

**PAI – 4. VULNAWEB**  
**AUDITORÍA DE SEGURIDAD EN SISTEMAS**  
**INFORMÁTICOS Y ANÁLISIS DE**  
**VULNERABILIDADES EN APLICACIONES WEB**  
**PARA EMPRESA DE COMERCIO ELECTRÓNICO**

Ángel Jesús Varela Vaca  
Grupo de Investigación **IDEA Research Group**,  
Universidad de Sevilla



“Nos requieren para llevar a cabo un análisis que permitan **auditar los sistemas informáticos** que se usan (equipos de sobremesa, servidores y dispositivos móviles) y **las aplicaciones** correspondientes de una empresa, por si presentan vulnerabilidades que puedan provocar ataques”.

Se propone a los Security Teams de INSEGUS alcanzar los objetivos siguientes:

1. *Realizar la **auditoría de seguridad para sistemas informáticos de sobremesa, portátiles y dispositivos móviles** que utilizan los usuarios de la empresa de comercio electrónico*
2. *Realizar la configuración de una herramienta de escaneo de **vulnerabilidades Web** y que permita además llevar a cabo trazabilidad de las peticiones/respuestas HTTP/HTTPS*

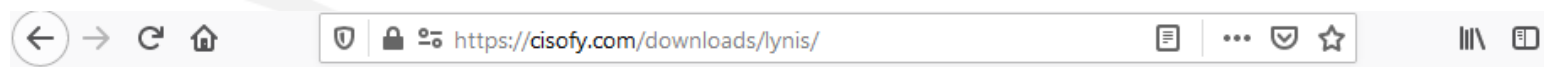
Se propone a los Security Teams de INSEGUS alcanzar los objetivos siguientes:

3. *Auditar las aplicaciones Web que dan soporte a las actividades de la empresa cliente, identificando las posibles vulnerabilidades de seguridad, tales como **Inyecciones, XSS, CSRF, Path Traversal, etc...** y mostrar las pruebas que ha realizado (mientras nos llega la autorización de la empresa de comercio electrónico, indicando todos los aspectos para tener en cuenta en la auditoría Web, se realizarán pruebas sobre determinado servidor Web vulnerable de prueba en local)*

**NOTA MUY IMPORTANTE:** Estas herramientas no deben ser utilizadas contra servidores en producción para los que no se encuentre debidamente autorizado. El objeto de dar a conocer cómo realizar auditorías de seguridad informática de sistemas informáticos y aplicaciones Web, y se debe evitar el uso de dichas herramientas para otros fines ilegales o no lícitos

# Tarea 1. Auditoría de Seguridad y Bastionado de un determinado sistema informático de sobremesa

Obtener el índice de hardening que tiene el equipo informático de sobremesa concreto y realizar las acciones correspondientes para alcanzar el índice de hardening requerido por la Política de Seguridad de la empresa cliente



[Solutions](#) [Demo](#) [Pricing](#) [Support](#)

» [Home](#) » Downloads

## Download Lynis

### Description

Lynis is a security auditing tool for UNIX derivatives like Linux, macOS, BSD, Solaris, AIX, and others. It performs an in-depth security scan. Software packages are available via <https://packages.cisofy.com>.

### Requirements

Shell and basic utilities

### Permissions

```
[*] Users, Groups and Authentication
-----
- Search administrative accounts...           [ OK ]
- Checking SUID...                             [ FOUND ]
- Checking sticky bit...                       [ OK ]
- Checking group file /etc/group file...       [ OK ]
- Test group files (passwd)...                 [ OK ]
- Checking login shells...                     [ WARNING ]
- Checking non unique group ID's...           [ OK ]
- Checking non unique group names...          [ OK ]
- Checking LDAP authentication support...      [ NOT ENABLED ]
- Check /etc/passwd file...                   [ NOT FOUND ]

[ Press (ENTER) to continue, or (CTRL)+C to stop ]

[*] Shell
-----
- Checking console TTY...                       [ WARNING ]
- Checking shells from /etc/shells...           [ OK ]
  Result: found 4 shells (valid shells: 4).

[ Press (ENTER) to continue, or (CTRL)+C to stop ]

[*] File system
-----
- [FRODO] Checking LFF mount points (EXT4)... [ OK ]
- Sudo swap partition (EXT4)...                [ OK ]
- Testing swap partition...                    [ OK ]
- Checking /etc/crontab file...                 [ WARNING ]
- Checking /tmp sticky bit...                  [ OK ]
```

