CSYE 6225
Fall 2018

Web Application Firewall Penetration Testing

Submitted By:
Dhanisha Phadate (001859234)
Palak Sharma (001834478)
Garvit Chawla (001859169)

Web Application Firewall

The objective of this assignment is to deploy AWS WAF to the Application Load Balancer (ALB) that fronts your web servers running on EC2. Use AWS WAF to Mitigate OWASP's Top 10 Web Application Vulnerabilities. All WAF resources and web security rules to your application cloudformation stack.

Penetration Testing

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. **You will document attacks on your own web application with and without the AWS WAF in place.**

Your report should provide details on following along with screenshots:

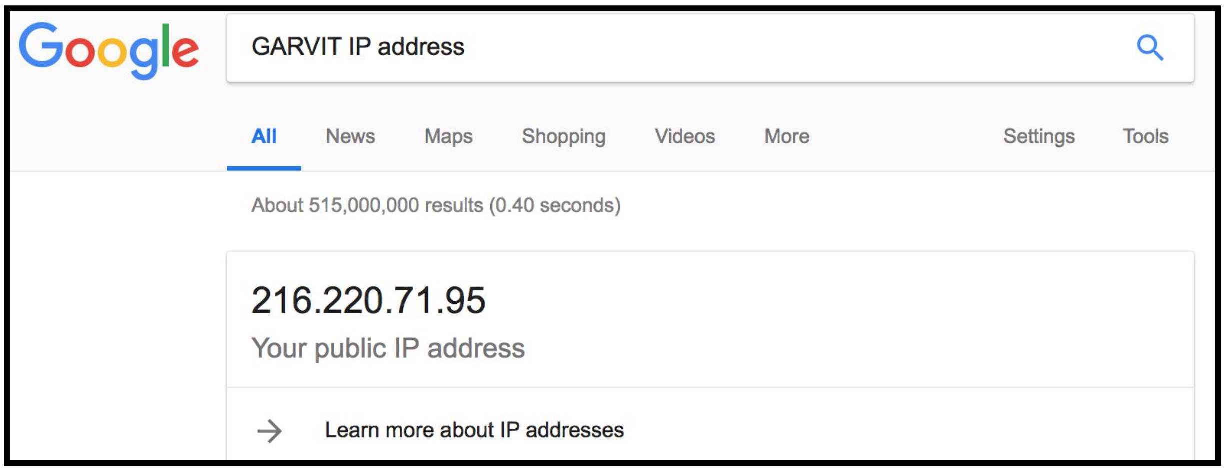
- Attack Vector
- Result
- Why did you choose this specific attack vector?

1. <u>OWASP Top 10 - A7 - Insufficient Attack Protection and A2 - Broken Authentication</u>

IP Blacklisting: Matches IP addresses that should not be allowed to access content.

Attack Vector: A hacker or cracker can gain access to a computer and deliver payload or malicious code. Hacker can access Bank accounts etc and we can stop that by Blacklisting them for a while until the user provides his/her credentials.

My Public IP Address = 216.220.71.95


GARVIT IP address

All News Maps Shopping Videos More Settings Tools

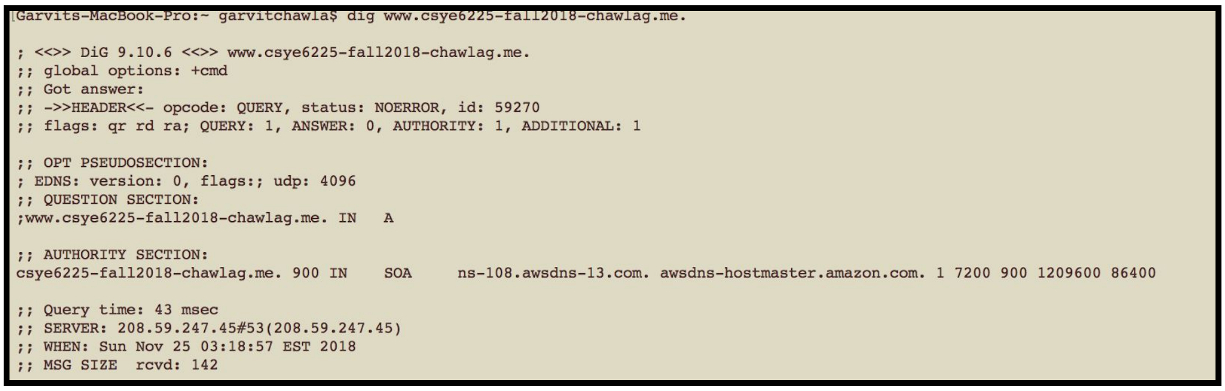
About 515,000,000 results (0.40 seconds)

216.220.71.95

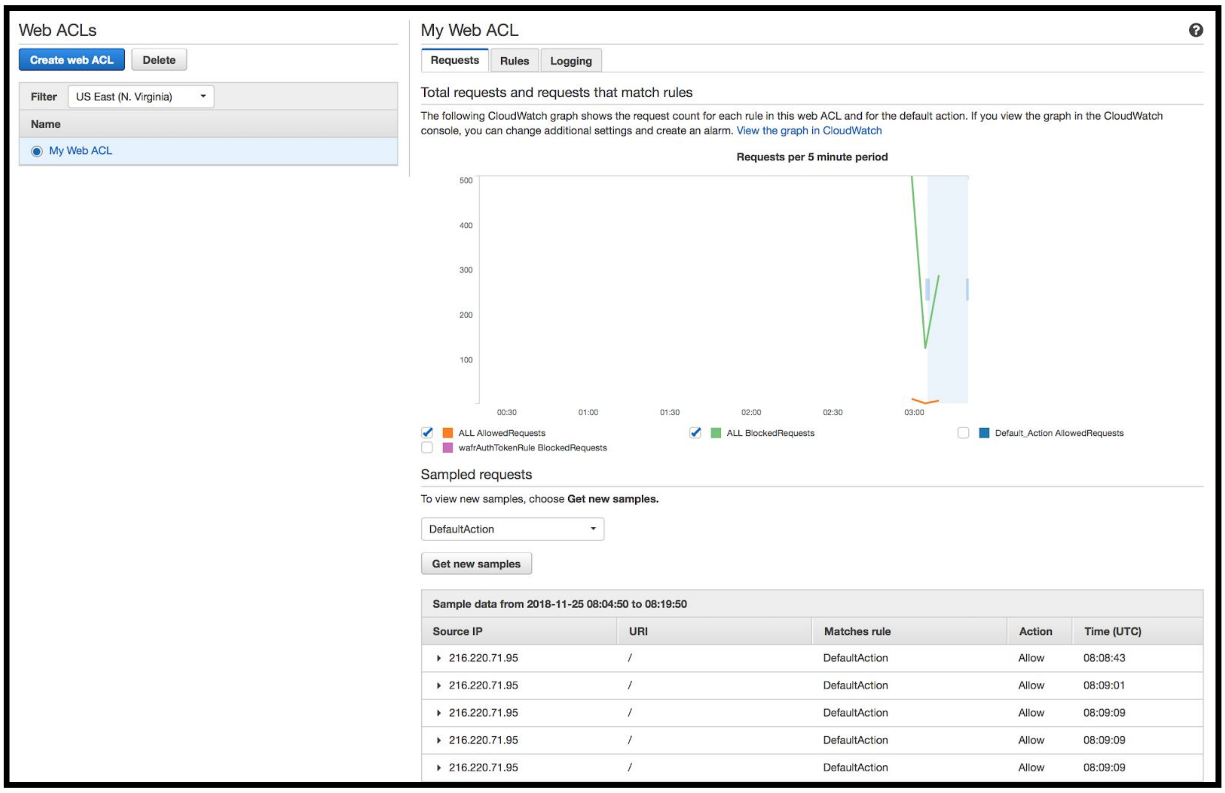
Your public IP address

Learn more about IP addresses

dig www.csye6225-fall2018-chawlag.me.


```
Garvits-MacBook-Pro:~ garvitchawla$ dig www.csye6225-fall2018-chawlag.me.

; <<>> DiG 9.10.6 <<>> www.csye6225-fall2018-chawlag.me.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59270
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.csye6225-fall2018-chawlag.me. IN   A

;; AUTHORITY SECTION:
csye6225-fall2018-chawlag.me. 900 IN    SOA     ns-108.awsdns-13.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

;; Query time: 43 msec
;; SERVER: 208.59.247.45#53(208.59.247.45)
;; WHEN: Sun Nov 25 03:18:57 EST 2018
;; MSG SIZE  rcvd: 142
```

Checking the no of requests sent at Web ACL and we can see the no. of Allowed and Blocked Requests.



