PENETRATION TEST REPORT

OBJECTIVE:

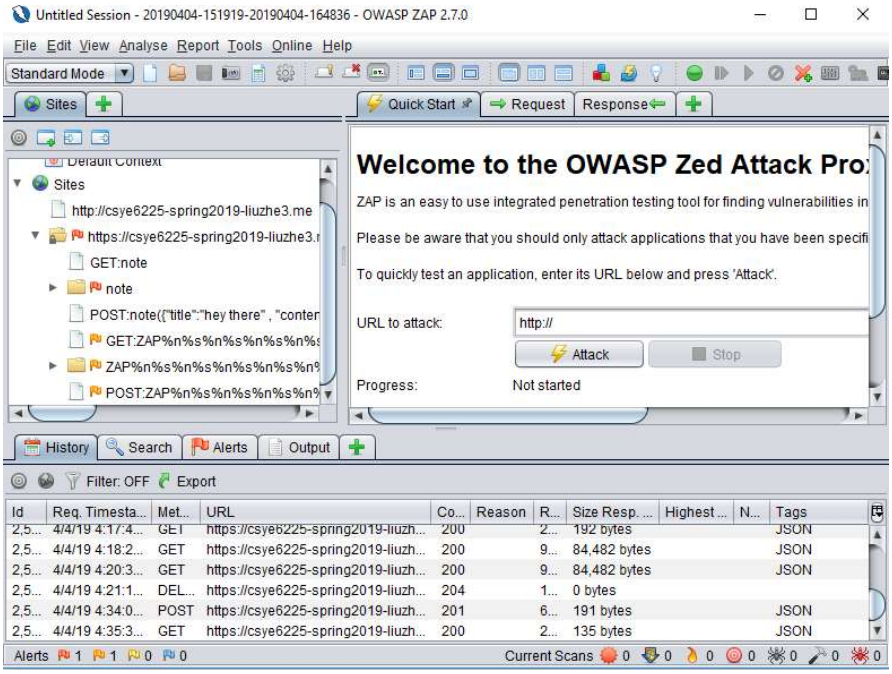
Identify and test your application against at least 3 attack vectors that do not exploit UI vulnerabilities. - You will document your findings in a PDF (Google doc exported as PDF) and commit it to your GitHub repository. - Your report should be as detailed as possible.

APPROACH:

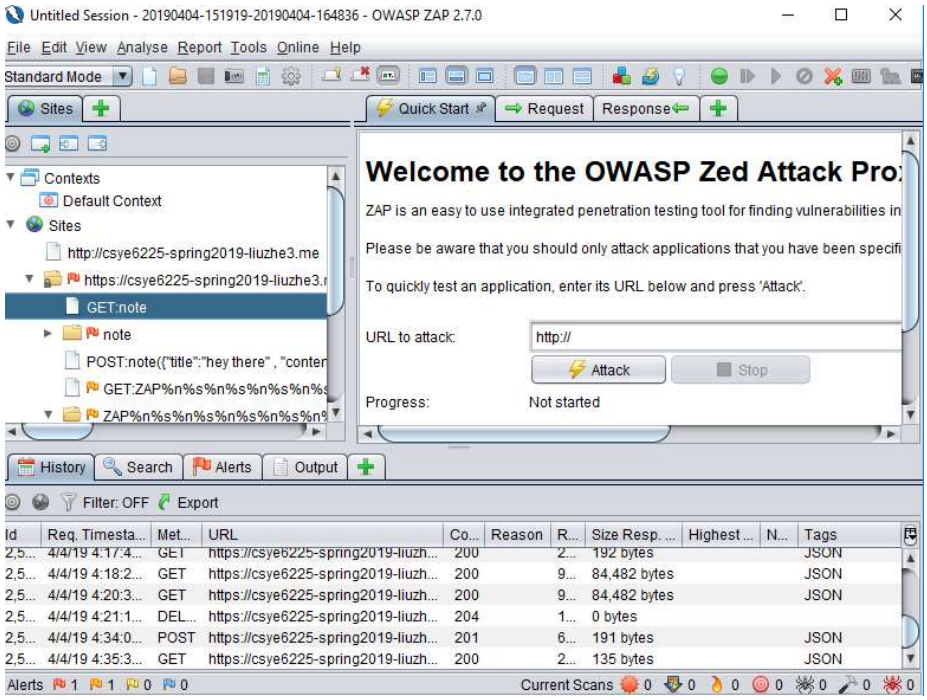
Use **OWASP ZAP** security test, to check the vulnerabilities with and without AWS WAF.
AWS WAF is a firewall that helps us protect our websites and web applications against various attacks at HTTP protocol level. With the use of OWASP ZAP we were able to test major penetration tests for the application. The three which appeared in the report has been listed below.
We ran the tests using two URL's with
https://csye6225-spring2019-{domain-name}.me which had AWS WAF enabled and
https://nowaf.csye6225-spring2019-{domain-name}.me which didn't have AWS WAF.

