**Herramienta utilizada Modo Standard:**

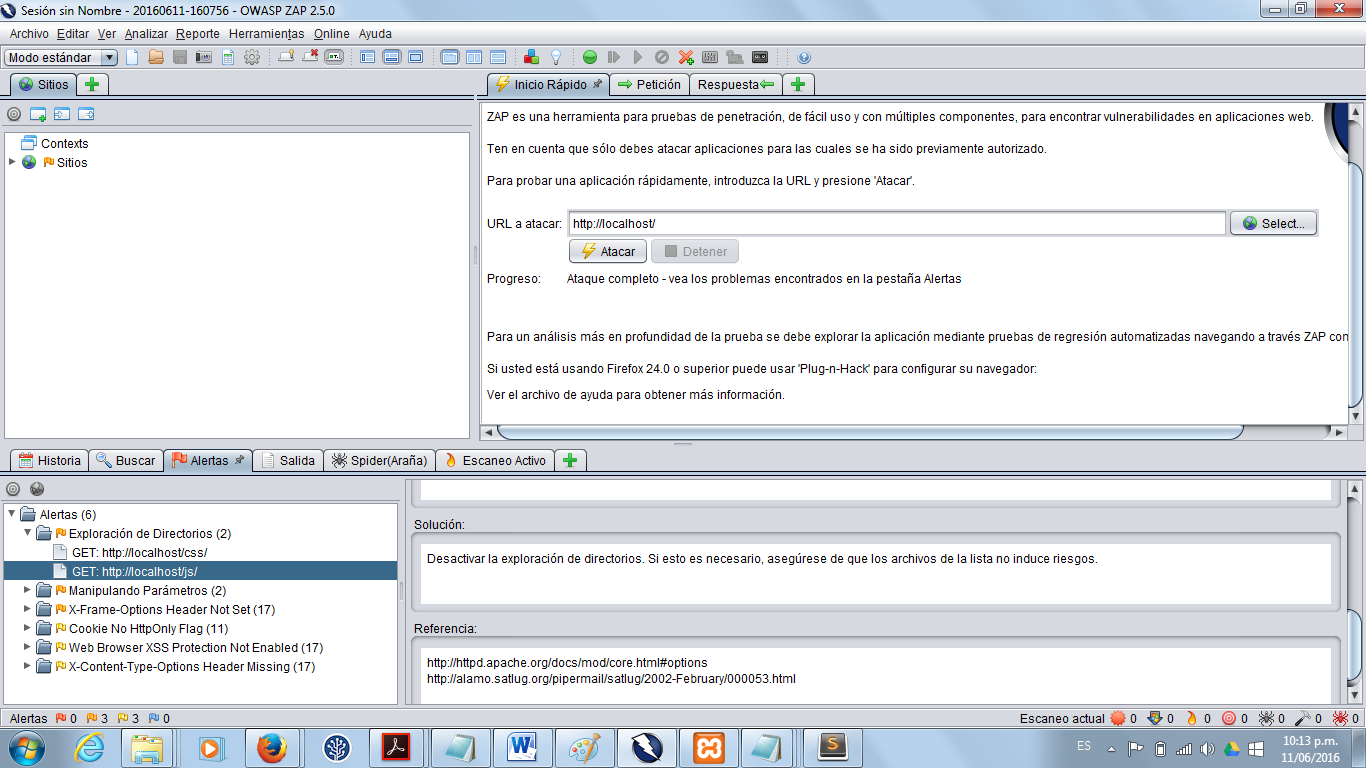
**OWASP Zed Attack Proxy**

https://www.owasp.org/index.php/OWASP\_Zed\_Attack\_Proxy\_Project

“*The OWASP Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing. ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.*”

