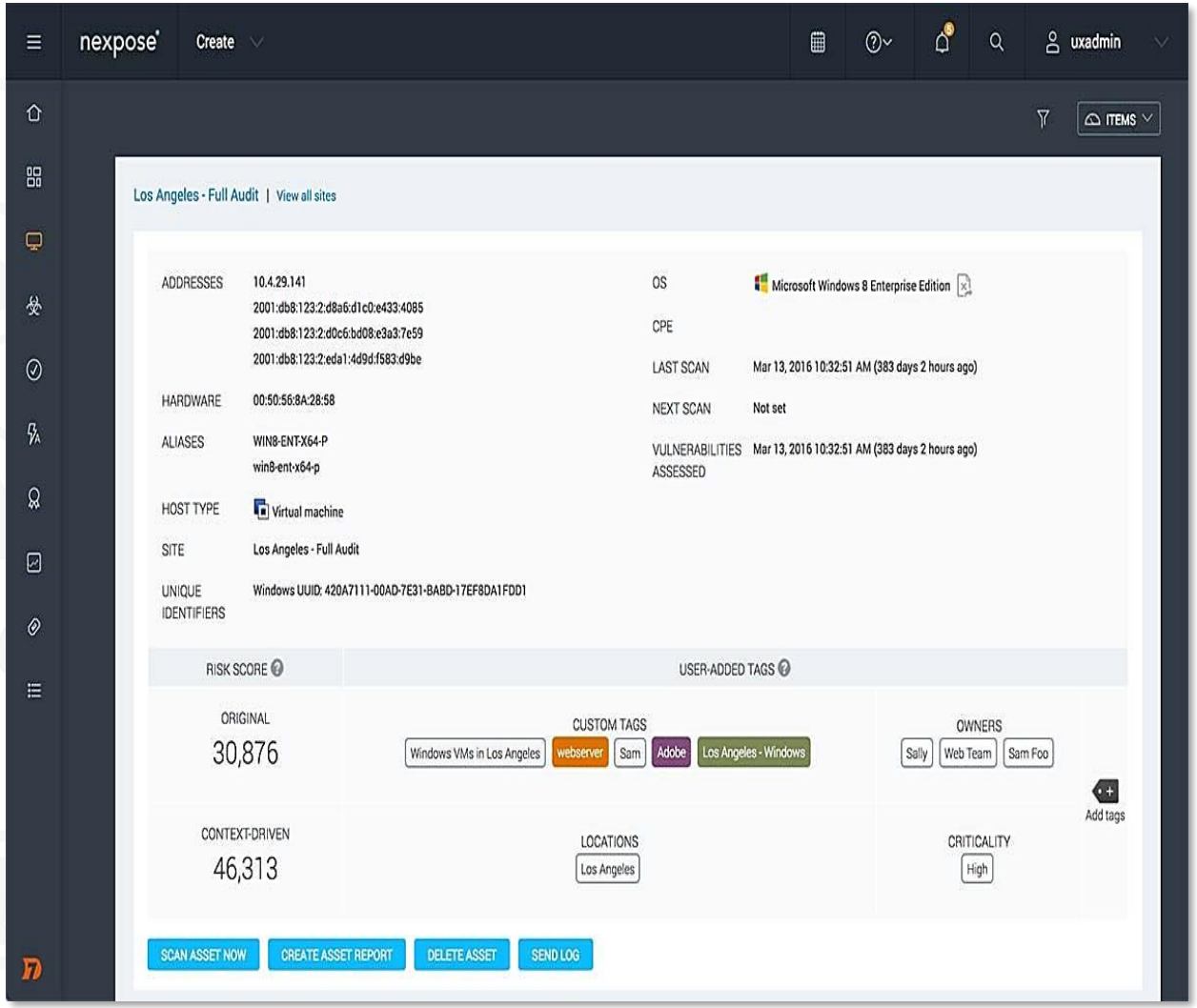
Fuente: https://null-byte.wonderhowto.com/how-to/perform-large-scale-network-security-audit-with-openvass-gsa-0179340/



NEXPOSE

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

- **Considerada la herramienta de descubrimiento automático de vulnerabilidades más potente**
  - Plataforma de gestión de vulnerabilidades
    - Riesgos, seguimiento de vulnerabilidades, vulnerabilidades en contenedores...
  - Descubre vulnerabilidades y muestra sus posibles exploits
  - Puede usar más exploits que **Metasploit** (que veremos posteriormente)
  - Muestra más vulnerabilidades y funciona a mayor escala que otras herramientas similares
  - No es gratis (prueba de 30 días)
- **Tutorial**
  - https://www.javatpoint.com/ethical-hacking-installing-nexpose



(1) Análisis de un ejemplo de salida OpenVAS / Nessus

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

< Ir al Índice

Fuente: Bing Chat AI

Herramientas complementarias de escaneo para la web

Escaneo automático para la web (herramientas adicionales)

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

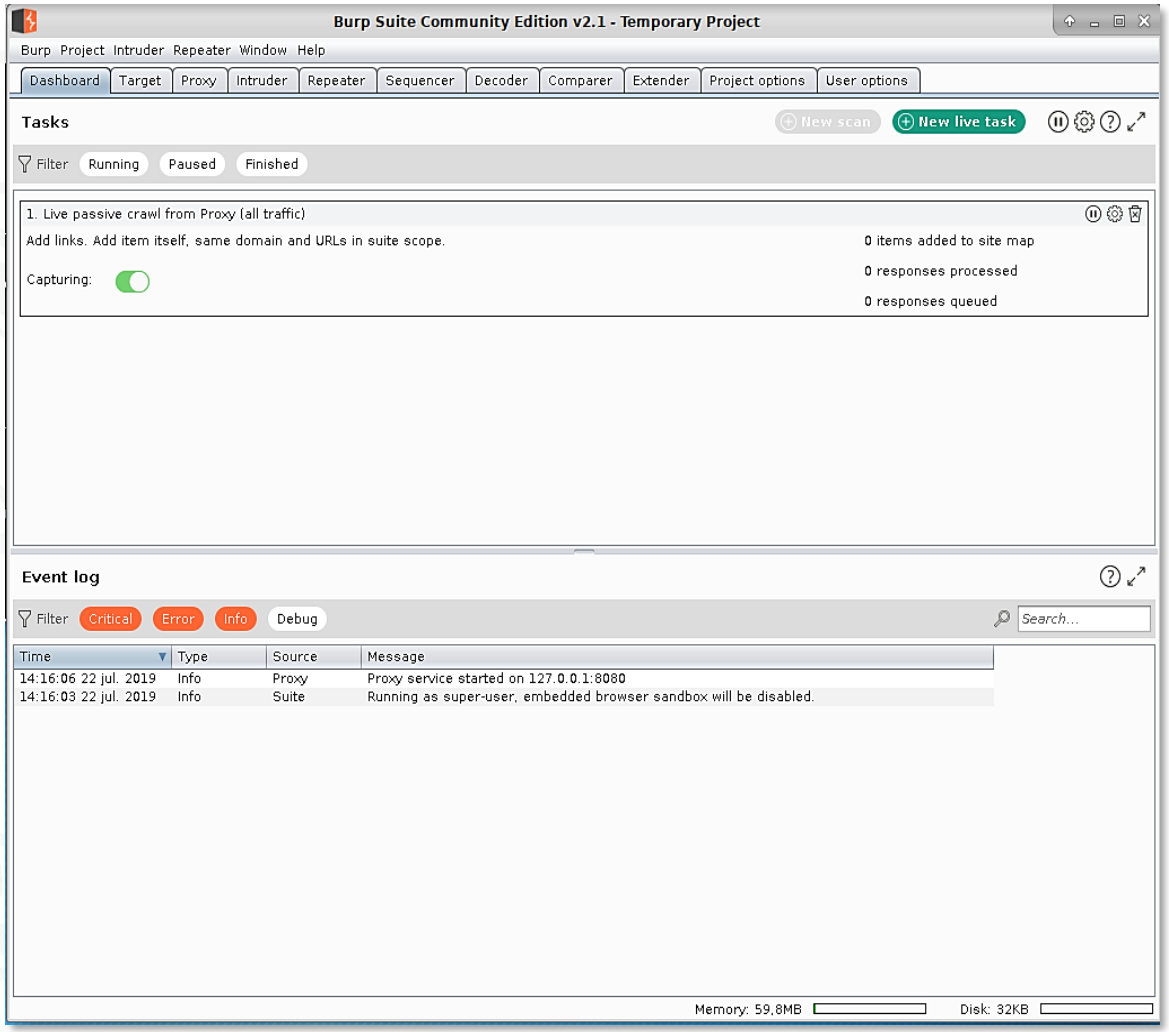
¿Por qué otra categoría de herramientas?