ABOUT THE TOOL USED FOR PENETRATION TEST

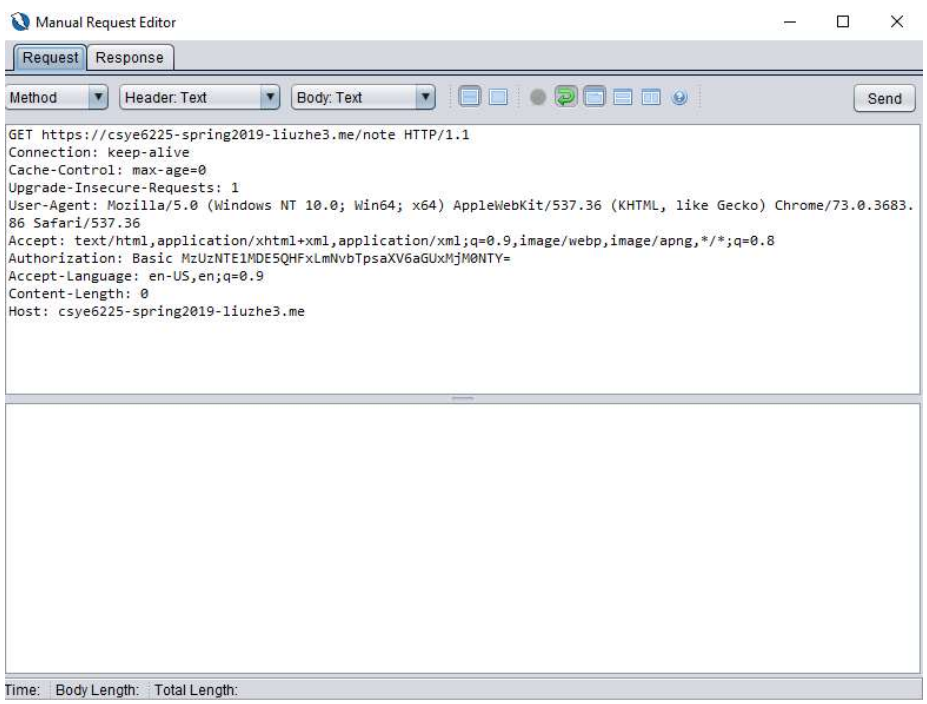
OWASP ZAP is used to generate a report for the series of tests used to conduct on an application.



The tests have been created in the left pane of the window tailoring the tests for the required CRUD Functionality.



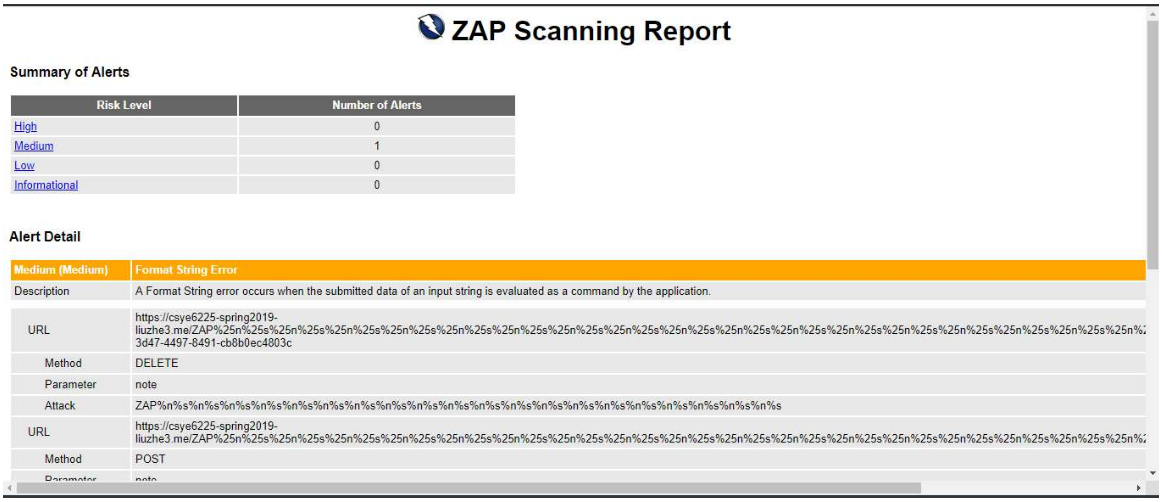
On clicking attack, the tool runs a set of tests which can be configured for various threats



The three vectors being tested from the above are:

1. **SQL Injection:**

   It occurs when an application sends untrusted data to an interpreter, like placement of malicious code in SQL statements to manipulate the system. The system tested for two of these and the Report has been attached below.