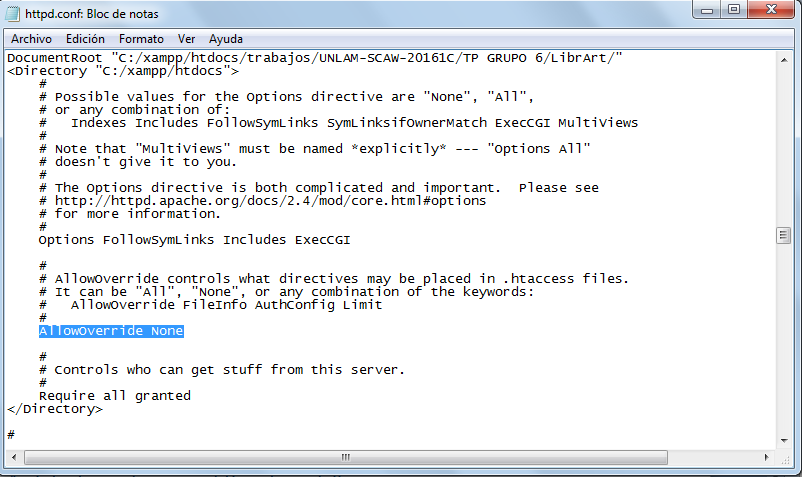
Esta herramienta es un complemento para la seguridad de nuestro sitio, no contempla todas las vulnerabilidades o ataques cubiertos para el Level 2.

**Escaneamos:**



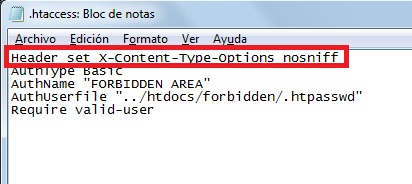
1. **Exploración de directories (2 errores)**

**Solución**: Desactivar la exploración de directorios. Para esto modificamos dentro del archivo “httpd.conf” en el tag <Directory></Directory> la opción “AllowOverride” con “All” por “None”

