Information Security - UE20CS346

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : 'H'

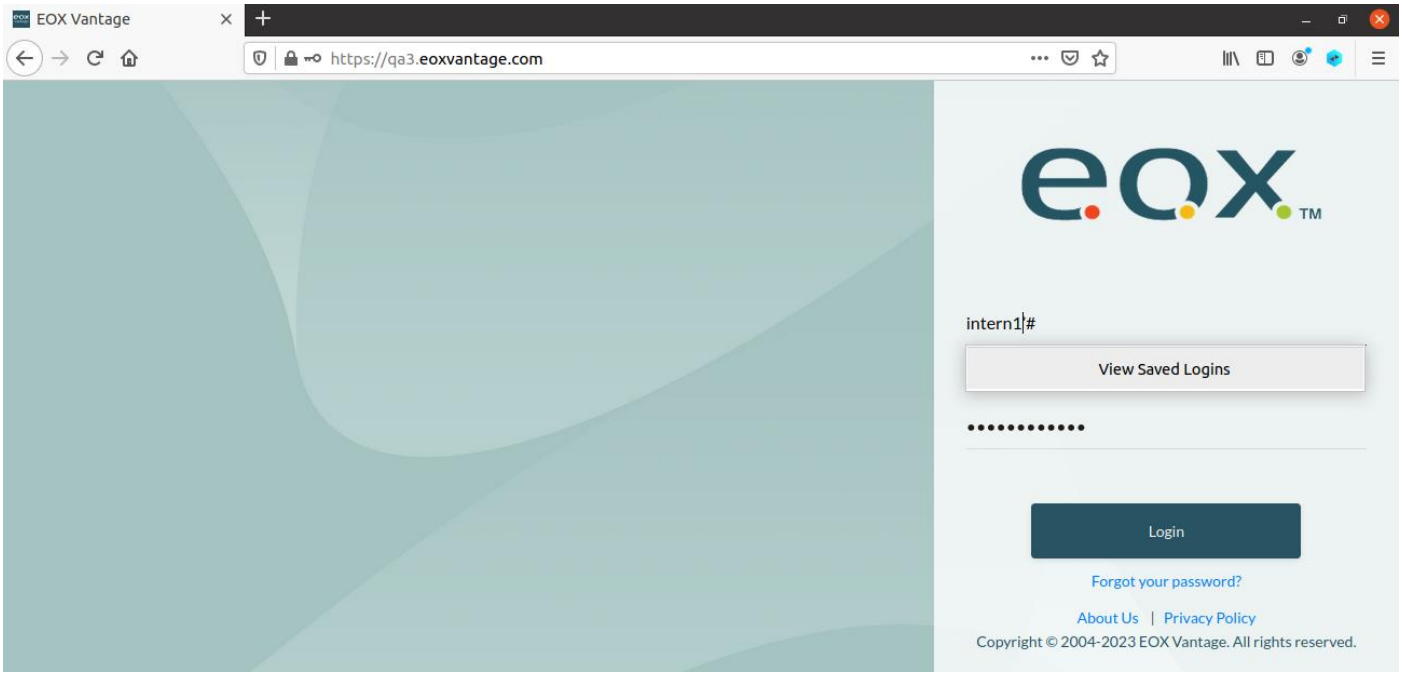
Penetration Testing Lab

Website : eoxvantage

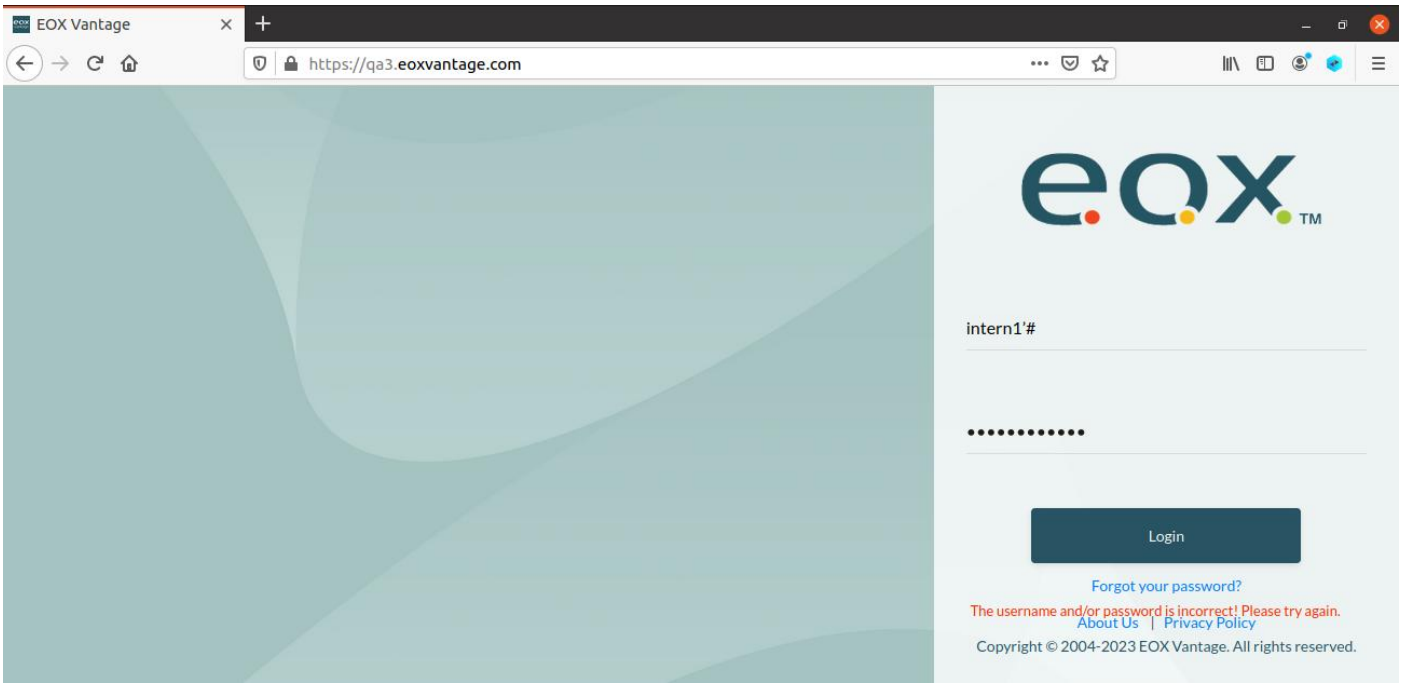
URL : https://qa3.eoxvantage.com/

Attack SQL Injection :

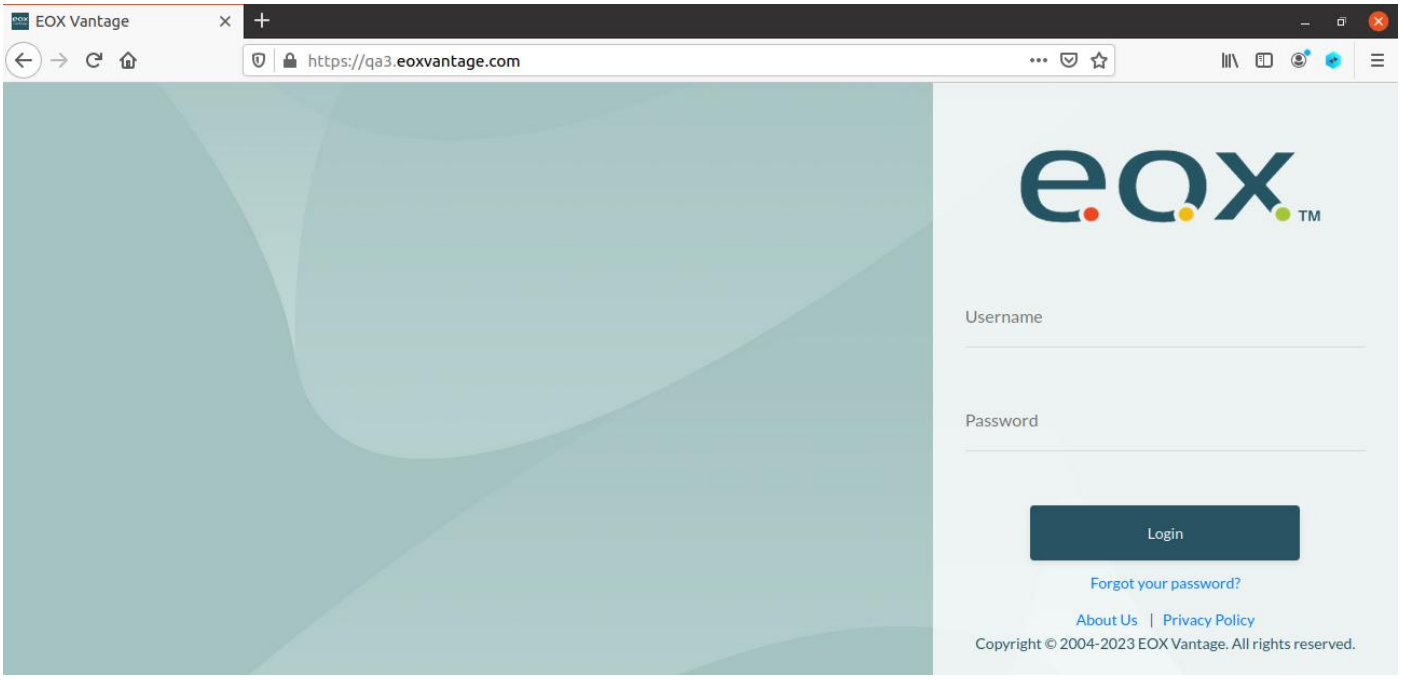
- Trying to execute a simple SQL injection attack "Inter1' #"
- The SQL injection attack "intern1'#" in the username field is a classic example of an attempt to exploit a vulnerability in a web application that allows user input to be included in SQL queries without proper sanitization or validation.
- In this attack, the attacker is attempting to inject a single quote character ('), which is a special character in SQL, into the username field of a login form. This is done to try and break out of the SQL query and execute their own code or query.
- The # character is used to comment out the rest of the SQL query, so that any subsequent characters are ignored. This is often used as a technique to bypass additional query parameters or filters.
- If the web application is vulnerable to SQL injection, the attacker may be able to successfully authenticate as the "intern1" user, or even gain access to the underlying database and potentially extract sensitive information or modify data.