Total requests and requests that match rules

The following CloudWatch graph shows the request count for each rule in this web ACL and for the default action. If you view the graph in the CloudWatch console, you can change additional settings and create an alarm. View the graph in CloudWatch

Requests per 5 minute period
500
400
300
200
100
00:30
01:00
01:30
02:00
02:30
03:00
ALL AllowedRequests
ALL BlockedRequests
Default_Action AllowedRequests
wafrAuthTokenRule BlockedRequests

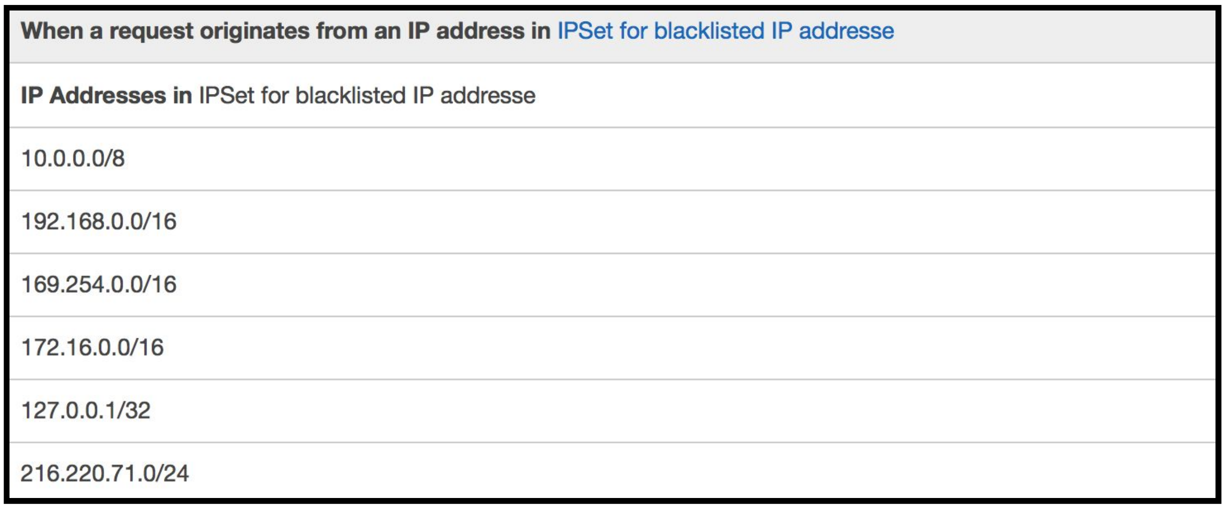
Sampled requests

To view new samples, choose **Get new samples.**

Sample data from 2018-11-25 08:04:50 to 08:19:50

Source IP	URI	Matches rule	Action	Time (UTC)
216.220.71.95	/	DefaultAction	Allow	08:08:43
216.220.71.95	/	DefaultAction	Allow	08:09:01
216.220.71.95	/	DefaultAction	Allow	08:09:09
216.220.71.95	/	DefaultAction	Allow	08:09:09
216.220.71.95	/	DefaultAction	Allow	08:09:09

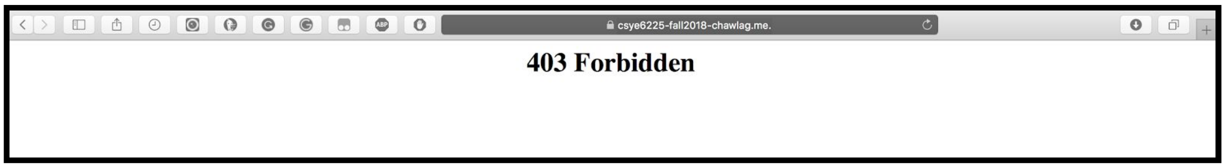
After creating WAF and Blacklisting my Public IP Address we can see that the domain is blacklisted.



When a request originates from an IP address in IPSet for blacklisted IP addresse

IP Addresses in IPSet for blacklisted IP addresse
10.0.0.0/8
192.168.0.0/16
169.254.0.0/16
172.16.0.0/16
127.0.0.1/32
216.220.71.0/24

403 Forbidden Blacklisted IP Address



403 Forbidden

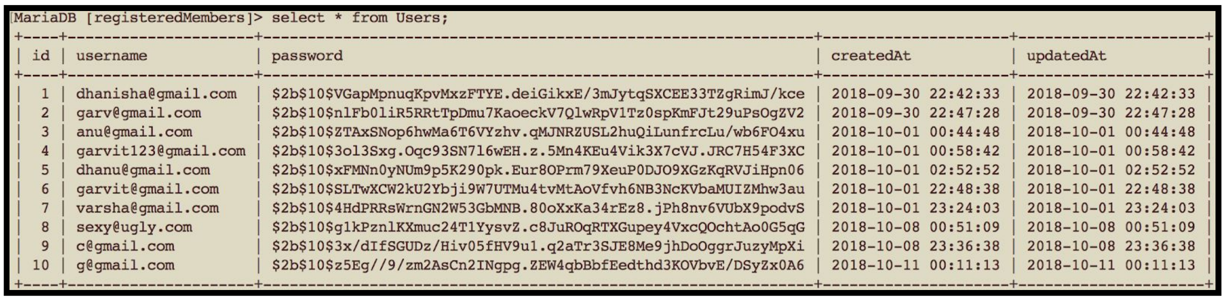
Result: The IP Address has been blacklisted.

Why choose this attack vector? Attackers choose this attack vector as they access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools.

2. **<u>OWASP Top 10 - A1 - Injection</u>**

Attack Vector: By inserting unsanitized data into requests to the interpreter, an attacker can alter the intent of the requests and cause unexpected actions.

MariaDB> select * from Users;

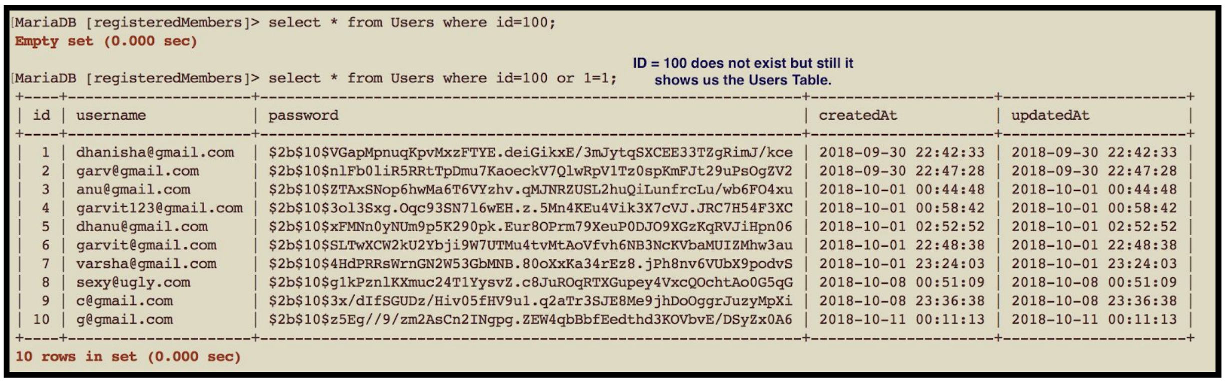


```
MariaDB [registeredMembers]> select * from Users;
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
| id | username            | password                                                     | createdAt           | updatedAt           |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
|  1 | dhanisha@gmail.com  | $2b$10$VGapMpnuqKpvMxzFTYE.deiGikxE/3mJytqSXCEE33TZgRimJ/kce | 2018-09-30 22:42:33 | 2018-09-30 22:42:33 |
|  2 | garv@gmail.com      | $2b$10$nlFb0liR5RRtTpDmu7KaoeckV7QlwRpV1Tz0spKmFJt29uPsOgZV2 | 2018-09-30 22:47:28 | 2018-09-30 22:47:28 |
|  3 | anu@gmail.com       | $2b$10$ZTAxSNop6hwMa6T6VYzhv.qMJNRZUSL2huQiLunfrcLu/wb6FO4xu | 2018-10-01 00:44:48 | 2018-10-01 00:44:48 |
|  4 | garvit123@gmail.com | $2b$10$3ol3Sxg.Oqc93SN7l6wEH.z.5Mn4KEu4Vik3X7cVJ.JRC7H54F3XC | 2018-10-01 00:58:42 | 2018-10-01 00:58:42 |
|  5 | dhanu@gmail.com     | $2b$10$xFMNn0yNUm9p5K290pk.Eur8OPrm79XeuP0DJO9XGzKqRVJiHpn06 | 2018-10-01 02:52:52 | 2018-10-01 02:52:52 |
|  6 | garvit@gmail.com    | $2b$10$SLTwXCW2kU2Ybji9W7UTMu4tvMtAoVfvh6NB3NcKVbaMUIZMhw3au | 2018-10-01 22:48:38 | 2018-10-01 22:48:38 |
|  7 | varsha@gmail.com    | $2b$10$4HdPRRsWrnGN2W53GbMNB.80oXxKa34rEz8.jPh8nv6VUbX9podvS | 2018-10-01 23:24:03 | 2018-10-01 23:24:03 |
|  8 | sexy@ugly.com       | $2b$10$g1kPznlKXmuc24T1YysvZ.c8JuROqRTXGupey4VxcQOchtAo0G5qG | 2018-10-08 00:51:09 | 2018-10-08 00:51:09 |
|  9 | c@gmail.com         | $2b$10$3x/dIfSGUDz/Hiv05fHV9u1.q2aTr3SJE8Me9jhDoOggrJuzyMpXi | 2018-10-08 23:36:38 | 2018-10-08 23:36:38 |
| 10 | g@gmail.com         | $2b$10$z5Eg//9/zm2AsCn2INgpg.ZEW4qbBbfEedthd3KOVbvE/DSyZx0A6 | 2018-10-11 00:11:13 | 2018-10-11 00:11:13 |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
```

MariaDB> select * from Users where id=100;

Nothing shows up as there is no id of 100.