- **Las aplicaciones web son omnipresentes hoy en día y tienen sus propios tipos de vulnerabilidades específicas**
- **Las herramientas anteriores también son capaces de detectarlas**
  - Pero su alcance es muy amplio y requieren mucho tiempo para completar el escaneo
  - Probablemente nos den información que no necesitamos si solo buscamos vulnerabilidades web
  - Estas vulnerabilidades dependen de las tecnologías / frameworks utilizados para implementar esas aplicaciones
  - Estas herramientas se centran únicamente en la web y nos permiten realizar análisis especializados de forma más eficiente
  - **Descubriendo vulnerabilidades más rápido** (y con menos consumo de recursos)
- **Por tanto, complementan a las anteriores y otras que veremos en otras partes de la asignatura**

BURP SUITE

http://portswigger.net/burp/

- Es una herramienta multiusos
  - **Proxy interceptor**: permite inspeccionar y modificar el tráfico entre el navegador y el servidor
  - **Spider:** inspección de la web automática / manual
    - Un spider manual recopila información de una web mientras navegas por ella
    - No tiene las limitaciones de los spider automáticos
  - **Escáner:** detectando varios tipos de vulnerabilidades en aplicaciones web
  - Un **módulo de intrusión** para encontrar / explotar vulnerabilidades
  - Un módulo para realizar **ataques de repetición** (replay attacks)
  - Análisis de la **fortaleza de tokens de sesión**
  - Desafortunadamente, algunas de estas características sólo están en la versión de pago



BURP SUITE

Usos de la versión gratuita

- Ver los parámetros GET y POST de cualquier petición y sus respuestas
- "Congelar" la petición antes de que vaya al servidor y modificar **CUALQUIER PARTE DE ELLA**
  - Cabeceras, parámetros, sus valores, cookies...
  - Una vez que se ha realizado toda la validación del cliente (JavaScript)
    - Por lo tanto, con herramientas de este estilo, la validación en el cliente no es efectiva (puede saltarse fácilmente)
- **Modificar toda la información** que se envía desde el cliente al servidor
  - Provocando errores que no son posibles de otro modo...

Admite **extensiones** que mejoran mucho su funcionalidad

- Lista de las más útiles: https://github.com/snoopysecurity/awesome-burp-extensions
- Extensión para rotar la IP en cada petición: https://www.kitploit.com/2019/08/iprotate-extension-for-burp-suite-which.html
- Extensión para encontrar vulnerabilidades XSS: https://github.com/wish-i-was/femida

Hay otras aplicaciones similares

- 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

VALIDACIÓN DEL LADO DEL CLIENTE

- **Cuando decimos que las validaciones del cliente se pueden saltar nos referimos a que ciertas páginas confían en ella pensando que es una medida de seguridad real**
  - Eso es un gran error, **con un gran coste**
  - Scripts como este validan la entrada del cliente… (**NOTA**: este script es de una web real)
  - ...pero una vez que llegan a **Burp** pueden modificarse **¡haciendo todo este código inútil!**

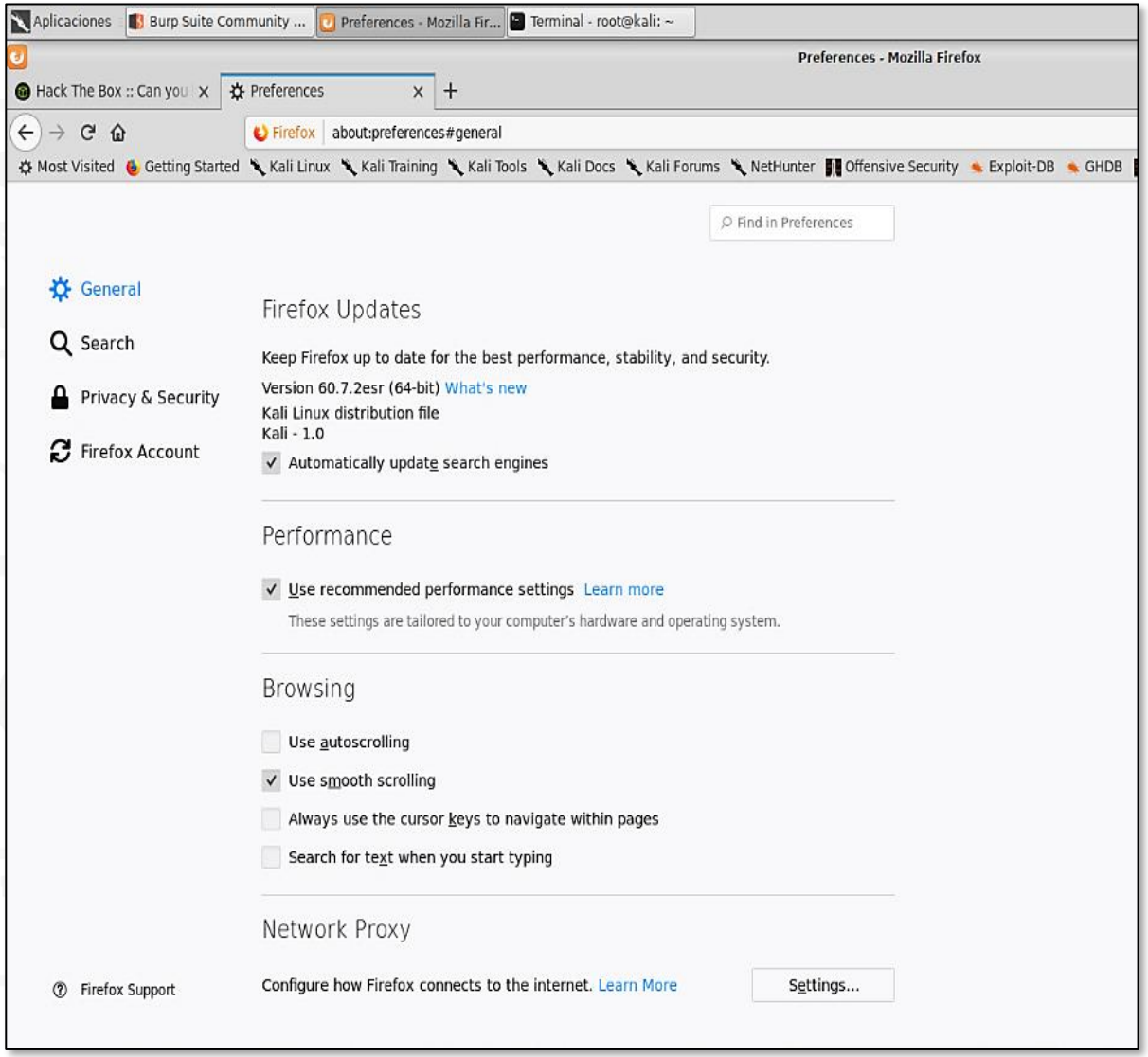
```
//comprobacion SQL injection
function chequear_sql(elmFORM)
{
  var mensaje, patron;
  var token_trobat = new Array();
  var cnjFORM = document.getElementById(elmFORM);

  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;
}
```