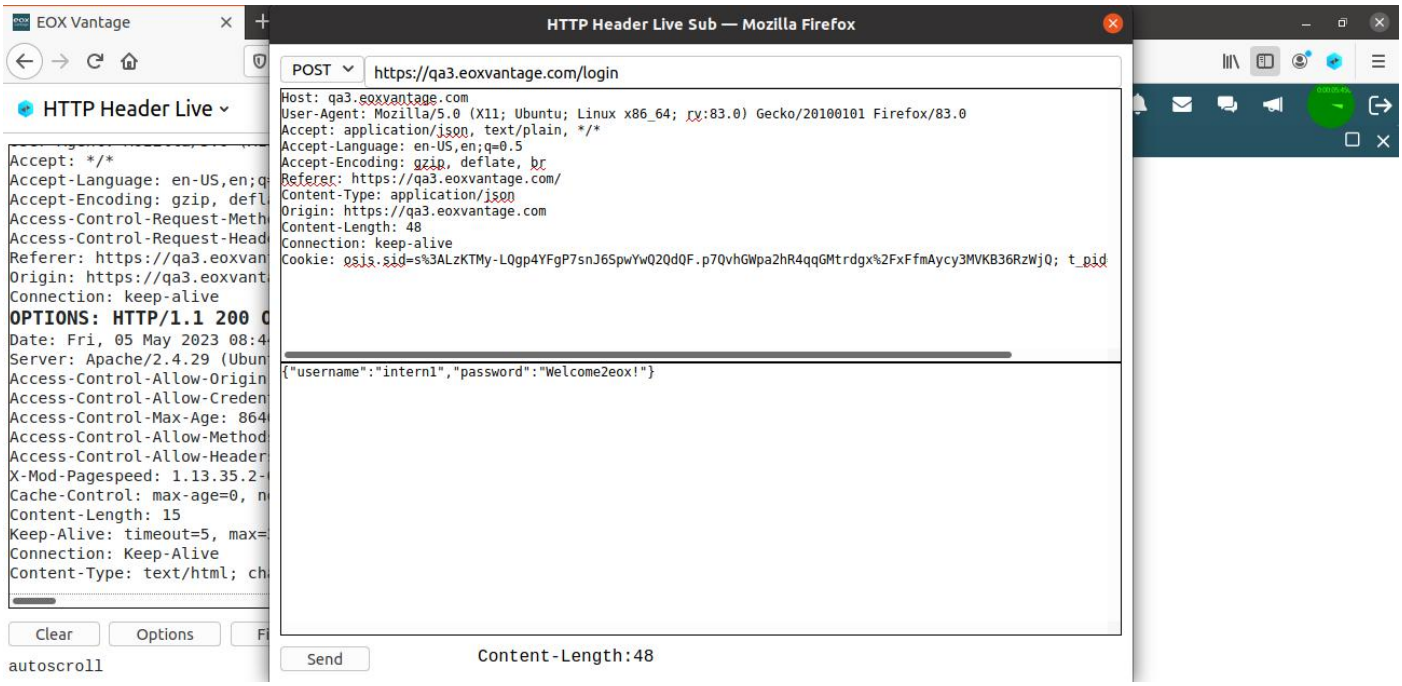
- I Guess this website is prune to SQL Injection as the attack failed to execute the query.



