Name: Ko Ko Win

ID: 31842305

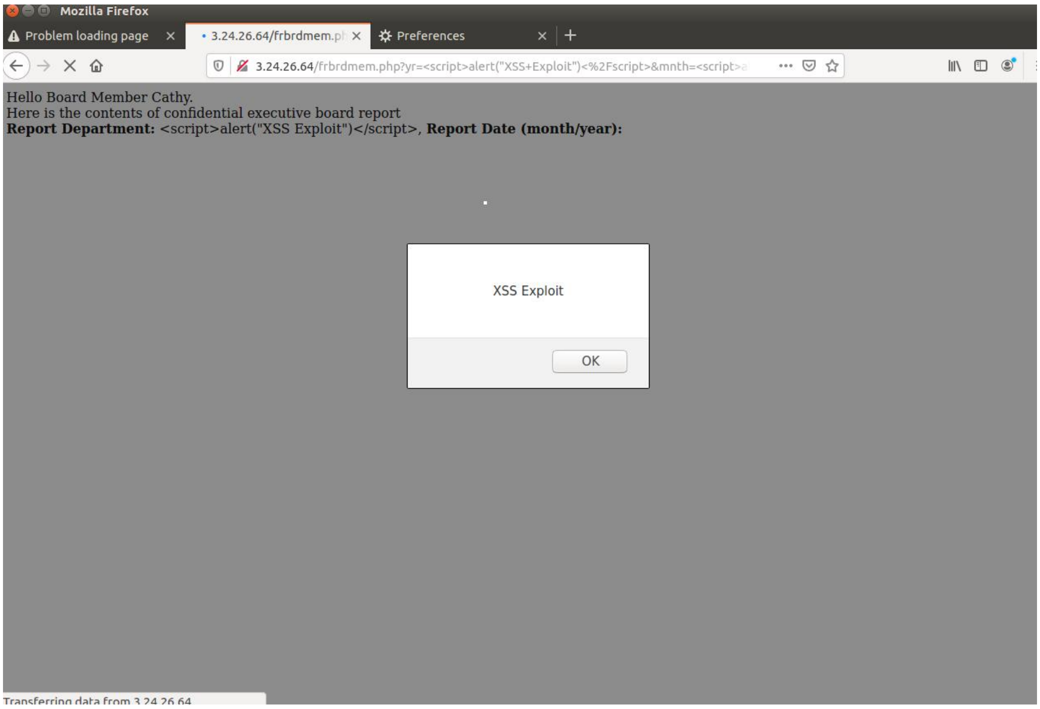
Task A.1

There is no reflected XSS vulnerability exist in the home page. However, in the greeting page the attacker might inject his/her malicious script in the year, month, and department parameter.

Task A.2

TEST

In the home page login there are total of three input which are Username, Password and location. When I embedded the script **<script>alert("XSS Exploit")</script>** inside Username and Password it shows **"Board member authentication rejected!"** so we can conclude that XSS vulnerabilities does not exist in the log in page. The reason the XSS vulnerability does not exist in Username and Password is because it checks for input validation. On the other hand, in the board member greeting page it accepts three input as well which are Year, Month and Department. When I embedded the script **<script>alert("XSS Exploit")</script>** the alert popped up like shown below in the image when the script is embedded inside the Month parameter but it does not have any effect on the other two parameters. Therefore, we can conclude that XSS vulnerabilities exist in the board member greeting page but only in the month parameter.



Mozilla Firefox
Problem loading page
3.24.26.64/frbrdmem.p
Preferences
3.24.26.64/frbrdmem.php?yr=<script>alert("XSS+Exploit")<%2Fscript>&mnth=<script>a

Hello Board Member Cathy.
Here is the contents of confidential executive board report
Report Department: <script>alert("XSS Exploit")</script>, **Report Date (month/year):**

