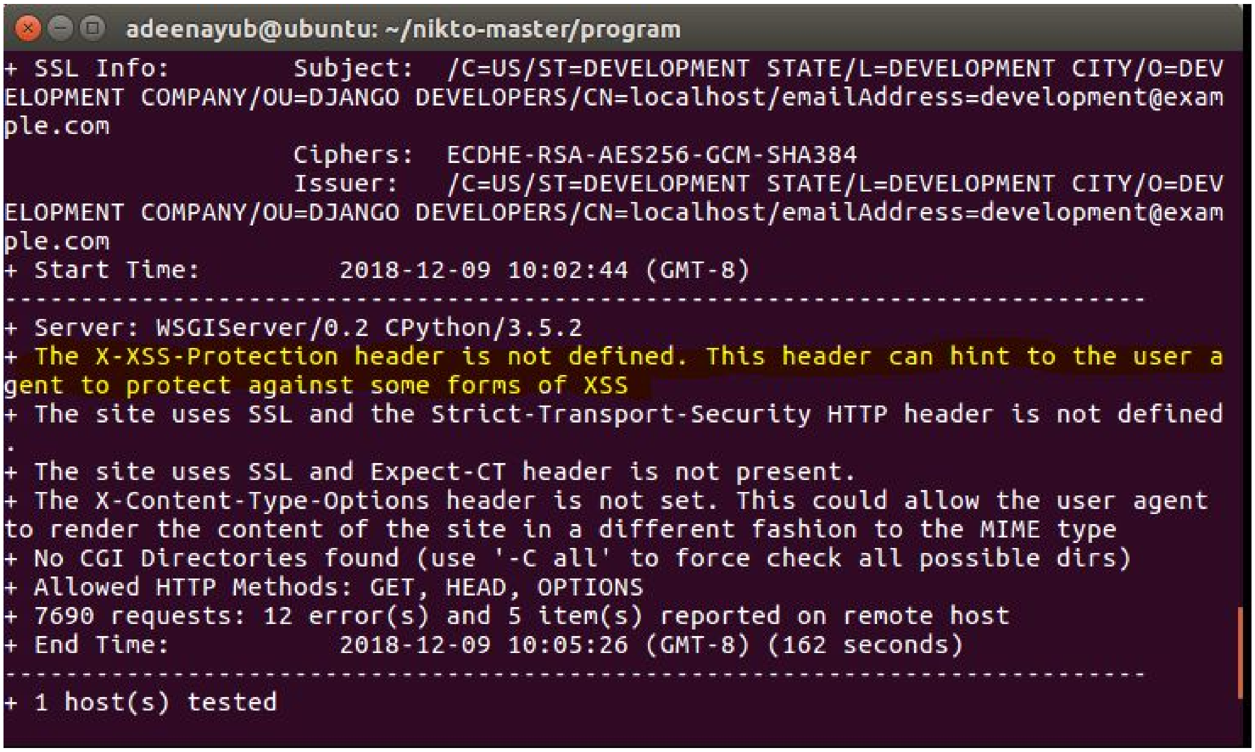
Lasya Namineni (ln1026)
Adeen Ayub(aa6243)

