




buuctf web

原创

[hercu1iz](#)  已于 2022-03-01 20:00:41 修改  2976  收藏

文章标签: [前端](#) [web安全](#) [安全](#)

于 2022-02-19 15:18:49 首次发布

初雪

本文链接: https://blog.csdn.net/weixin_44309300/article/details/122713521

版权

pentest

[\[极客大挑战 2019\]EasySQL](#)

[\[HCTF 2018\]WarmUp](#)

[\[极客大挑战 2019\]Havefun](#)

[\[ACTF2020 新生赛\]Include](#)

[\[强网杯 2019\]随便注](#)

[\[SUCTF 2019\]EasySQL](#)

[\[ACTF2020 新生赛\]Exec](#)

[\[极客大挑战 2019\]Secret File](#)

[\[极客大挑战 2019\]LoveSQL](#)

[\[GXYCTF2019\]Ping Ping Ping](#)

[\[极客大挑战 2019\]Knife](#)

[\[极客大挑战 2019\]Http](#)

[\[极客大挑战 2019\]Upload](#)

[\[ACTF2020 新生赛\]Upload](#)

[\[RoarCTF 2019\]Easy Calc](#)

[\[极客大挑战 2019\]BabySQL](#)

[\[极客大挑战 2019\]PHP](#)

[\[ACTF2020 新生赛\]BackupFile](#)

[\[护网杯 2018\]easy_tornado](#)

[\[极客大挑战 2019\]BuyFlag](#)

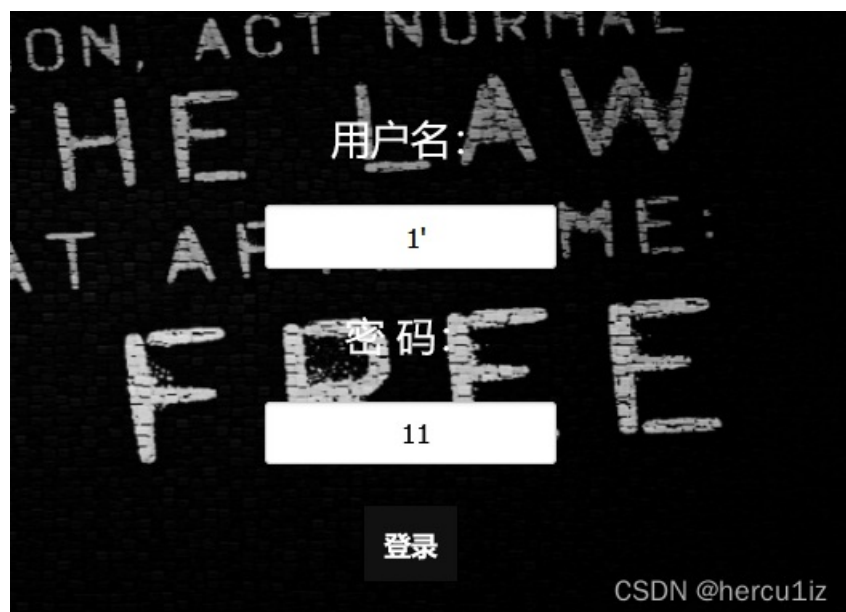
[\[HCTF 2018\]admin](#)

[\[BJDCTF2020\]Easy MD5](#)

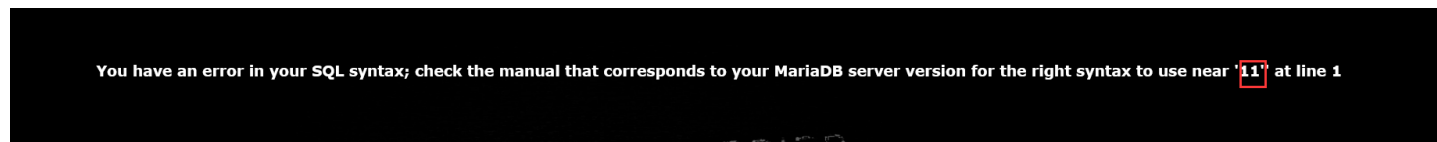
[\[ZJCTF 2019\]NiZhuanSiWei](#)

[\[SUCTF 2019\]CheckIn](#)

[\[极客大挑战 2019\]EasySQL](#)



单引号闭合



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

第一个引号闭合前引号，#注释后面闭合的引号

原理:

```
sql="select * from user where username=' 'and password=' '
```

```
sql="select * from user where username=' 1'or 1=1 # 'and password=' '
```