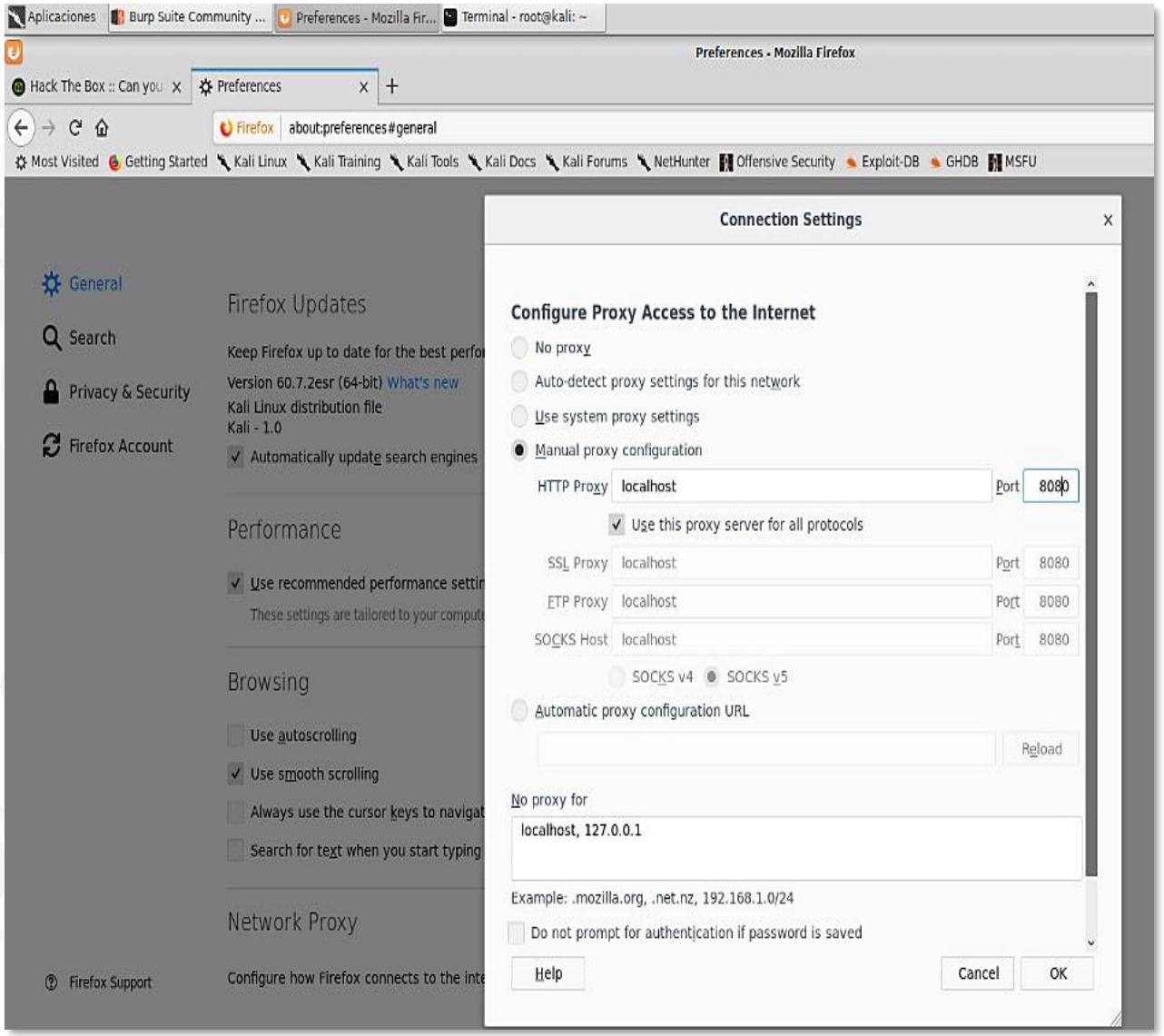
Burp HTTP proxy

- Para usar el proxy **Burp** es necesario decirle al navegador que vamos a usar un proxy para enviar peticiones
- Esto se configura en con opciones que todos los navegadores tienen
- Por ejemplo, en **Firefox** está en **General – Network Proxy**