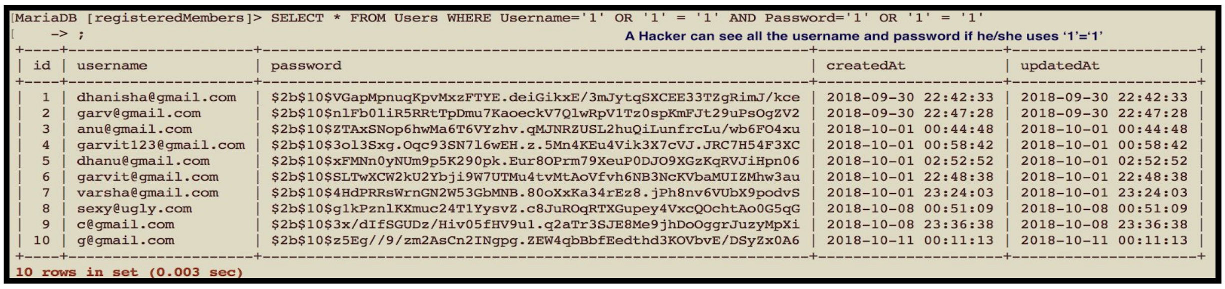
MariaDB> There are only 10 id in the table, but still the query shows the whole table as we have provided OR 1=1;



```
MariaDB [registeredMembers]> select * from Users where id=100;
Empty set (0.000 sec)

MariaDB [registeredMembers]> select * from Users where id=100 or 1=1;
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
| id | username            | password                                                     | createdAt           | updatedAt           |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
|  1 | dhanisha@gmail.com  | $2b$10$VGapMpnuqKpvMxzFTYE.deiGikxE/3mJytqSXCEE33TZgRimJ/kce | 2018-09-30 22:42:33 | 2018-09-30 22:42:33 |
|  2 | garv@gmail.com      | $2b$10$nlFb0liR5RRtTpDmu7KaoeckV7QlwRpV1Tz0spKmFJt29uPsOgZV2 | 2018-09-30 22:47:28 | 2018-09-30 22:47:28 |
|  3 | anu@gmail.com       | $2b$10$ZTAxSNop6hwMa6T6VYzhv.qMJNRZUSL2huQiLunfrcLu/wb6FO4xu | 2018-10-01 00:44:48 | 2018-10-01 00:44:48 |
|  4 | garvit123@gmail.com | $2b$10$3ol3Sxg.Oqc93SN7l6wEH.z.5Mn4KEu4Vik3X7cVJ.JRC7H54F3XC | 2018-10-01 00:58:42 | 2018-10-01 00:58:42 |
|  5 | dhanu@gmail.com     | $2b$10$xFMNn0yNUm9p5K290pk.Eur8OPrm79XeuP0DJO9XGzKqRVJiHpn06 | 2018-10-01 02:52:52 | 2018-10-01 02:52:52 |
|  6 | garvit@gmail.com    | $2b$10$SLTwXCW2kU2Ybji9W7UTMu4tvMtAoVfvh6NB3NcKVbaMUIZMhw3au | 2018-10-01 22:48:38 | 2018-10-01 22:48:38 |
|  7 | varsha@gmail.com    | $2b$10$4HdPRRsWrnGN2W53GbMNB.80oXxKa34rEz8.jPh8nv6VUbX9podvS | 2018-10-01 23:24:03 | 2018-10-01 23:24:03 |
|  8 | sexy@ugly.com       | $2b$10$g1kPznlKXmuc24T1YysvZ.c8JuROqRTXGupey4VxcQOchtAo0G5qG | 2018-10-08 00:51:09 | 2018-10-08 00:51:09 |
|  9 | c@gmail.com         | $2b$10$3x/dIfSGUDz/Hiv05fHV9u1.q2aTr3SJE8Me9jhDoOggrJuzyMpXi | 2018-10-08 23:36:38 | 2018-10-08 23:36:38 |
| 10 | g@gmail.com         | $2b$10$z5Eg//9/zm2AsCn2INgpg.ZEW4qbBbfEedthd3KOVbvE/DSyZx0A6 | 2018-10-11 00:11:13 | 2018-10-11 00:11:13 |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
10 rows in set (0.000 sec)
```

ID = 100 does not exist but still it shows us the Users Table.

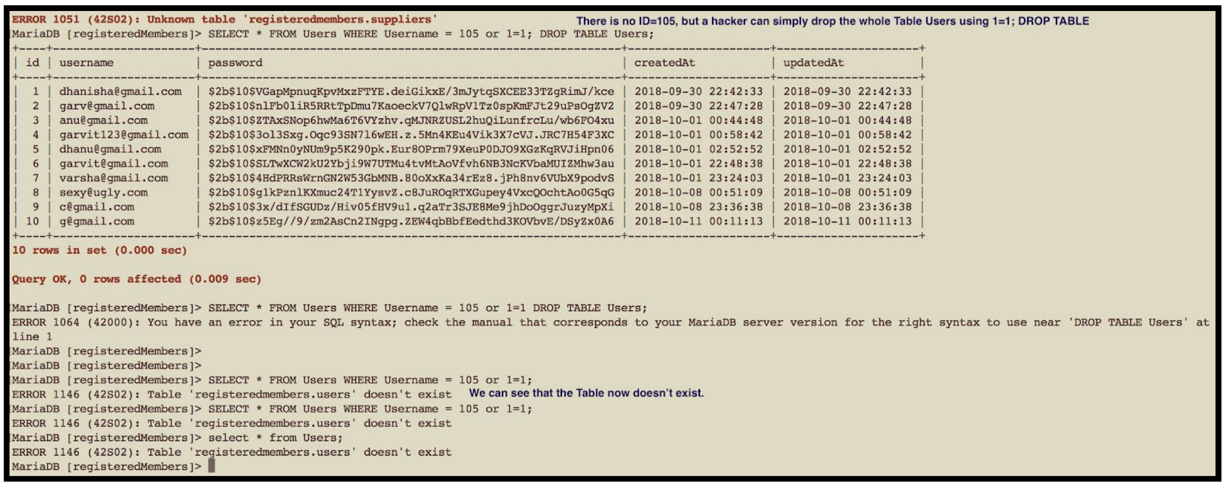
MariaDB> The username and the password was not provided but still query shows up the whole table because we have ORed username and password each with 1.



```
MariaDB [registeredMembers]> SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR '1' = '1'
    -> ;
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
| id | username            | password                                                     | createdAt           | updatedAt           |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
|  1 | dhanisha@gmail.com  | $2b$10$VGapMpnuqKpvMxzFTYE.deiGikxE/3mJytqSXCEE33TZgRimJ/kce | 2018-09-30 22:42:33 | 2018-09-30 22:42:33 |
|  2 | garv@gmail.com      | $2b$10$nlFb0liR5RRtTpDmu7KaoeckV7QlwRpV1Tz0spKmFJt29uPsOgZV2 | 2018-09-30 22:47:28 | 2018-09-30 22:47:28 |
|  3 | anu@gmail.com       | $2b$10$ZTAxSNop6hwMa6T6VYzhv.qMJNRZUSL2huQiLunfrcLu/wb6FO4xu | 2018-10-01 00:44:48 | 2018-10-01 00:44:48 |
|  4 | garvit123@gmail.com | $2b$10$3ol3Sxg.Oqc93SN7l6wEH.z.5Mn4KEu4Vik3X7cVJ.JRC7H54F3XC | 2018-10-01 00:58:42 | 2018-10-01 00:58:42 |
|  5 | dhanu@gmail.com     | $2b$10$xFMNn0yNUm9p5K290pk.Eur8OPrm79XeuP0DJO9XGzKqRVJiHpn06 | 2018-10-01 02:52:52 | 2018-10-01 02:52:52 |
|  6 | garvit@gmail.com    | $2b$10$SLTwXCW2kU2Ybji9W7UTMu4tvMtAoVfvh6NB3NcKVbaMUIZMhw3au | 2018-10-01 22:48:38 | 2018-10-01 22:48:38 |
|  7 | varsha@gmail.com    | $2b$10$4HdPRRsWrnGN2W53GbMNB.80oXxKa34rEz8.jPh8nv6VUbX9podvS | 2018-10-01 23:24:03 | 2018-10-01 23:24:03 |
|  8 | sexy@ugly.com       | $2b$10$g1kPznlKXmuc24T1YysvZ.c8JuROqRTXGupey4VxcQOchtAo0G5qG | 2018-10-08 00:51:09 | 2018-10-08 00:51:09 |
|  9 | c@gmail.com         | $2b$10$3x/dIfSGUDz/Hiv05fHV9u1.q2aTr3SJE8Me9jhDoOggrJuzyMpXi | 2018-10-08 23:36:38 | 2018-10-08 23:36:38 |
| 10 | g@gmail.com         | $2b$10$z5Eg//9/zm2AsCn2INgpg.ZEW4qbBbfEedthd3KOVbvE/DSyZx0A6 | 2018-10-11 00:11:13 | 2018-10-11 00:11:13 |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
10 rows in set (0.003 sec)
```

A Hacker can see all the username and password if he/she uses ‘1’=‘1’

MariaDB> By changing the query and OR it with 1=1; DROP TABLE Users; the hacker can drop the Table. The Table now doesn't exist.