[HCTF 2018]WarmUp

PHP文件包含

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <meta http-equiv="X-UA-Compatible" content="ie=edge">
7   <title>Document</title>
8 </head>
9 <body>
10  <!--source.php-->
11
12  <br></body>
13 </html>
```

CSDN @hercu1iz

满足以下验证即可绕过验证，文件包含读取文件

```
if (! empty($_REQUEST['file'])
    && is_string($_REQUEST['file'])
    && emmm::checkFile($_REQUEST['file']))
) {
    include $_REQUEST['file'];
    exit;
}
```

```

class emmm
{ public static function checkFile(&$page)
{
    //白名单列表
    $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
    //isset()判断变量是否声明is_string()判断变量是否是字符串 &&用了逻辑与两个值都为真才执行if里面的值
    if (! isset($page) || !is_string($page)) {
        echo "you can't see it A";
        return false;
    }
    //检测传进来的值是否匹配白名单列表$whitelist 如果有则执行真
    if (in_array($page, $whitelist)) {
        return true;
    }
    //过滤问号的函数(如果$page的值有? 则从?之前提取字符串)
    $_page = mb_substr(
        $page,
        0,
        mb_strpos($page . '?', '?')//返回$page.?里卖弄?号出现的第一个位置
    );

    //第二次检测传进来的值是否匹配白名单列表$whitelist 如果有则执行真
    if (in_array($_page, $whitelist)) {
        return true;
    }
    //url对$page解码
    $_page = urldecode($page);

    //第二次过滤问号的函数(如果$page的值有? 则从?之前提取字符串)
    $_page = mb_substr(
        $_page,
        0,
        mb_strpos($_page . '?', '?')
    );
    //第三次检测传进来的值是否匹配白名单列表$whitelist 如果有则执行真
    if (in_array($_page, $whitelist)) {
        return true;
    }
    echo "you can't see it";
    return false;
}
}

```

注:

```

mb_strpos (haystack ,needle )返回要查找的字符串在别一个字符串中首次出现的位置
// haystack: 要被检查的字符串。
// needle: 要搜索的字符串

```

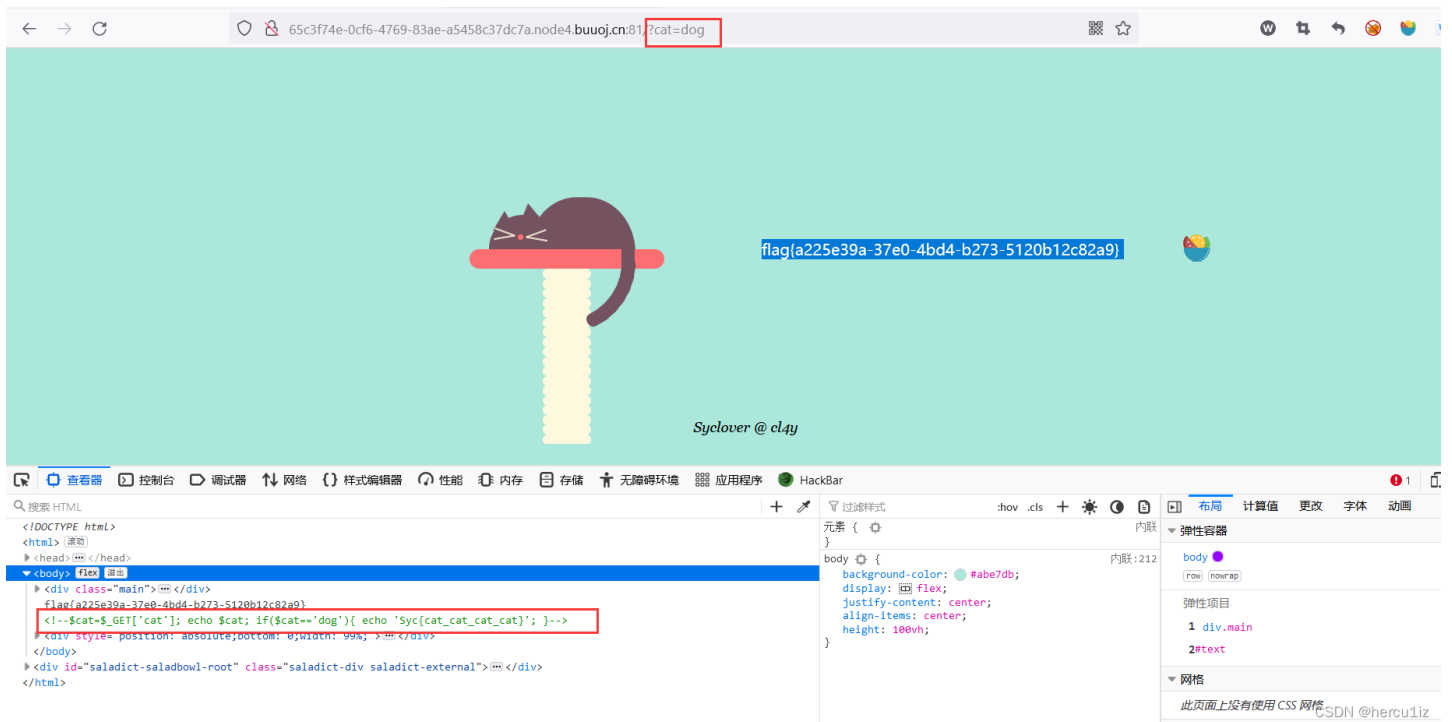
```