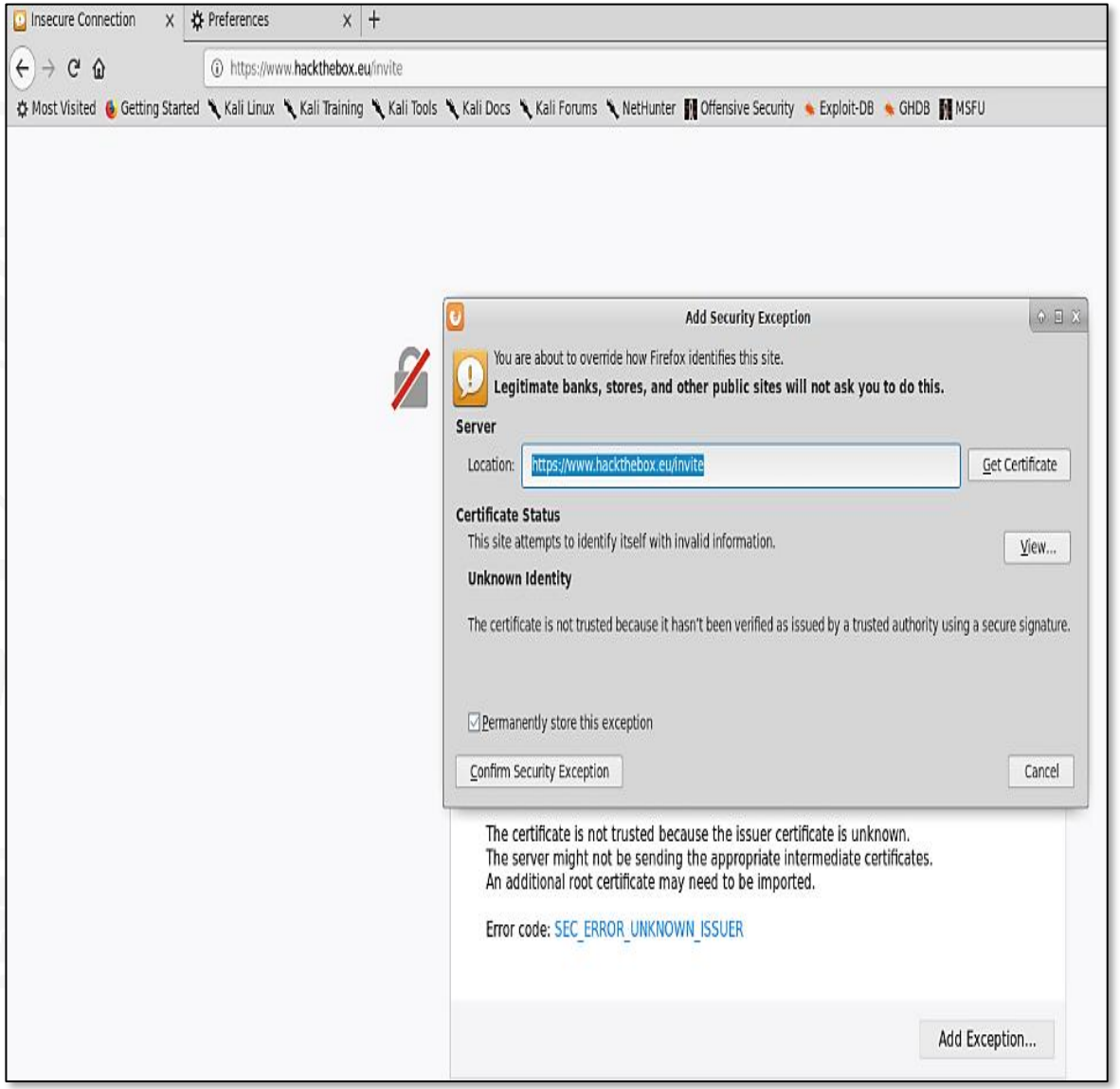
BURP HTTP PROXY

- Una vez que **Burp** arranca, permanece a la escucha en **localhost**, puerto 8080
- Por tanto, eso es lo que debemos indicar en el navegador para usar **Burp** como proxy para todo
- ¡Ahora podemos "interceptar" todo el tráfico HTTP que generemos!
- Tanto las peticiones como sus respuestas



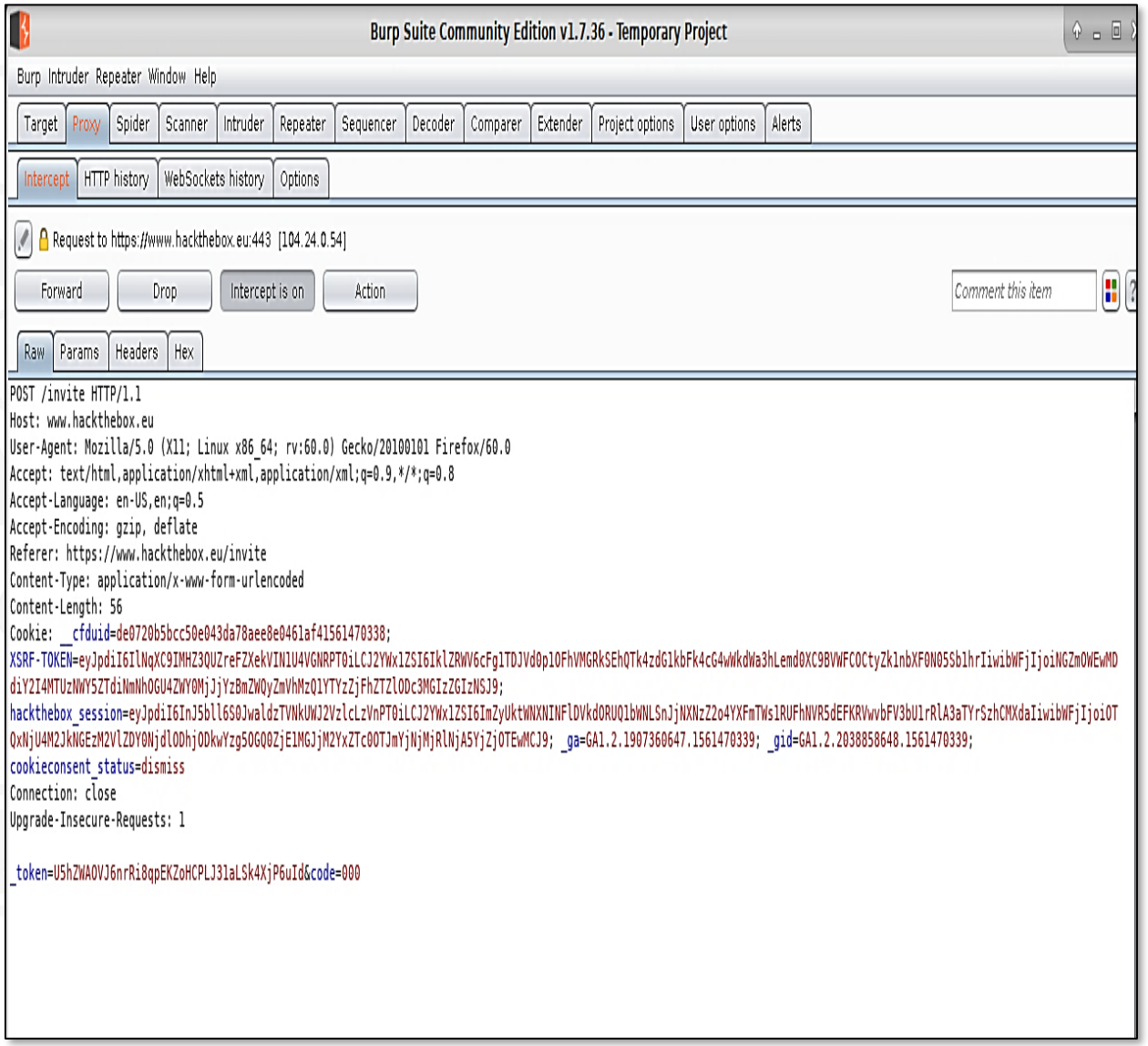
Burp HTTP proxy: Inspección

- ¡A veces el navegador da errores!
- Cuando usamos HTTPs, usar un proxy puede hacer que el navegador muestre un aviso de posible AitM
  - ¡Hay un intermediario interceptando una conexión supuestamente segura!
  - En este caso podemos añadir una excepción...¡porque es exactamente lo que pasa!
- Pero si te pasa en la vida real, con una web que no suele dar estos avisos...
  - **¡Puede ser exactamente eso!**
  - O el administrador no ha renovado los certificados correctamente
  - O alguien está haciendo un Attacker-in-the-Middle (AitM) para robarte los datos, ¡**cuidado**!



