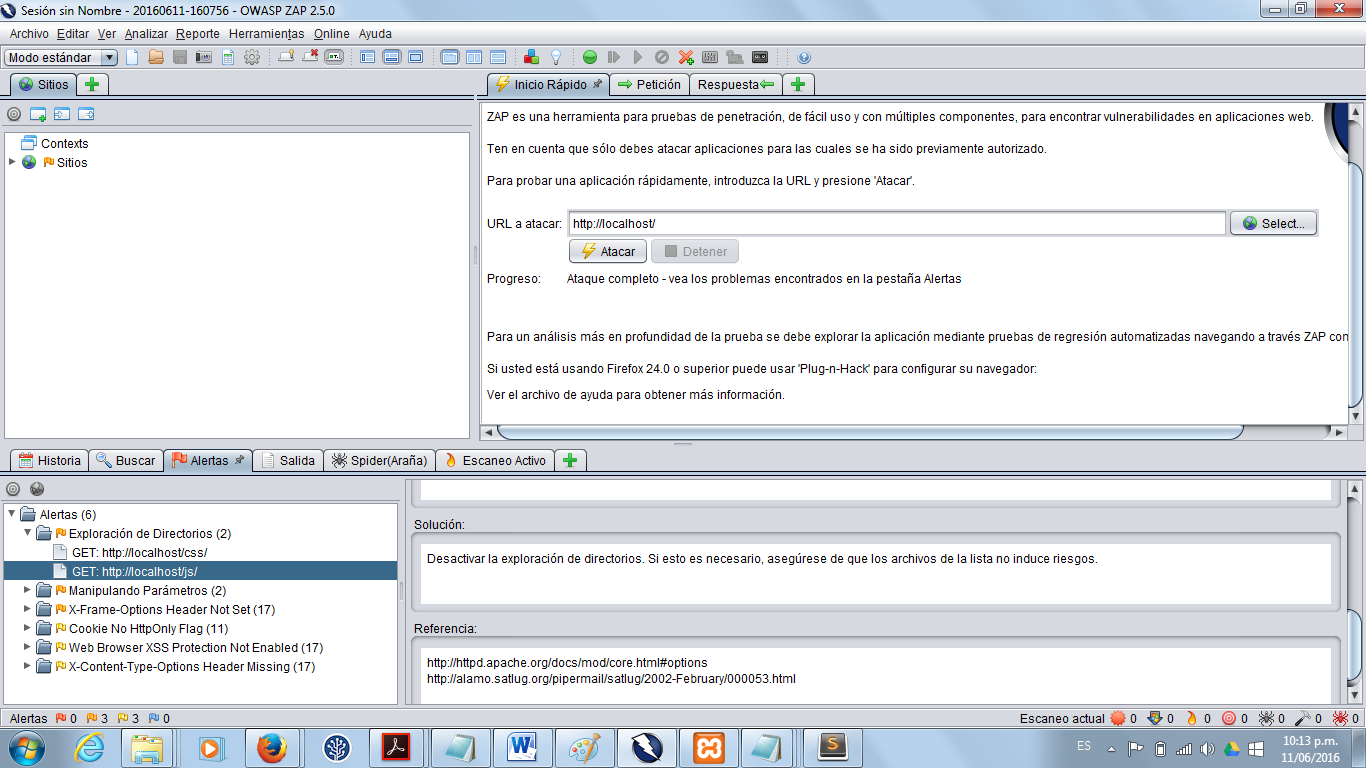
**Herramienta utilizada:**

**OWASP Zed Attack Proxy**

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

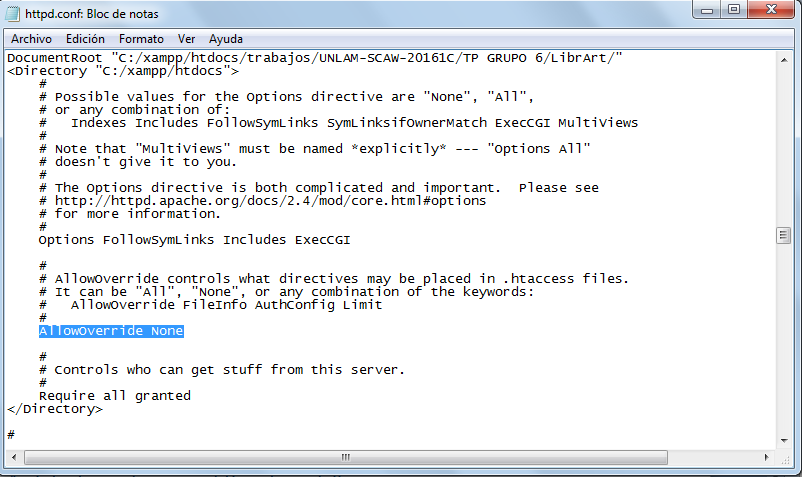
“*The OWASP Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration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

**Escaneamos:**



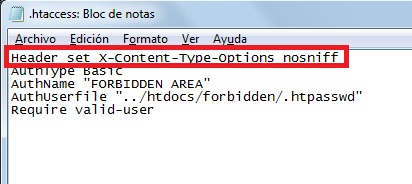
1. **Exploración de directories (2 errores)**