- Trying to Login While HTTP Header Live is On



- When Logging in while the HTTP header Live is On we are clearly able see the user name and password in the https POST request header. This might effect user credentials if someone is sniffing the packets on the same network.

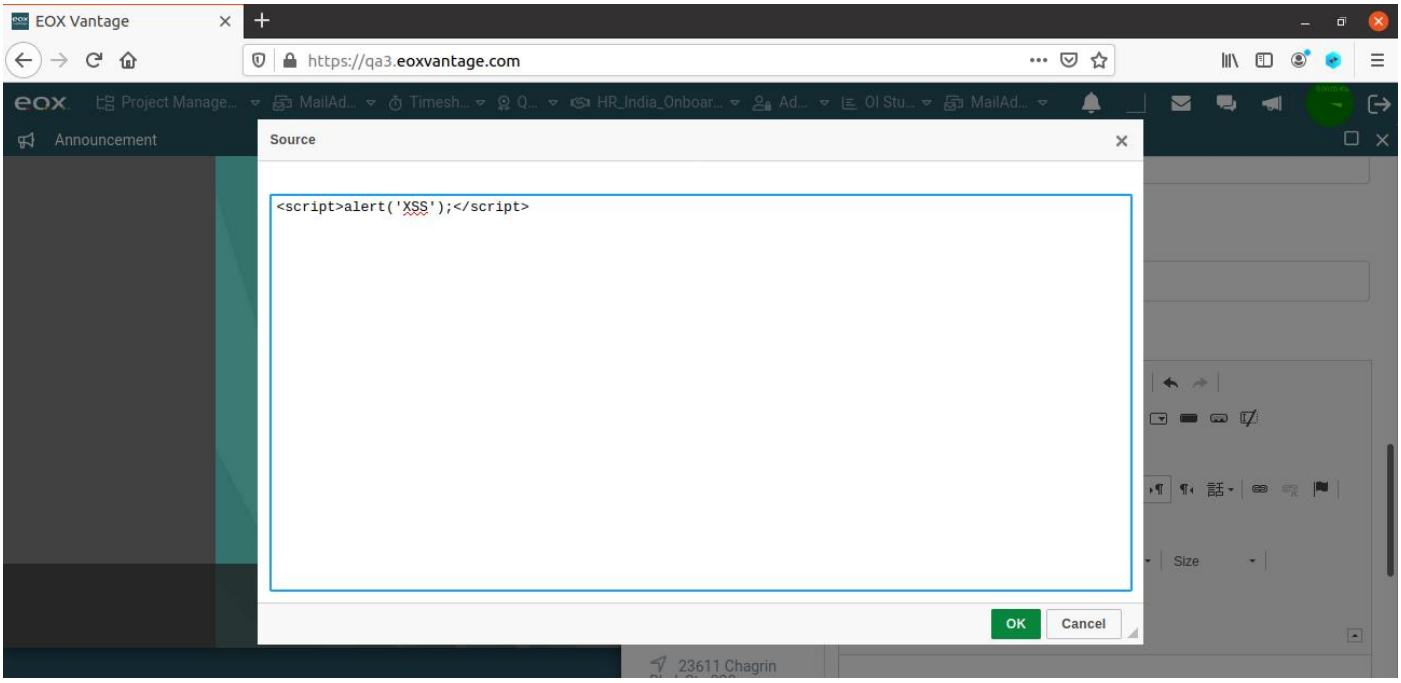


XSS Attack :