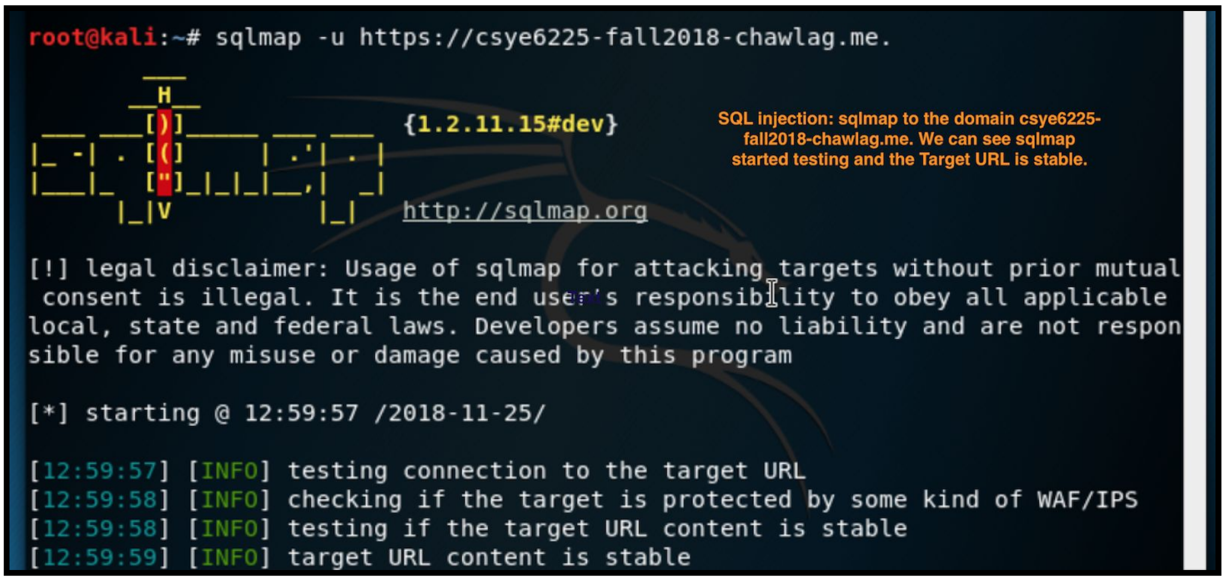


There is no ID=105, but a hacker can simply drop the whole Table Users using 1=1; DROP TABLE

```
ERROR 1051 (42S02): Unknown table 'registeredmembers.suppliers'
MariaDB [registeredMembers]> SELECT * FROM Users WHERE Username = 105 or 1=1; DROP TABLE Users;
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
| id | username            | password                                                     | createdAt           | updatedAt           |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
|  1 | dhanisha@gmail.com  | $2b$10$VGapMpnuqKpvMxzFTYE.deiGikxE/3mJytqSXCEE33TZgRimJ/kce | 2018-09-30 22:42:33 | 2018-09-30 22:42:33 |
|  2 | garv@gmail.com      | $2b$10$nlFb0liR5RRtTpDmu7KaoeckV7QlwRpV1Tz0spKmFJt29uPsOgZV2 | 2018-09-30 22:47:28 | 2018-09-30 22:47:28 |
|  3 | anu@gmail.com       | $2b$10$ZTAxSNop6hwMa6T6VYzhv.qMJNRZUSL2huQiLunfrcLu/wb6FO4xu | 2018-10-01 00:44:48 | 2018-10-01 00:44:48 |
|  4 | garvit123@gmail.com | $2b$10$3ol3Sxg.Oqc93SN716wEH.z.5Mn4KEu4Vik3X7cVJ.JRC7H54F3XC | 2018-10-01 00:58:42 | 2018-10-01 00:58:42 |
|  5 | dhanu@gmail.com     | $2b$10$xFMNn0yNUm9p5K290pk.Eur8OPrm79XeuP0DJO9XGzKqRVJiHpn06 | 2018-10-01 02:52:52 | 2018-10-01 02:52:52 |
|  6 | garvit@gmail.com    | $2b$10$SLTwXCW2kU2Ybji9W7UTMu4tvMtAoVfvh6NB3NcKVbaMUIZMhw3au | 2018-10-01 22:48:38 | 2018-10-01 22:48:38 |
|  7 | varsha@gmail.com    | $2b$10$4HdPRRsWrnGN2W53GbMNB.80oXxKa34rEz8.jPh8nv6VUbX9podvS | 2018-10-01 23:24:03 | 2018-10-01 23:24:03 |
|  8 | sexy@ugly.com       | $2b$10$g1kPznlKXmuc24T1YysvZ.c8JuROqRTXGupey4VxcQOchtAo0G5qG | 2018-10-08 00:51:09 | 2018-10-08 00:51:09 |
|  9 | c@gmail.com         | $2b$10$3x/dIfSGUDz/Hiv05fHV9ul.q2aTr3SJE8Me9jhDoOggrJuzyMpXi | 2018-10-08 23:36:38 | 2018-10-08 23:36:38 |
| 10 | g@gmail.com         | $2b$10$z5Eg//9/zm2AsCn2INgpg.ZEW4qbBbfEedthd3KOVbvE/DSyZx0A6 | 2018-10-11 00:11:13 | 2018-10-11 00:11:13 |
+----+---------------------+--------------------------------------------------------------+---------------------+---------------------+
10 rows in set (0.000 sec)

Query OK, 0 rows affected (0.009 sec)

MariaDB [registeredMembers]> SELECT * FROM Users WHERE Username = 105 or 1=1 DROP TABLE Users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'DROP TABLE Users' at
line 1
MariaDB [registeredMembers]>
MariaDB [registeredMembers]>
MariaDB [registeredMembers]> SELECT * FROM Users WHERE Username = 105 or 1=1;
ERROR 1146 (42S02): Table 'registeredmembers.users' doesn't exist
MariaDB [registeredMembers]> SELECT * FROM Users WHERE Username = 105 or 1=1;
ERROR 1146 (42S02): Table 'registeredmembers.users' doesn't exist
MariaDB [registeredMembers]> select * from Users;
ERROR 1146 (42S02): Table 'registeredmembers.users' doesn't exist
MariaDB [registeredMembers]>
```

We can see that the Table now doesn't exist.

Result: The Table was deleted even though the query was not correct. After creating WAF, we can see that the target domain is stable on sqlmap.



SQL injection: sqlmap to the domain csye6225-fall2018-chawlag.me. We can see sqlmap started testing and the Target URL is stable.

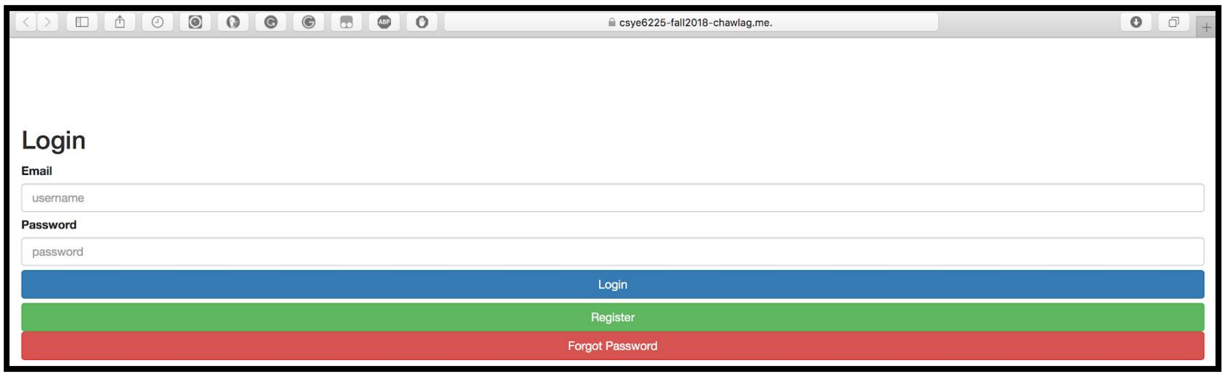
```
root@kali:~# sqlmap -u https://csye6225-fall2018-chawlag.me.

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.2.11.15#dev}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 12:59:57 /2018-11-25/

[12:59:57] [INFO] testing connection to the target URL
[12:59:58] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:59:58] [INFO] testing if the target URL content is stable
[12:59:59] [INFO] target URL content is stable
```

Why choose this attack vector? Attackers use almost any source of data as an injection vector, environment variables, parameters, external and internal web services, and all types of users and these vulnerabilities are very often in SQL. Injection can result in data loss or denial of access.

