CSRF account takeover Explained Automated/Manual

Vulnerables Follow
Oct 26, 2018 · 2 min read

Here is the second CSRF vulnerability which leads to full account takeover and as it is patched, we decided to share the PoC also. So when Anti-CSRF token is implemented, your website will include a random generated number or token to every page which is impossible to guess by the attacker so website will include it when they serve it to you. It differs each time they serve any page to anybody so attacker won't be able to generate a valid request because of the wrong token.

. . .

Vulnerability: CSRF/XSRF (Cross site request forgery)
Severity: Critical
Owasp rank: (OTG-SESS-005)

Cross site request forgery (Patched)

- So the vulnerable website is https://openmenu.com
- Create two accounts csrfattacker (Mozilla) and csrfvictim (Chrome) or you can also test it with one account.
- Open any web proxy tool and turn intercept on to catch the request of the profile change.
- After login in both accounts with different browsers go to account settings and click on account settings in mozilla, Fill up the mendatory fields and click on save changes.(Pic below)

Request

- We can exploit the form both ways manual/automated and here in the PoC we've explained both methods. So more detailed exploitation you

can go through video.

- So right click on the intercepted request and select Engagement tools and click on **'Generate PoC request'**, Here copy HTML and save it as open.html

Exploit

- change the email id in the html if you want takeover with email.
- In new tab in chrome open open.html and click on submit request and you'll get victim's account with Email/Password changed, to cross verify you can refresh the first tab.

- Below is the video PoC

PoC

25-Sep-2018 → Bug Reported

26-sep-2018 → Bug Triaged

27-sep-2018 → Bug Fixed

Have a happy hunting 😀

Security Infosec Vulnerability Csrf Bug Bounty

127 claps

WRITTEN BY

Vulnerables

Vulnerabilities | Write-ups | Publication link is below | https://medium.com/vulnerables

Follow

InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Powered by Hackrew

Follow

See responses (1)

More From Medium

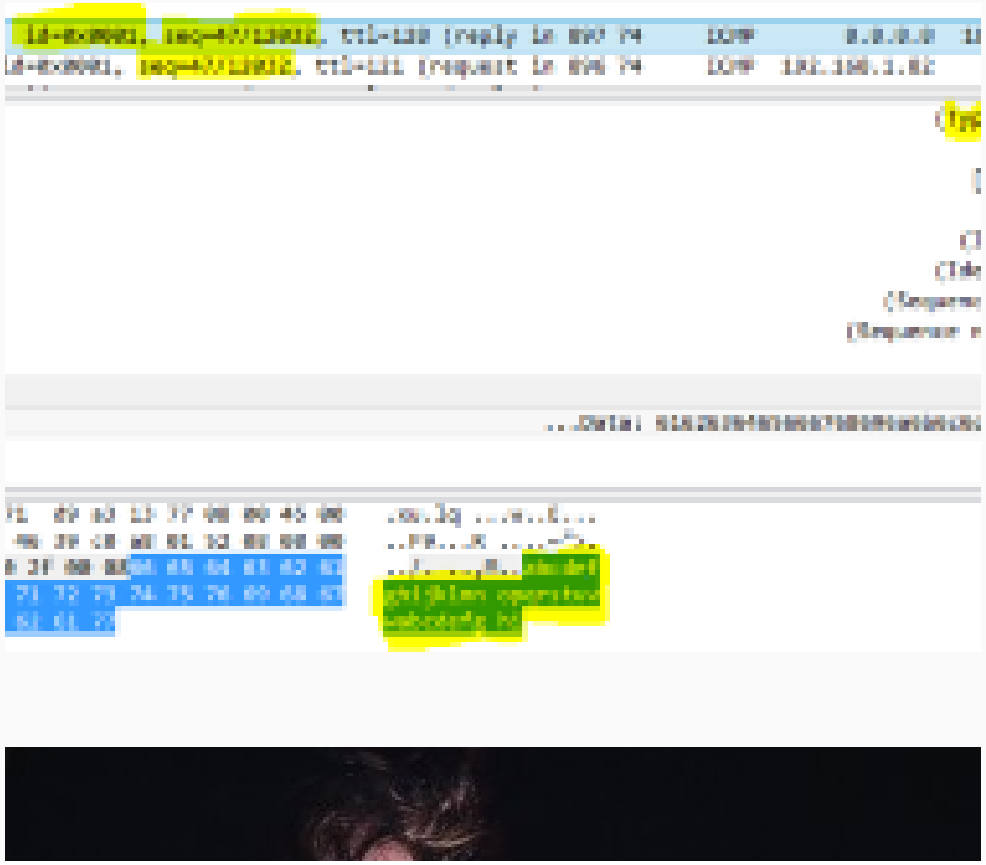
More from InfoSec Write-ups

Ping Power — ICMP Tunnel

Nir Chako in InfoSec Write-ups

Dec 17, 2018 · 8 min read

1.1K



More from InfoSec Write-ups

Picture Yourself Becoming a Hacker Soon (Beginner's Guide)

Abanikanda in InfoSec Write-ups
Aug 16 · 16 min read ★

483

More from InfoSec Write-ups

Antivirus Evasion with Python

Marcelo Sacchetin in InfoSec Write-ups
Jun 11 · 6 min read ★

610