ZAP Scanning Report

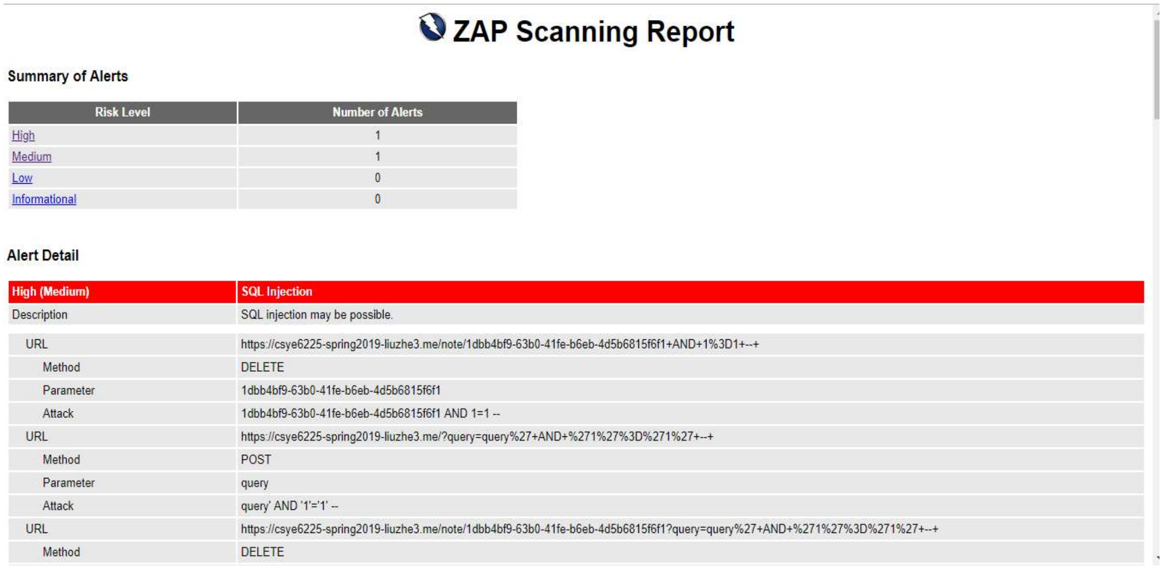
Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	0

Alert Detail

Medium (Medium)	Format String Error
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	https://csye6225-spring2019-liuzhe3.me/ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n% 3d47-4497-8491-cb8b0ec4803c
Method	DELETE
Parameter	note
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	https://csye6225-spring2019-liuzhe3.me/ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%
Method	POST

Fig. 1: Testing with AWS AFP



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	1
Low	0
Informational	0

Alert Detail

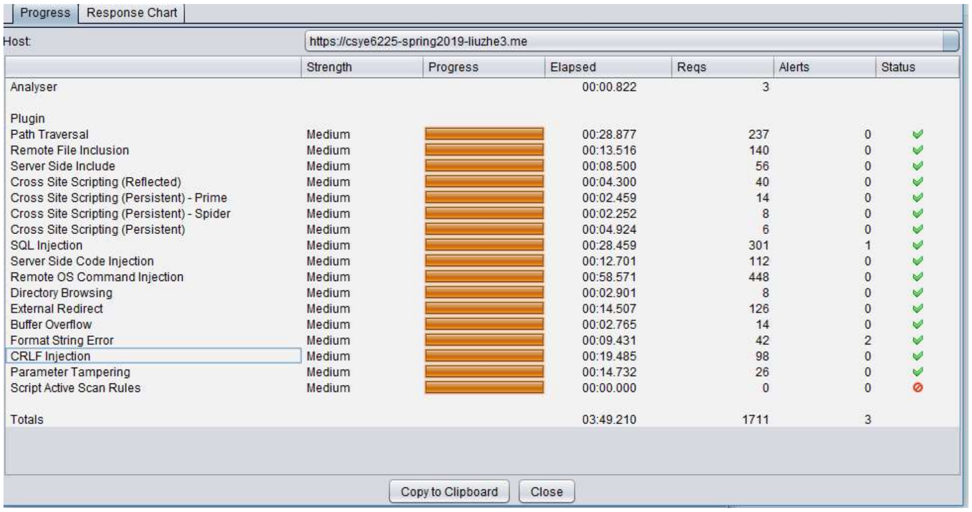
High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	https://csye6225-spring2019-liuzhe3.me/note/1dbb4bf9-63b0-41fe-b6eb-4d5b6815f6f1+AND+1%3D1+--+
Method	DELETE
Parameter	1dbb4bf9-63b0-41fe-b6eb-4d5b6815f6f1
Attack	1dbb4bf9-63b0-41fe-b6eb-4d5b6815f6f1 AND 1=1 --
URL	https://csye6225-spring2019-liuzhe3.me/?query=query%27+AND+%271%27%3D%271%27+--+
Method	POST
Parameter	query
Attack	query' AND '1'='1' --
URL	https://csye6225-spring2019-liuzhe3.me/note/1dbb4bf9-63b0-41fe-b6eb-4d5b6815f6f1?query=query%27+AND+%271%27%3D%271%27+--+
Method	DELETE

