**Using NSlook up on the URL to get the IP address(target IP) of the webserver**

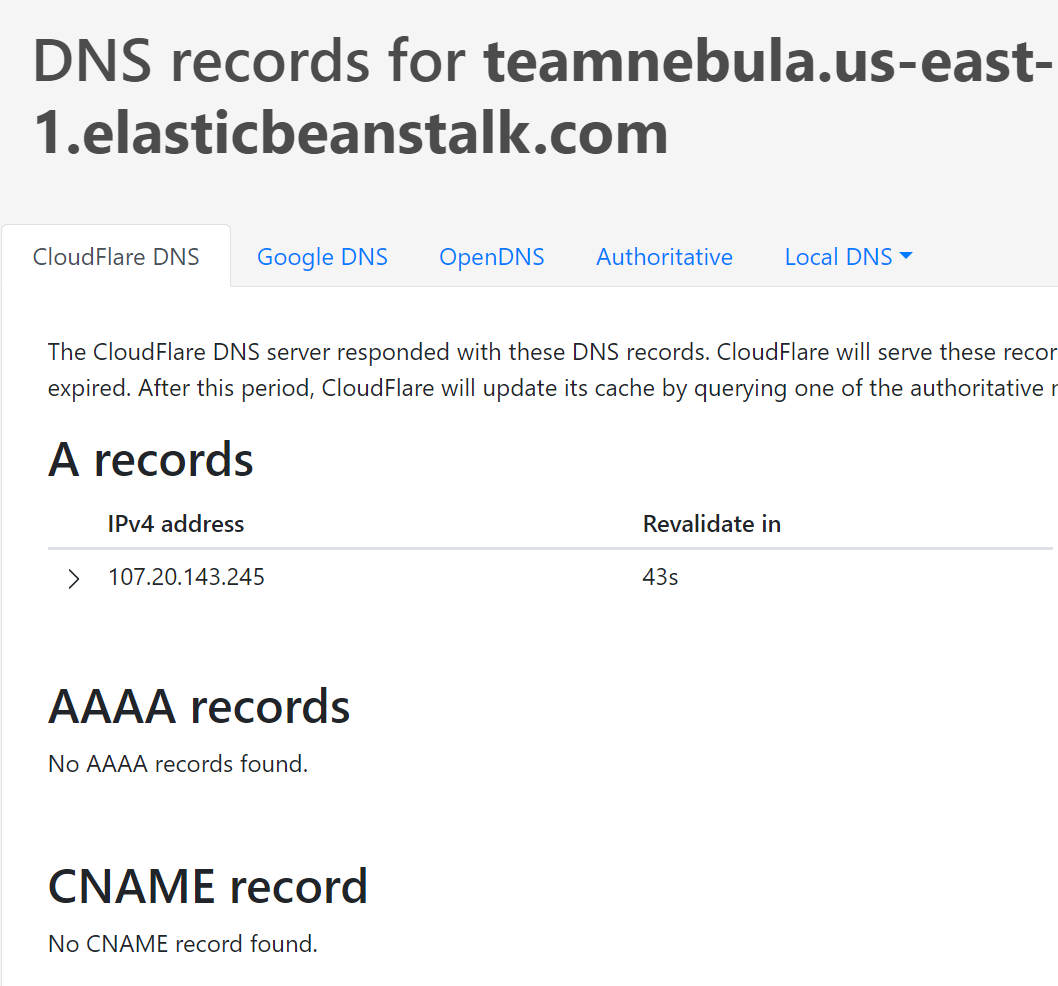


Figure 1: NS lookup

Using Zenmap a tool on Kali Linux which a graphical version of the nmap

**Using Zenmap with target IP discovered in the NS Look up**

nmap -T4 -A -v 107.20.143.245

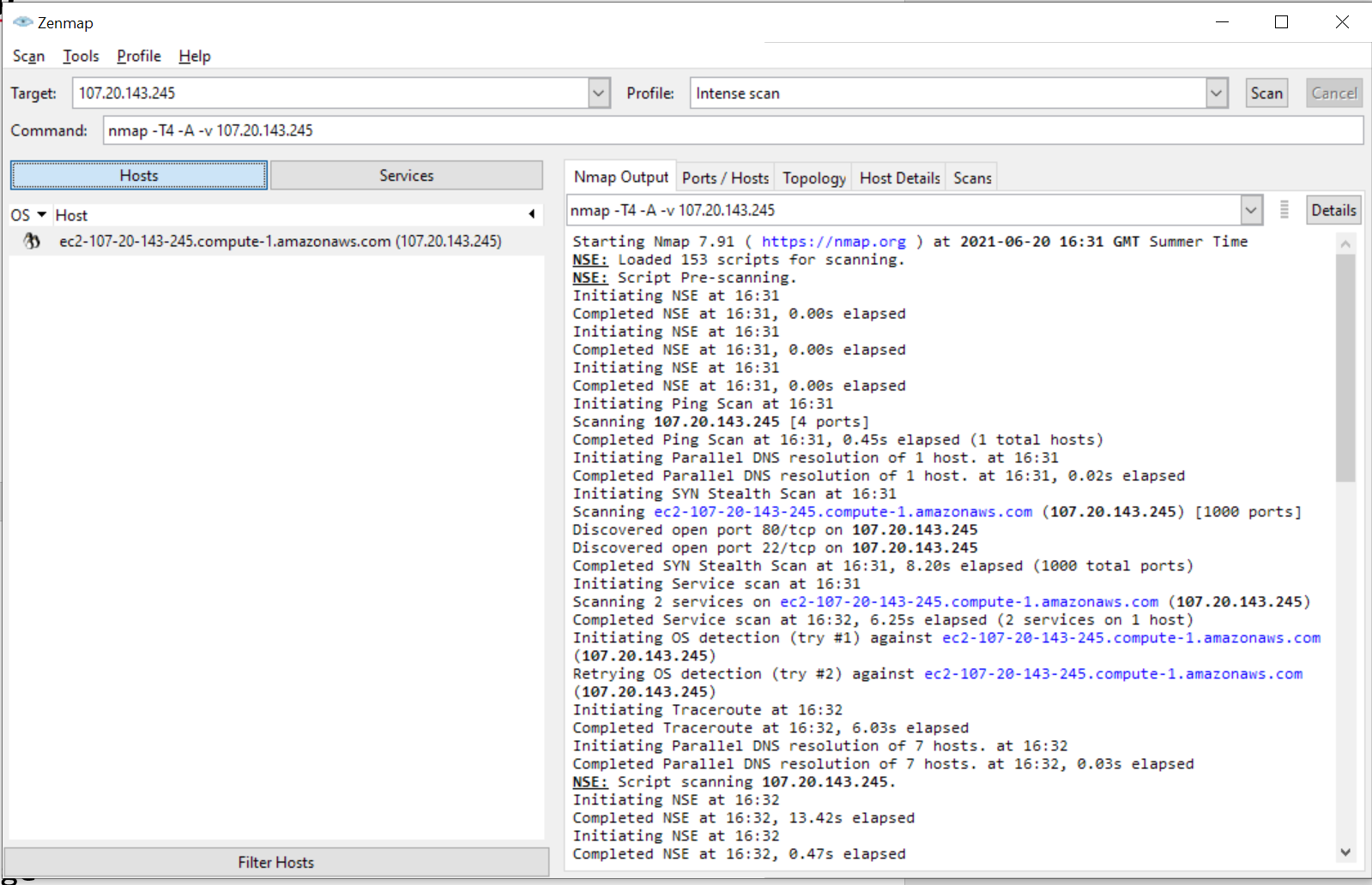


Fig 2: Zenmap interface

**what Operating system?**

the operating systems its using is Linux 5.0-5.4 version range

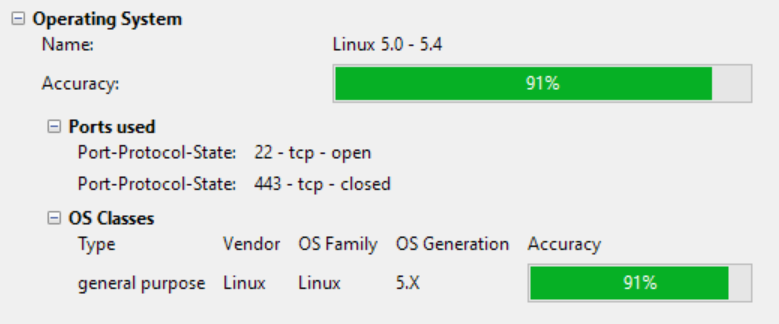


Fig 2: Operating system detection

**What web server software is it running?**

Apache httpd

**Is it running a CMS (wordpress, Drupal etc)?**

It runs Amazon web services

**Where is it hosted?**

ec2-107-20-143-245.compute-1.amazonaws.com

**Does it have any open ports?**

Port 22 and 80 which belong to SSH and HTTP respectively as shown below

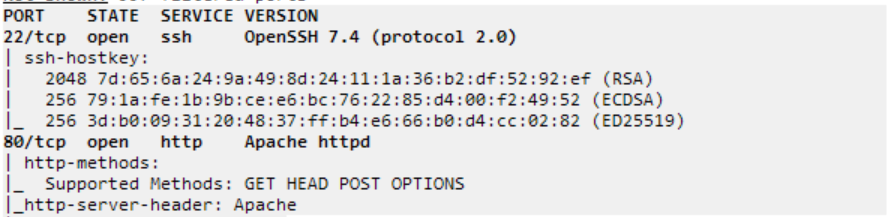


Fig 3: open ports

**Does the site have any known vulnerabilities?**

The vulnerability is highlighted in the figures below using ZAP .