****

1. **X-Content-Type-Options Header Missing (17 errores)**

**Solución**: Activar el Content-Type header. Primero agregamos la línea al archivo “.htacces” del Apache

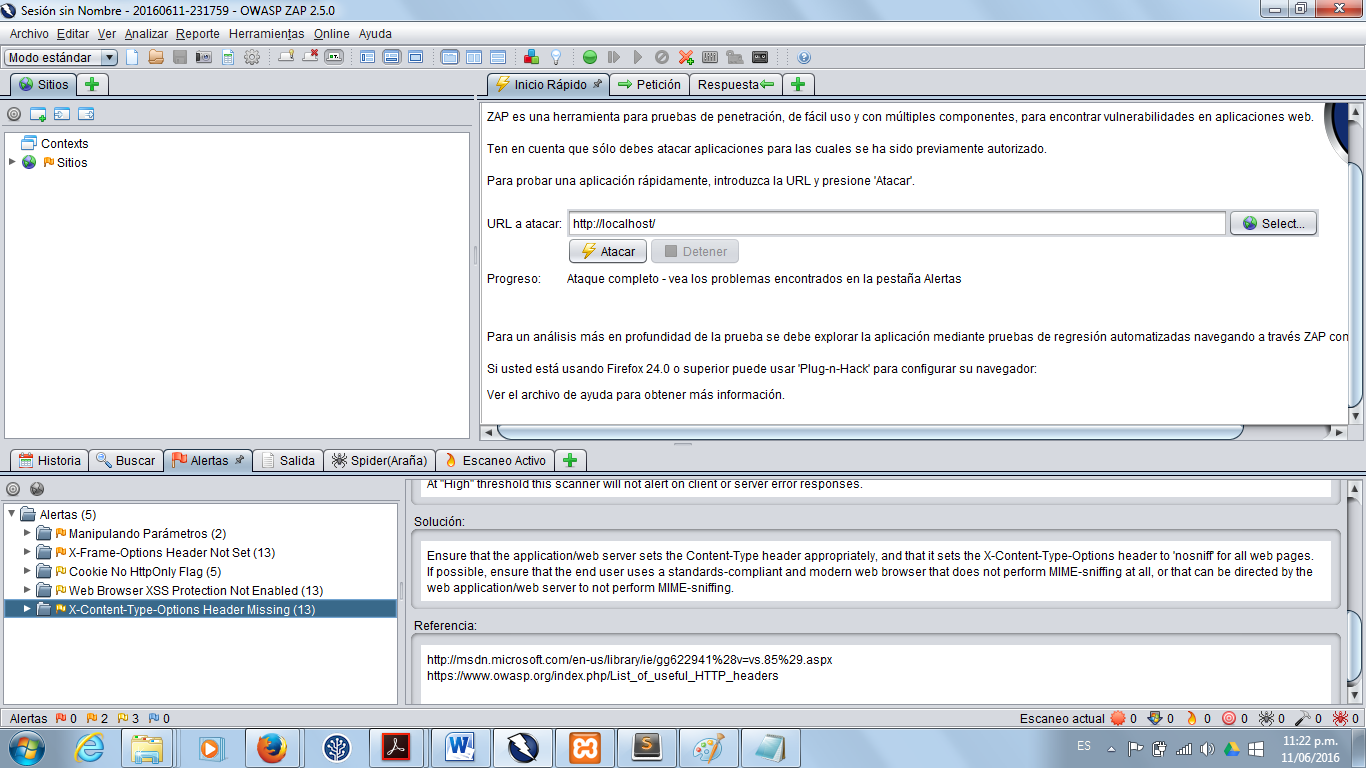


Actualiza:

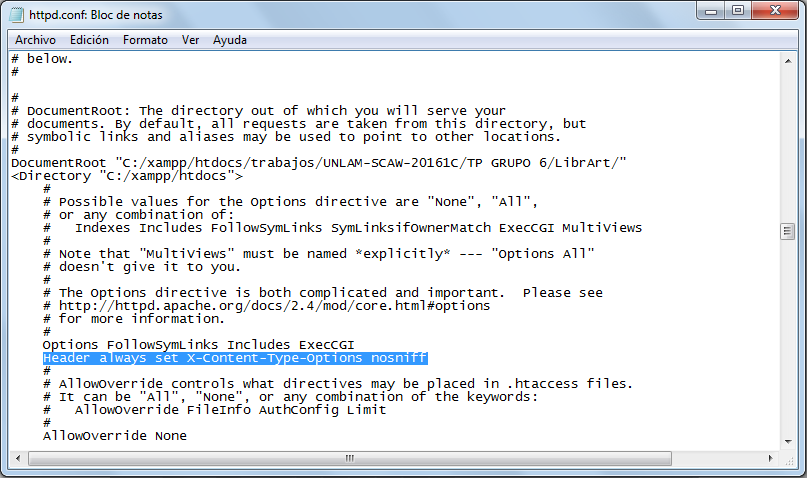
**X-Content-Type-Options Header Missing** (13 errores)

