

已知跨站脚本攻击漏洞的利用

(游伟 中国人民大学)

一、利用搜索引擎收集漏洞利用信息

已知在 Discuz 论坛系统 v3.4 以下的版本，其排行页面存在存储型 XSS 漏洞。我们希望通过搜索引擎找到使用了受漏洞影响的站点，对其进行攻击。

Google search results for "discuz xss漏洞".

找到约 47,000 条结果 (用时 0.28 秒)

<https://cloud.tencent.com > developer > article>

漏洞复现| Discuz 7.2 反射型xss漏洞- 云+社区 - 腾讯云

2019年9月24日 — 漏洞复现| Discuz 7.2 反射型xss漏洞 ... 二、漏洞演示漏洞POC地址: .
<http://127.0.0.1/Discuz/logging.php?action=logout&formhash=b1abb3e2&...>

<http://chybeta.github.io > 2018/10/15 > Discuz-v3-4-排...>

Discuz v3.4 排行页面存储型XSS漏洞分析 - Chybeta

2018年10月15日 — 2018年10月12日, Discuz官方修复了一处XSS漏洞:
您已浏览过该网页 2 次。上次访问日期: 22-3-7

<https://www.xinglianwangluo.com > cms > discuz>

discuz X25 某功能存在xss漏洞以及解决方案 - 帝国cms源码

本文重点解决discuzX25某功能存在xss漏洞以及解决方案问题,希望能够帮助你。... discuz X25
广播回复存在xss漏洞html、脚本未过滤。修复方案: 过滤下就ok了

<https://blog.csdn.net > pygain > article > details>

Discuz x2 XSS漏洞_帽子不够白的博客

2016年10月31日 — Discuz x2 cms 针对拥有编辑权限的管理员存在存储型xss, 构造合理的
payload可拿到管理员cookiepayload:[align="onmouseover="alert(1)];

Google search results for "site:*.com intext:powered by discuz! x3.3 intext:游戏".

<http://adn365.com > archiver > tid-3950>

玩不懂我们魔力怎么办- 游戏讨论区- Discuz! Board

2021年12月2日 — 下面有技术跟一个玩家的聊天, 大家可以看看玩不懂我们魔力怎么办,Discuz!
Board.

<http://adn365.com > archiver > tid-3739>

Discuz! Board - 回忆阿卡斯- 游戏讨论区

2021年3月17日 — 先选【否】, 然后到达阿卡斯, 如下图然后开始【走】迷宫, 如下图1楼2楼3
楼到4楼的时候双击礼包就可以获得金币了回忆阿卡斯,Discuz! Board.

<http://adn365.com > archiver > tid-3929>

一些新动漫形象, 大家喜欢吗? - Powered by Discuz! Archiver

Discuz! Board's Archiver. 论坛, 游戏讨论区, 一些新动漫形象, 大家喜欢吗? admin 发表于
2021-11-11 01:08:09. 一些新动漫形象, 大家喜欢吗?

<https://club.sanguosha.com > ...>

提示信息- 玩家社区_三国杀官方社区- Powered by Discuz!

抵制不良游戏|拒绝盗版游戏|注意自我保护|谨防受骗上当|适度游戏益脑|沉迷游戏伤身|合理安排时
间|享受健康生活 网络文化经营许可证浙网文[2016]0251-121号 文网游备 ...

<https://qp.16163.com > archiver > fid-953>

唐|白鹿苑- 第3页- 网易手机游戏官网论坛- Powered by Discuz! Archiver

网易手机|游戏|官网论坛's Archiver. 论坛, 唐|白鹿苑. 查看完整版本: 唐|白鹿苑. Powered by
Discuz! X3.3 Archiver © 2001-2017 Comsenz Inc.

以下介绍几个可用于进行漏洞利用信息收集的搜索引擎及其常见的用法:

1、Google hacking: <https://www.google.com>

- **site:** 搜索指定的域名的网页内容,可以用来搜索子域名、跟此域名相关的内容

示例:

- | | |
|---------------------------|----------------------------|
| 1 site: zhihu.com | 搜索跟 zhihu.com 相关的网页 |
| 2 “web 安全” site:zhihu.com | 搜索 zhihu.com 跟 web 安全相关的网页 |
| 3 “SQL 注入” site:csdn.net | 在 csdn.net 搜索跟 SQL 注入相关的内容 |
| 4 “教程” site:pan.baidu.com | 在百度网盘中国搜索教程 |

- **filetype:** 搜索指定文件类型

示例:

- | | |
|-----------------------------------|---------------------|
| 1 “web 安全” filetype:pdf | 搜索跟安全书籍相关的 PDF 文件 |
| 2 nmap filetype:ppt | 搜索跟 nmap 相关的 PPT 文件 |
| 3 site:csdn.net filetype:pdf | 搜索 CSDN 网站中的 PDF 文件 |
| 4 filetype:pdf site:www.51cto.com | 搜索 51cto 的 PDF 文件 |

- **inurl:** 搜索 URL 存在特定关键字的网页,可以用来搜寻有注入点的网站

示例:

- | | |
|--------------------------|------------------------------|
| 1 inurl:.php?id= | 搜搜网址中有 “php?id” 的网页 |
| 2 inurl:view.php=? | 搜索网址中有 “view.php=” 的网页 |
| 3 inurl:jsp.php=? | 搜索网址中有 “jsp.php=” 的网页 |
| 4 inurl:asp.php=? | 搜索网址中有 “asp.php=” 的网页 |
| 5 inurl:/admin/login.php | 搜索网址中有 “admin/login.php” 的网页 |
| 6 inurl:login | 搜索网址中有 “login” 等登陆网页 |

- **intitle:** 搜索标题存在特定关键字的网页

示例:

- | | |
|---------------------------------------|-------------------------|
| 1 intitle:后台管理 | 搜索网页标题是 “后台管理” 的相关网页 |
| 2 intitle:后台管理 filetype:php | 搜索网页标题是 “后台管理” 的 PHP 网页 |
| 3 intitle:index of "keyword" | 搜索此关键字相关的索引目录信息 |
| 4 intitle:index of “parent directory” | 搜索根目录相关的索引目录信息 |
| 5 intitle:index of “password” | 搜索密码相关的索引目录信息 |
| 6 intitle:index of “admin” | 搜索后台管理页面信息 |

- **intext:** 搜索正文存在特定关键字的网页

示例:

- 1 **intext:** Powered by Discuz 搜索 discuz 论坛相关的页面
- 2 **intext:** Powered by wordpress 搜索 wordpress 制作的博客网址
- 3 **intext:** Powered by *CMS 搜索*CMS 相关的页面
- 4 **intext:** Powered by xxx inurl:login 搜索此类网址的后台登录页面

- **符号**

示例:

- 1 **-keyword** 强制结果不要出现此关键字, 例如: 电影 -黑客
- 2 ***keyword** 模糊搜索, 强制结果包含此关键字, 例如: 电影 一个叫*决定*
- 3 **"keyword"** 强制搜索结果出现此关键字, 例如: 书籍“web 安全”

2、shodan hacking: <https://www.shodan.io>

shodan (撒旦搜索引擎) 是由 **web** 工程师马瑟利编写的, 被称为“最可怕的搜索引擎”, 可扫描一切联网的设备。除了常见的 **web** 服务器, 还能扫描防火墙、路由器、交换机、摄像头、打印机等一切联网设备。国内有相应的替代工具: **zoomeye** (钟馗之眼), 由知道创宇出品, <https://www.zoomeye.org>。

- **hostname:**主机/域名 用于搜索主机和域名
- **port:**端口号 用于搜索指定端口号
- **org:**组织/公司 用于搜索指定组织/公司
- **product:**系统/软件 用于搜索指定系统/软件
- **version:**版本 用于搜索指定的软件版本
- **geo:**经纬度 用于搜索指定经纬度
- **net:** <target ip address> 用于搜索指定 IP 地址或网段

二、Discuz 排行页面存储型 XSS 漏洞的利用

简要分析

source/module/misc/misc_ranklist.php:166

```
<?php

function getranklist_members($offset = 0, $limit = 20) {
    require_once libfile('function/forum');
    $members = array();
    $stopusers = C::t('home_show')->fetch_all_by_unitprice($offset, $limit, true);

    foreach($stopusers as $member) {
        $member['avatar'] = avatar($member['uid'], 'small');
        $member['note'] = dhtmlspecialchars($member['note']);
        $members[] = $member;
    }
    return $members;
}
```

Dz在此处获取到 `$member['note']` 后调用了 `dhtmlspecialchars` 进行过滤，在 `source/function/function_core.php:203` 会对 `'&'`, `'"`, `'<`, `'>`进行实体编码。

```
<?php

function dhtmlspecialchars($string, $flags = null) {
    if(is_array($string)) {
        . . .
    } else {
        if($flags === null) {
            $string = str_replace(array('&', '"', '<', '>'), array('&', '"', '<', '>'), $string);

        } else {
            . . .
        }
    }
    return $string;
}
```

从 `getranklist_members` 返回后 `source/include/misc/misc_ranklist_index.php:113`

```
<?php
. . .
if($ranklist_setting['member']['available']) {
    $memberlist = getranklist_members(0, 27);
}
. . .
include template('diy:ranklist/ranklist');
```

进行模板的渲染在 `data/template/1_diy_ranklist_ranklist.tpl.php:32`

```
<?php if($memberlist) { ?> <a href="home.php?mod=space&uid=<?php echo
$memberlist['0']['uid'];?>&do=profile" target="_blank" id="bid_<?php echo
$memberlist['0']['uid'];?>"
class="hm" <?php if($memberlist['0']['note']) { ?> onmouseover="showTip(trhis)"
tip="<?php echo $memberlist['0']['username'];?>: <?php echo
$memberlist['0']['note'];?>"<?php } ?>><?php echo
avatar($memberlist[0][uid],middle);?></a> <?php } ?>
```

可以看到在 `tip` 属性中输出了 `$memberlist['0']['note']`。在之前有一个 `onmouseover` 事件，跟入 `showTip(trhis)` 在 `static/js/common.js:1062`

```
function showTip(ctrlobj) {
    $F('_showTip', arguments);
}
```

跟入 `_showTip`，在 `static/js/common_extra.js:912`

```
function _showTip(ctrlobj) {
    if(!ctrlobj.id) {
        ctrlobj.id = 'tip_' + Math.random();
    }
    menuid = ctrlobj.id + '_menu';
    if(!$(menuid)) {
        var div = document.createElement('div');
        div.id = ctrlobj.id + '_menu';
        div.className = 'tip tip_4';
        div.style.display = 'none';
        div.innerHTML = '<div class="tip_horn"></div><div class="tip_c">' + ctrlobj.getAttribute('tip'
        $('append_parent').appendChild(div);
    }
    $(ctrlobj.id).onmouseout = function () { hideMenu('', 'prompt'); };
    showMenu({'mtype':'prompt','ctrlid':ctrlobj.id,'pos':'12!','duration':2,'zindex':JSMENU['zIndex']}
}
```

通过 `ctrlobj.getAttribute('tip')` 获取tip属性的值，由于 `getAttribute` 获取的内容会自动反转义，即前面在 `dhtmlspecialchars` 编码过的内容又被解码了一次。此后拼接到div标签的 `innerHTML` 中，最后输出到页面上造成了 XSS

关于 `getAttribute`，可以用下面代码测试：

```
<html>
<div name="<a>" id="div">test</div>
<script>
div1 = document.getElementById("div");
align = div1.getAttribute("name");

alert(align);
</script>
```

漏洞复现

该CMS中，排行榜功能是默认开启的。在地址 <http://127.0.0.1/misc.php?mod=ranklist&type=member> 的上榜宣言中输入payload

竞价排行

美女排行

帅哥排行

积分排行

好友数排行

邀请排行

发帖

排行榜公告:

自己当前的竞价单价: 1 ,当前排名 1 ,再接再厉!

竞价单价越多，竞价排名越靠前，您的主页曝光率也会越高；

上榜用户的主页被别人有效浏览一次，将从竞价金钱中扣除您设定的竞价值(恶意刷新访问不

我也要上榜

我的上榜宣言

最多50个汉字，会显示在榜单中

竞价单价

(修改单价)

增加竞价金钱

不要超过自己的金钱 0

1

100

增加

在上面箭头所指的输入框中输入：

``

注： `<`是<的 HTML 编码， `>`是>的 HTML 编码， Discuz 没有进行足够的过滤。

在 <http://127.0.0.1/misc.php?mod=ranklist> 当鼠标移动到头像上触发 `onmouseover` 事件，执行xss