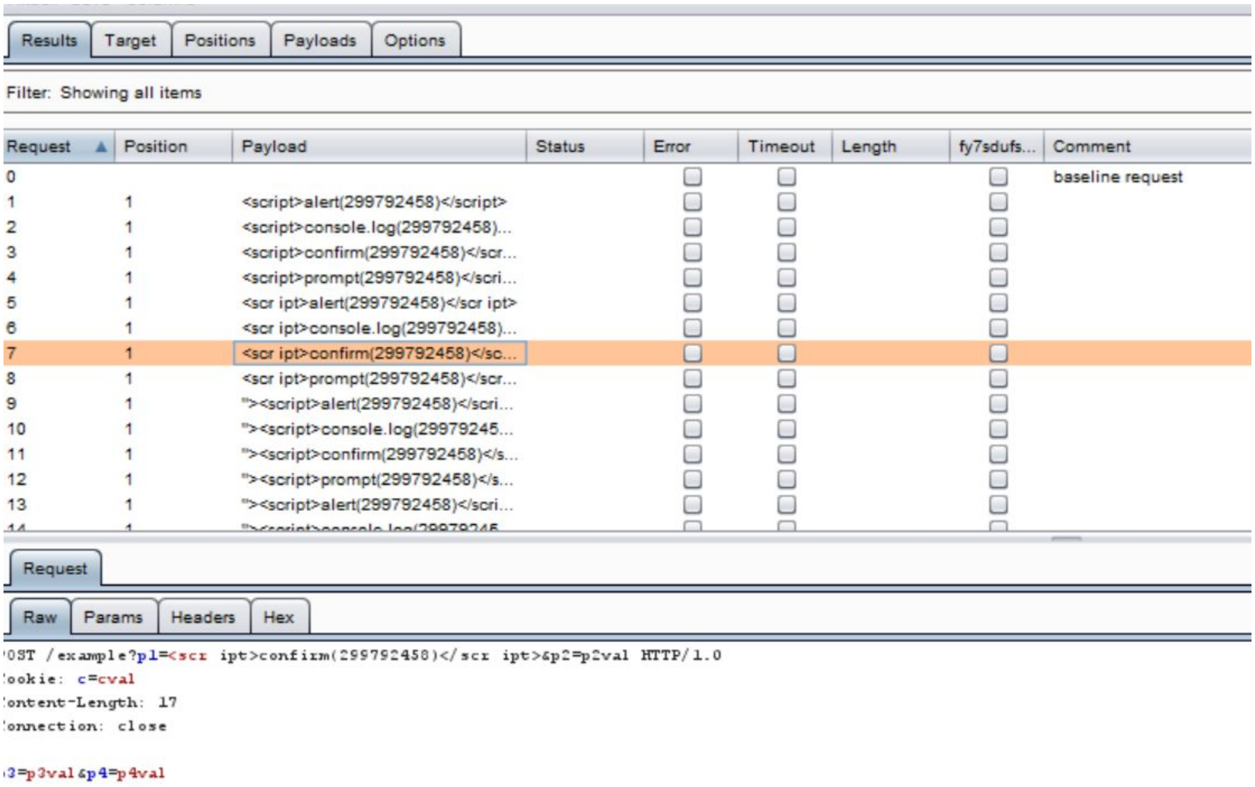
Security Assessment Results

1.X-XSS-Protection header is not defined.



```
+ SSL Info:        Subject:  /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
+ Start Time:         2018-12-09 10:02:44 (GMT-8)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.5.2
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS
+ 7690 requests: 12 error(s) and 5 item(s) reported on remote host
+ End Time:           2018-12-09 10:05:26 (GMT-8) (162 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- **Status:**
    - **Completed**- The vulnerability has been removed.
- **Source:**.This vulnerability was found through vulnerability assessment.
- **Risk:** The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- **Business Impact Statement:** This vulnerability, if exploited, can cause attacks like stealing legitimate user session cookies through which the attackers can impersonate them and access sensitive information. Other common attacks include stealing user credentials, exfiltrating sensitive data and performing unauthorised operations.
- **Recommended Corrective Action:** Use XSS Filter which can block the malicious script from loading. Another recommended action is to immediately expire a session if the user is logged in from different IP addresses.
- **Link to Control(s)/Test Case(s):** Below shown is the screenshot of xss attack. The attack couldn’t pass through.



Filter: Showing all items

Request ▲	Position	Payload	Status	Error	Timeout	Length	fy7sdufs...	Comment
0				□	□		□	baseline request
1	1	<script>alert(299792458)</script>		□	□		□	
2	1	<script>console.log(299792458)...		□	□		□	
3	1	<script>confirm(299792458)</scr...		□	□		□	
4	1	<script>prompt(299792458)</scri...		□	□		□	
5	1	<scr ipt>alert(299792458)</scr ipt>		□	□		□	
6	1	<scr ipt>console.log(299792458)...		□	□		□	
7	1	<scr ipt>confirm(299792458)</sc...		□	□		□	
8	1	<scr ipt>prompt(299792458)</scr...		□	□		□	
9	1	"><script>alert(299792458)</scri...		□	□		□	
10	1	"><script>console.log(29979245...		□	□		□	
11	1	"><script>confirm(299792458)</s...		□	□		□	
12	1	"><script>prompt(299792458)</s...		□	□		□	
13	1	"><script>alert(299792458)</scri...		□	□		□	
14	1	"><script>console.log(29979245		□	□		□	

```
'OST /example?p1=<scr ipt>confirm(299792458)</scr ipt>&p2=p2val HTTP/1.0
:ookie: c=cval
:ontent-Length: 17
:onnection: close