Screenshot of Lynis

## Tarea 1. Auditoría de Seguridad y Bastionado de un determinado sistema informático de sobremesa

### ➤ sudo lynis -Q

```
Follow-up:
-----
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====

Lynis security scan details:

Hardening index : 53 [#####          ]
Tests performed : 214
Plugins enabled : 1

Components:
- Firewall           [V]
- Malware scanner    [X]


Lynis Modules:
- Compliance Status  [?]
- Security Audit     [V]
- Vulnerability Scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data                : /var/log/lynis-report.dat
```



*Aplicar la correspondiente auditoría para alcanzar el hardening index especificado en la Política de Seguridad (no inferior a 68), mediante las correspondientes actuaciones que tienen que ser todas documentadas en el informe final de este proyecto*

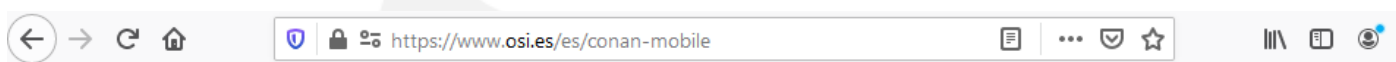
## *Tarea 1. Auditoría de Seguridad y Bastionado de un determinado sistema informático de sobremesa*

- Junto al hardening index aparecerán un conjunto de sugerencias
    - Si la salida es **[OK]** se considera como resultado ESPERADO
    - Si la salida es **[WARNING]** es un resultado NO ESPERADO (de acuerdo a la política, no quiere decir que sea malo)
    - Si la salida es **[NO FOUND]**, como que no se ha encontrado el objeto de testeo
  - Información adicional en fichero: /var/log/lynis.log
  - Indique también las razones por las cuales ha seleccionado unas determinadas acciones y no otras.
- 
- A cartoon illustration of a man in a suit sitting at a desk, looking at a laptop with a question mark on the screen, appearing to be in deep thought or troubleshooting.
- El **browser** deberá tener la configuración segura para comunicaciones de comercio electrónico. En el informe del Proyecto se indicará las acciones llevadas a cabo para realizar una configuración segura de dicho browser para las conexiones



## Tarea 2. Auditoría de Seguridad de un dispositivo móvil

Utilizar una herramienta para obtener una configuración “hard” del dispositivo móvil y realizar las acciones correspondientes para alcanzar el hardening requerido por la Política de Seguridad de la empresa cliente



¿Quiénes somos? Encuesta de valoración PORTALES INCI Contacto Bolet

Ponte al día Campañas Protégete Recursos Juegos educativos Iniciativas Ayuda

Inicio » Recursos » CONAN mobile

### CONAN mobile

CONAN mobile es una aplicación gratuita que te ayuda a proteger tu dispositivo móvil Android. Te permite mostrándote soluciones a posibles riesgos a los que esté expuesto y proporcionándote algunos consejos. Invitamos a descargarlo gratuitamente en [Google Play](#) y a analizar el nivel de seguridad de tu dispositivo.



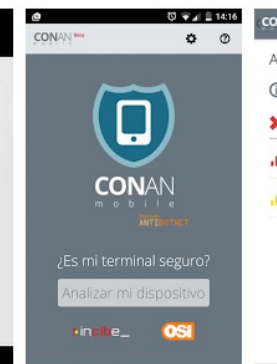
### CONAN mobile

INCIBE Herramientas

★★★★★ 1.397

Para todos

Añadir a la lista de deseos





## Tarea 2. Auditoría de Seguridad de un dispositivo móvil

- El resultado del análisis está dividido en cuatro secciones:
  - **Configuración:** describe los problemas de configuración encontrados
  - **Aplicaciones:** muestra incidencias detectadas en las aplicaciones instaladas.
  - **Permisos:** Acceso a los permisos declarados por las aplicaciones por orden de peligrosidad.
  - **Servicio Proactivo:** eventos de seguridad detectados y eventos sobre las conexiones realizadas por las aplicaciones del dispositivo, así como información extendida de las mismas





## Tarea 2. Auditoría de Seguridad de un dispositivo móvil

- Alcanzar en cada dispositivo móvil del Security Team el hardening especificado en la Política de Seguridad de la empresa cliente:

Para la seguridad de las transmisiones con esta empresa de comercio electrónico a través de dispositivos móviles se requiere:

Respecto a la configuración del dispositivo:

- No tener habilitada la instalación de software de orígenes desconocidos
- No tener el dispositivo móvil *rooteado o jailbreak*
- Tener instaladas todas las actualizaciones del fabricante del dispositivo del sistema operativo y de la aplicación browser
- No conectarse a redes Wifi sin seguridad adecuada o con SSID oculta
- No tener activado el dispositivo Bluetooth durante las conexiones Web

Respecto a las aplicaciones instaladas

- No tener instaladas aplicaciones maliciosas o sospechosas de serlo.
- No tener abiertas conexiones de red de aplicaciones diferentes al browser y que se consideren sospechosas
- No tener habilitados permisos de otras aplicaciones para lectura de información sobre lo que el browser se descarga/envía.