Fig. 2: Testing without AWS AFP

2. **CRLF Injection:**

   A CRLF injection attack is one of several types of injection attacks. It can be used to escalate to more malicious attacks such as Cross-site Scripting (XSS), page injection, web

cache poisoning, cache-based defacement, and more. A CRLF injection vulnerability exists if an attacker can inject the CRLF characters into a web application, for example using a user input form or an HTTP request.



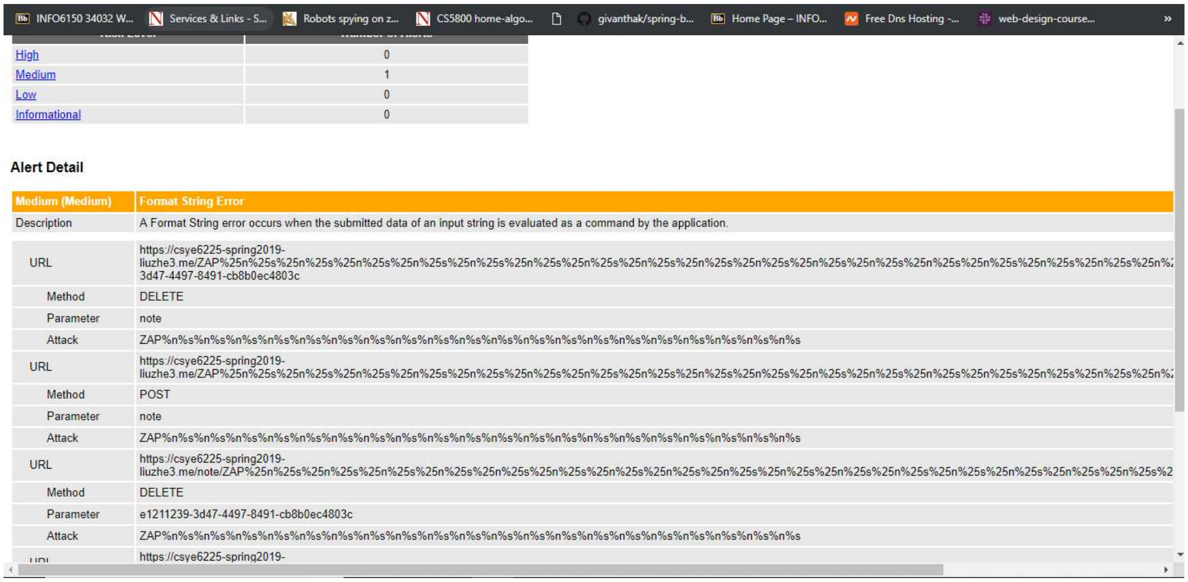
Host: https://csye6225-spring2019-liuzhe3.me