mb_substr(str, start, length) 函数返回字符串的一部分。
//str 必需。从该 string 中提取子字符串。
//start 必需。规定在字符串的何处开始。
//length 可选。规定要返回的字符串长度。默认是直到字符串的结尾。

```

</source.php?file=hint.php?../../../../../../../../ffffl1ll1aaaagggg>

[极客大挑战 2019]Havefun



[ACTF2020 新生赛]Include

参考: <https://blog.csdn.net/destiny1507/article/details/82347371>

[强网杯 2019]随便注

<https://www.cnblogs.com/wjw-zm/p/12359735.html>

[SUCTF 2019]EasySQL

sql堆叠

`*,1`

https://blog.csdn.net/weixin_44866139/article/details/105857487

[ACTF2020 新生赛]Exec

过滤不当

<https://blog.csdn.net/vanarrow/article/details/108181645>

[极客大挑战 2019]Secret File

php为协议php://fileter `?file=php://filter/convert.base64-encode/resource=`

文件包含

<https://www.cnblogs.com/g0udan/p/12244878.html>

[极客大挑战 2019]LoveSQL

标准爆库, 表, 字段

https://blog.csdn.net/qq_45521281/article/details/105533626

[GXCTF2019]Ping Ping Ping

ping:cmd命令连接, 难度在对字符串做了过滤。

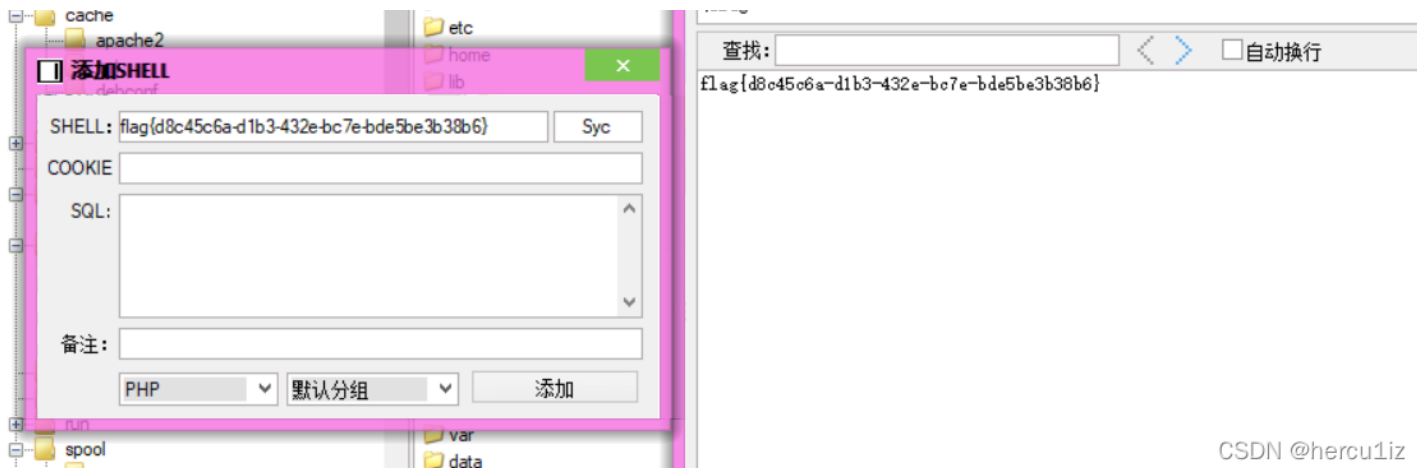
注:

在linux的shell中IFS表示 Internal Field Separator (内部字段分隔符)

https://blog.csdn.net/sinat_34761046/article/details/114698231

[极客大挑战 2019]Knife

菜刀连一下ok



CSDN @hercu1iz

[极客大挑战 2019]Http

`onclick="return false" href="Secret.php">氛围!`

查看源码

或者用burp去扫也可以探测到这个文件

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project opti

Site map Scope Issue definitions

filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://node4.buuoj.cn:28288

- /
- Secret.php
- assets

Contents

Host	Method	URL	Params	Stat...	Length	MIME type	
http://node4.buuoj.cn:...	GET	/		200	4259	HTML	Sycl
http://node4.buuoj.cn:...	GET	/Secret.php		200	2591	HTML	Sycl
http://node4.buuoj.cn:...	GET	/assets/css/images/ar...		200	667	XML	
http://node4.buuoj.cn:...	GET	/assets/js/ie/html5shi...		200	2643	script	
http://node4.buuoj.cn:...	GET	/assets/js/ie/respond...		200	4855	script	
http://node4.buuoj.cn:...	GET	/assets/js/jquery.min.js		200	96224	script	
http://node4.buuoj.cn:...	GET	/assets/js/jquery.scroll...		200	2490	script	
http://node4.buuoj.cn:...	GET	/assets/js/jquery.scroll...		200	1098	script	
http://node4.buuoj.cn:...	GET	/assets/js/main.js		200	2492	script	

再根据提示添加http请求头字段即可。

https://blog.csdn.net/qq_45163122/article/details/105905864

[极客大挑战 2019]Upload

注:

```
phtml 一般是指嵌入了php代码的html文件，但是同样也会作为php解析  
GIF89a 图片头文件欺骗(https://www.cnblogs.com/hcfllyy/p/3568839.html?utm_source=tuicool&utm_medium=referral)
```

https://blog.csdn.net/qq_45163122/article/details/105907554

[ACTF2020 新生赛]Upload

跟上题目一样思路。唯一区别多一个前端JS验证，直接F12把验证JS时间删掉。

[RoarCTF 2019]Easy Calc

get请求，通过php字符串解析特性绕过，实现信息泄露查看。

https://blog.csdn.net/weixin_44077544/article/details/102630714

[极客大挑战 2019]BabySQL

关键字被过滤，双写绕过

<https://www.cnblogs.com/h3zh1/p/12548753.html>

[极客大挑战 2019]PHP

```
url+ ?select=0:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}
```

php反序列化学习: https://blog.csdn.net/weixin_42751456/article/details/88758908

绕过参考: https://blog.csdn.net/weixin_44077544/article/details/103542260

[ACTF2020 新生赛]BackupFile

php弱类型知识点

https://blog.csdn.net/weixin_45674567/article/details/106412484

[护网杯 2018]easy_tornado

参考: https://blog.csdn.net/weixin_45642610/article/details/112519061

SSTI服务器端模板注入(Server-Side Template Injection): https://blog.csdn.net/zz_Caleb/article/details/96480967

```
import hashlib  
  
hash = hashlib.md5() #创建md5加密对象  
hash.update("/f1111111111lag".encode('UTF-8')) #更新对象要加密的字符串，要先UTF-8编码成二进制，因为md5只加密二进制  
s1=hash.hexdigest()#以十六进制输出密文  
hash = hashlib.md5()#按要求重复步骤  
hash.update(("d13a08f3-5f4b-4668-8eee-295a52b9830a"+s1).encode('utf-8'))  
print(hash.hexdigest())
```

[极客大挑战 2019]BuyFlag

strcmp()函数漏洞(前提: 5.3之前的php中)

https://blog.csdn.net/weixin_44348894/article/details/105333137

[HCTF 2018]admin

直接弱密码就进去了...

正解: https://blog.csdn.net/weixin_44677409/article/details/100733581

[BJDCTF2020]Easy MD5

md5(string,raw)

md5不能处理数组

<https://blog.csdn.net/RABCDXB/article/details/113732210>

[ZJCTF 2019]NiZhuanSiWei

绕过->读取->反序列化

<https://www.cnblogs.com/gaonuoqi/p/12255777.html>

[SUCTF 2019]CheckIn

```
exif_imagetype()
```

```
(PHP 4 >= 4.3.0, PHP 5, PHP 7, PHP 8)
```

```
exif_imagetype - 判断一个图像的类型
```

说明:

```
exif_imagetype(string $filename): int
```

```
exif_imagetype() 读取一个图像的字节并检查其签名。
```

本函数可用来避免调用其它 `exif` 函数用到了不支持的文件类型上和 `$_SERVER['HTTP_ACCEPT']` 结合使用来检查浏览器是否可以显示某个指定的图像。

参数:

```
filename -- 被检查的图像文件名。
```

返回值:

如果发现了恰当的签名则返回一个对应的常量, 否则返回 `false`。返回值和 `getimagesize()` 返回的数组中的索引 `2` 的值是一样的, 但本函数快得多。

菜刀连了半天不知道怎么没连上去, 用第二种方法读出flag

<https://blog.csdn.net/RABCDXB/article/details/113623796>