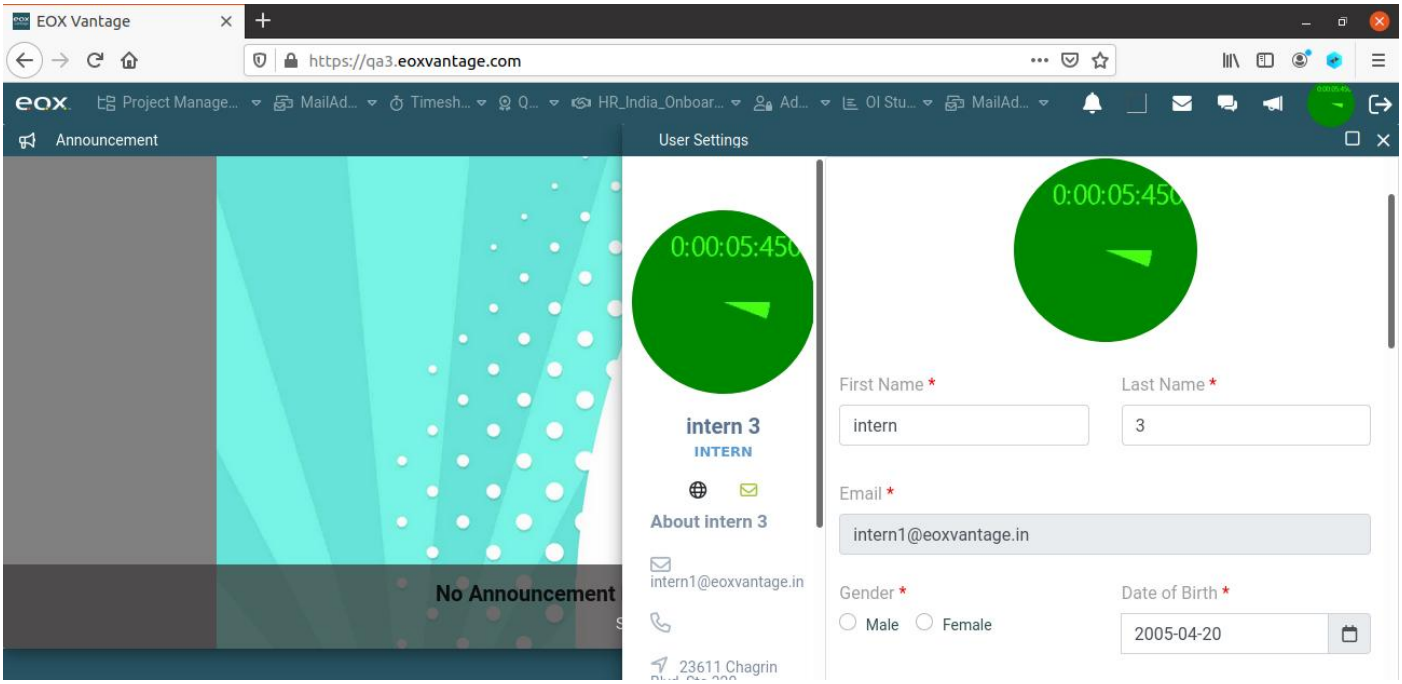
- The XSS attack "<script>alert('XSS');</sript>" in the "about me" field of a user profile is a common example of a cross-site scripting (XSS) attack.

- In this attack, the we are attempting to inject a malicious script into the web page that will execute when the user views the profile. The script in this case is an alert message that will pop up a dialog box with the text "XSS".

- If the web application is vulnerable to XSS, the attacker may be able to execute other, more malicious scripts that could steal sensitive information, modify the content of the web page, or perform other unauthorized actions on behalf of the user.



➢ After saving and refreshing the page, script was not effective or page was not effected at all that means the website is immune to the XSS attack.



- After tring out some simple attacks got know that this website is secure and immune to the attacks that we have tried such ad XSS, SQL Injection, CSRF.

- To find out the vulnerabilities present in the Target Website Im going to use a tool called “OWASP ZAP”.