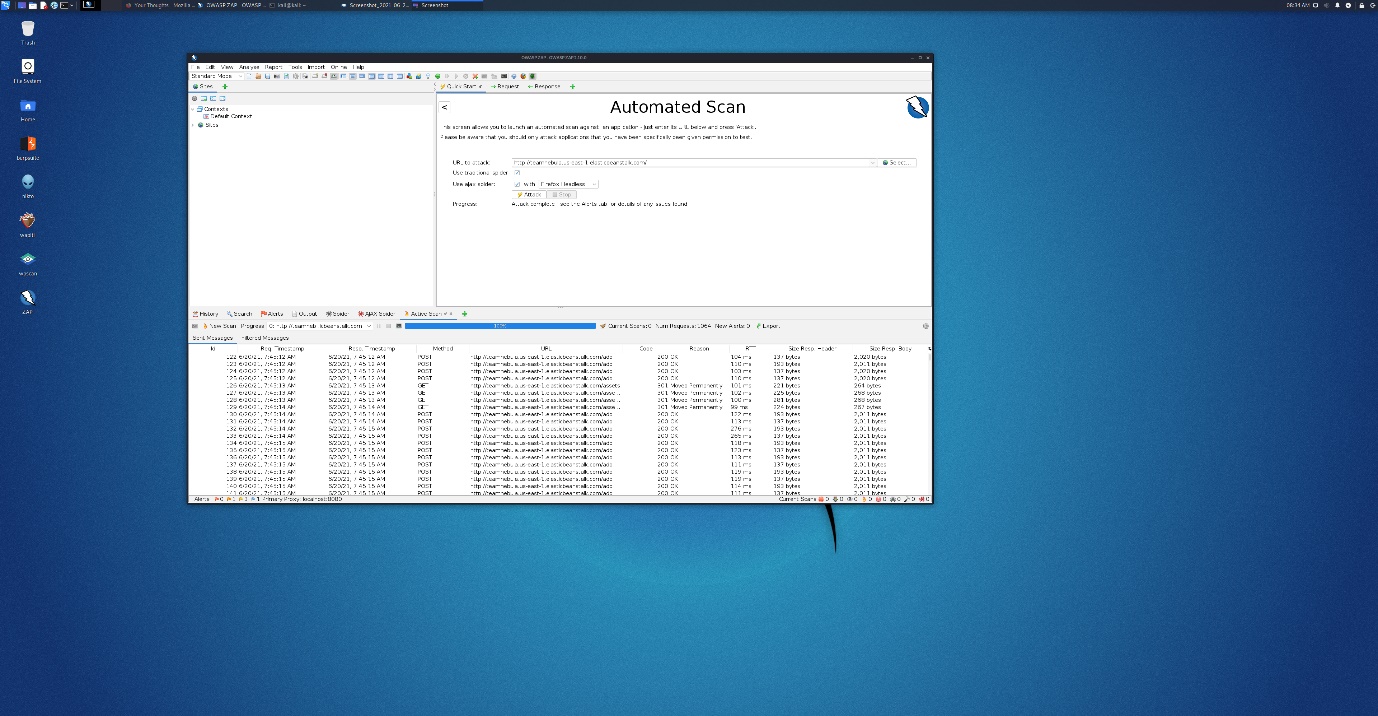


Figure 4a: Zap with target URL

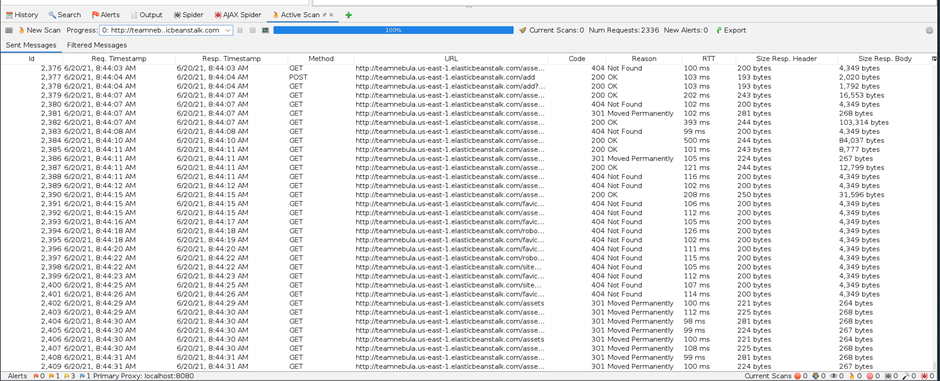


Fig 4b: Zap with active scan

The figure 5 below shows one of the vulnerabilities discovered called X-frame Options Header which also shows a risk level of Medium.