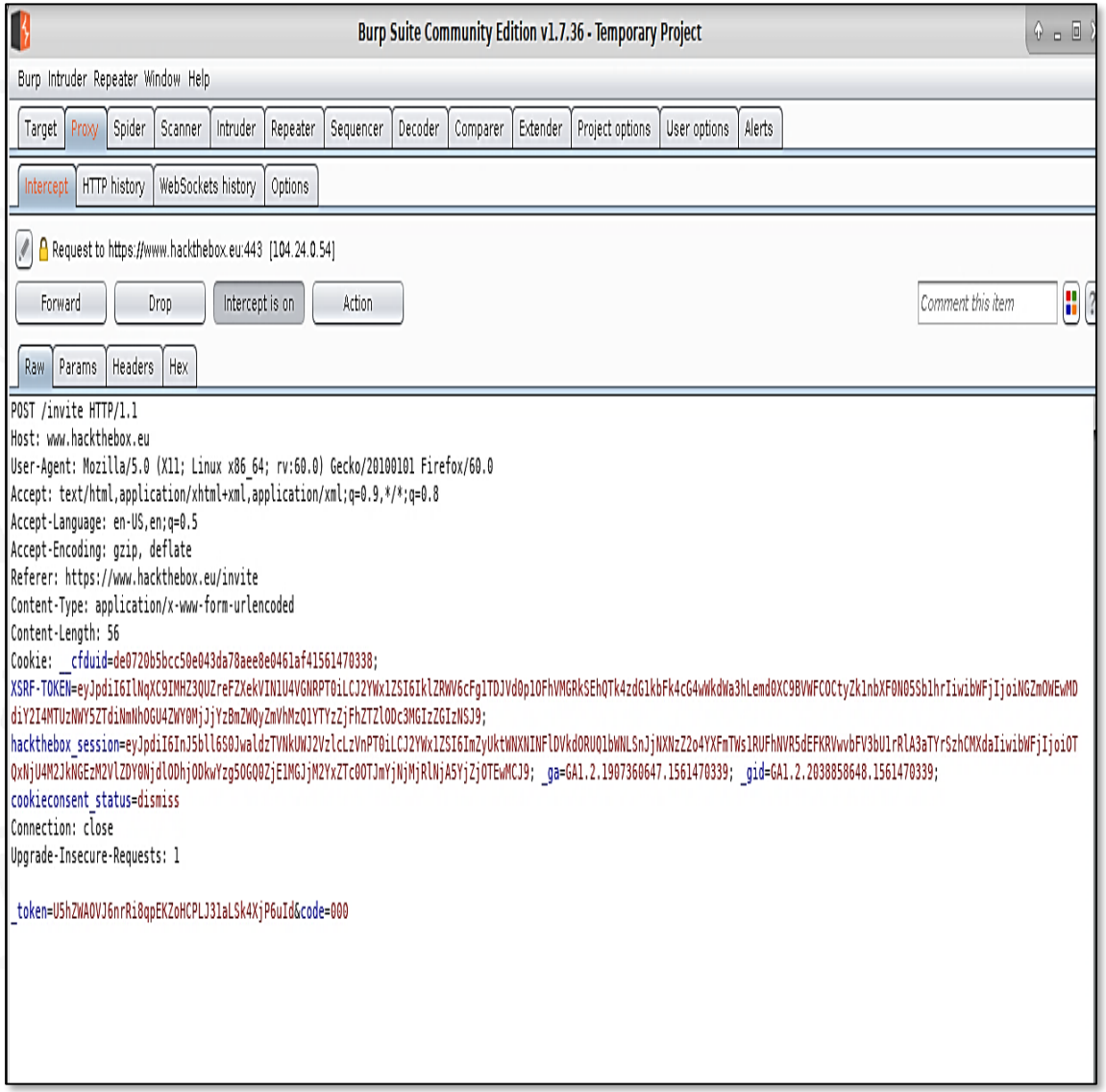
BURP HTTP PROXY: INSPECCIÓN

- **Para examinar el tráfico HTTP podemos**
  - **Clicar en Forward**: Envía una petición e intercepta la correspondiente respuesta
    - O, si la petición genera más peticiones a otras URLs, intercepta la siguiente petición
  - **Deshabilitar la intercepción**: el navegador se comporta de forma normal
    - Ninguna petición o respuesta es interceptada y no se capturan datos
- ***¿Qué tipos de datos podemos esperar?***



BURP HTTP PROXY: INSPECCIÓN

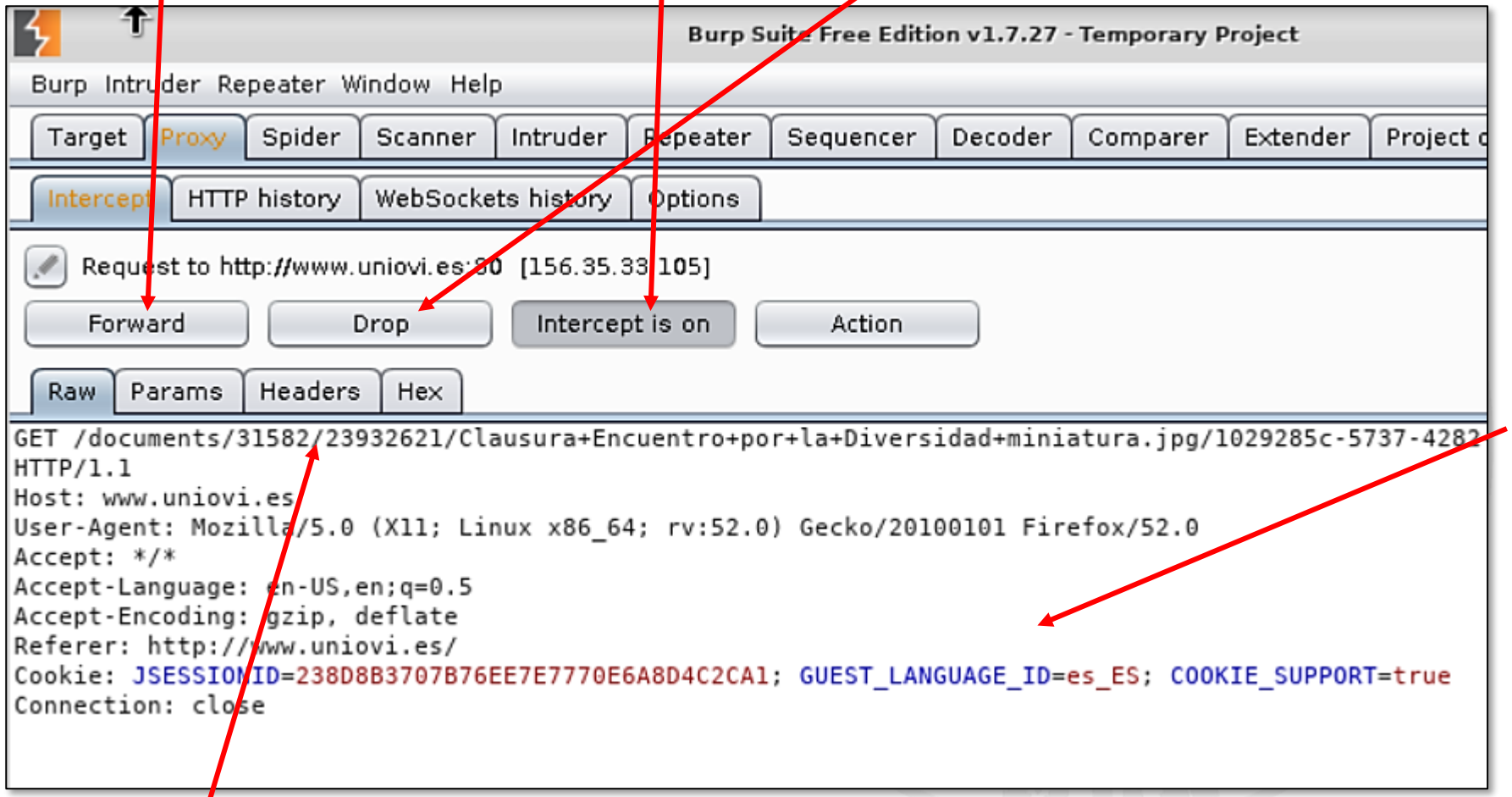
- **La cabecera de la petición** HTTP
  - En este caso no tiene nada reseñable
- Una **cookie** con un ID de sesión: realmente aleatorio, no predecible
  - No podemos suplantar usuarios fácilmente
  - Solo podríamos hacerlo si robamos una válida
- `__cfuid`: **ID de sesión** que indica que el servicio está detrás de **CloudFlare**
  - CDN, **Tema 5**
  - Está "blindado" contra un gran número de ataques
- **Sabemos cómo ver y modificar el tráfico HTTP a voluntad**
  - Nos abre muchas opciones de inspeccionar aplicaciones
  - ¿Qué posibilidades? Mira la siguiente transparencia



Envía al servidor la solicitud modificada

Habilitar esto detiene y muestra cada solicitud que realizamos desde el navegador

Al pulsar esto se descarta la solicitud, por lo que el servidor no la recibirá



Modificar los parámetros de URL para ver qué sucede

Se puede modificar el cuerpo de la solicitud y ver lo que sucede ☺. Ejemplos:

- **"Nuevo" método HTTP**: JET en lugar de GET
- **Versiones** HTTP inexistentes o erróneas
- **Host** O **Referer** apuntando a otras páginas
- Cambios en la Cookie: Otro ID de sesión...
- Hay **muchas opciones**: Se puede modificar la petición completa, y con esta herramienta nos saltamos cualquier tipo de validación del lado del cliente que la página tenga
- ¡El código fuente del lado cliente es 100% tuyo!