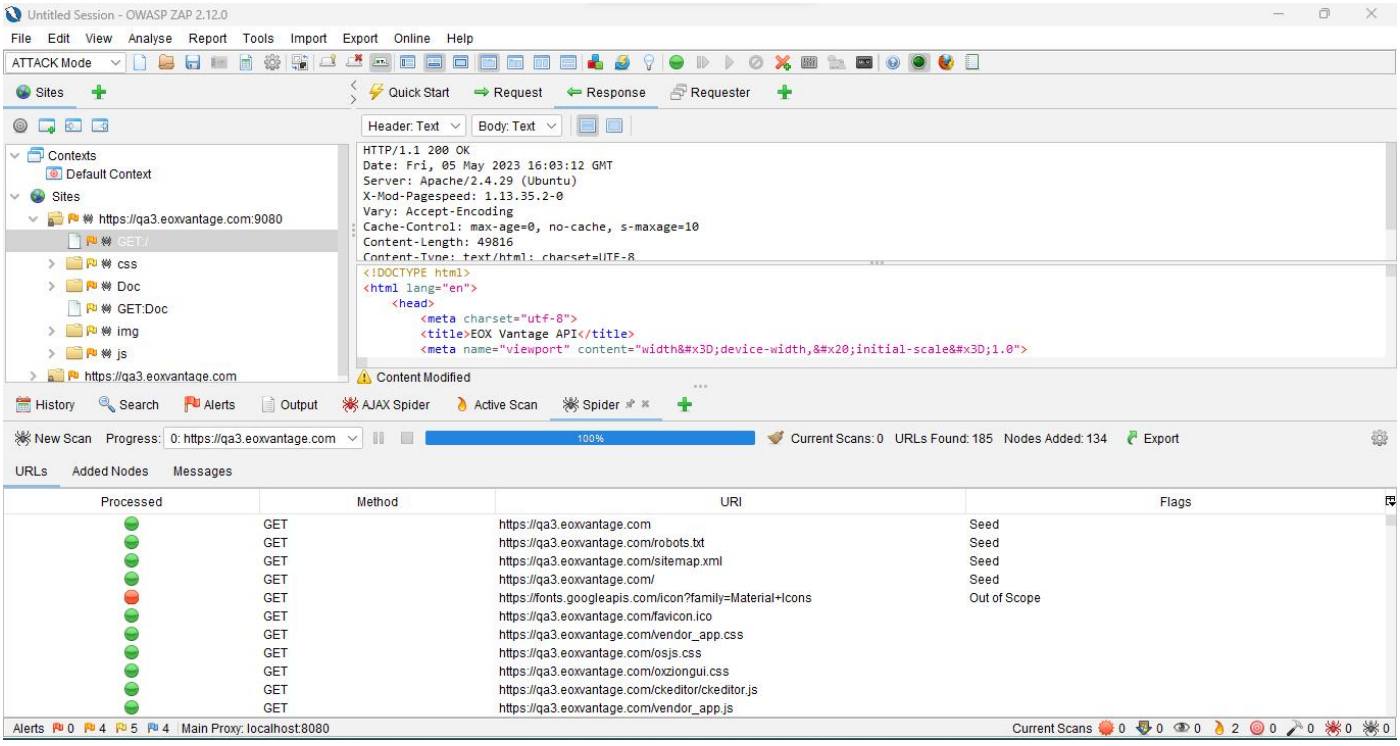
OWASP ZAP is a popular open-source web application security scanner that can detect a wide range of vulnerabilities in web applications. It is one of the most widely used web application security tools, and is often used by developers, penetration testers, and security professionals to identify and address security vulnerabilities in web applications.

OWASP ZAP (short for Zed Attack Proxy) is designed to be easy to use, even for users with little or no experience in web application security. It offers a range of features and capabilities, including automated scanning, manual testing, and reporting and analysis tools.