Figure 5: X Frame Options Header not set

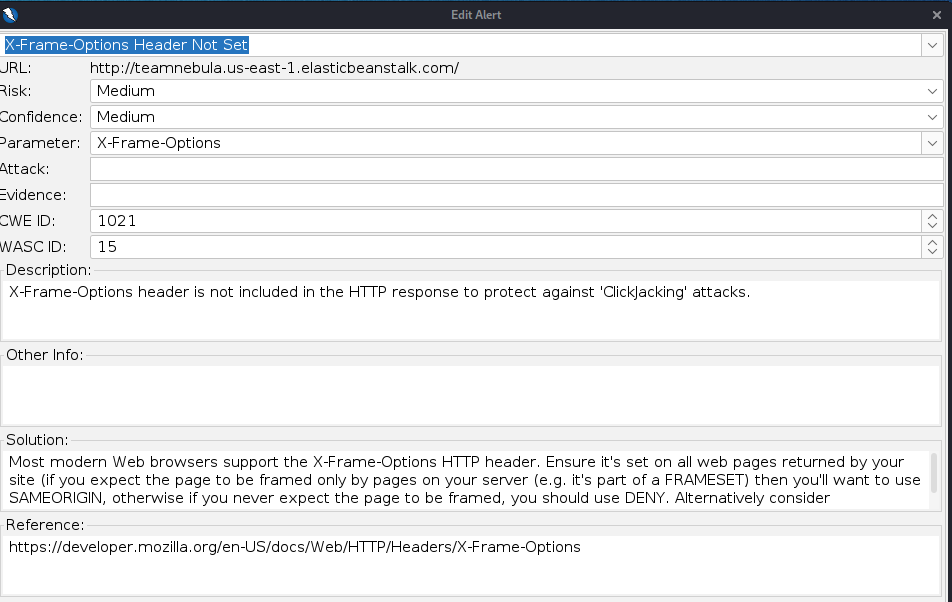


Figure 6: X frame Options Header Not Set

Figure 7 below also show Absence of the Anti-CSRF Tokens which shows a low risk level.

