HACETTEPE UNIVERSITY

COMPUTER ENGINEERING DEPARTMENT

BBM459 SECURE PROGRAMMING LAB - 2023 SPRING

Assignment 4

May 13, 2023

Student names:	*Student Numbers:*
Yiğit Emir İŞIKÇI	2200356028
Abdullah Mert DİNÇER	2200356016

1 Problem Definition

The primary aim of this assignment is to gain a hands-on understanding of Cross-Site Scripting (XSS) vulnerabilities and the importance of proper security measures in web development. By simulating an XSS attack, we learn how these vulnerabilities can be exploited to steal sensitive user information and the significance of robust web security practices to mitigate such risks.

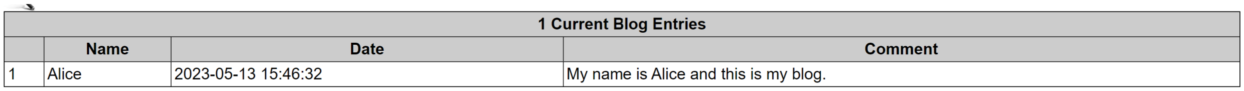
2 LAB TASKS

2.1 Creating Users

We have created these users: Alice, Bob, Charlie, Dan and Eve and we set their passwords to thier names in lowercase letters.

2.2 Alice adds an entry to her blog.

Firstly, we login as Alice. Then we add an entry which is ”My name is Alice and this is my blog.”.

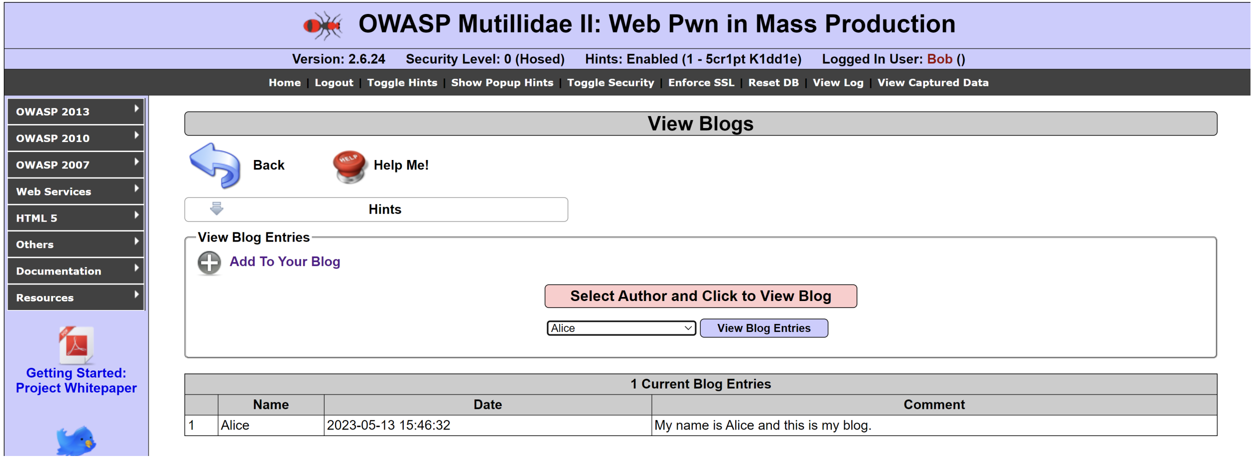


1 Current Blog Entries

	Name	Date	Comment
1	Alice	2023-05-13 15:46:32	My name is Alice and this is my blog.

2.2.1 Bob views Alice’s blog.

We log out of Alice’s account, then log as Bob and navigated to Alice’s blog.



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In User: Bob ()

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
View Blogs
Back
Help Me!
Hints
View Blog Entries
Add To Your Blog
Select Author and Click to View Blog
View Blog Entries

Alice

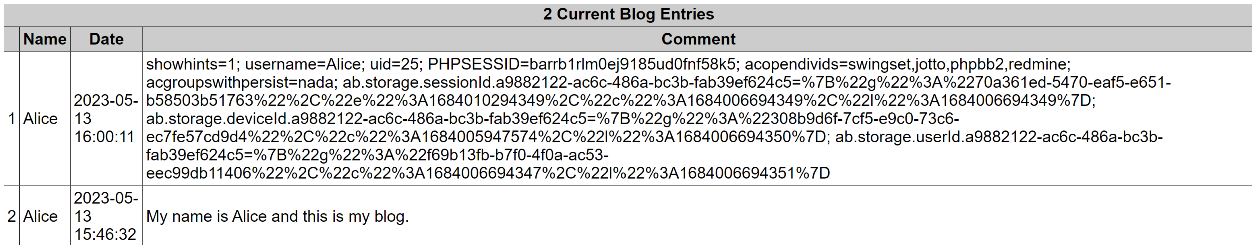
1 Current Blog Entries

	Name	Date	Comment
1	Alice	2023-05-13 15:46:32	My name is Alice and this is my blog.

2.3 Alice adds to her blog an entry that contains a Javascript code that shows their cookies to the users who visit her blog.