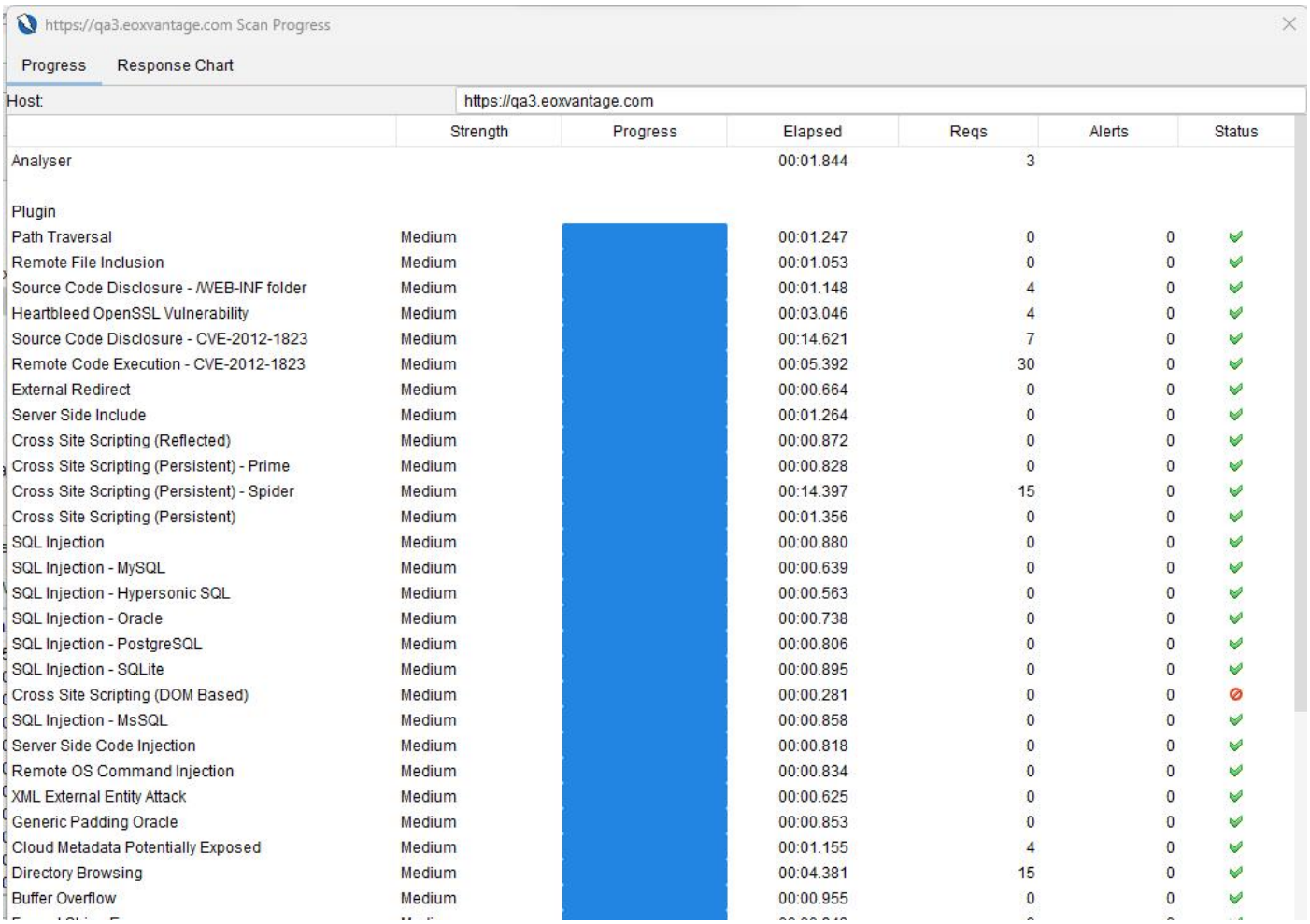
Some of its key features include:

- Active and passive scanning for vulnerabilities
- Support for a wide range of web application technologies and protocols
- Fuzzing and other testing techniques to identify vulnerabilities
- Support for automated testing and integration with continuous integration (CI) tools
- Detailed reporting and analysis tools to help identify and prioritize vulnerabilities.

OWASP ZAP Tool :