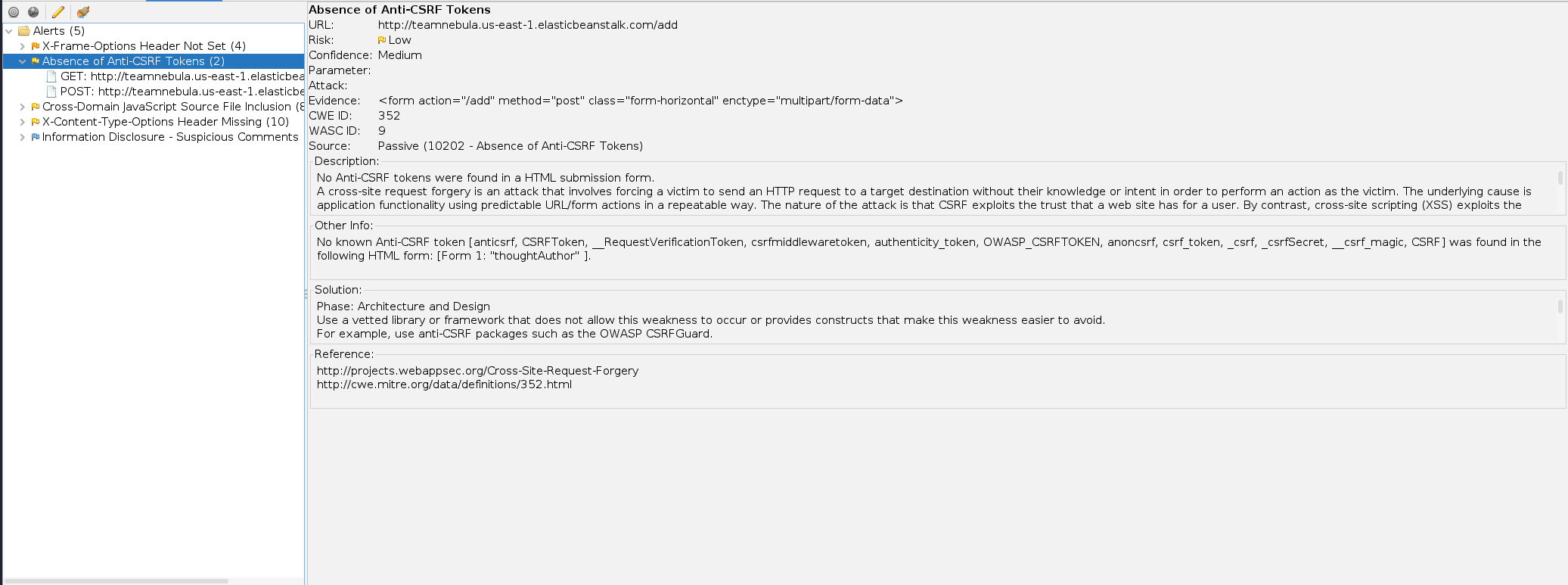


Figure 7: Absence of Anti-CSRF Tokens

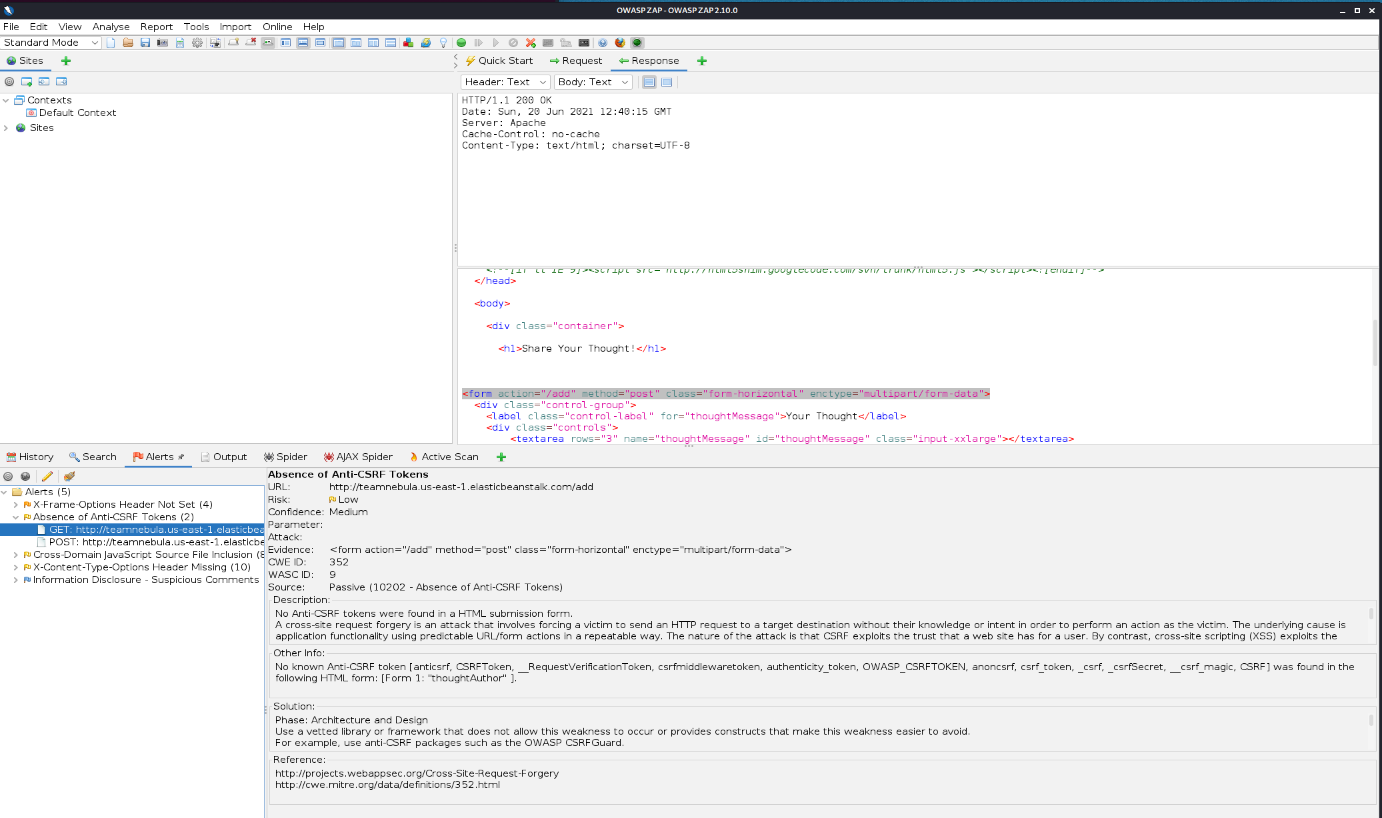


