Exploiting cross-site scripting to steal cookies

Explanation

Stealing cookies is a traditional way to exploit XSS. Most web applications use cookies for session handling. You can exploit cross-site scripting vulnerabilities to send the victim's cookies to your own domain, then manually inject the cookies into the browser and impersonate the victim.

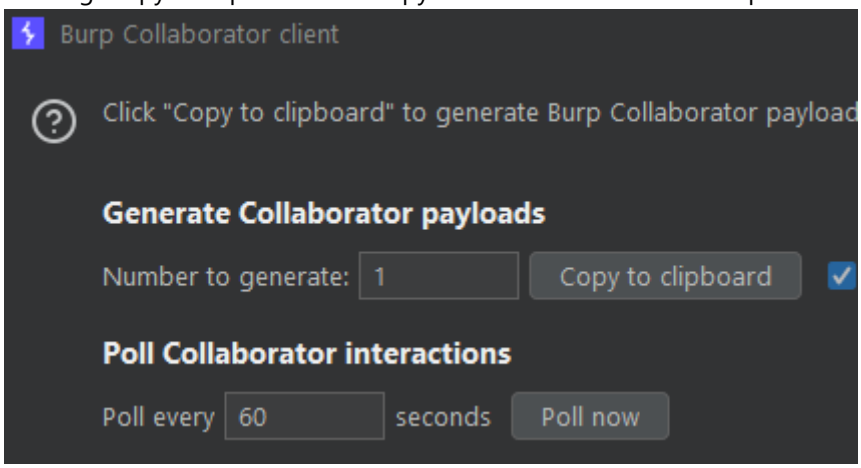
In practice, this approach has some significant limitations:

- The victim might not be logged in.
- Many applications hide their cookies from JavaScript using the `HttpOnly` flag.
- Sessions might be locked to additional factors like the user's IP address.
- The session might time out before you're able to hijack it.

Lab

Dial up a collaborator session

Clicking "copy to clipboard" will copy the domain information required for the cookie theft script.

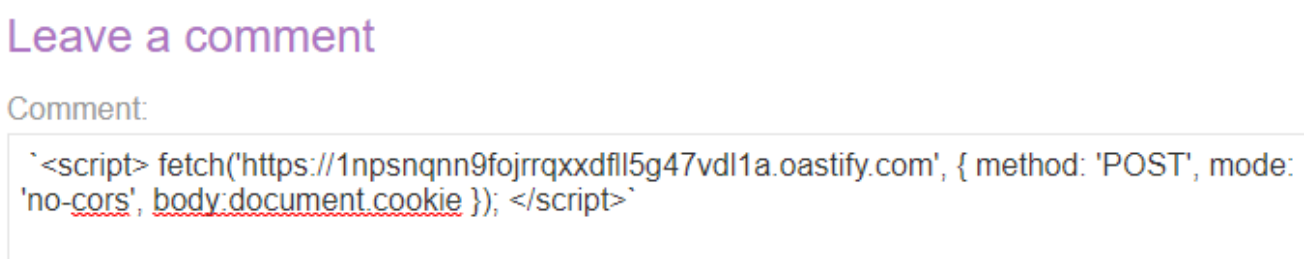


I used the following script from the guide

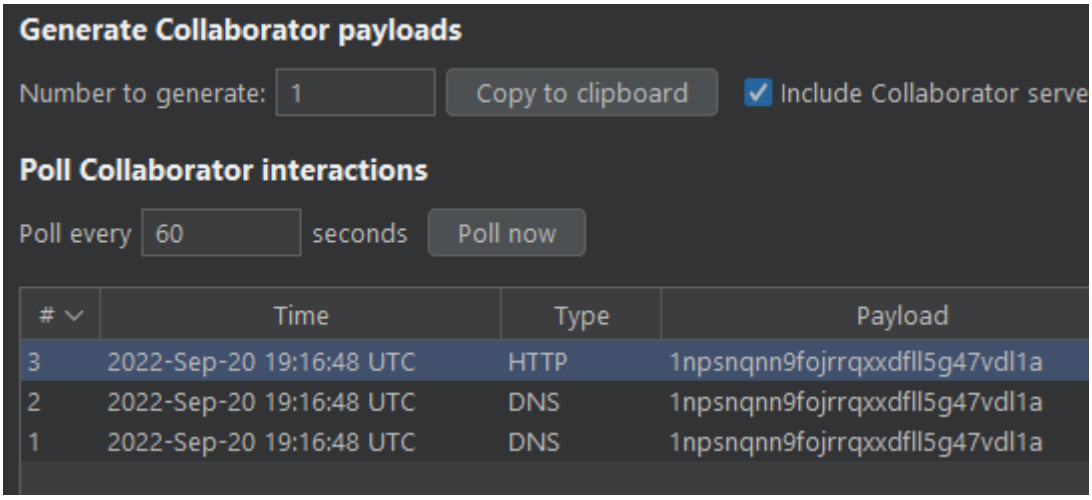
I wasn't sure on the best script to use so the solution guide gave me a hint.