	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			00:00.822	3		
Plugin						
Path Traversal	Medium	▬	00:28.877	237	0	✓
Remote File Inclusion	Medium	▬	00:13.516	140	0	✓
Server Side Include	Medium	▬	00:08.500	56	0	✓
Cross Site Scripting (Reflected)	Medium	▬	00:04.300	40	0	✓
Cross Site Scripting (Persistent) - Prime	Medium	▬	00:02.459	14	0	✓
Cross Site Scripting (Persistent) - Spider	Medium	▬	00:02.252	8	0	✓
Cross Site Scripting (Persistent)	Medium	▬	00:04.924	6	0	✓
SQL Injection	Medium	▬	00:28.459	301	1	✓
Server Side Code Injection	Medium	▬	00:12.701	112	0	✓
Remote OS Command Injection	Medium	▬	00:58.571	448	0	✓
Directory Browsing	Medium	▬	00:02.901	8	0	✓
External Redirect	Medium	▬	00:14.507	126	0	✓
Buffer Overflow	Medium	▬	00:02.765	14	0	✓
Format String Error	Medium	▬	00:09.431	42	2	✓
CRLF Injection	Medium	▬	00:19.485	98	0	✓
Parameter Tampering	Medium	▬	00:14.732	26	0	✓
Script Active Scan Rules	Medium	▬	00:00.000	0	0	⊘
Totals			03:49.210	1711	3	

Report for the overall tests conducted

3. Cross site scripting:

XSS is a form when web applications use user data send to the browser without proper methods and sanitization.



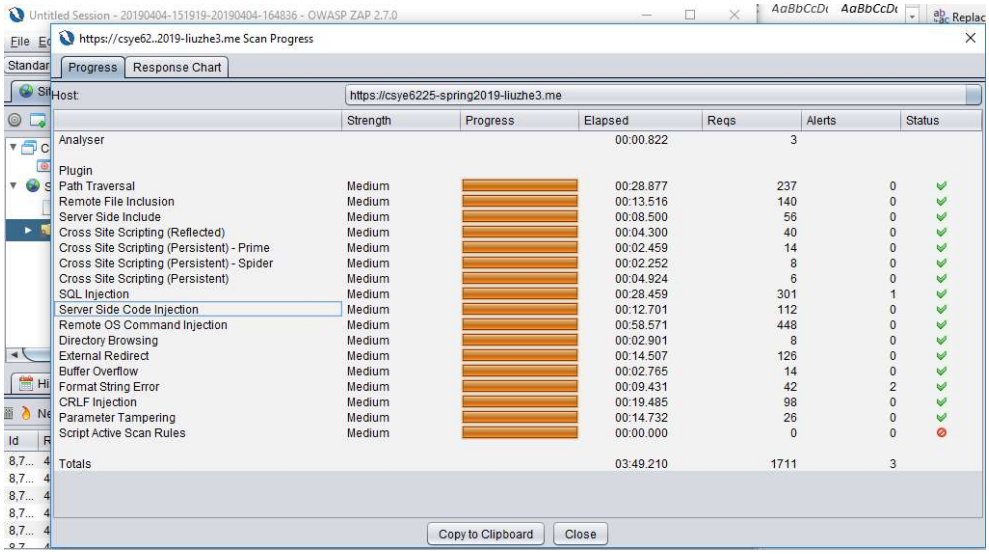
High	0
Medium	1
Low	0
Informational	0

Alert Detail

Medium (Medium)	Format String Error
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	https://csye6225-spring2019-liuzhe3.me/ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%2 3d47-4497-8491-cb8b0ec4803c
Method	DELETE
Parameter	note
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	https://csye6225-spring2019-liuzhe3.me/ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%2
Method	POST
Parameter	note
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	https://csye6225-spring2019-liuzhe3.me/note/ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%2
Method	DELETE
Parameter	e1211239-3d47-4497-8491-cb8b0ec4803c
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	https://csye6225-spring2019-

CONCLUSION:

The outcome has been recorded for the above security threats.



	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			00:00.822	3		
Plugin						
Path Traversal	Medium		00:28.877	237	0	✔
Remote File Inclusion	Medium		00:13.516	140	0	✔
Server Side Include	Medium		00:08.500	56	0	✔
Cross Site Scripting (Reflected)	Medium		00:04.300	40	0	✔
Cross Site Scripting (Persistent) - Prime	Medium		00:02.459	14	0	✔
Cross Site Scripting (Persistent) - Spider	Medium		00:02.252	8	0	✔
Cross Site Scripting (Persistent)	Medium		00:04.924	6	0	✔
SQL Injection	Medium		00:28.459	301	1	✔
Server Side Code Injection	Medium		00:12.701	112	0	✔
Remote OS Command Injection	Medium		00:58.571	448	0	✔
Directory Browsing	Medium		00:02.901	8	0	✔
External Redirect	Medium		00:14.507	126	0	✔
Buffer Overflow	Medium		00:02.765	14	0	✔
Format String Error	Medium		00:09.431	42	2	✔
CRLF Injection	Medium		00:19.485	98	0	✔
Parameter Tampering	Medium		00:14.732	26	0	✔
Script Active Scan Rules	Medium		00:00.000	0	0	⊘
Totals			03:49.210	1711	3	