Debe presentar a INSEGUS un conjunto de pruebas que muestre las posibilidades de una para comprobar la correcta trazabilidad de las peticiones HTTP/HTTPS sin modificación alguna de los parámetros de las peticiones y las respuestas obtenidas desde el servidor de prueba



[Home](#) [Blog](#) [Videos](#) [Documentation](#) [Community](#) [Download](#)

### OWASP® Zed Attack Proxy (ZAP)

The world's most widely used web app scanner. Free and open source. Actively maintained by a dedicated international team of volunteers.



[Home](#) [Blog](#) [Videos](#) [Documentation](#) [Community](#) [Download](#)

### Download ZAP

- Checksums for all of the ZAP downloads are maintained on the [2.10.0 Release Page](#) and in the relevant [version files](#).
- As with all software we strongly recommend that ZAP is only installed and used on operating systems and JREs that are fully patched and actively maintained.

#### ZAP 2.10.0

[Windows \(64\) Installer](#)

133 MB

[Download](#)

[Windows \(32\) Installer](#)

133 MB

[Download](#)

[Linux Installer](#)

134 MB

[Download](#)

[Linux Package](#)

131 MB

[Download](#)

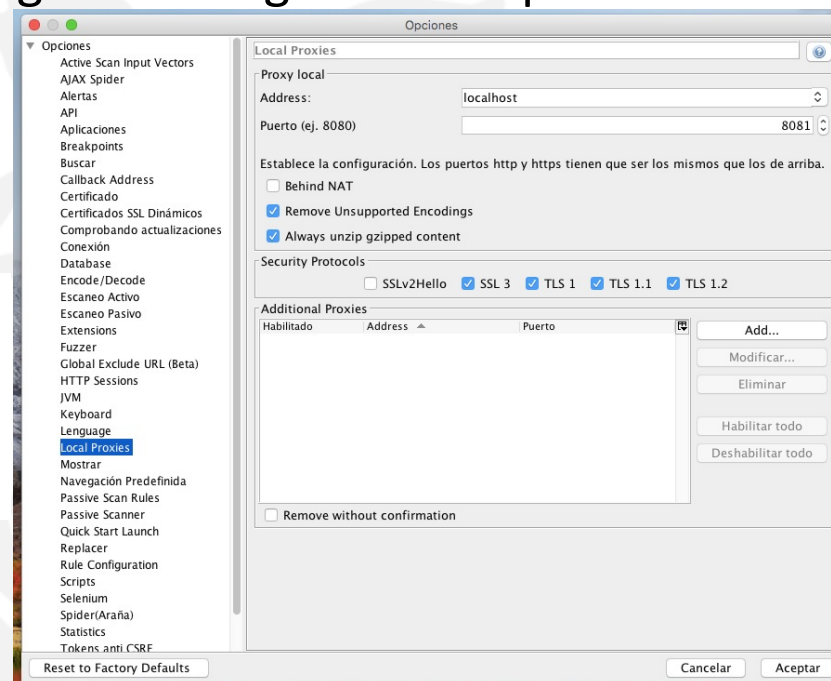
[MacOS Installer](#)

199 MB

[Download](#)