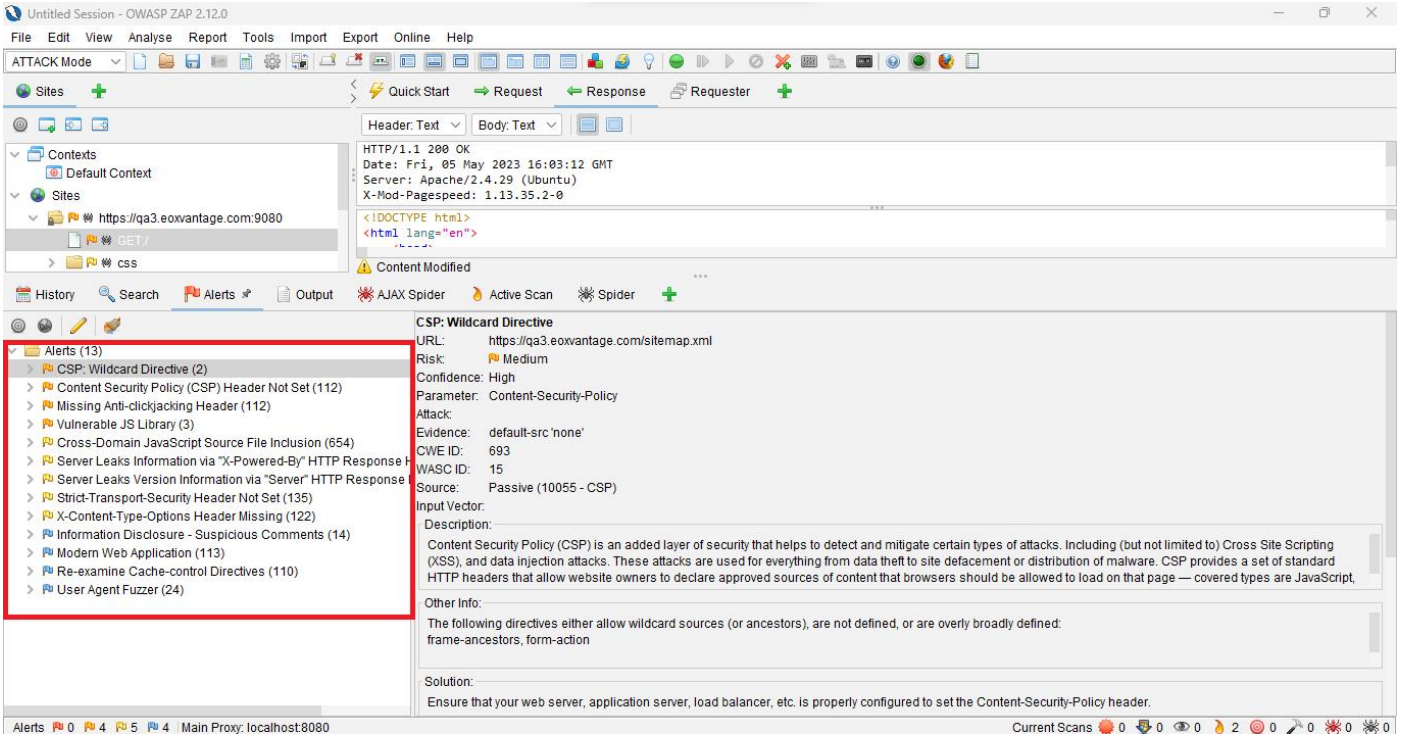


Scanning :



	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			00:01.844	3		
Plugin						
Path Traversal	Medium		00:01.247	0	0	
Remote File Inclusion	Medium		00:01.053	0	0	
Source Code Disclosure - /WEB-INF folder	Medium		00:01.148	4	0	
Heartbleed OpenSSL Vulnerability	Medium		00:03.046	4	0	
Source Code Disclosure - CVE-2012-1823	Medium		00:14.621	7	0	
Remote Code Execution - CVE-2012-1823	Medium		00:05.392	30	0	
External Redirect	Medium		00:00.664	0	0	
Server Side Include	Medium		00:01.264	0	0	
Cross Site Scripting (Reflected)	Medium		00:00.872	0	0	
Cross Site Scripting (Persistent) - Prime	Medium		00:00.828	0	0	
Cross Site Scripting (Persistent) - Spider	Medium		00:14.397	15	0	
Cross Site Scripting (Persistent)	Medium		00:01.356	0	0	
SQL Injection	Medium		00:00.880	0	0	
SQL Injection - MySQL	Medium		00:00.639	0	0	
SQL Injection - Hypersonic SQL	Medium		00:00.563	0	0	
SQL Injection - Oracle	Medium		00:00.738	0	0	
SQL Injection - PostgreSQL	Medium		00:00.806	0	0	
SQL Injection - SQLite	Medium		00:00.895	0	0	
Cross Site Scripting (DOM Based)	Medium		00:00.281	0	0	
SQL Injection - MsSQL	Medium		00:00.858	0	0	
Server Side Code Injection	Medium		00:00.818	0	0	
Remote OS Command Injection	Medium		00:00.834	0	0	
XML External Entity Attack	Medium		00:00.625	0	0	
Generic Padding Oracle	Medium		00:00.853	0	0	
Cloud Metadata Potentially Exposed	Medium		00:01.155	4	0	
Directory Browsing	Medium		00:04.381	15	0	
Buffer Overflow	Medium		00:00.955	0	0	

Alerts/vulnerabilities Found after the scan.



Report Generated :

ZAP Scanning Report

Sites: https://qa3.eoxvantage.com:9080 https://qa3.eoxvantage.com

Generated on Fri, 5 May 2023 22:34:09

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	5
Informational	4

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	112
Missing Anti-clickjacking Header	Medium	112
Vulnerable JS Library	Medium	3
Cross-Domain JavaScript Source File Inclusion	Low	654
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	13
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	136
Strict-Transport-Security Header Not Set	Low	135
X-Content-Type-Options Header Missing	Low	122
Information Disclosure - Suspicious Comments	Informational	14
Modern Web Application	Informational	113
Re-examine Cache-control Directives	Informational	110
User Agent Fuzzer	Informational	24

Note : The Report Generated by ZAP Tool is also Attached with the submission which consists of the Vulnerabilities with description, evidence, solution etc.

==========**********==========