`![[Pasted image 20220920203413.png]]`

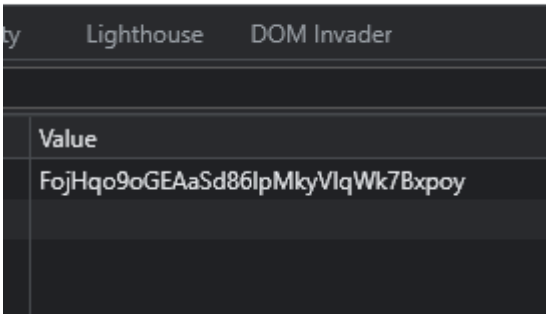
Paste into the comments and post



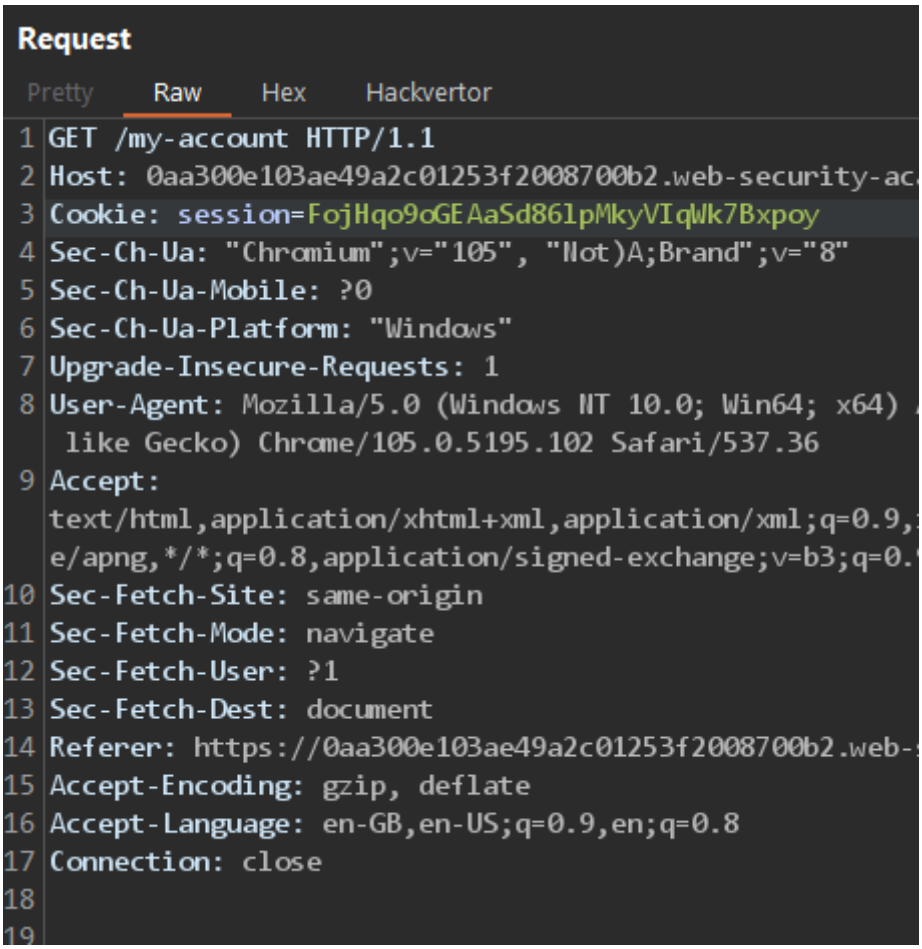
Back in collaborator, click 'poll now' to refresh and then review the HTTP requests.



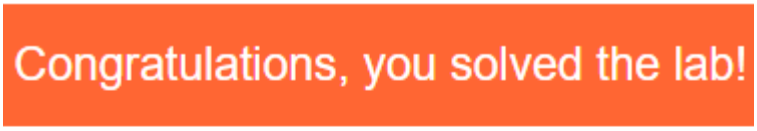
Paste the session token into the cookie value field in F12 developer tools and refresh.



You can use repeater as well..



A wild admin should now appear



My Account

Your username is: administrator