¿Qué pasa si provocamos un error? ¡Enumeración!

Framework utilizado para crear la página!

¡Versión y tipo de servidor!

¡Versión y tipo de software y servidor web!

Herramientas de enumeración adicionales de Burp suite

- **Aparte de la manipulación de peticiones, hay otras dos herramientas de Burp que son muy útiles en el proceso de enumeración**
  - **Burp Repeater**: herramienta para manipular manualmente y volver a enviar mensajes individuales de HTTP y WebSocket, analizando la respuesta de las aplicaciones
    - Puede usarse para cambiar valores de parámetros y probar vulnerabilidades originadas en la entrada del usuario
    - Enviando peticiones en una secuencia específica para probar fallos en la lógica
    - Y reenviar peticiones desde Burp Scanner
    - ...
    - **Tutorial**: https://portswigger.net/burp/documentation/desktop/tools/repeater/using
  - **Burp Spider**: Crawler automático de todas las páginas de un sitio web
    - Podemos descargar el sitio completo y analizar sus contenidos localmente en detalle
    - **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

Seguridad de Sistemas Informáticos

- **Escáner web GPL**
- **Ejecuta un conjunto de pruebas sobre un servidor web buscando**
  - Más de 6500 archivos peligrosos o CGIs
  - Versiones antiguas del software del servidor
  - Problemas conocidos de configuración
  - Versión instalada del servidor y sus servicios
    - Problemas conocidos de esas versiones
- **Wikto (versión Windows) añade más características, haciéndolo más potente**
- **Consume pocos recursos, especialmente en comparación con OpenVAS o 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

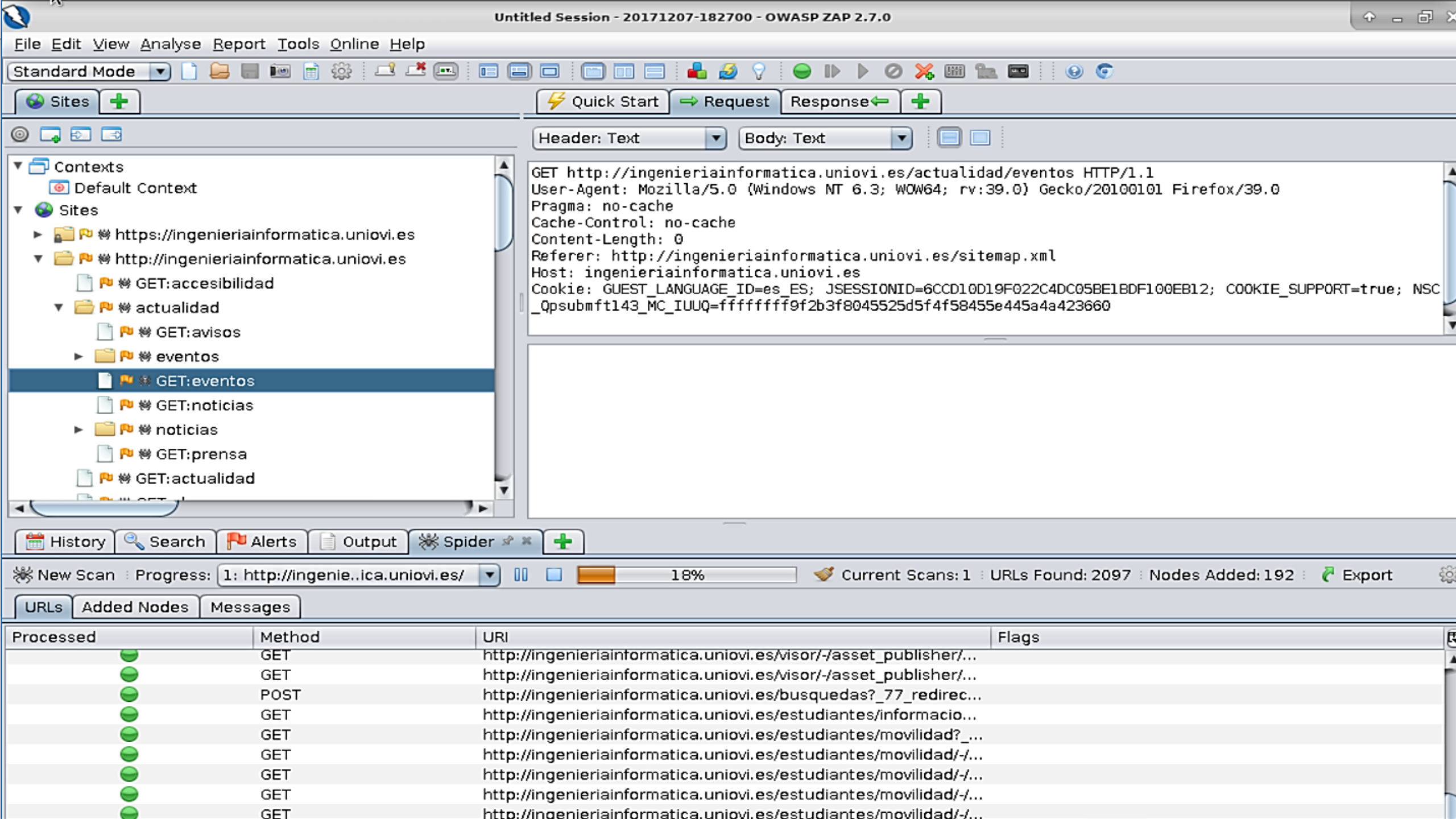
TUNING OPTIONS

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)

Zed Attack Proxy (ZAP)

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

- **Escáner de seguridad web de código abierto utilizado como herramienta profesional para pentesting**
  - Una de las herramientas más famosas y utilizadas para estos fines
- **Cuando se utiliza como servidor proxy, permite a los usuarios manipular todo el tráfico que pasa a través de él, incluyendo HTTPS, como hace Burp**
- **También incluye varios análisis de seguridad pasivos y/o activos que le permiten encontrar vulnerabilidades en las webs escaneadas**
  - Incluyendo técnicas de **fuzzing** y **fuerza bruta**
- **Cuenta con varios plugins que mejoran su funcionalidad**
- **También lo veremos en el Laboratorio 10 como herramienta DAST (Tema 6)**
- **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/-/...