**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

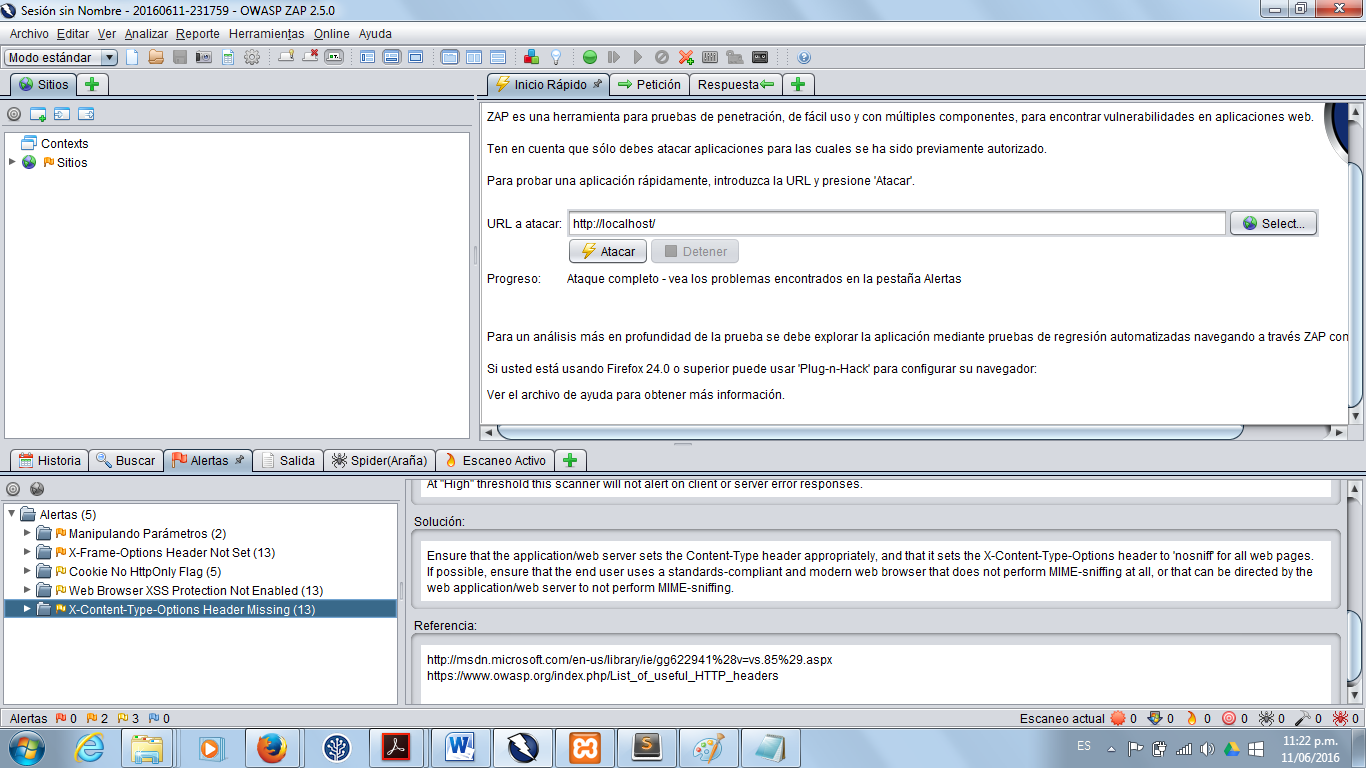


Actualiza:

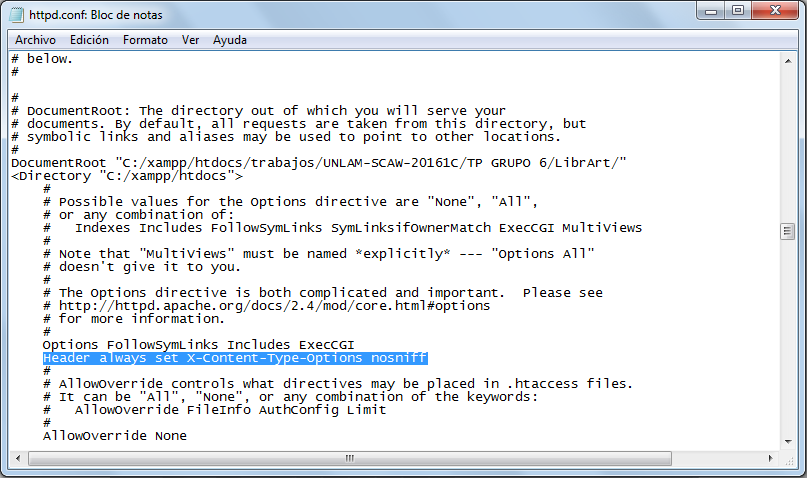
**X-Content-Type-Options Header Missing** (13 errores)

