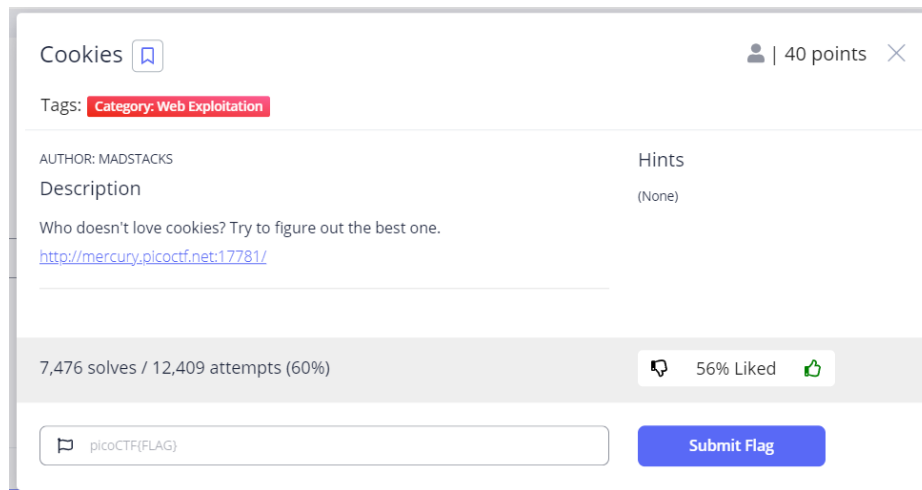


PicoCTF Web Exploitation Assessment

IE2062 – Web Security

Student Registration Number	Student Name
	Aththanayaka P.A.G.P.B.

In this report I am going to explain how I did a simple CTF activity related to cookies. This particular CTF was provided by PicoCTF and category of this CTF is Web Exploitation. Cookies is the name of this activity, and 40 points will be given to the users who will be able to capture the flag successfully. There are no hints provided with this activity.



There is a small description within the details of this activity saying,

Who doesn't love cookies? Try to figure out the best one.

And also, there is a link below the description. That is the link of the site which contains the flag we want to find out. As the last part of this information box, there is a space to put the flag and submit.

Tools

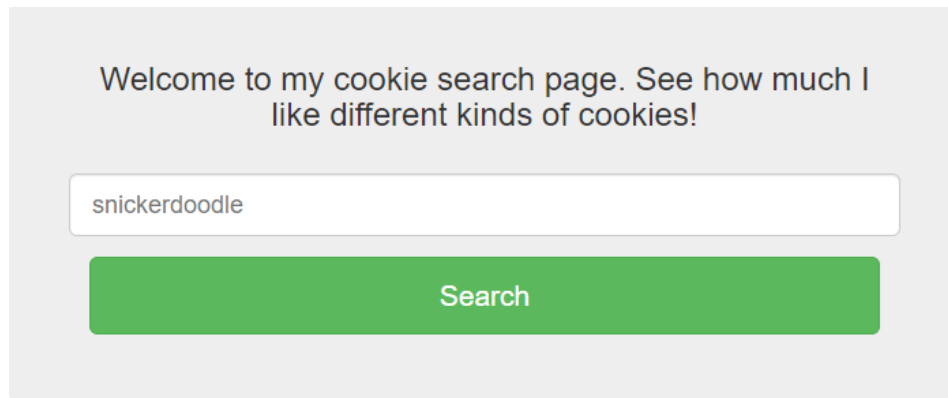
I found two tools to do this activity

1. Edit this cookie
2. Burp Suit

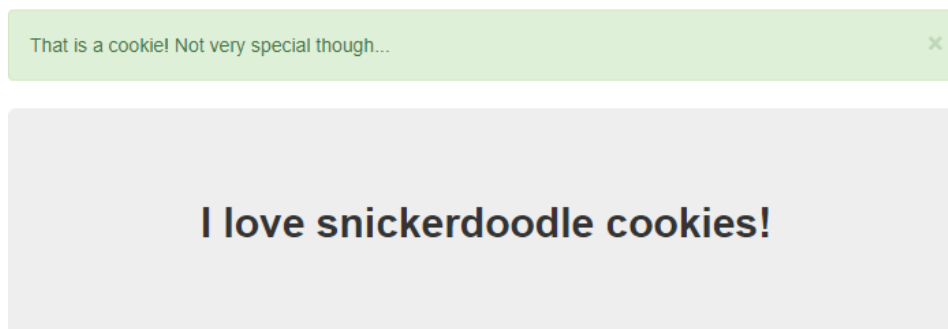
Edit this cookie is a cookie management extension which we can see the cookie details and edit them within the browser. Burp Suit is the most popular vulnerability finder and proxy-based tool which used to check the security state of web-based applications. In my opinion, use Edit this cookie extension is the easiest way to find the flag of this activity.