Figure 8a: Anti-CSRF Get flaws

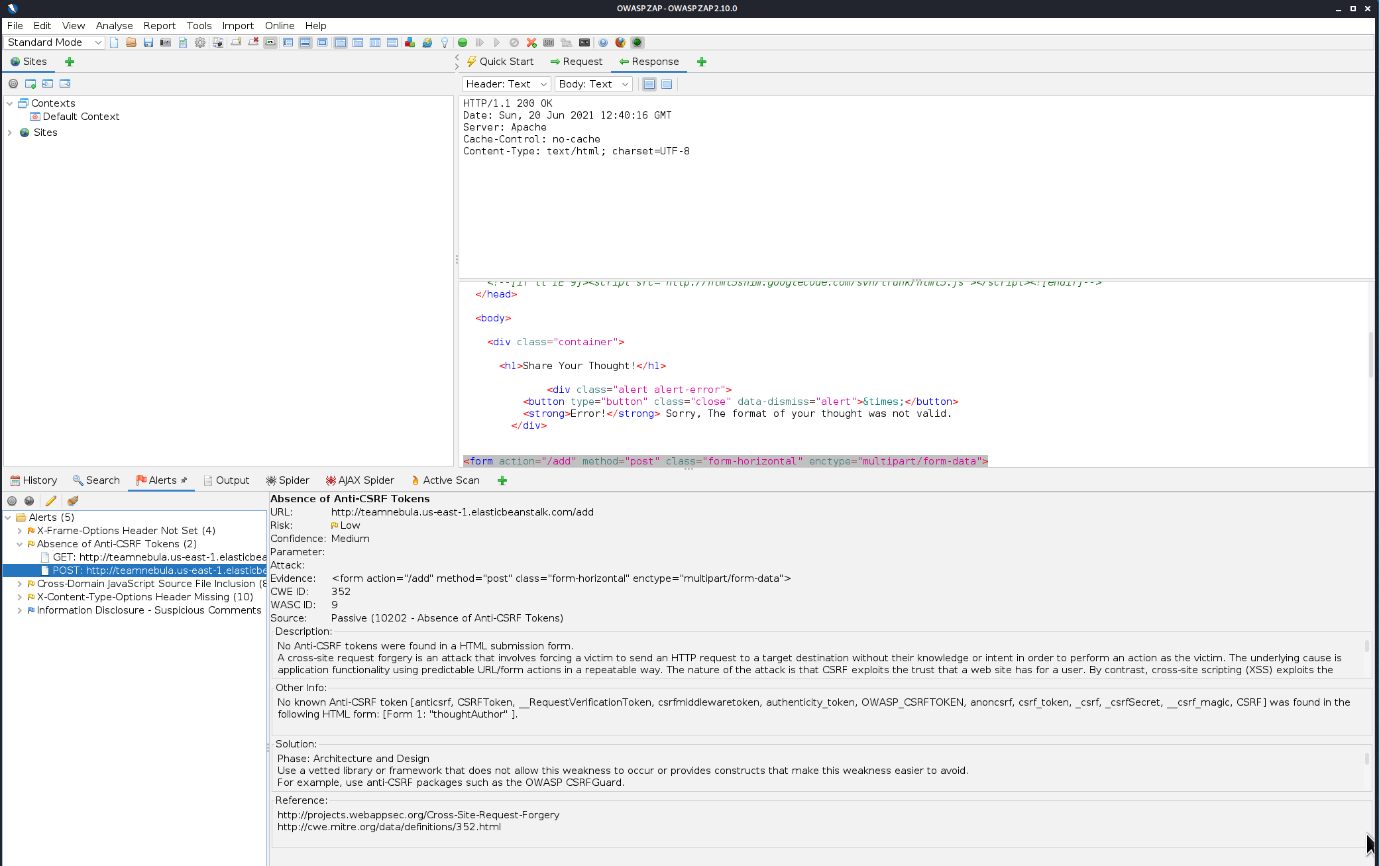


Fig 8b: Anti CSRF POST

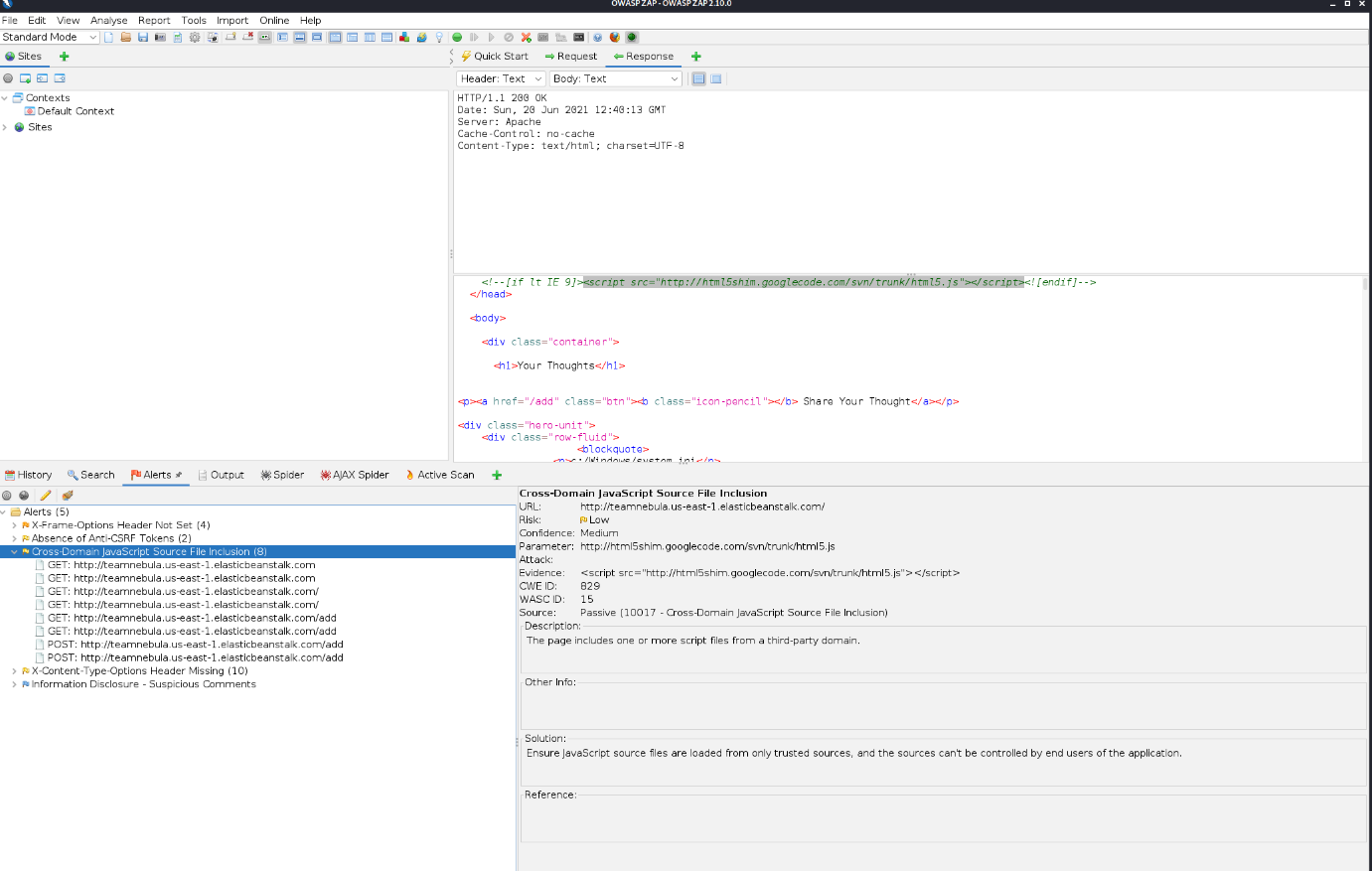