Alice adds a blog entry with the code

```
<script>document.write(document.cookie)</script>
```

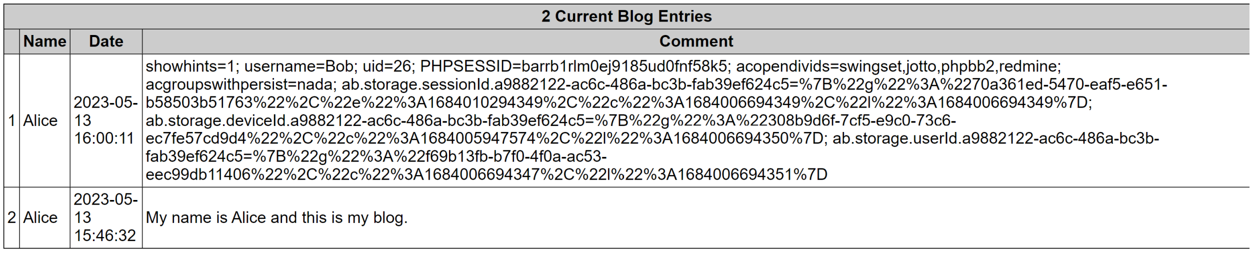


2 Current Blog Entries			
	Name	Date	Comment
1	Alice	2023-05-13 16:00:11	showhints=1; username=Alice; uid=25; PHPSESSID=barrb1rlm0ej9185ud0fnf58k5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; ab.storage.sessionId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%2270a361ed-5470-eaf5-e651-b58503b51763%22%2C%22e%22%3A1684010294349%2C%22c%22%3A1684006694349%2C%22l%22%3A1684006694349%7D; ab.storage.deviceId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%22308b9d6f-7cf5-e9c0-73c6-ec7fe57cd9d4%22%2C%22c%22%3A1684005947574%2C%22l%22%3A1684006694350%7D; ab.storage.userId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%22f69b13fb-b7f0-4f0a-ac53-eec99db11406%22%2C%22c%22%3A1684006694347%2C%22l%22%3A1684006694351%7D
2	Alice	2023-05-13 15:46:32	My name is Alice and this is my blog.

This entry was unique, as it contained a piece of JavaScript code specifically designed to display the cookie data of any user who views the blog entry.

2.3.1 Bob views Alice's blog.

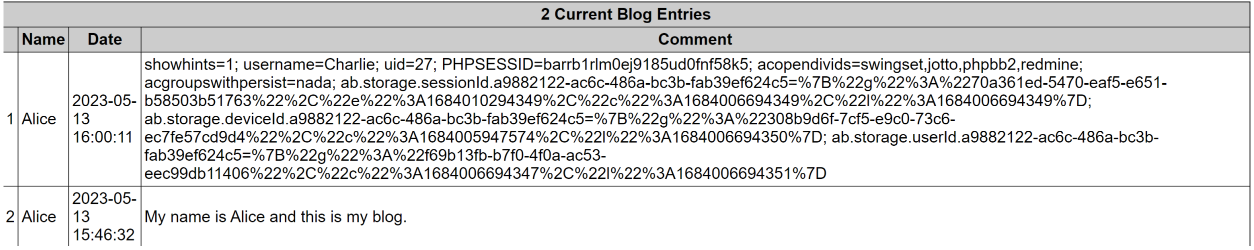
Next, we logged out of Alice's account and logged back into the application as Bob. We navigated to Alice's blog and viewed the blog entry she had created. Upon viewing the blog, the JavaScript code embedded in the blog entry executed, displaying Bob's cookie data on the page.



2 Current Blog Entries			
	Name	Date	Comment
1	Alice	2023-05-13 16:00:11	showhints=1; username=Bob; uid=26; PHPSESSID=barrb1rlm0ej9185ud0fnf58k5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; ab.storage.sessionId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%2270a361ed-5470-eaf5-e651-b58503b51763%22%2C%22e%22%3A1684010294349%2C%22c%22%3A1684006694349%2C%22l%22%3A1684006694349%7D; ab.storage.deviceId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%22308b9d6f-7cf5-e9c0-73c6-ec7fe57cd9d4%22%2C%22c%22%3A1684005947574%2C%22l%22%3A1684006694350%7D; ab.storage.userId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%22f69b13fb-b7f0-4f0a-ac53-eec99db11406%22%2C%22c%22%3A1684006694347%2C%22l%22%3A1684006694351%7D
2	Alice	2023-05-13 15:46:32	My name is Alice and this is my blog.

2.3.2 Charlie views Alice's blog.

We repeated the process with Charlie. After logging out of Bob's account, we logged in as Charlie and navigated to Alice's blog. Just like with Bob, the JavaScript code executed when Charlie viewed the blog, revealing Charlie's cookie data on the page.



2 Current Blog Entries			
	Name	Date	Comment
1	Alice	2023-05-13 16:00:11	showhints=1; username=Charlie; uid=27; PHPSESSID=barrb1rlm0ej9185ud0fnf58k5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; ab.storage.sessionId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%2270a361ed-5470-eaf5-e651-b58503b51763%22%2C%22e%22%3A1684010294349%2C%22c%22%3A1684006694349%2C%22l%22%3A1684006694349%7D; ab.storage.deviceId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%22308b9d6f-7cf5-e9c0-73c6-ec7fe57cd9d4%22%2C%22c%22%3A1684005947574%2C%22l%22%3A1684006694350%7D; ab.storage.userId.a9882122-ac6c-486a-bc3b-fab39ef624c5=%7B%22g%22%3A%22f69b13fb-b7f0-4f0a-ac53-eec99db11406%22%2C%22c%22%3A1684006694347%2C%22l%22%3A1684006694351%7D
2	Alice	2023-05-13 15:46:32	My name is Alice and this is my blog.

3 References

https://openai.com/
https://stackoverflow.com/