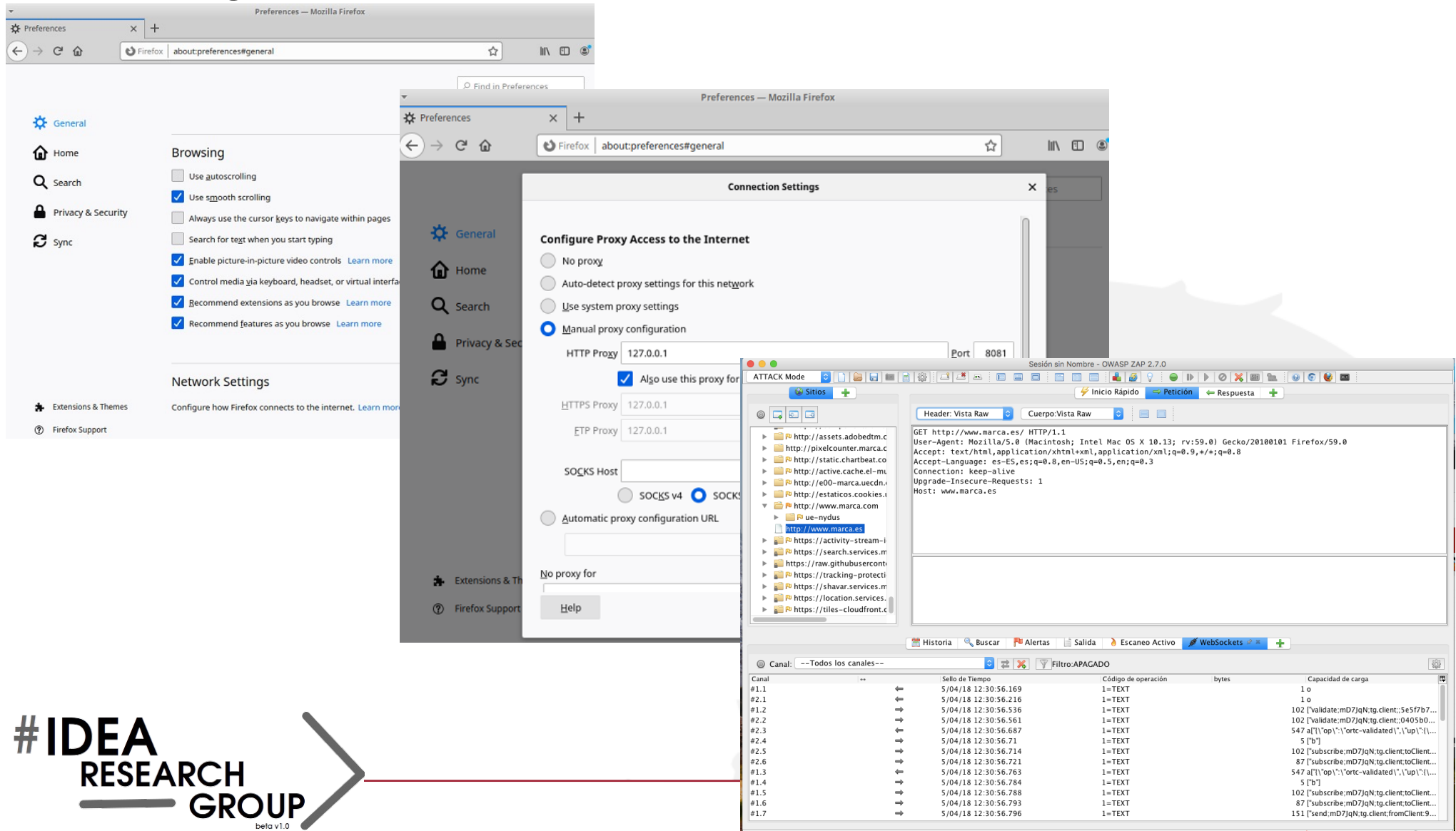
## Tarea 3. Auditoría de vulnerabilidades en aplicaciones Web y Trazabilidad de peticiones/respuestas para los protocolos HTTP / HTTPS

- Ejemplo: Herramientas Dynamic Application Security Testing (**DAST**) que usan la metodología de testing de seguridad de caja-negra
- **OWASP ZAP** es un marco de trabajo para la trazabilidad de peticiones/respuestas HTTP/HTTPS y analizar posibles vulnerabilidades de las aplicaciones web
- Para poder **interceptar el tráfico** (peticiones/respuestas) en la herramienta en la pestaña “Proxy” tendremos que configurar los siguientes aspectos
  - **Address: dirección IP de escucha (localhost)**
  - **Port: puerto de escucha (8081)**



# Tarea 3. Auditoría de vulnerabilidades en aplicaciones Web y Trazabilidad de peticiones/respuestas para los protocolos HTTP / HTTPS

- Configuración externa del cliente web



The image shows a composite of three screenshots related to web client configuration and traffic analysis:

- Firefox Preferences (General):** Shows the 'Browsing' section with options like 'Use smooth scrolling' and 'Enable picture-in-picture video controls' checked. The 'Network Settings' section is also visible.
- Firefox Connection Settings:** Shows the 'Configure Proxy Access to the Internet' section. The 'Manual proxy configuration' option is selected, with HTTP, HTTPS, and FTP proxies all set to 127.0.0.1 on port 8081. The 'SOCKS Host' field is empty, and 'SOCKS v4' is selected.
- OWASP ZAP (Zed Attack Proxy):** Shows the 'Sesión sin Nombre - OWASP ZAP 2.7.0' window. The 'Header: Vista Raw' tab is active, displaying the raw HTTP request for 'GET http://www.marca.es/ HTTP/1.1'. The request includes headers like 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:59.0) Gecko/20100101 Firefox/59.0' and 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8'. The 'Cuerpo: Vista Raw' tab is also visible, showing the raw response body.

### Modo intercepción de peticiones con OWASP ZAP

- Es posible activar un modo especial de ejecución donde capturaremos las peticiones y antes de ser respondidas por el servidor podremos visionar la petición incluso modificarla y reenviarla al servidor modificadas
- Este es un caso de ejemplo de Man-in-the-Middle (**MitM**)
- Para activar el modo de intercepción sólo tenemos que activar un **“Breakpoint”**, desde el botón verde situado en la barra de menús de ZAP



- Una vez activada dicha opción ZAP se pondrá en modo recepción de peticiones y podremos capturar peticiones
- También podremos editar las peticiones y cambiar valores

## Tarea 4. Análisis de vulnerabilidades Web para Servidor de Pruebas

Realizar una detección y análisis de las vulnerabilidades y presentar todos los resultados obtenidos y las posibles recomendaciones (plan de mitigación) para evitar todo este tipo de vulnerabilidades Web, al menos para la inyección SQL, Path/Directory Traversal, XSS reflejado y almacenado (posiciones A1, A5 y A7 respectivamente en OWASP Top Ten 2017)



Se debe presentar el entorno simulado o de desarrollo propio que ha utilizado para hacer las correspondientes pruebas.

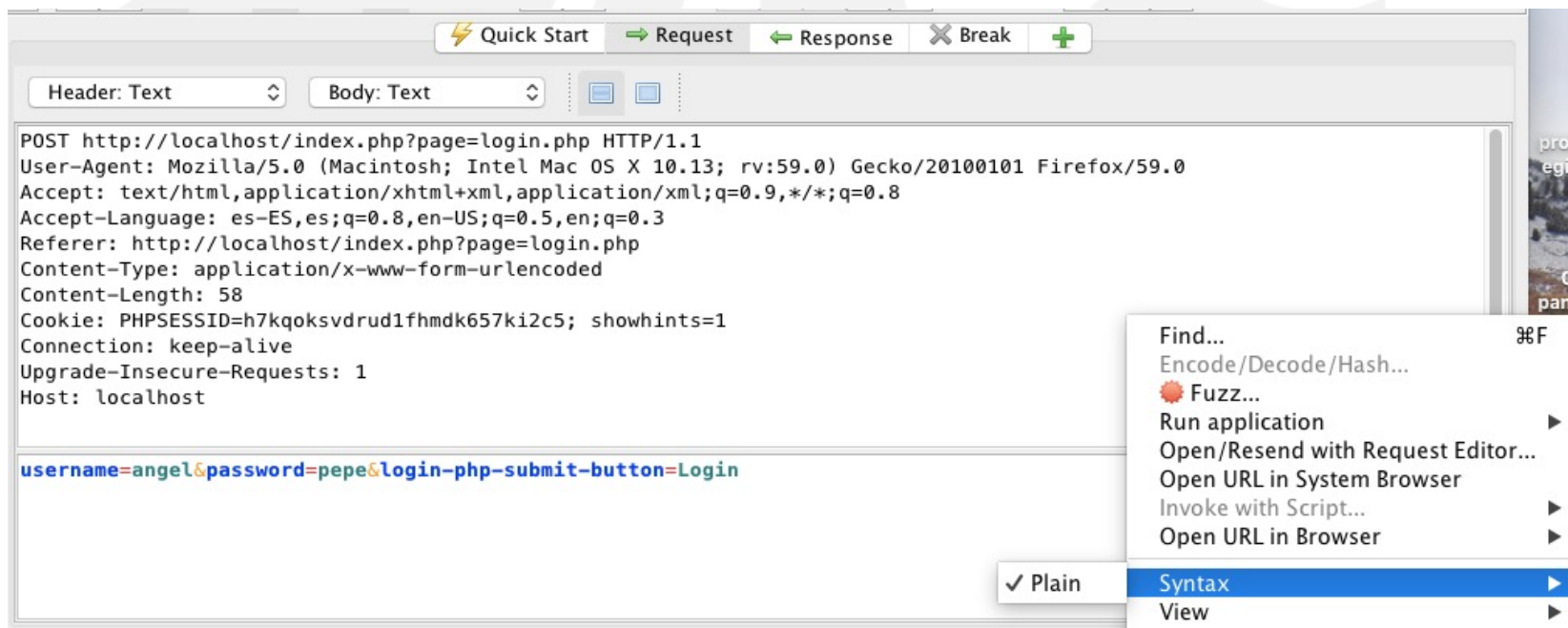
Las satisfacción del cliente será mayor si el entorno que se utilice para hacer las pruebas es diferente al propuesto en el ejemplo del manual de la práctica (OWASP Mutillidae).