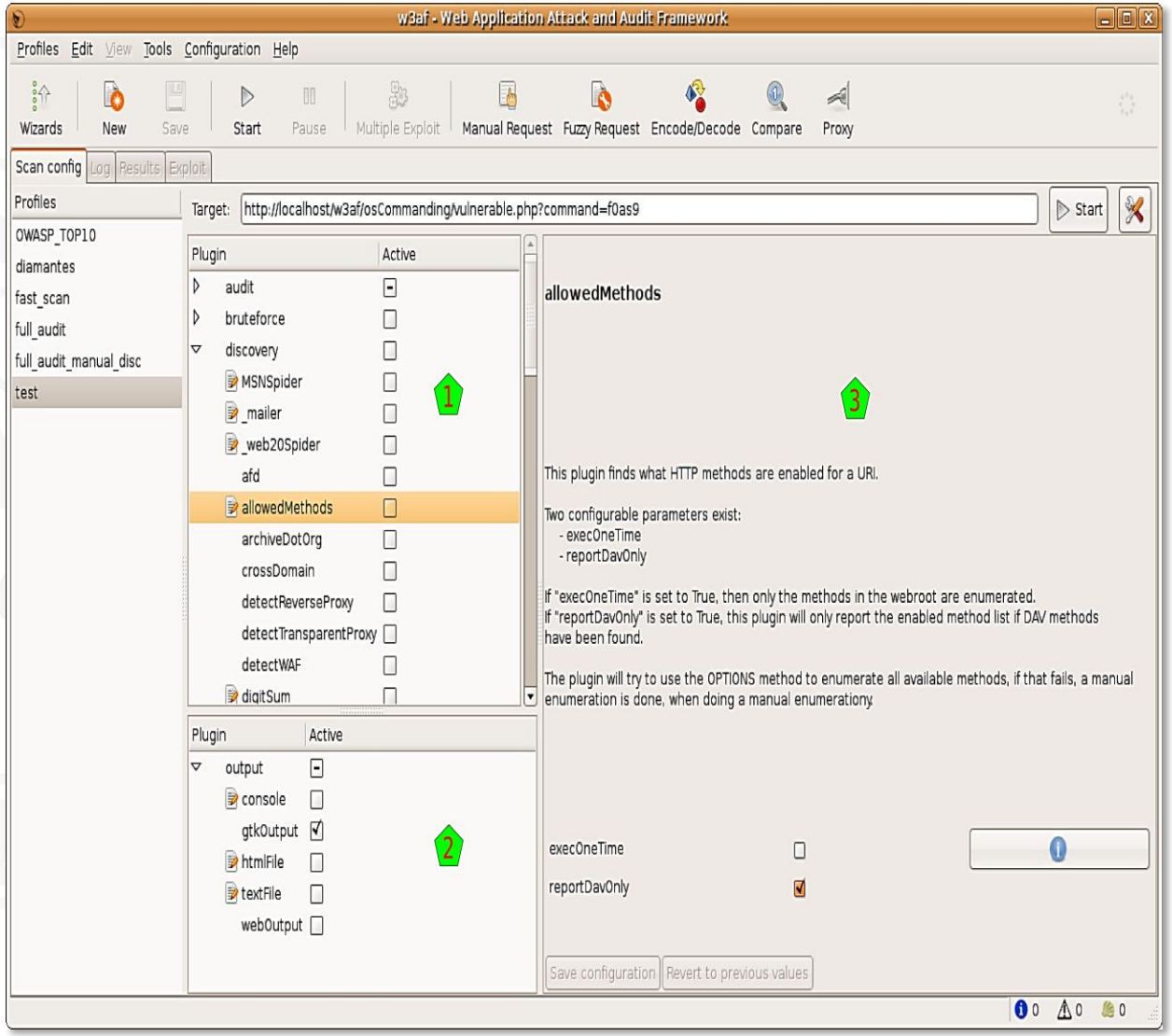
W3AF

http://w3af.org/

Seguridad de Sistemas Informáticos

- Un framework de auditoría y ataque de aplicaciones web
- Permite encontrar y explotar vulnerabilidades
- Contiene muchas vulnerabilidades web conocidas
  - Incluidas las del Top 10 de OWASP
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Tutorial
  - http://docs.w3af.org/en/latest/basic-ui.html

Fuente: http://docs.w3af.org/en/latest/gui/scanning.html

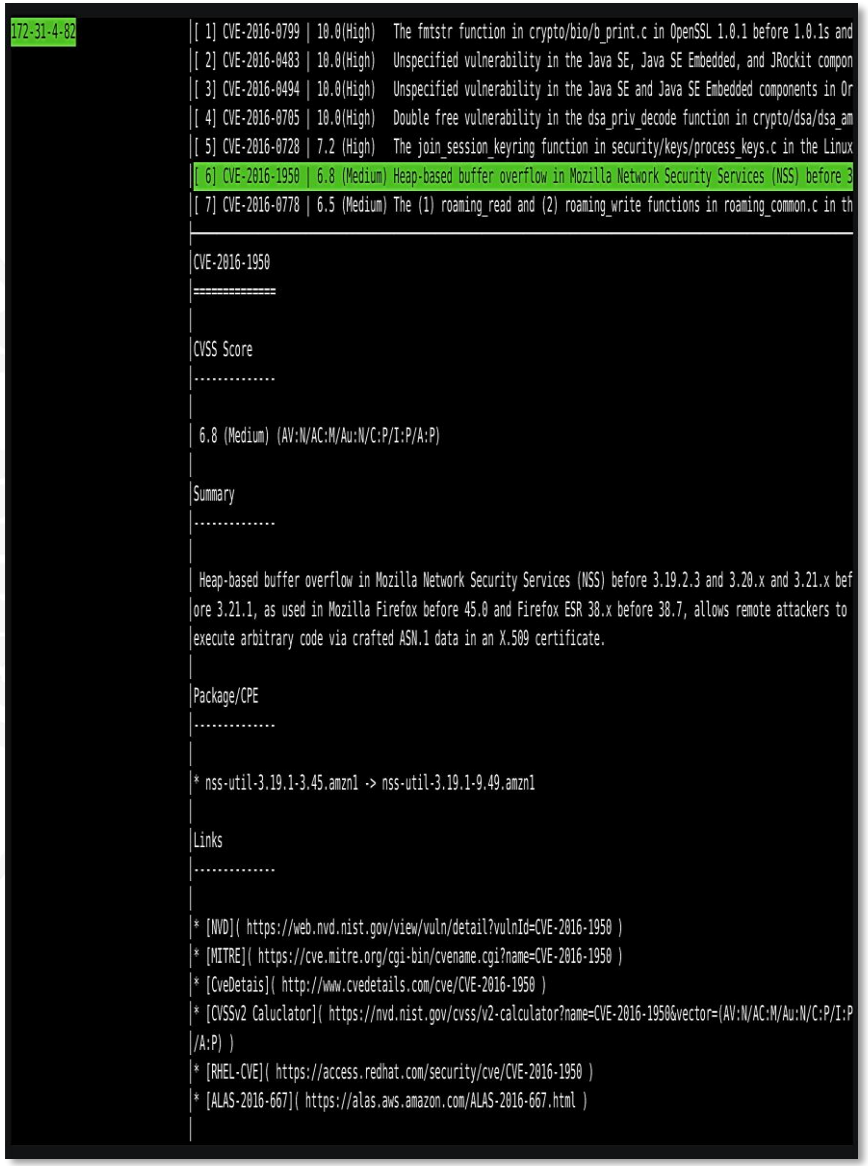


VULS

https://vuls.io/

- **Usa varias BBDD (NVD, JVN, OVAL, RHSA / ALAS / ELSA / FreeBSD-SA…) para detectar vulnerabilidades**
  - Podría detectarlas aunque no tengan parches publicados
- **Permite escaneos remotos (vía SSH) y locales e implementa dos modos de análisis**
  - **Fast scan**: escanea sin privilegio de `root`, sin acceso a Internet, y casi sin carga para el servidor analizado
  - **Deep scan**
- **Detecta vulnerabilidades conocidas en paquetes que no sean del SO**
  - Como ejecutables compilados por el usuario, bibliotecas de lenguaje y frameworks, etc.
- **Instalación y tutorial**
  - https://www.howtoforge.com/tutorial/how-to-install-and-use-vuls-vulnerability-scanner-on-ubuntu/
  - https://vuls.io/docs/en/tutorial.html