Solution

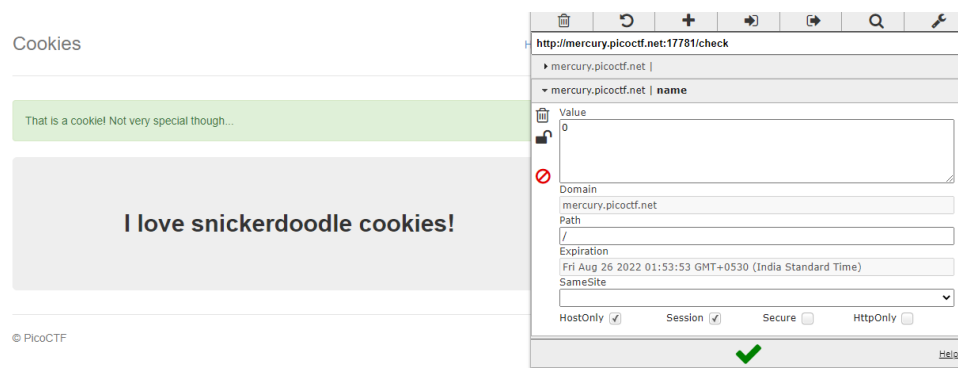
In the first page, we can see this content. There is a text box and a search box. We have to type snickerdoodle and click search to go the next page.

A screenshot of a web page with a light gray background. At the top, it says "Welcome to my cookie search page. See how much I like different kinds of cookies!". Below this is a white text input field containing the text "snickerdoodle". Underneath the input field is a green rectangular button with the word "Search" in white text.

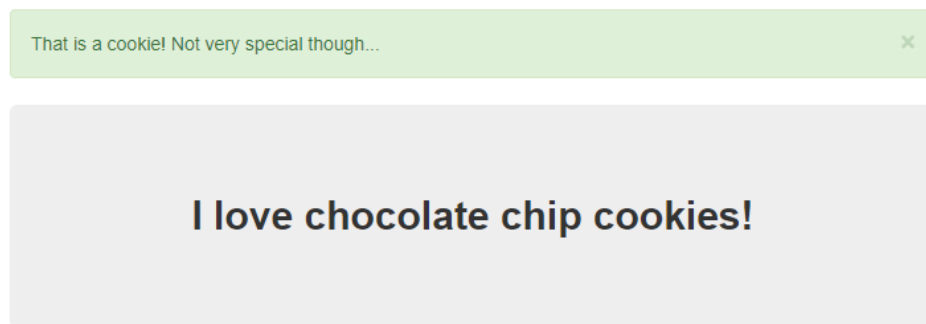
When we click search button, we will be redirected to the next page which displays this sentence. We can see the cookie type we entered in the previous step displays as a part of that sentence. Therefore, we can assume that word is saved as a cookie in our browser.



As the next step we can open Edit this cookie extension in my browser. It will display some details about the cookies along with the name value, domain, and the expiration details. Name value of this cookie is shown as 0. Therefore, we can assume that the cookie name of the word 'snickerdoodle' is 0.



Then we can change the value of cookie name and see whether the sentence is changing. As an example, if we put 1 as the value of cookie name, the sentence will be change like this



As the next step, we need to find how many cookies are there in this activity. To find that there is no other way than using the brute force method. By using brute force method, we can see that an error will be displayed when we enter 29 as the value of the cookie name.



Therefore, we can assume that there are only 28 cookies in this activity.

As the next step we have to use brute force method and enter all the values between 1 to 28 as the cookie name value and check whether we can find a flag.

The following are the values obtained by entering the cookie name values from 1 to 28.



1. I love chocolate chip cookies!
2. I love oatmeal raisin cookies!
3. I love gingersnap cookies!
4. I love shortbread cookies!
5. I love peanut butter cookies!
6. I love whoopie pie cookies!
7. I love sugar cookies!
8. I love molasses cookies!
9. I love kiss cookies!
10. I love biscotti cookies!
11. I love butter cookies!
12. I love spritz cookies!
13. I love snowball cookies!
14. I love drop cookies!
15. I love thumbprint cookies!
16. I love pinwheel cookies!
17. I love wafer cookies!
18. Flag: picoCTF{3[REDACTED]35}
19. I love macaroon cookies!
20. I love fortune cookies!
21. I love crinkle cookies!
22. I love icebox cookies!
23. I love gingerbread cookies!
24. I love tassie cookies!
25. I love lebkuchen cookies!
26. I love macaron cookies!
27. I love black and white cookies!
28. I love white chocolate macadamia cookies!

As we can see in the 18th time, we were able to find the flag of this activity. Therefore,

Flag: picoCTF{3[REDACTED]35}

should be the correct answer. By entering this flag into the submission box, I explained earlier we can check whether it is the correct answer.



 | 40 points 

As in the picture above I was able to gain 40 points by entering the flag I found which was in the 18th cookie.

Other methods to solve this activity

1. By using Burp Suit also, we can capture this flag. By using the proxy tab, we can capture the request and change the cookie name and forward it to the server. It is very similar to the process I did using the Edit this cookie extension.
2. By using a script also, we can solve this activity. It gives all the results at the same time, but it is bit complex than the brute forcing method.

.....

Thankyou