**X-Frame-Options Header Not Set** (13 errores)

**Web Browser X-XSS-Protection Not Enable** (13 errores)

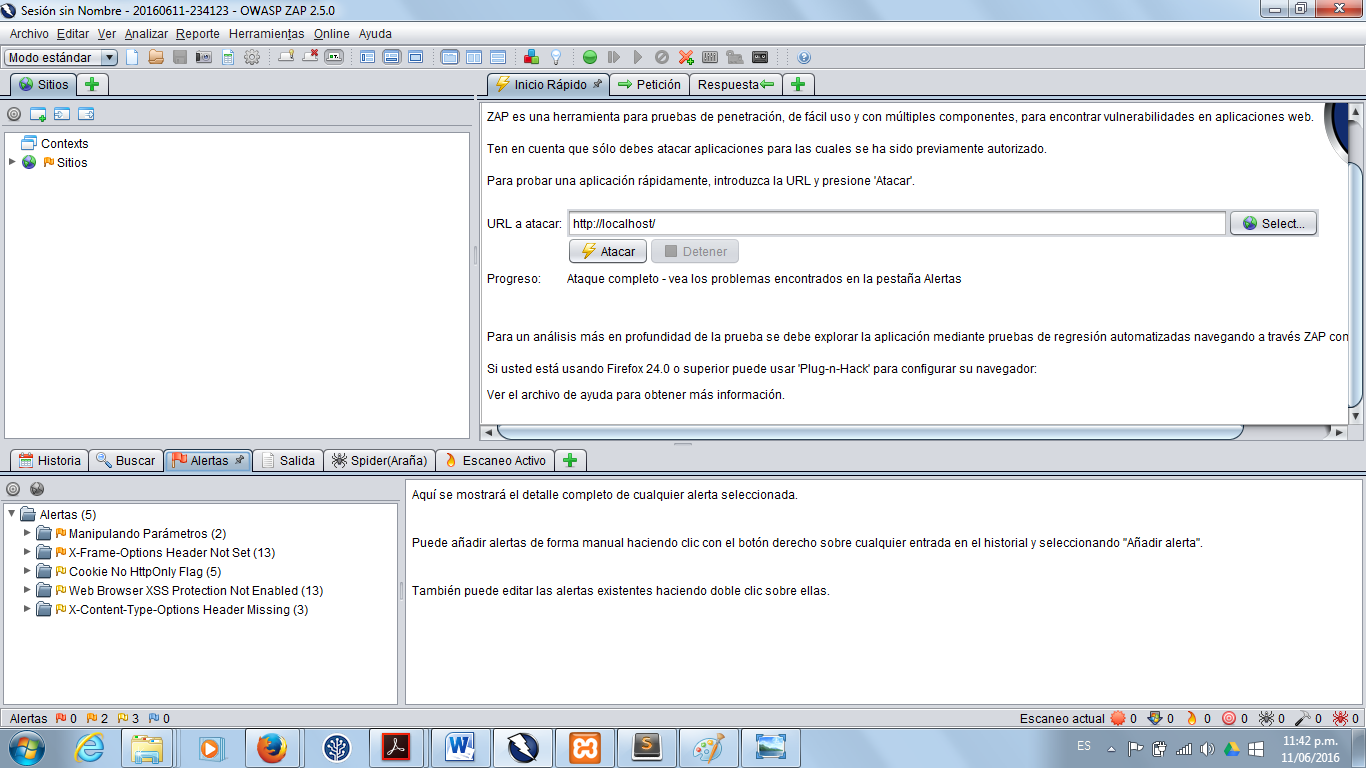


Agregamos la linea tambien al archivo “httpd.conf” del Apache dentro del tag <Directory></Directory>



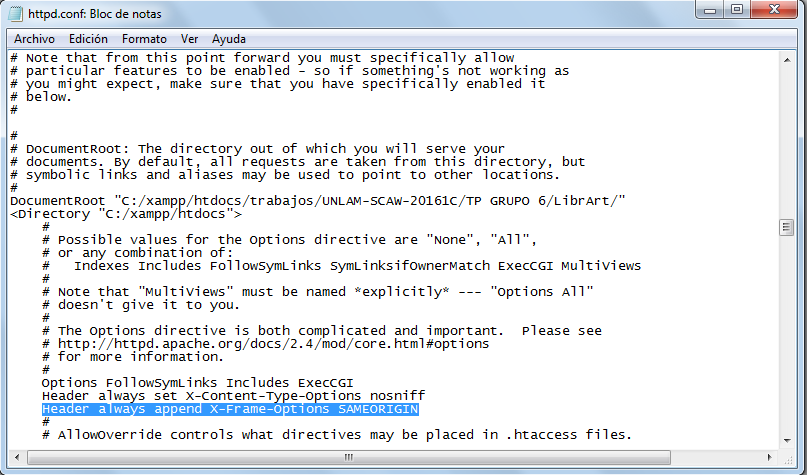
Actualiza:

**X-Content-Type-Options Header Missing** (3 errores)



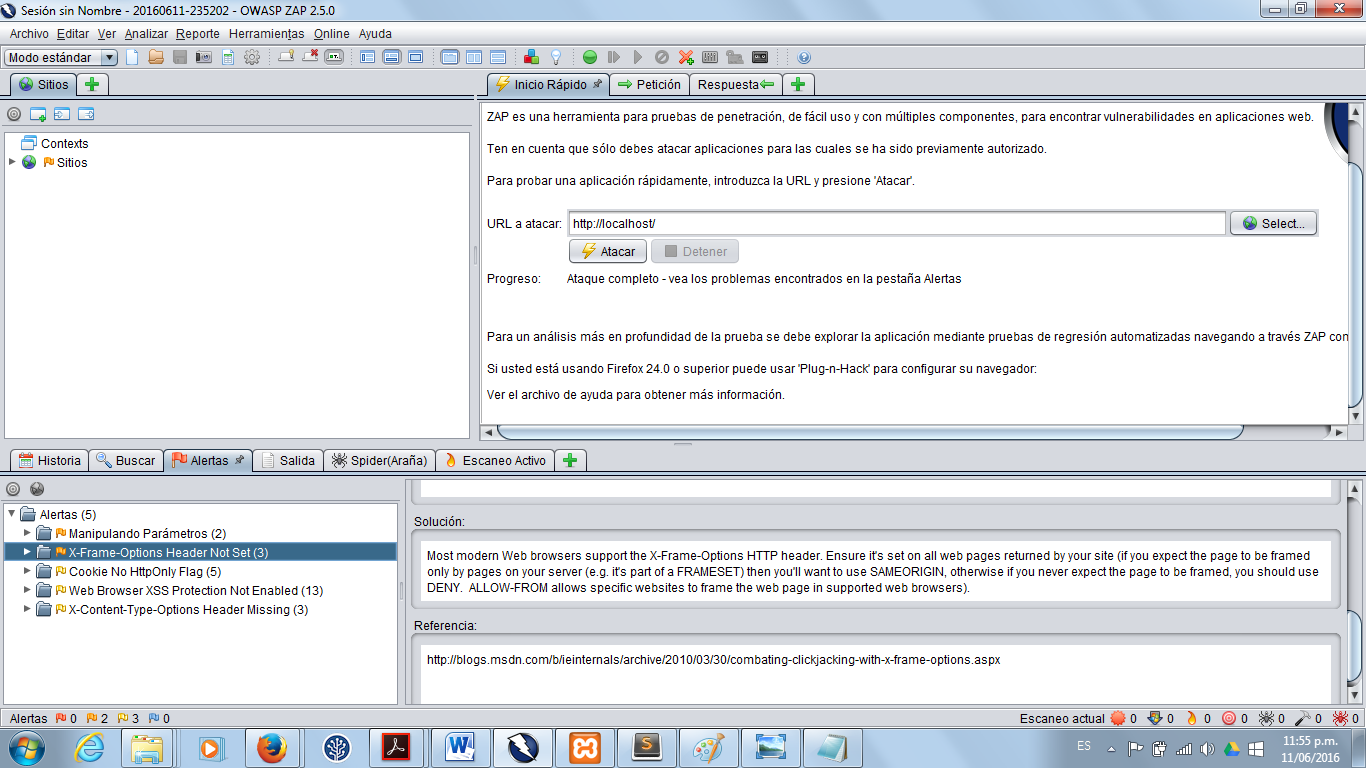
1. **X-Frame-Options Header Not Set (13 errores)**

**Solución**: Activar X-Frame-Options HTTP header. Agregamos la linea al archivo “httpd.conf” del Apache dentro del tag <Directory></Directory>



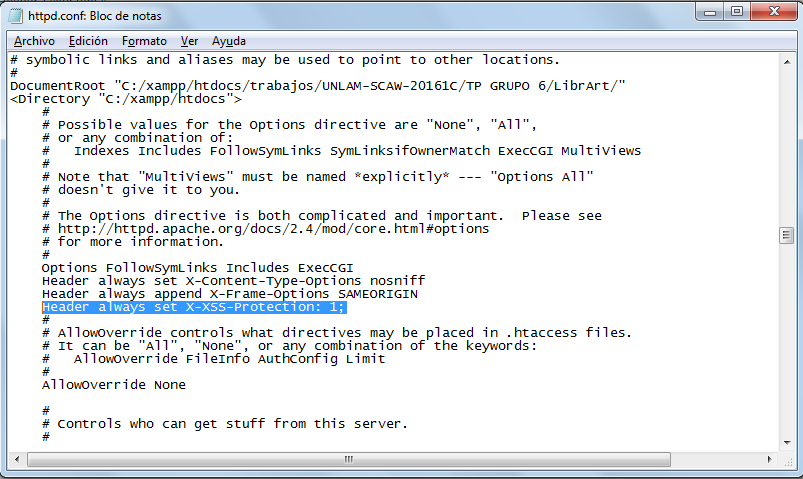
Actualiza:

**X-Frame-Options Header Not Set** (3 errores)



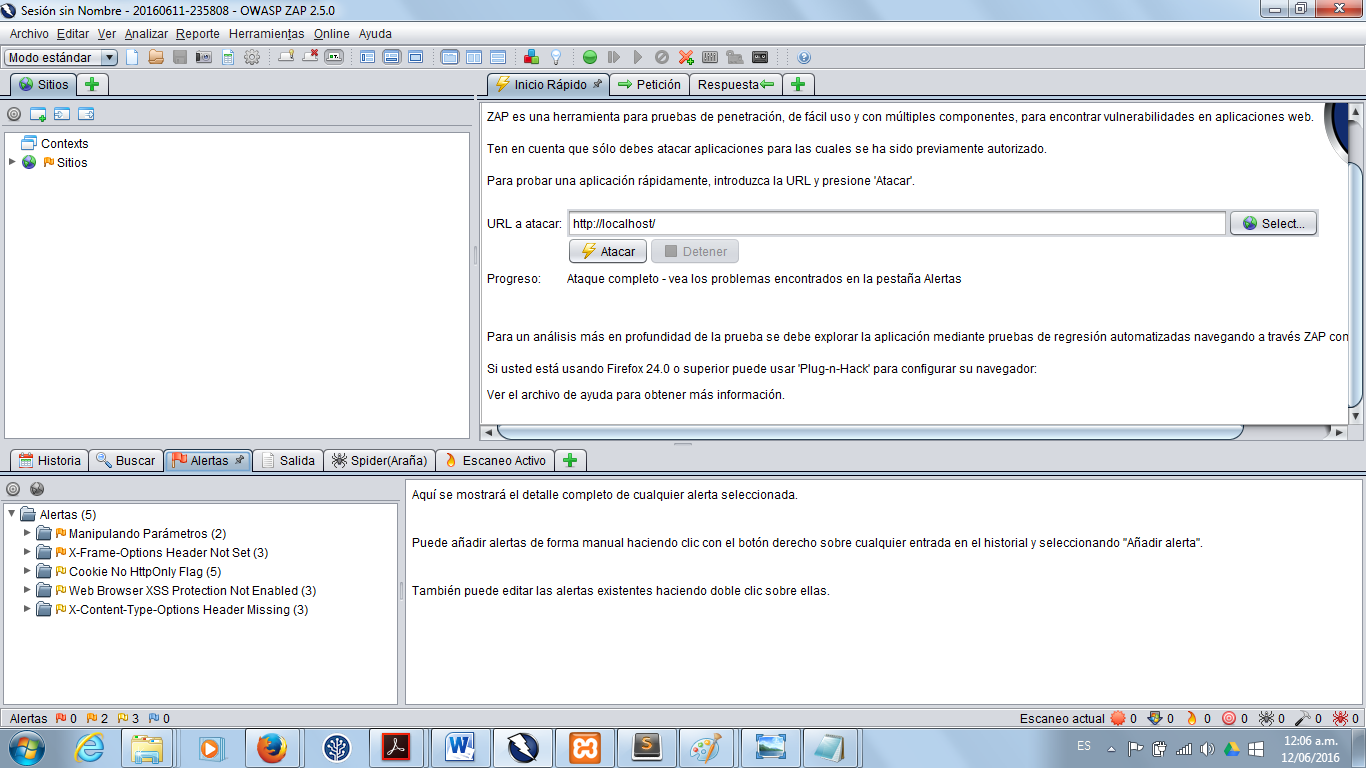
1. **Web browser XSS Protection Not Enable**

**Solución**: Activar el XSS Protection. Agregamos la linea al archivo “httpd.conf” del Apache dentro del tag <Directory></Directory>



Actualiza:

**Web browser XSS Protection Not Enable** (3 errores)



**ASVS-3.0 para nivel 2**

**Authentication Verification Requirements**

* Verify password entry fields allow, or encourage, the use of passphrases, and do not prevent long passphrases/highly complex passwords being entered.