:3=p3val&p4=p4val
```

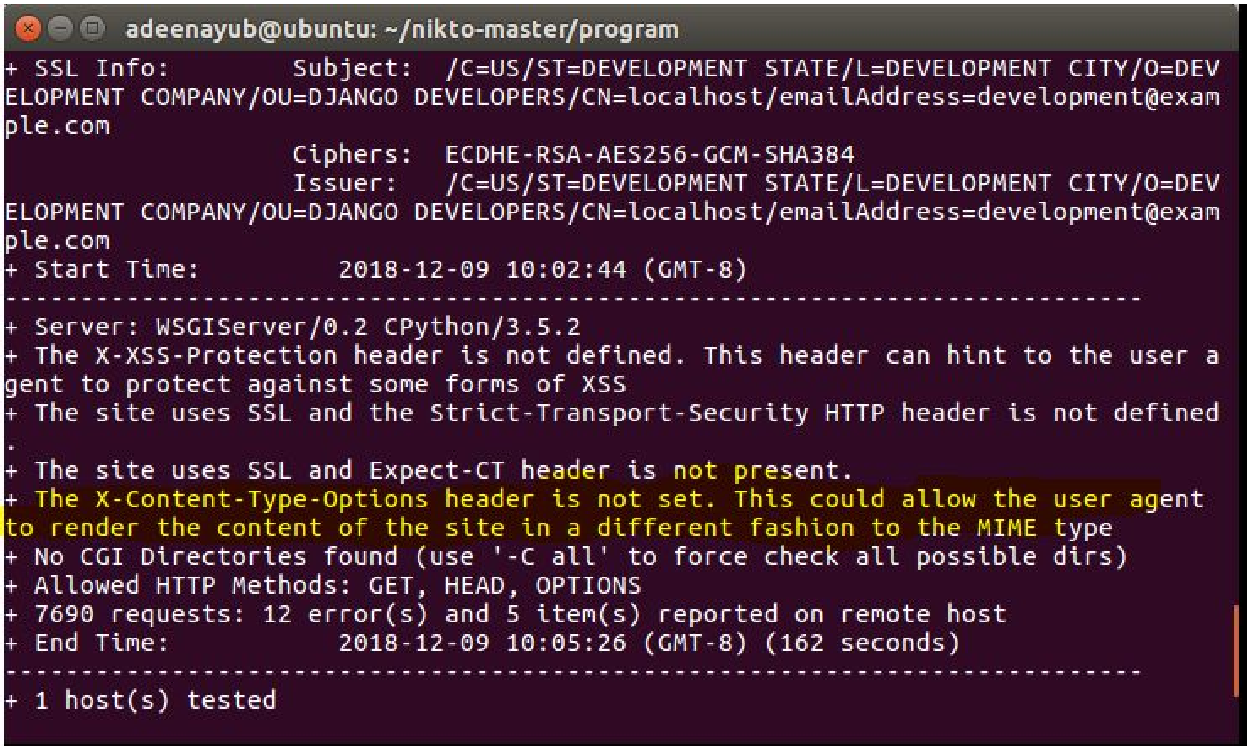
- **Likelihood: High**

- **Impact:** High

Risk Level: High

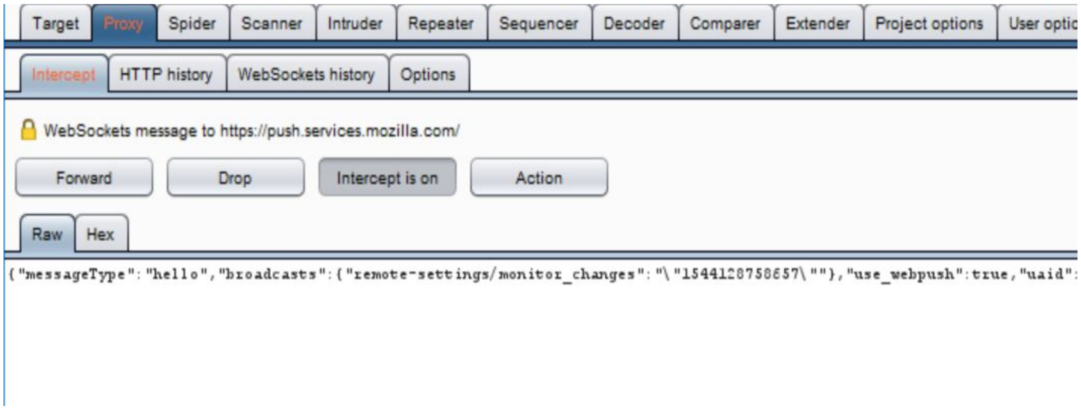
2. The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

Lasya Namineni (ln1026)
Adeen Ayub(aa6243)