3. **<u>OWASP Top 10 - A2</u>** - **<u>Blacklist bad/hijacked JWT tokens or session IDs and Broken Authentication</u>**
Matches the specific values in the cookie or Authorization header for JWT it is sufficient to check the signature.

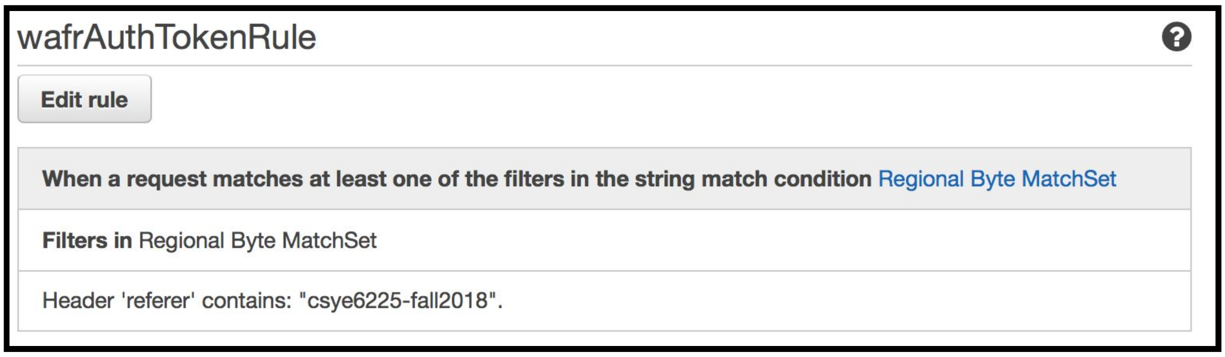
Attack Vector: Typosquatting or URL hijacking is where hijackers register misspelt versions of your domain name to sent the traffic to malicious sites.

Before creating WAF, we could access the domain.


csye6225-fall2018-chawlag.me.

Login
Email
username
Password
password
Login
Register
Forgot Password

Created a WAF where a request matches at least one of the filters in the string match condition.
It will block any domain which contains “csye6225-fall2018” in it. We can change **the rule so it allows only those domains which have “csye6225-fall2018” in it.**


wafrAuthTokenRule

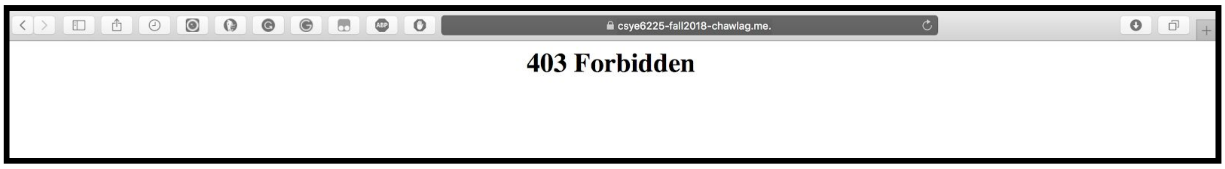
Edit rule

When a request matches at least one of the filters in the string match condition Regional Byte MatchSet

Filters in Regional Byte MatchSet

Header 'referer' contains: "csye6225-fall2018".

After WAF was created, the server will not fulfill the request.


csye6225-fall2018-chawlag.me.

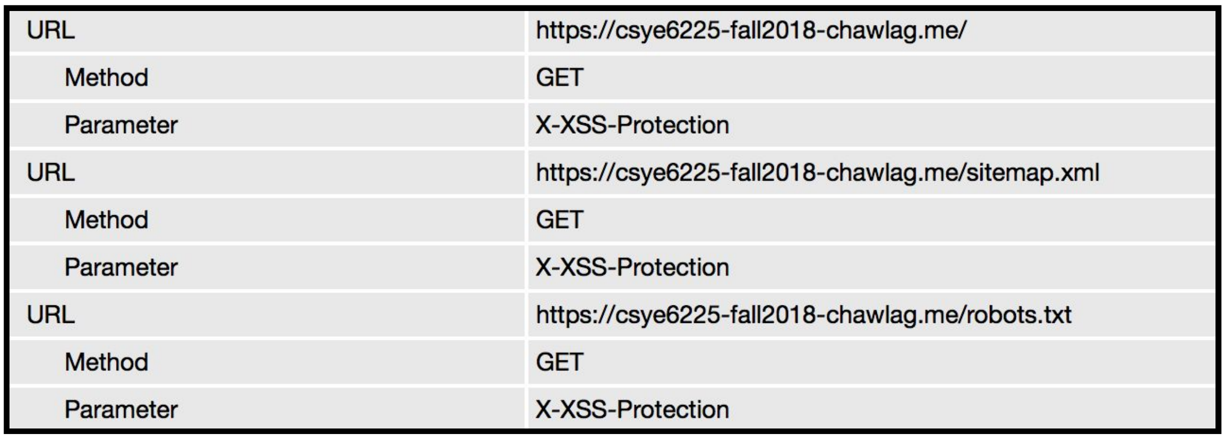
403 Forbidden

Result: Forbidden
Why choose this attack vector? People aren’t aware of the threat they pose to domains. Therefore, registering all possible versions of our domain name including singular and plural versions, all common domain extensions and hyphenated and non hyphenated word matters.

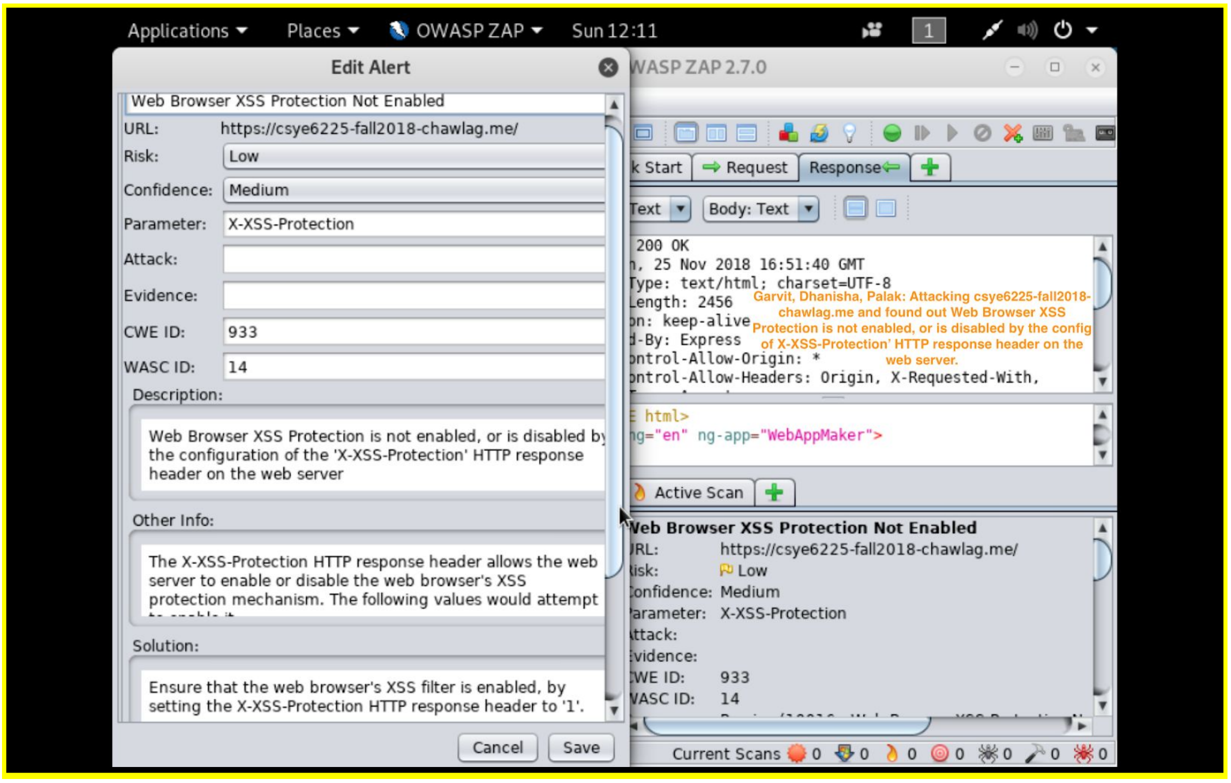
4. <u>**OWASP Top 10 - A3 - Cross-Site Scripting (XSS)**</u>
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server.
Attack Vector: XSS flaws occur when web applications include user provided data in web pages that is sent to the browser without proper sanitization.

If a user search on our web app aren’t correctly sanitized, a malicious user can embed a malicious script in the search.
<script src=”https://csye6225-fall2018-chawlag.me/exploit.js” type=”text/javascript” />

<u>**Solution:**</u> Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'. A very common component to match if your application accepts form input. AWS WAF only evaluates the first 8 KB of the body content.