## Tarea 4. Análisis de vulnerabilidades Web para Servidor de Pruebas

### Modo testeo de inyecciones con OWASP ZAP

- Para realizar las pruebas de inyección no es necesario probar uno a uno las diferentes cadenas/payloads
- OWASP ZAP está provisto de un “**Fuzzer**” que permite una vez interceptada una petición, repetir la misma con diferentes parámetros de entrada
- Para ello sobre cualquier petición “Request” que disponga de parámetros le damos botón derecho y tenemos la opción “Fuzz”

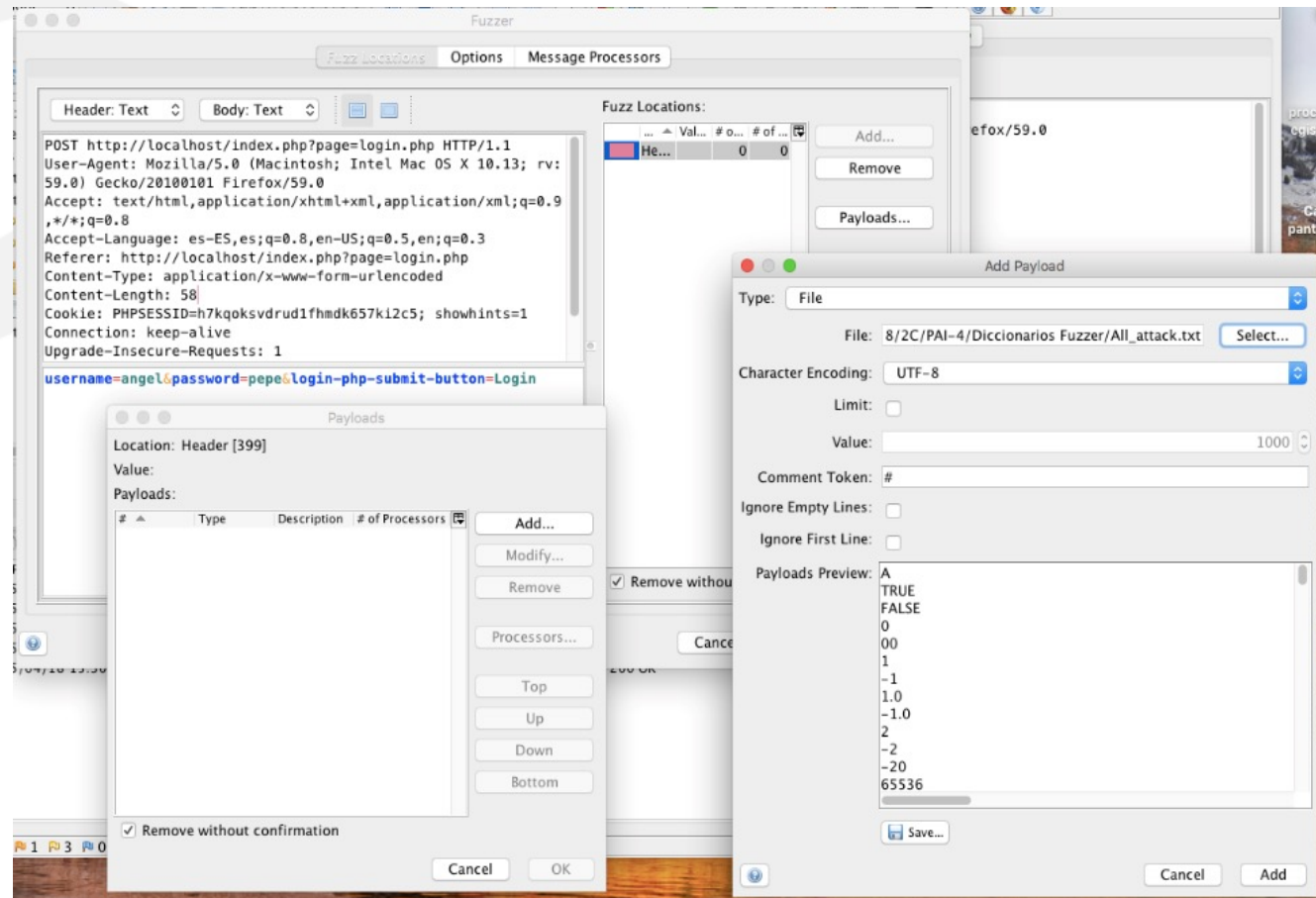




## Tarea 4. Análisis de vulnerabilidades Web para Servidor de Pruebas

### Modo testeo de inyecciones con OWASP ZAP

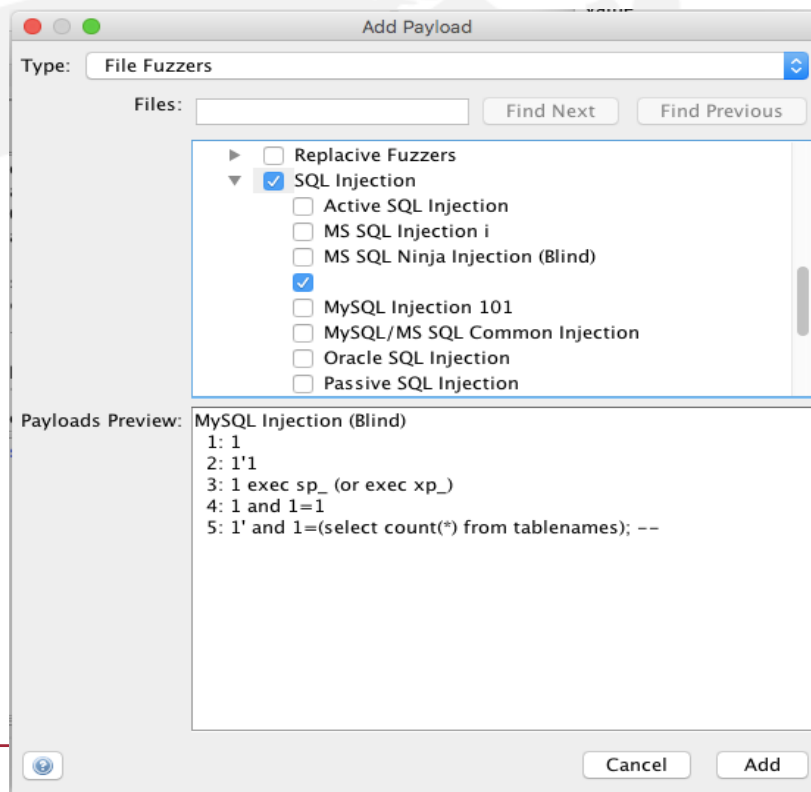
- El **Fuzzer** nos permitirá configurar que parámetros usaremos para introducir las diferentes cadenas de búsqueda para probar en las peticiones