```
+ SSL Info:        Subject:  /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
+ Start Time:         2018-12-09 10:02:44 (GMT-8)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.5.2
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS
+ 7690 requests: 12 error(s) and 5 item(s) reported on remote host
+ End Time:           2018-12-09 10:05:26 (GMT-8) (162 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Status : Completed
- Source: This vulnerability was found by vulnerability assessment.
- Risk: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
- Business Impact Statement: Can result in MIME attacks which are common with websites that allow user uploaded content to be published on the websites. Attackers can perform XSS attacks by injecting malicious code in files that are acceptable by the website ultimately causing the victim to execute the code by downloading the file.
- Recommended Corrective Action: Set the X-Content-Type-Options: nosniff header
- Link to control(s)/Test Case(s): was able to intercept the request when tested in burp suite



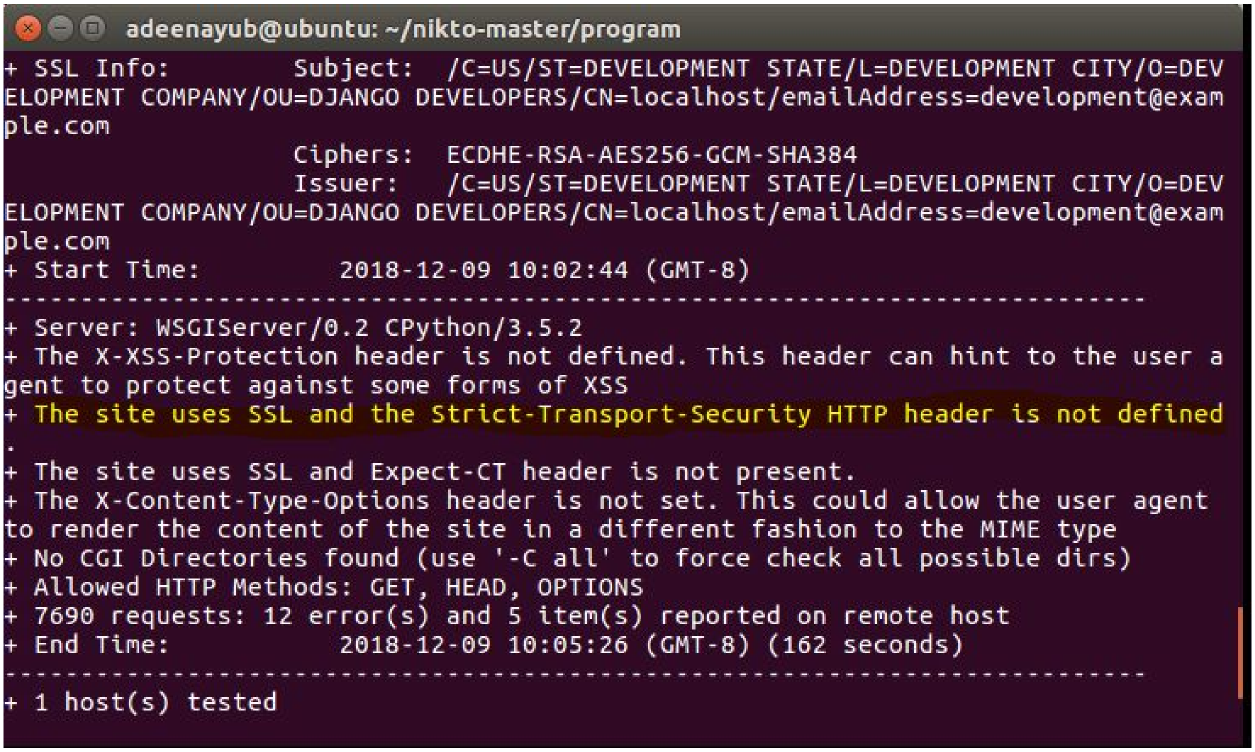
WebSockets message to https://push.services.mozilla.com/

```
{"messageType":"hello","broadcasts":{"remote-settings/monitor_changes":"\"1544128758657\""},"use_webpush":true,"uaid":
```