URL	https://csye6225-fall2018-chawlag.me/
Method	GET
Parameter	X-XSS-Protection
URL	https://csye6225-fall2018-chawlag.me/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
URL	https://csye6225-fall2018-chawlag.me/robots.txt
Method	GET
Parameter	X-XSS-Protection



Web Browser XSS Protection Not Enabled
URL: https://csye6225-fall2018-chawlag.me/
Risk: Low
Confidence: Medium
Parameter: X-XSS-Protection
Attack:
Evidence:
CWE ID: 933
WASC ID: 14

Description:
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Other Info:
The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt

Solution:
Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

```
 200 OK
n, 25 Nov 2018 16:51:40 GMT
Type: text/html; charset=UTF-8
Length: 2456
on: keep-alive
d-By: Express
ontrol-Allow-Origin: *
ontrol-Allow-Headers: Origin, X-Requested-With,
```

Garvit, Dhanisha, Palak: Attacking csye6225-fall2018-chawlag.me and found out Web Browser XSS Protection is not enabled, or is disabled by the config of X-XSS-Protection' HTTP response header on the web server.

```
 html>
ng="en" ng-app="WebAppMaker">
```

Web Browser XSS Protection Not Enabled
URL: https://csye6225-fall2018-chawlag.me/
Risk: Low
Confidence: Medium
Parameter: X-XSS-Protection
Attack:
Evidence:
CWE ID: 933
WASC ID: 14

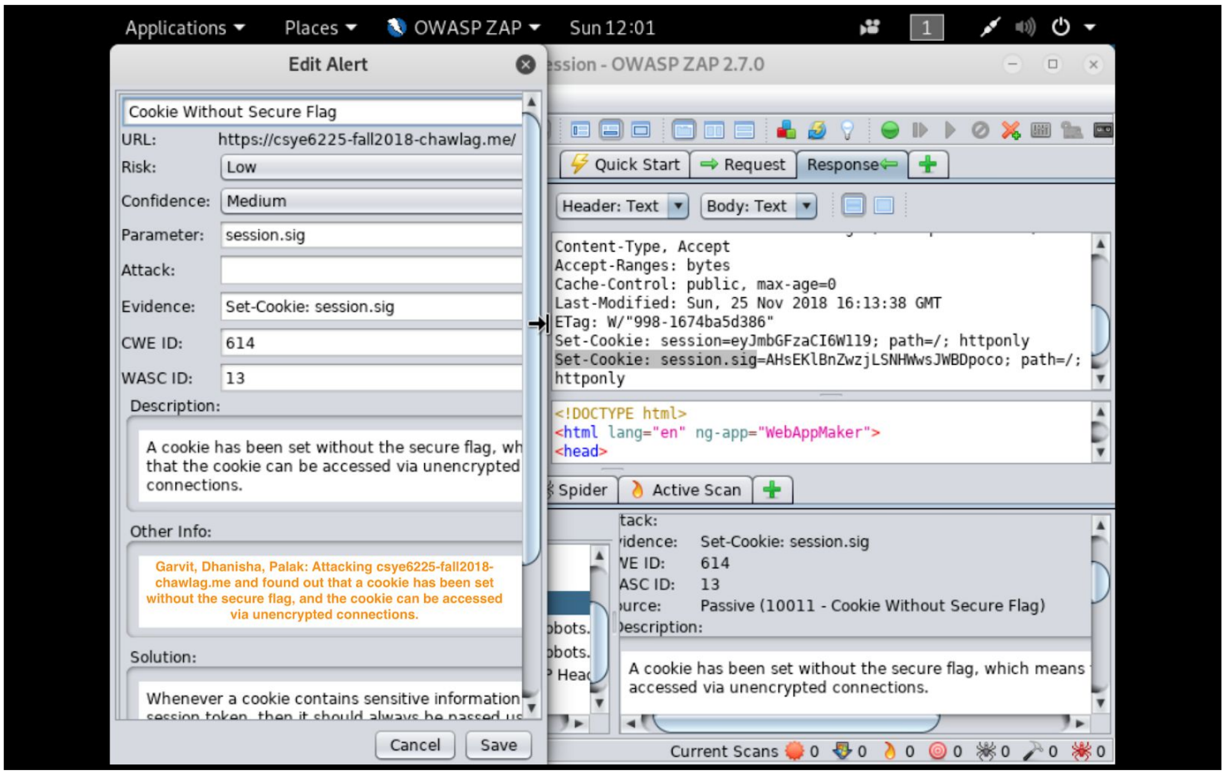
Result: The code then gets executed anytime a legitimate user loads our web page.

Why choose this attack vector? XSS attacks are relatively easy to mitigate in common scenarios because they require specific key HTML tag names in the HTTP request.

Additional Attacks Possible

5. Cookie Without Secure Flag

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.



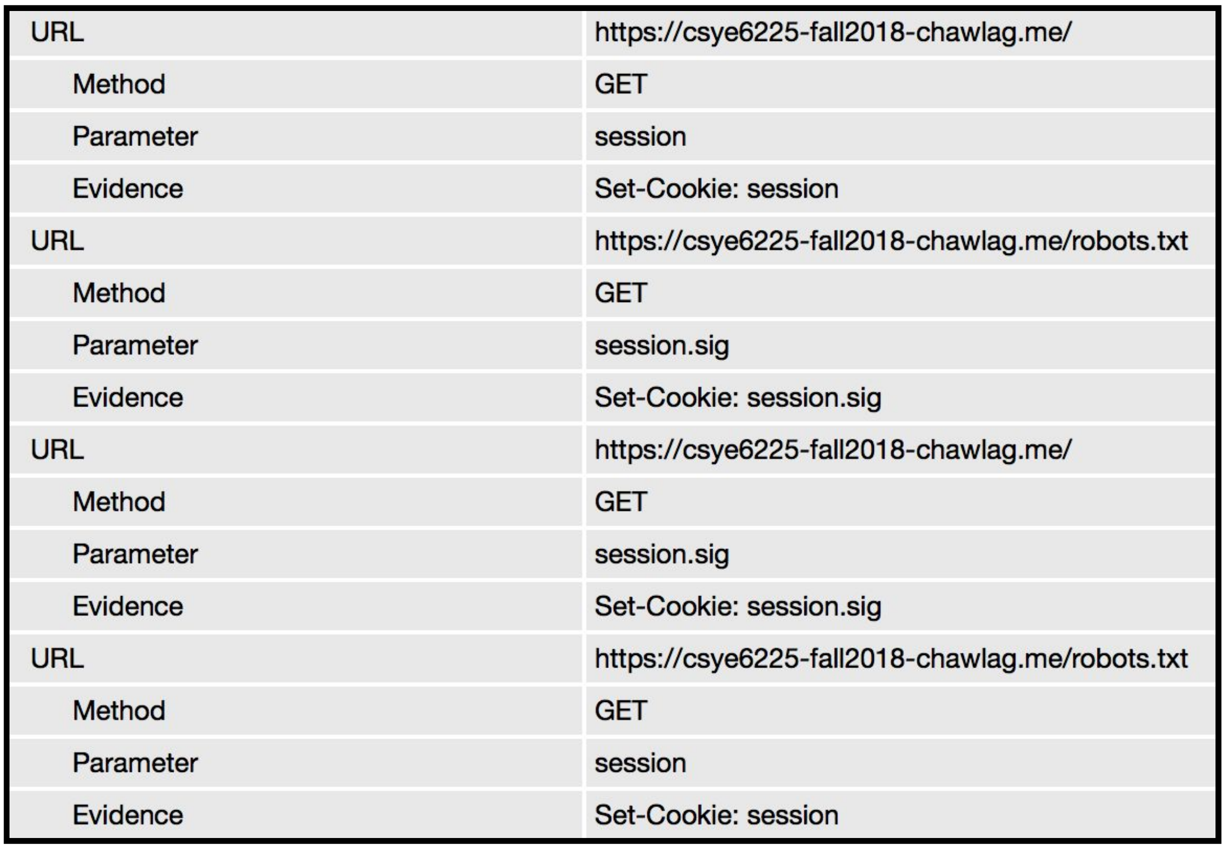
Cookie Without Secure Flag
URL: https://csye6225-fall2018-chawlag.me/
Risk: Low
Confidence: Medium
Parameter: session.sig
Attack:
Evidence: Set-Cookie: session.sig
CWE ID: 614
WASC ID: 13
Description:
A cookie has been set without the secure flag, wh
that the cookie can be accessed via unencrypted
connections.
Other Info:
Garvit, Dhanisha, Palak: Attacking csye6225-fall2018-chawlag.me and found out that a cookie has been set without the secure flag, and the cookie can be accessed via unencrypted connections.
Solution:
Whenever a cookie contains sensitive information

```
Content-Type, Accept
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sun, 25 Nov 2018 16:13:38 GMT
ETag: W/"998-1674ba5d386"
Set-Cookie: session=eyJmbGFzaCI6W119; path=/; httponly
Set-Cookie: session.sig=AHsEKlBnZwzjLSNHWwsJWBDpoco; path=/;
httponly
```

```
<!DOCTYPE html>
<html lang="en" ng-app="WebAppMaker">
<head>
```

tack:
idence: Set-Cookie: session.sig
VE ID: 614
ASC ID: 13
urce: Passive (10011 - Cookie Without Secure Flag)
escription:
A cookie has been set without the secure flag, which means
accessed via unencrypted connections.