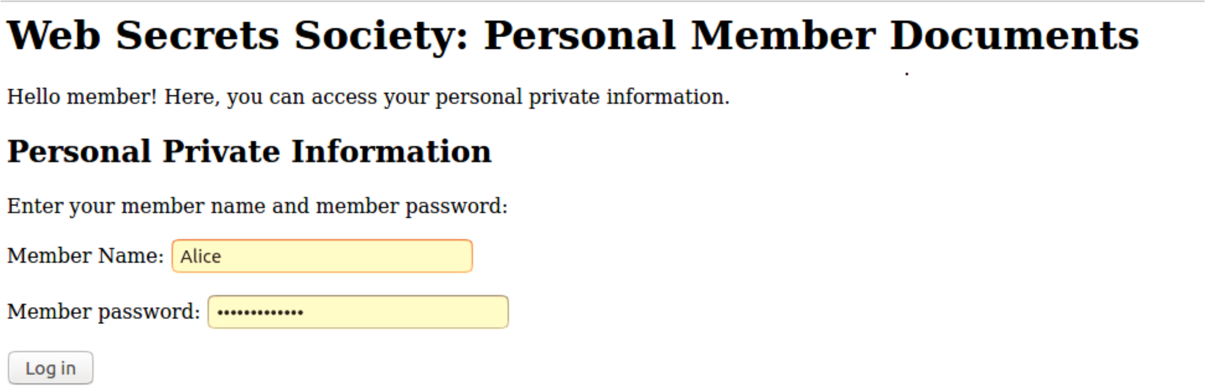
XSS Exploit

OK
Transferring data from 3.24.26.64

TASK B.1

Yes, Alice could gain unauthorised access to Bob personal private data by using CSRF attack. The website has session management vulnerabilities which causes Alice to hijack the user's session and modified the tokens. That token is used to impersonate as user to the web application.

Firstly, I entered the member's name and member password for Alice on the log in page and the access was granted.



Web Secrets Society: Personal Member Documents

Hello member! Here, you can access your personal private information.

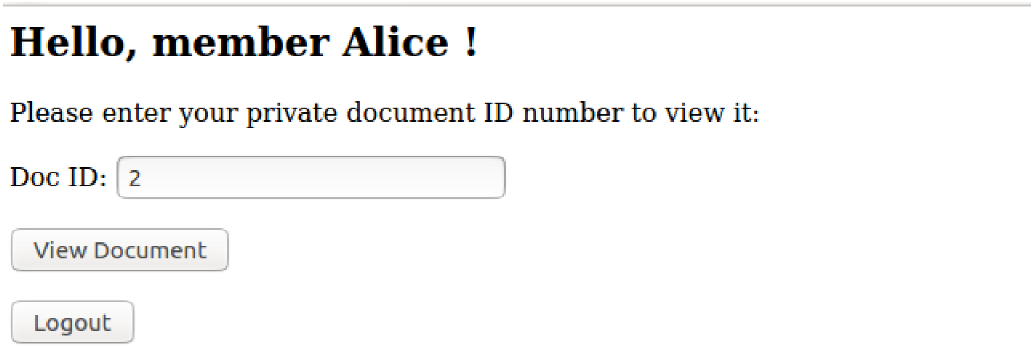
Personal Private Information

Enter your member name and member password:

Member Name: Alice

Member password: •••••••••••••

Secondly, I changed the proxy to manual proxy in the setting preferences and run the command for burp suite in the terminal. Moreover, in the Doc ID parameter I entered 2 as the Doc ID and pressed view document.

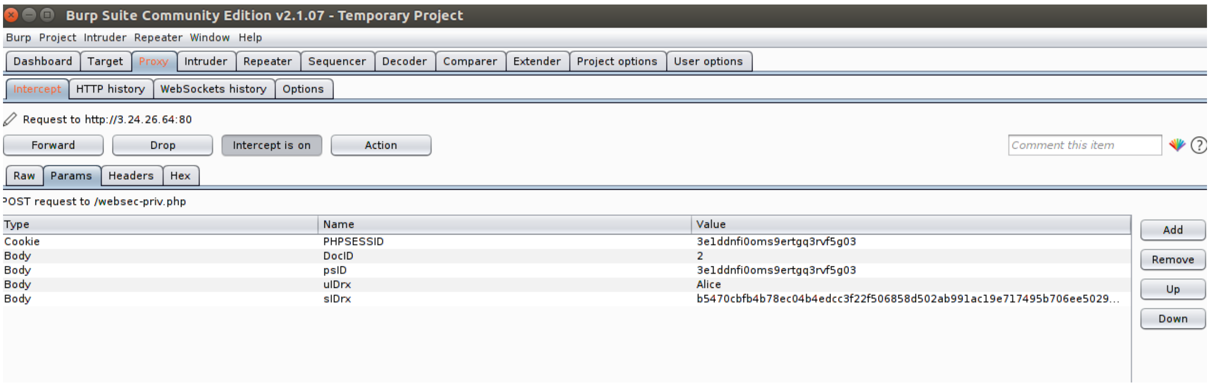


Hello, member Alice !

Please enter your private document ID number to view it:

Doc ID: 2

In burp suite application intercept was on and after pressing the view document button the following appears.