- Likelihood: Moderate
- Impact: High

- Risk Level; High

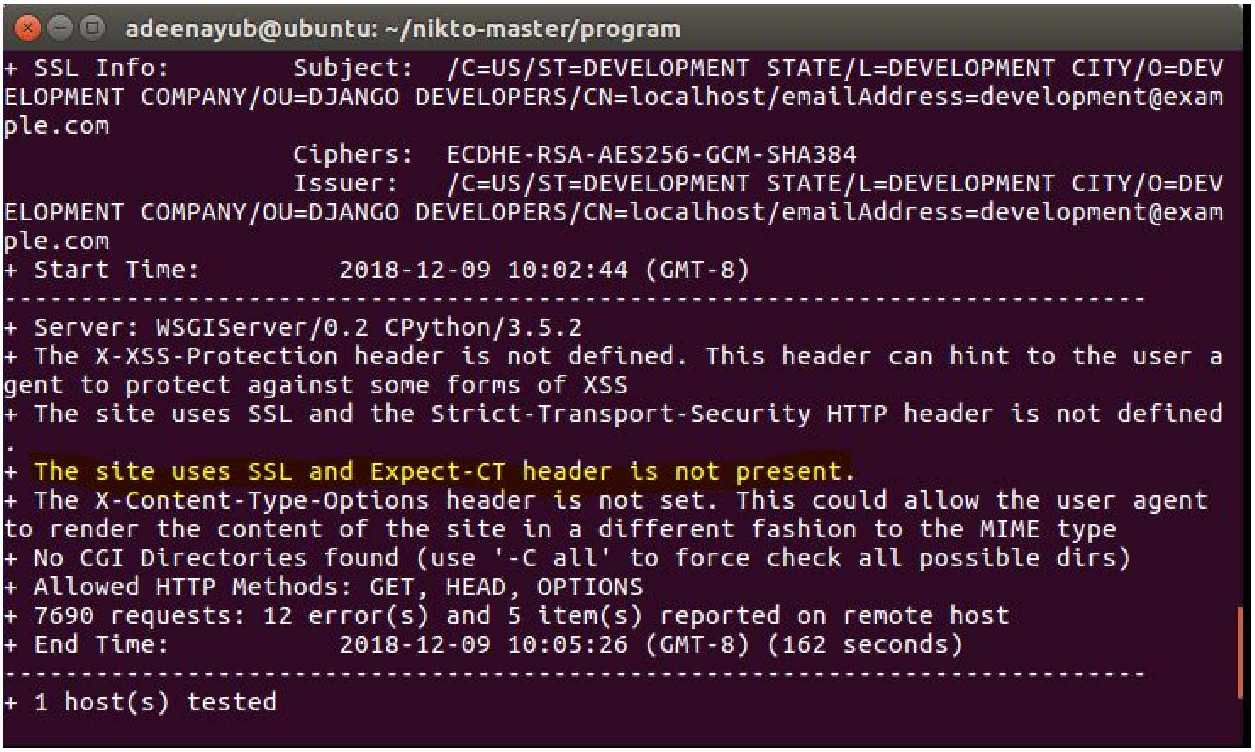
3- The site uses SSL and the Strict-Transport-Security HTTP header is not defined



```
+ SSL Info:        Subject:  /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
+ Start Time:         2018-12-09 10:02:44 (GMT-8)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.5.2
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS
+ 7690 requests: 12 error(s) and 5 item(s) reported on remote host
+ End Time:           2018-12-09 10:05:26 (GMT-8) (162 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Status : Completed
- Source :This vulnerability was found by vulnerability assessment.
- Risk: The site uses SSL and the Strict-Transport-Security HTTP header is not defined
- Business Impact Statement: Can result in SSLstrip attack enabling the attackers to downgrade a website from https to http without the user ever knowing. When a user visits the website, the attacker can redirect all https links to http and ultimately intercept all communication that takes place between the user and the website server. This can leak important information such as passwords, credit card credentials etc.
- Recommended Corrective Action: Set HSTS header which instructs the browser to strictly access pages on the websites via https(with an expiration date). In our case, we used the following header. SECURE_HSTS_SECONDS = 3153600
- Likelihood: Moderate
- Impact: High
- Risk Level; Moderate

4- The site uses SSL and Expect-CT header is not present.

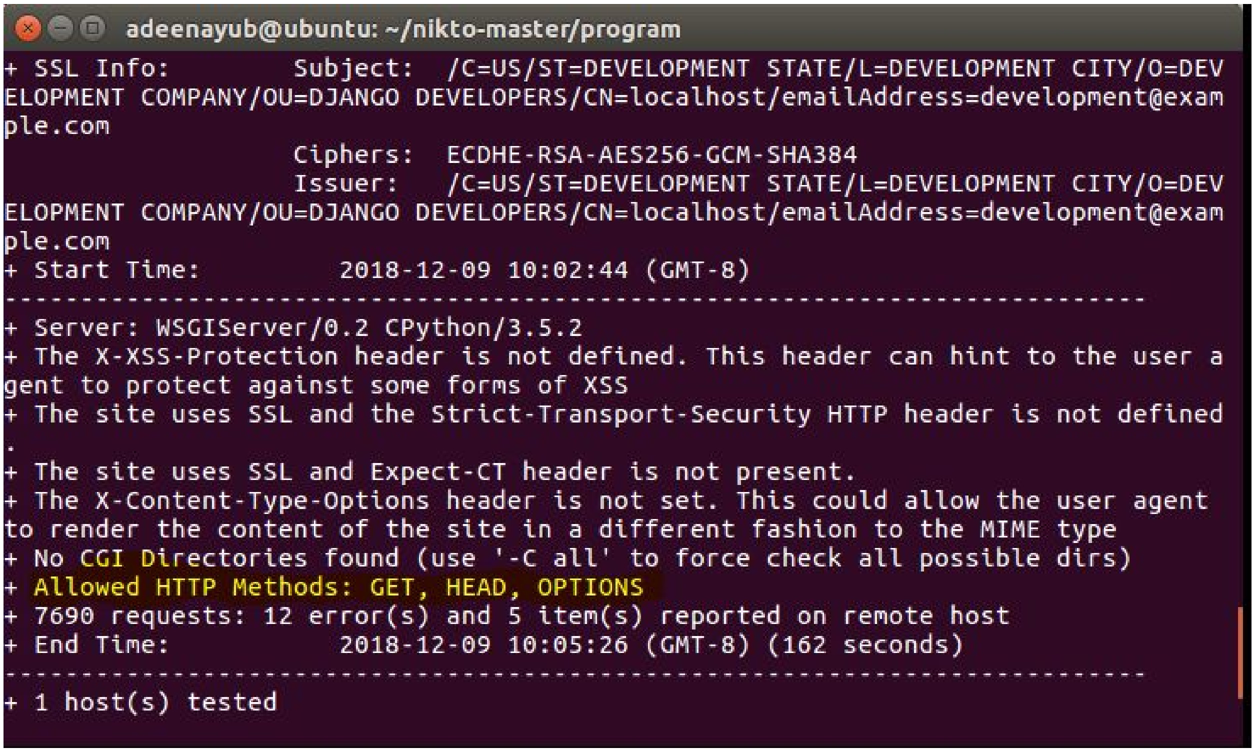