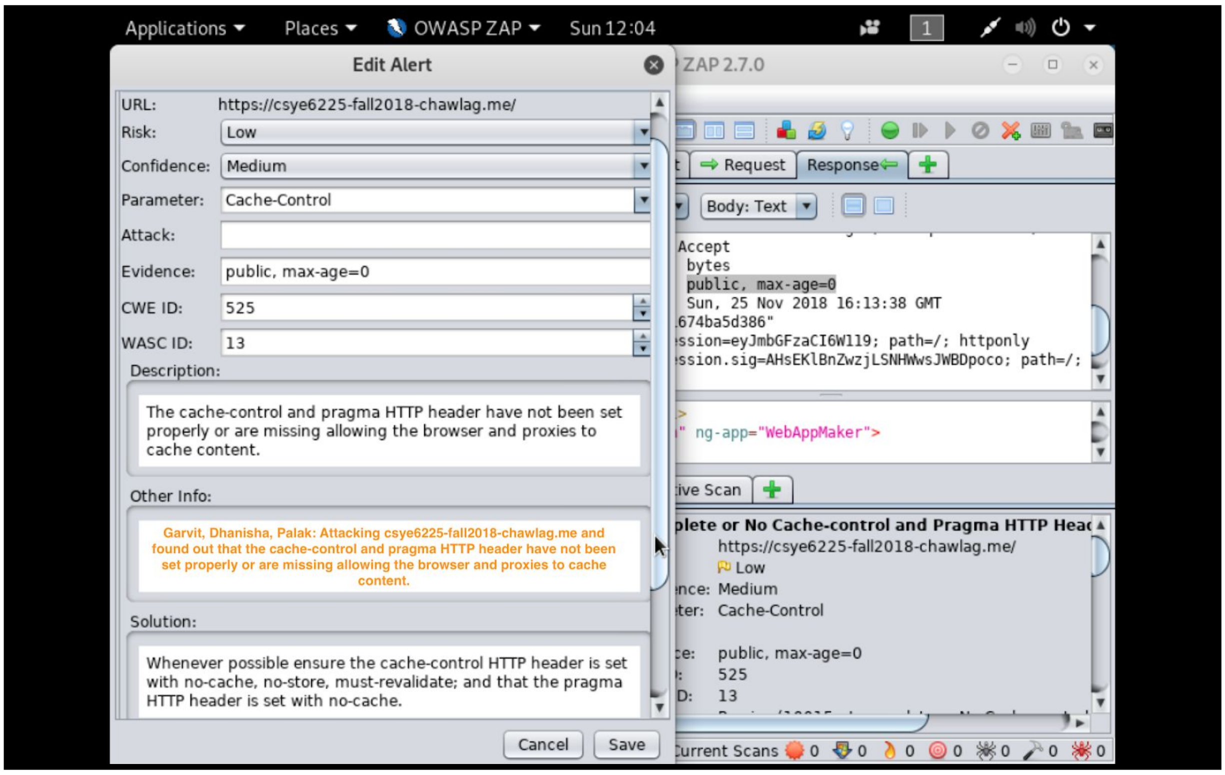
Solution: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.



URL	https://csye6225-fall2018-chawlag.me/
Method	GET
Parameter	session
Evidence	Set-Cookie: session
URL	https://csye6225-fall2018-chawlag.me/robots.txt
Method	GET
Parameter	session.sig
Evidence	Set-Cookie: session.sig
URL	https://csye6225-fall2018-chawlag.me/
Method	GET
Parameter	session.sig
Evidence	Set-Cookie: session.sig
URL	https://csye6225-fall2018-chawlag.me/robots.txt
Method	GET
Parameter	session
Evidence	Set-Cookie: session

6. **Incomplete or No Cache-control and Pragma HTTP Header Set**
The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

Solution: Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.


URL: https://csye6225-fall2018-chawlag.me/

Risk: Low

Confidence: Medium

Parameter: Cache-Control

Attack:

Evidence: public, max-age=0

CWE ID: 525

WASC ID: 13

Description:

The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

Other Info:

Garvit, Dhanisha, Palak: Attacking csye6225-fall2018-chawlag.me and found out that the cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

Solution:

Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.

```
Accept
 bytes
 public, max-age=0
 Sun, 25 Nov 2018 16:13:38 GMT
674ba5d386"
ssion=eyJmbGFzaCI6W119; path=/; httponly
ssion.sig=AHsEKlBnZwzjLSNHWwsJWBDpoco; path=/;
```

```
" ng-app="WebAppMaker">
```

plete or No Cache-control and Pragma HTTP Heac

https://csye6225-fall2018-chawlag.me/

Low

nce: Medium

ter: Cache-Control

e: public, max-age=0

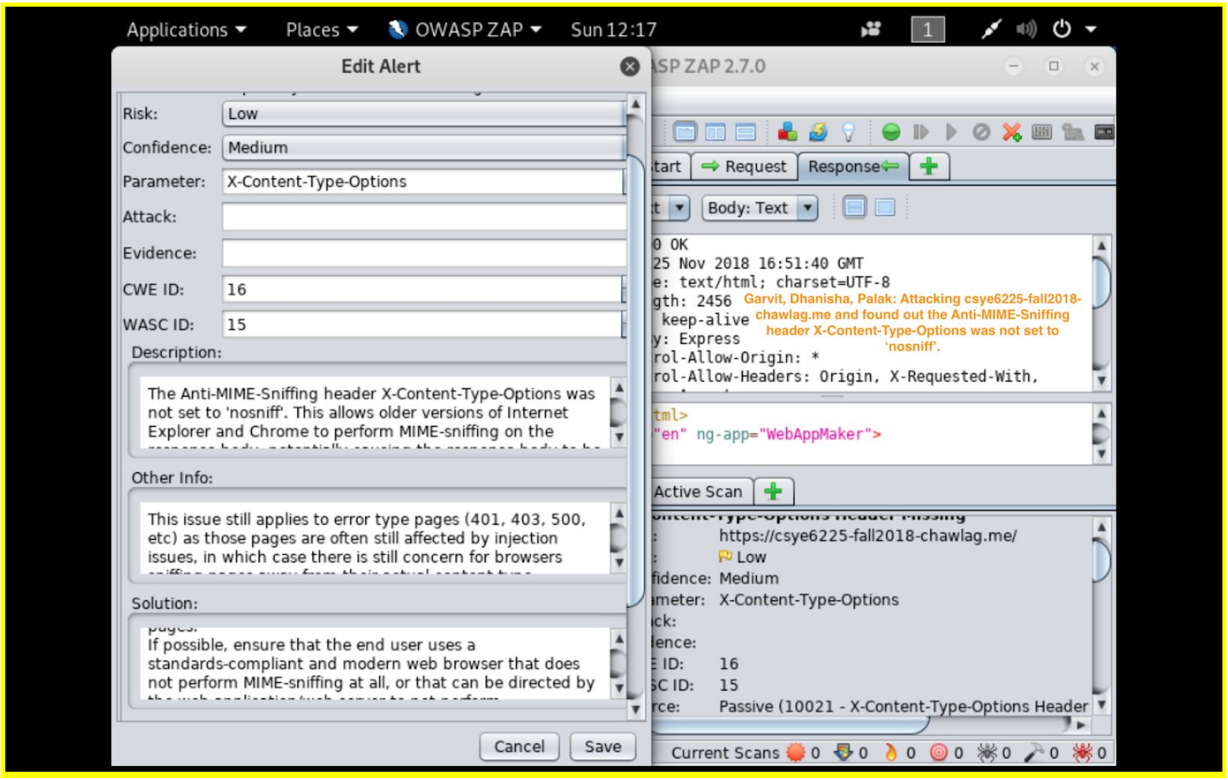
: 525

D: 13

7. **X-Content-Type-Options Header Missing**

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.