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

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

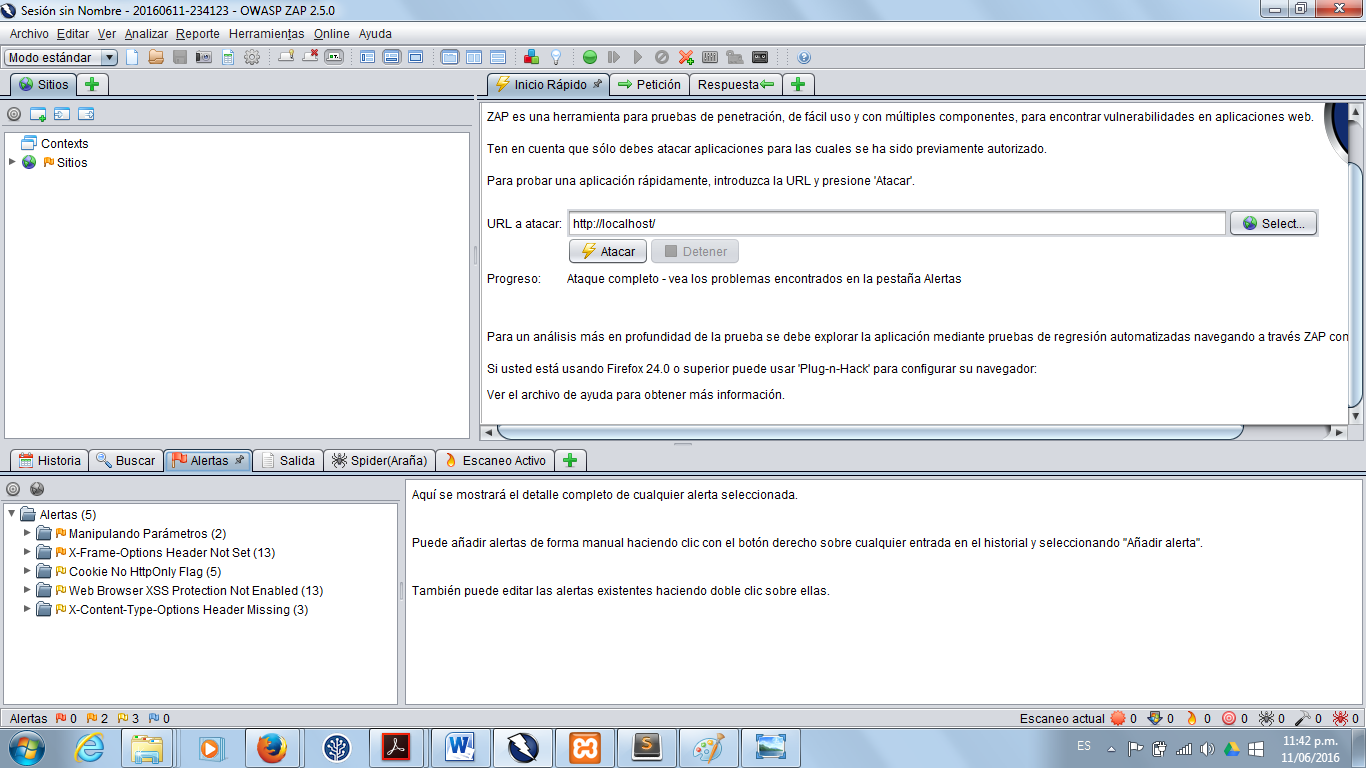


Agregamos la linea tambien al archivo “httpd.conf” del Apache dentro del tag <Directory></Directory>



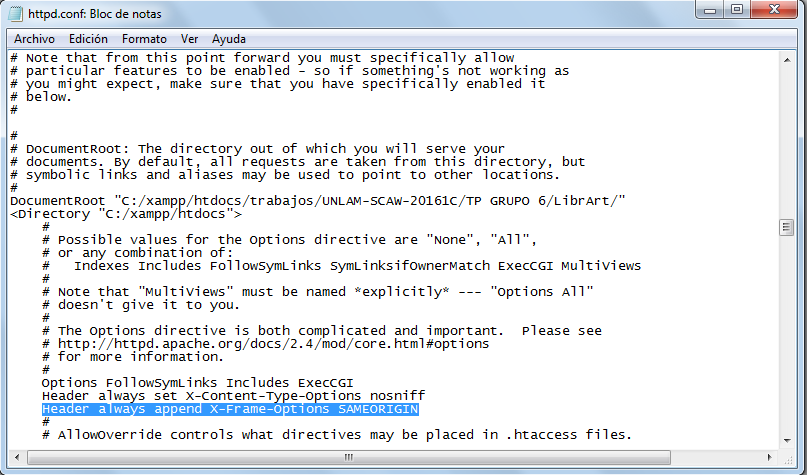
Actualiza:

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



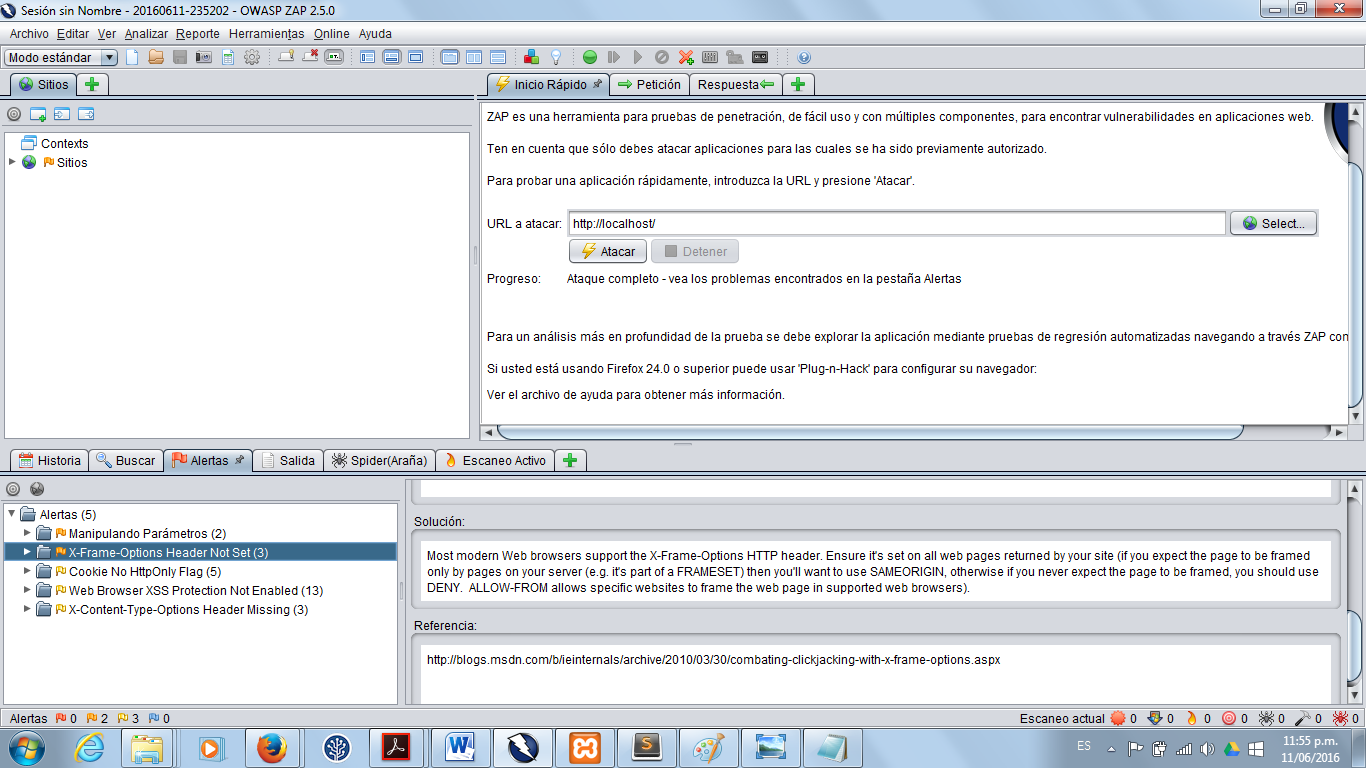
1. **X-Frame-Options Header Not Set (13 errores)**

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



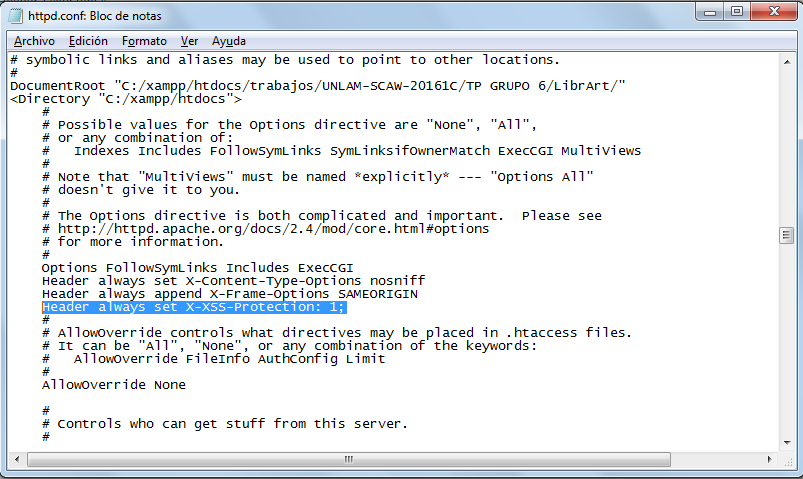
Actualiza:

**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)