```
+ SSL Info:        Subject:  /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
+ Start Time:         2018-12-09 10:02:44 (GMT-8)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.5.2
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS
+ 7690 requests: 12 error(s) and 5 item(s) reported on remote host
+ End Time:           2018-12-09 10:05:26 (GMT-8) (162 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Status: Active
- Source:This vulnerability was found by vulnerability assessment.
- Risk: The site uses SSL and Expect-CT header is not present.
- Business Impact Statement: Can cause invalid or expired certificates to be issued for a website.
- Recommended Corrective Action: Use Expect-CT header so the webserver can respond to such violations
- Likelihood: Moderate to Low
- Impact: Low
- Risk Level; Low

Lasya Namineni (ln1026)
Adeen Ayub(aa6243)

5- Allowed HTTP Methods: GET, HEAD, OPTIONS



```
+ SSL Info:        Subject:  /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/ST=DEVELOPMENT STATE/L=DEVELOPMENT CITY/O=DEV
ELOPMENT COMPANY/OU=DJANGO DEVELOPERS/CN=localhost/emailAddress=development@exam
ple.com
+ Start Time:         2018-12-09 10:02:44 (GMT-8)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.5.2
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS
+ 7690 requests: 12 error(s) and 5 item(s) reported on remote host
+ End Time:           2018-12-09 10:05:26 (GMT-8) (162 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Status : Rejected
- Source:This vulnerability was found by vulnerability assessment.
- Risk: Allowed HTTP Methods: GET, HEAD, OPTIONS
- Business Impact Statement: GET and HEAD alone are safe to use. Attackers can use OPTIONS as a shortcut to find another vulnerability but the method itself isn’t.
- Recommended Corrective Action: Disable Options if not needed.
- Likelihood: Low
- Impact: Low
- Risk Level; Low