Fig 9: Cross Domain Javascript Source File Inclusions

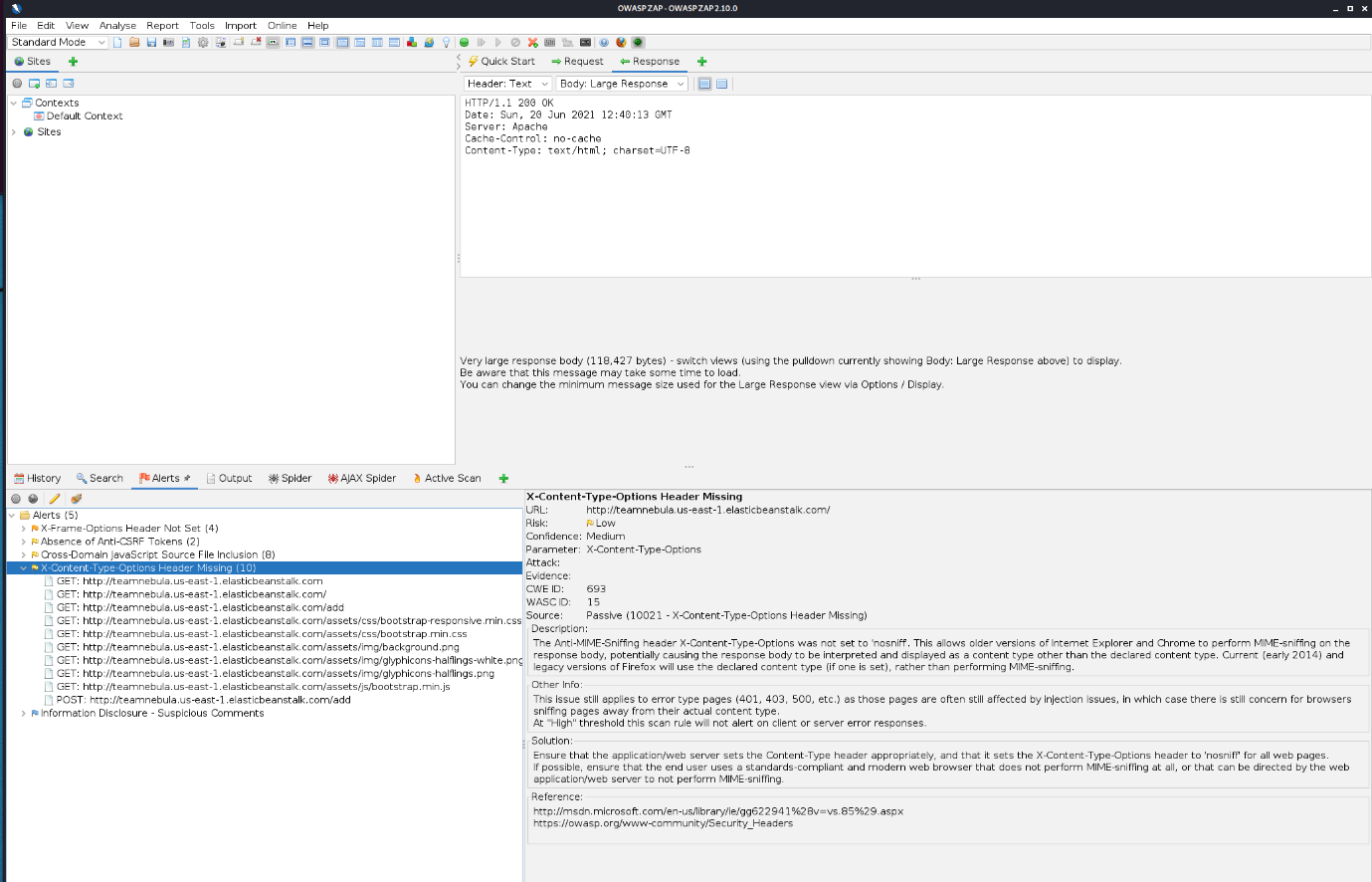