## Tarea 4. Análisis de vulnerabilidades Web para Servidor de Pruebas

### Modo testeo de inyecciones con OWASP ZAP

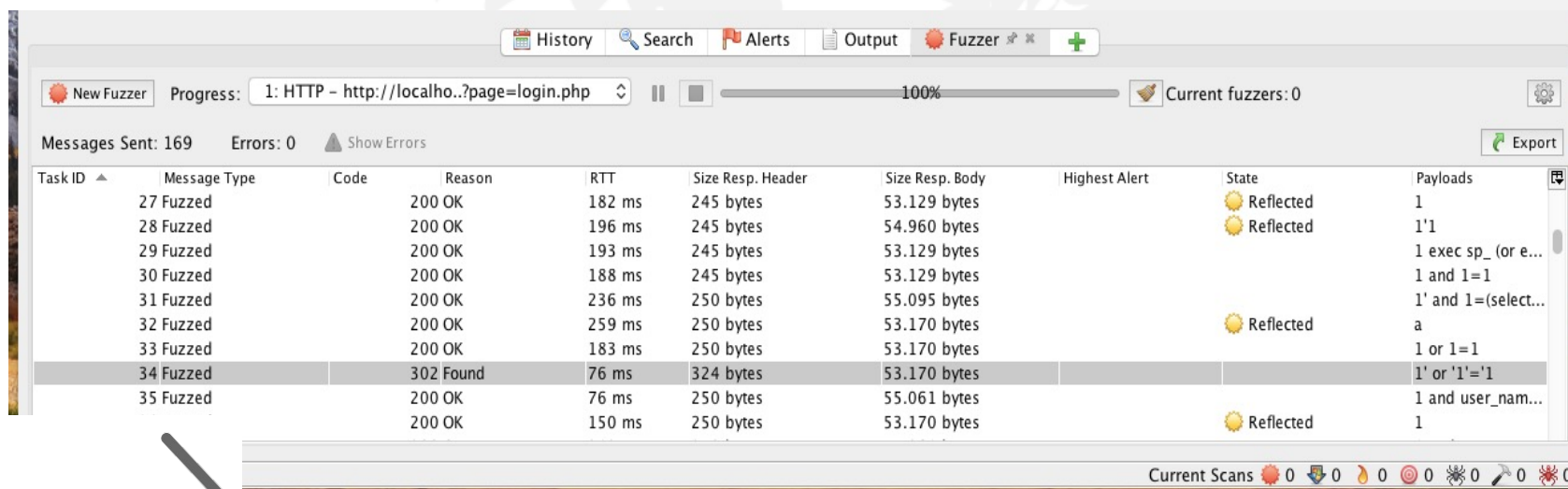
- También ZAP viene provisto con un conjunto de diccionarios de payloads precargados para hacer pruebas de inyecciones
- Marcamos la opción de “File Fuzzer”
- Dentro de la opción de “jbrofuzz” tenemos una sección de “SQL Injection” y dentro tenemos varios diccionarios de payloads predefinidos



## Tarea 4. Análisis de vulnerabilidades Web para Servidor de Pruebas

### Modo testeo de inyecciones con OWASP ZAP

- El Fuzzer se encargará de usar todas las cadenas del diccionario que hayamos introducido y tomar las respuestas, mostrándonos una pantalla de resultados
- Será trabajo nuestro identificar qué peticiones han dado resultados satisfactorios y ver qué cadenas son las más interesantes
- Todas aquellas peticiones marcadas como “Reflected” en su “Status” o como “Found” en su “Reason” son peticiones interesantes por sus resultados



| Task ID | Message Type | Code      | Reason | RTT    | Size Resp. Header | Size Resp. Body | Highest Alert | State     | Payloads            |
|---------|--------------|-----------|--------|--------|-------------------|-----------------|---------------|-----------|---------------------|
| 27      | Fuzzed       | 200 OK    |        | 182 ms | 245 bytes         | 53.129 bytes    |               | Reflected | 1                   |
| 28      | Fuzzed       | 200 OK    |        | 196 ms | 245 bytes         | 54.960 bytes    |               | Reflected | 1'1                 |
| 29      | Fuzzed       | 200 OK    |        | 193 ms | 245 bytes         | 53.129 bytes    |               |           | 1 exec sp_ (or e... |
| 30      | Fuzzed       | 200 OK    |        | 188 ms | 245 bytes         | 53.129 bytes    |               |           | 1 and 1=1           |
| 31      | Fuzzed       | 200 OK    |        | 236 ms | 250 bytes         | 55.095 bytes    |               |           | 1' and 1=(select... |
| 32      | Fuzzed       | 200 OK    |        | 259 ms | 250 bytes         | 53.170 bytes    |               | Reflected | a                   |
| 33      | Fuzzed       | 200 OK    |        | 183 ms | 250 bytes         | 53.170 bytes    |               |           | 1 or 1=1            |
| 34      | Fuzzed       | 302 Found |        | 76 ms  | 324 bytes         | 53.170 bytes    |               |           | 1' or '1'='1        |
| 35      | Fuzzed       | 200 OK    |        | 76 ms  | 250 bytes         | 55.061 bytes    |               |           | 1 and user_nam...   |
|         |              | 200 OK    |        | 150 ms | 250 bytes         | 53.170 bytes    |               | Reflected | 1                   |

### **Documento (30%)**

- Tamaño del informe.
- Calidad del informe aportado y justificaciones.
- Calidad de pruebas presentadas y resultados.

### **Código/Configuración aportada (70%)**

- Cumplimiento de requisitos establecidos por la empresa cliente
- Calidad de las auditorías realizadas y del hardening alcanzado
- Respuesta al conjunto de consultas planteadas
- Pruebas realizadas