Risk: Low
Confidence: Medium
Parameter: X-Content-Type-Options
Attack:
Evidence:
CWE ID: 16
WASC ID: 15

Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the

Other Info:

This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers

Solution:

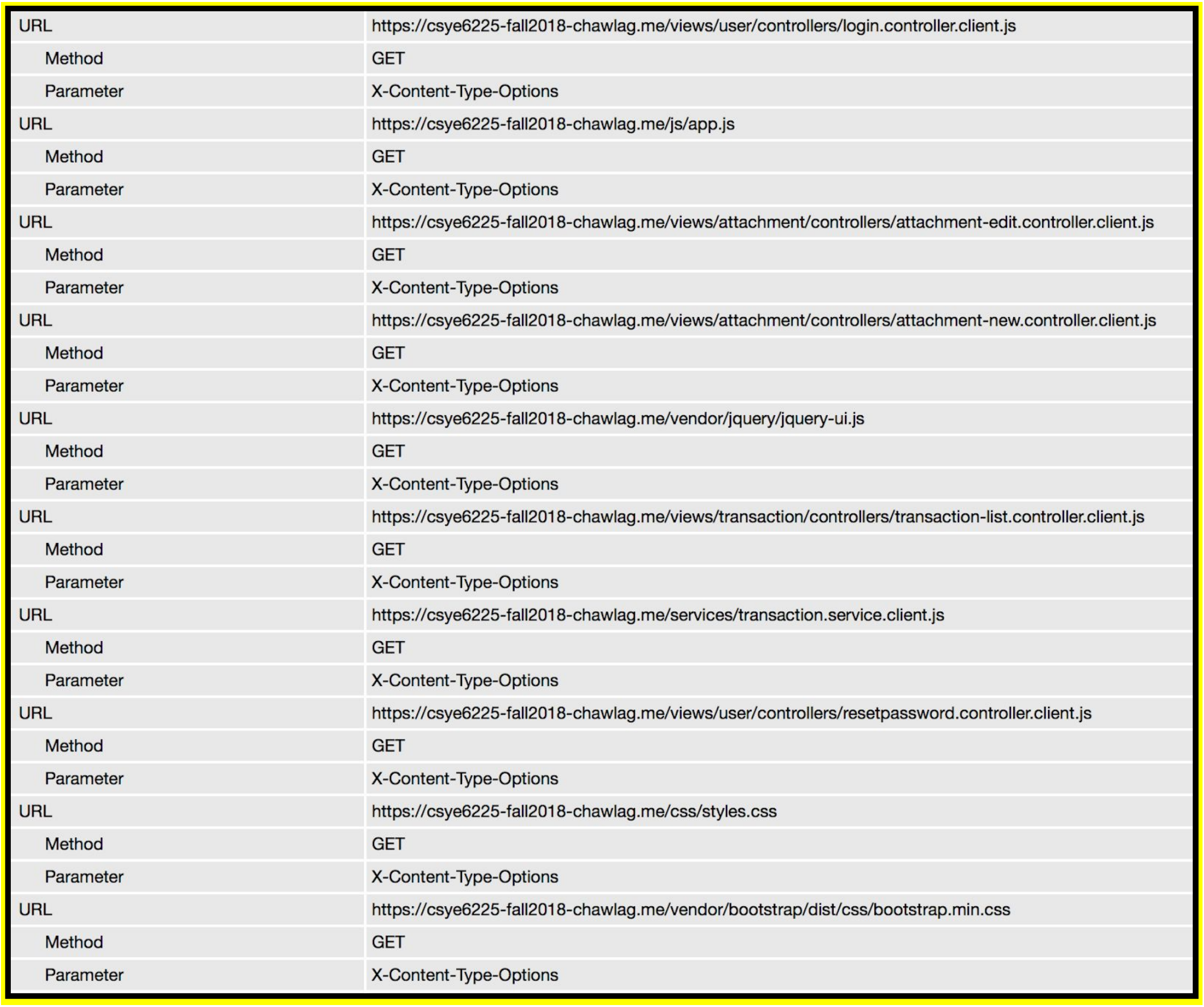
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by

```
0 OK
25 Nov 2018 16:51:40 GMT
e: text/html; charset=UTF-8
gth: 2456
 keep-alive
y: Express
rol-Allow-Origin: *
rol-Allow-Headers: Origin, X-Requested-With,
```

Garvit, Dhanisha, Palak: Attacking csye6225-fall2018-chawlag.me and found out the Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.

```
tml>
"en" ng-app="WebAppMaker">
```

https://csye6225-fall2018-chawlag.me/
Low
fidence: Medium
meter: X-Content-Type-Options
ck:
ence:
E ID: 16
C ID: 15
rce: Passive (10021 - X-Content-Type-Options Header

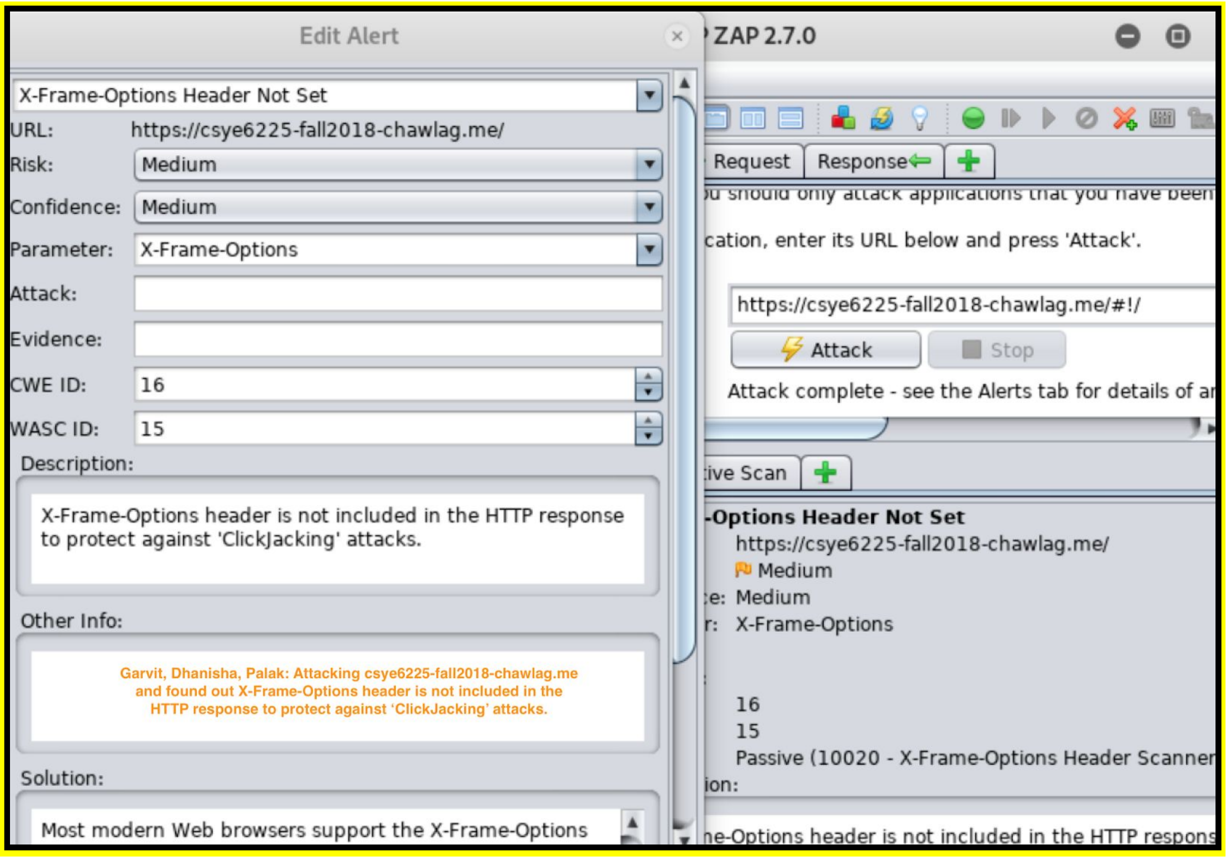


URL	https://csye6225-fall2018-chawlag.me/views/user/controllers/login.controller.client.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/js/app.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/views/attachment/controllers/attachment-edit.controller.client.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/views/attachment/controllers/attachment-new.controller.client.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/vendor/jquery/jquery-ui.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/views/transaction/controllers/transaction-list.controller.client.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/services/transaction.service.client.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/views/user/controllers/resetpassword.controller.client.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/css/styles.css
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chawlag.me/vendor/bootstrap/dist/css/bootstrap.min.css
Method	GET
Parameter	X-Content-Type-Options

8. **<u>X-Frame-Options Header Not Set</u>**
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

URL	https://csye6225-fall2018-chawlag.me/
Method	GET
Parameter	X-Frame-Options

<u>Solution</u>: Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site.



X-Frame-Options Header Not Set
URL: https://csye6225-fall2018-chawlag.me/
Risk: Medium
Confidence: Medium
Parameter: X-Frame-Options
Attack:
Evidence:
CWE ID: 16
WASC ID: 15
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Other Info:
Garvit, Dhanisha, Palak: Attacking csye6225-fall2018-chawlag.me and found out X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Solution:
Most modern Web browsers support the X-Frame-Options

ou should only attack applications that you have been
cation, enter its URL below and press 'Attack'.
https://csye6225-fall2018-chawlag.me/#!/
Attack complete - see the Alerts tab for details of ar
-Options Header Not Set
https://csye6225-fall2018-chawlag.me/
Medium
e: Medium
r: X-Frame-Options
16
15
Passive (10020 - X-Frame-Options Header Scanner
ion:
ne-Options header is not included in the HTTP respons

<u>References</u>:
1. OWASP Top 10 - 2017
2. https://www.kali.org
3. https://tools.kali.org
4. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
5. https://d0.awsstatic.com/whitepapers/Security/aws-waf-owasp.pdf