Figure 10: X-Content-Type-Options Header Missing

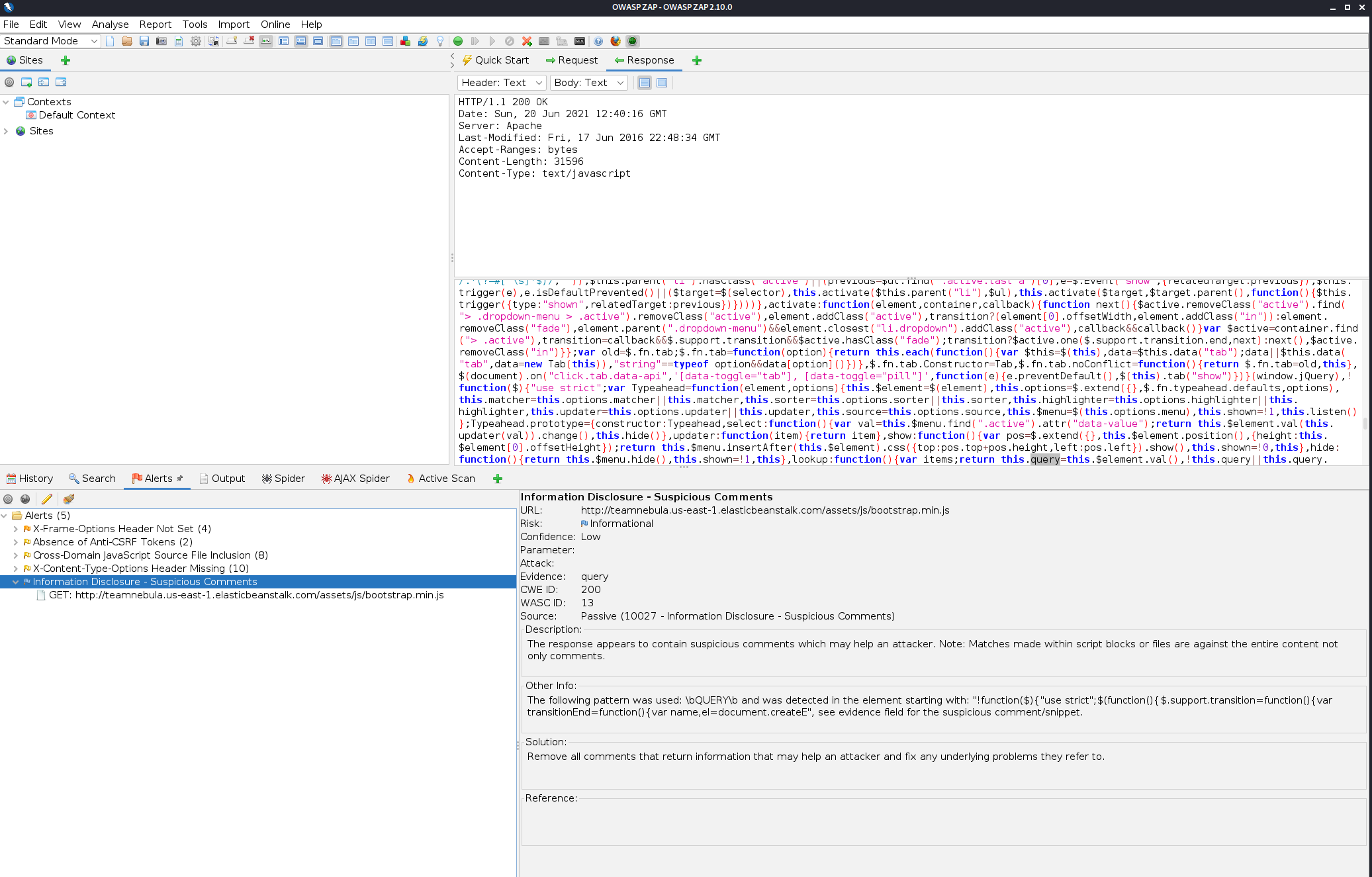


Figure 11: Information Disclosure Suspicious comments