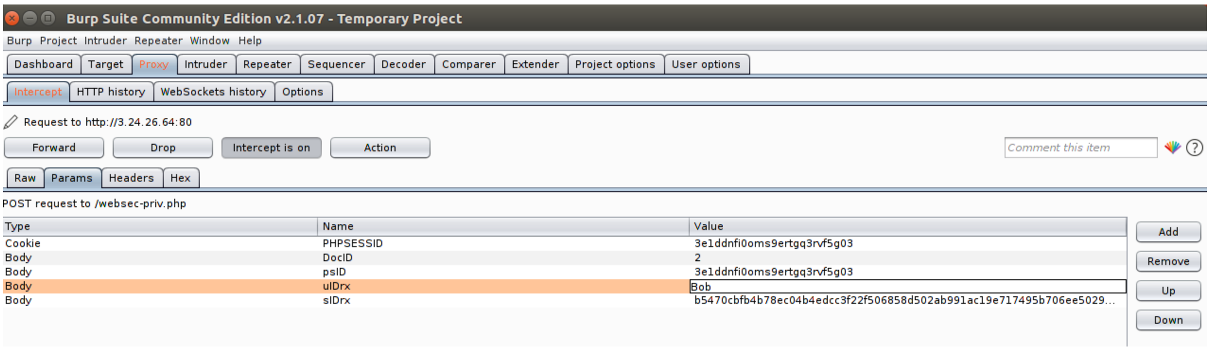
Burp Suite Community Edition v2.1.07 - Temporary Project

Request to http://3.24.26.64:80

POST request to /websec-priv.php

Type	Name	Value
Cookie	PHPSESSID	3e1ddnfi0oms9ertgq3rvf5g03
Body	DocID	2
Body	psID	3e1ddnfi0oms9ertgq3rvf5g03
Body	uIDrx	Alice
Body	sIDrx	b5470cbfb4b78ec04b4edcc3f22f506858d502ab991ac19e717495b706ee5029...

To gain unauthorised access as Bob I changed the name from Alice to Bob and pressed the forward button.

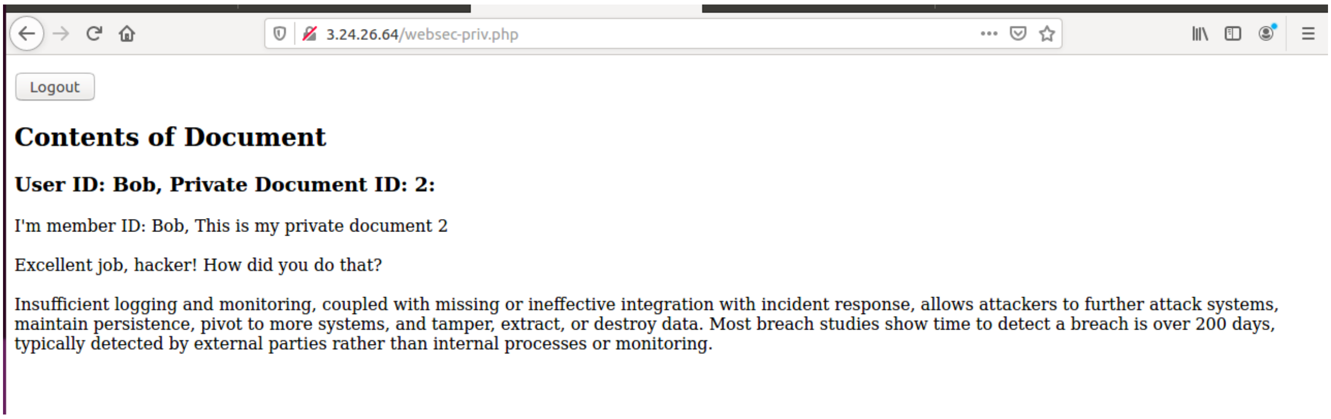

Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Add Remove Up Down

Request to http://3.24.26.64:80

POST request to /websec-priv.php

Type	Name	Value
Cookie	PHPSESSID	3e1ddnfi0oms9ertgq3rvf5g03
Body	DocID	2
Body	psID	3e1ddnfi0oms9ertgq3rvf5g03
Body	uIDrx	Bob
Body	sIDrx	b5470cbfb4b78ec04b4edcc3f22f506858d502ab991ac19e717495b706ee5029...

After pressing the forward button on the burp suite application, the following screen appears which shows that the Alice can gain unauthorised access to Bob private information.



Contents of Document

User ID: Bob, Private Document ID: 2:

I'm member ID: Bob, This is my private document 2

Excellent job, hacker! How did you do that?

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

I repeated the test with the Document ID 1 and the final result was the same.