Lo que hace es tomar de cada palabra el primer carácter y formarlo como clave.Ejemplo “Materia de seguridad en informatica” convierte a “Mdsei”.

Se puede sustituir las letras con caracteres especiales (adicional).

**Cuando creas o cambias tu Contraseña, podrías:**

* Agregar espacios entre las letras y palabras. Por ejemplo, en lugar de “PaybookEsMaravilloso”, puede ser “Paybook es Maravilloso” o en lugar de “Contraseña”, puede ser “Con tra se ña”.
* Combina letras, números y caracteres especiales (no valida actualmente)
* Usa mayúsculas y minúsculas (no valida actualmente)
* Procura al menos 10 caracteres, entre más caracteres sean mejor (no valida actualmente)

**Tu frase privada NO puede ser:**

* Tu nombre de Usuario, Documento o Clave (valida)



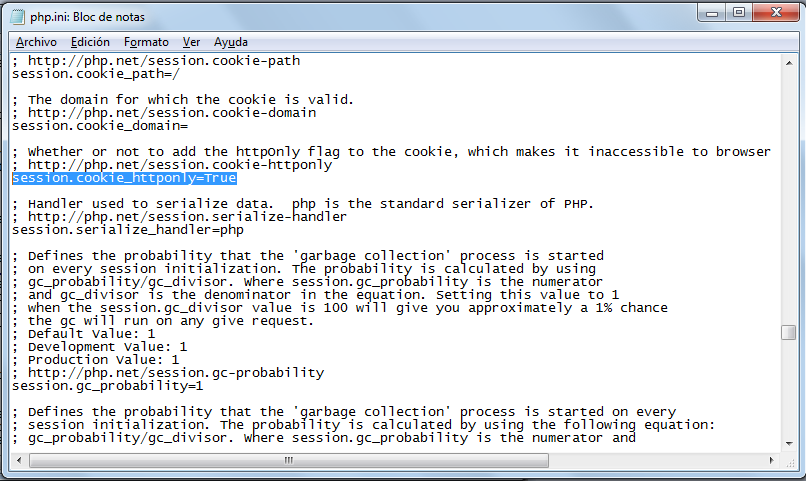
**Session Management Verification Requirements**

* Authentication session tokens additionally set the “HttpOnly” and “secure” attributes

**Using PHP to set HttpOnly**

For session cookies managed by PHP, the flag is set either permanently in php.ini. PHP manual on HttpOnly through the parameter:

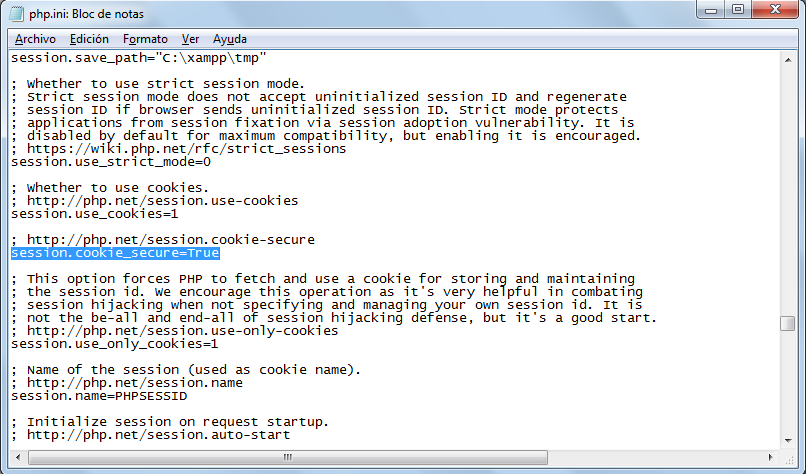
session.cookie\_httponly = True



**Using PHP to set SecureFlag**

For session cookies managed by PHP, the flag is set either permanently in php.ini PHP manual on SecureFlag through the parameter:

session.cookie\_secure = True



**HTTP security configuration verification requirements**

* Verify that the X-XSS-Protection: 1; mode=block header is in place.

Corregido anteriormente detectado por la herramienta ZAP.