Fuente: https://github.com/future-architect/vuls

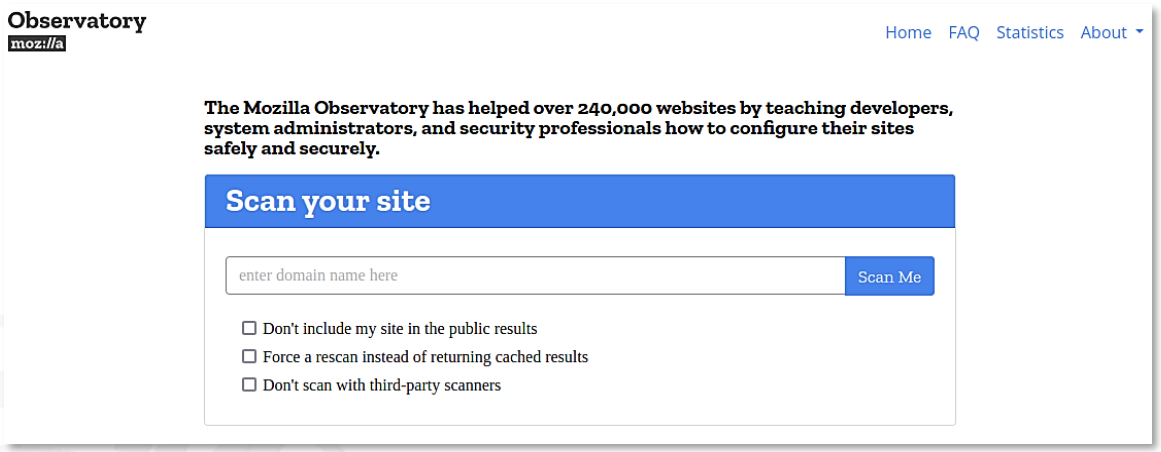


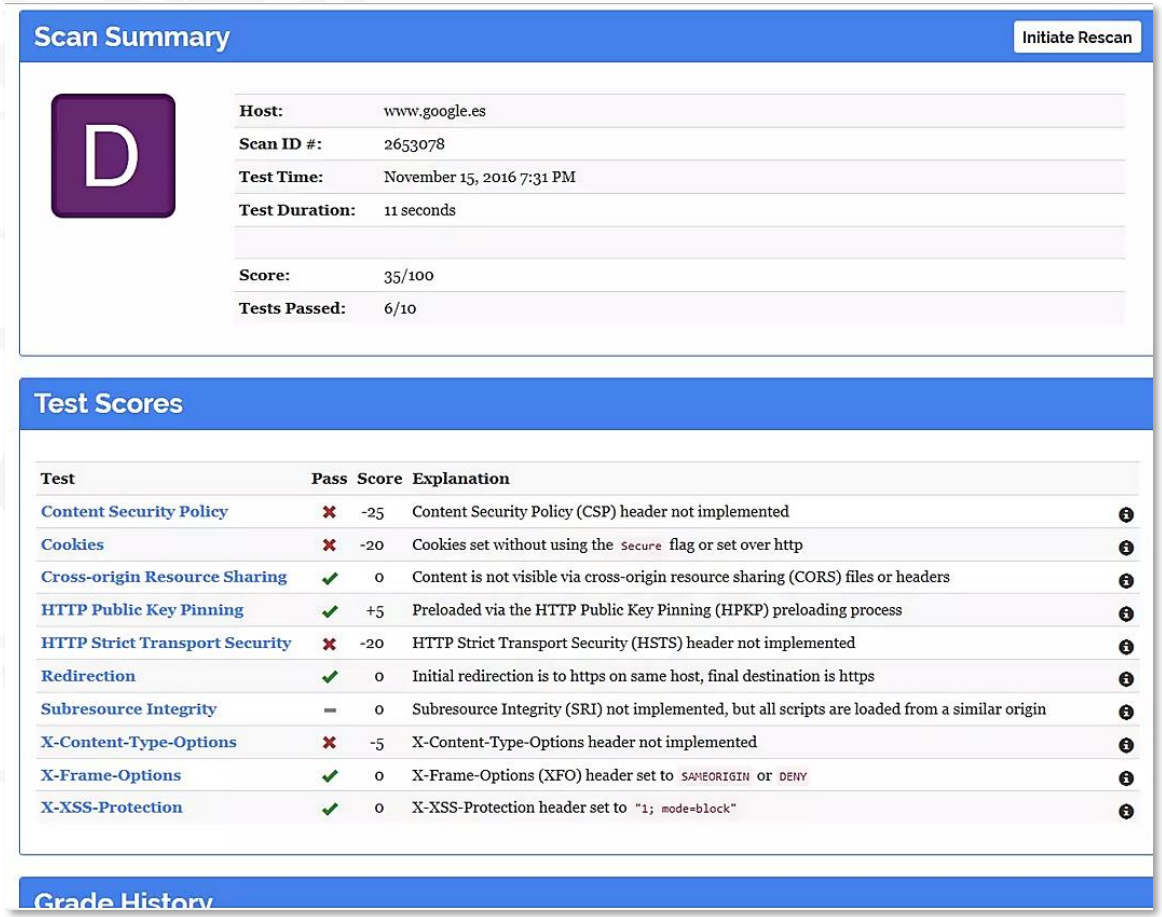
MOZILLA OBSERVATORY

https://observatory.mozilla.org/

Seguridad de Sistemas Informáticos

- **Es una herramienta online para analizar sitios webs en busca de posibles problemas conocidos**
- **No descubre en si vulnerabilidades**
  - Pero si problemas de configuración que pueden causarlas
- **No está por tanto de más usarla con nuestros propios sitios**
  - Para asegurarnos de que no se nos ha olvidado algo importante





(1) Usando Nikto contra un servidor web

Ejemplo de ejecución de Nikto


```
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

- **Los servidores / equipos comprometidos se usan para una gran variedad de propósitos maliciosos**
- **Uno de los más comunes es integrarse en una Botnet**
  - Una vez que está dentro, el equipo se usa para cualquier tipo de delito
  - DDoS, enviar mensajes de phising, albergar tiendas falsas…
- **Podemos verificar si nuestro equipo se ha detectado como parte de una Botnet con un servicio de la OSI**
  - https://www.osi.es/es/servicio-antibotnet
  - Además de detectar, también ofrece herramientas para solucionarlo

Lista de insignias para autoevaluación: Seminario 3

- Entender las ventajas y desventajas de las herramientas automatizadas de análisis de vulnerabilidades
- Comprender las implicaciones legales del uso de estas herramientas
- Entender la utilidad de las herramientas automáticas de análisis de vulnerabilidades para web
- Saber cómo lanzar un escaneo con **OpenVAS** contra un objetivo
- Saber cómo lanzar un análisis de vulnerabilidades con **Nikto** contra un objetivo web
- Conocer una serie de herramientas de escaneo automático que complementen los contenidos de teoría
- Conocer un "arsenal" de herramientas automatizadas capaces de descubrir vulnerabilidades web automáticamente

SEMINARIO 3
HERRAMIENTAS DE ESCANEO AUTOMÁTICO DE VULNERABILIDADES

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo