



Web安全研究之路

YongShao@网络尖刀

whoami

ID: 泳少

某甲方测试工程师

网络尖刀核心成员

email:ys@1aq.com





microsoft xss

搜索关键字microsoft xss

热门

最新

账号

照片

视频

更多选项



TvM @tvmtpt · 11月28日

XSS Hunting 2nd month: 3 Bounties | 1 HoF | XSS's Amazon eBay IBM Microsoft Huawei Dell Orange Nike Lego Ford Philips Siemens....



Odisseus @_odisseus · 11月28日

"The instances show the Windows Store App rendering HTML using the Microsoft #Edge engine." Possible #XSS attacks.
[bestsecuritysearch.com/microsoft-wind...](#)



Monorail

https://bugs.chromium.org/

Monorail, Monorail, Monorail!

List of Projects

1 - 23 of 23

Name	Your role	Stars	Updated	Summary
☆ angleproject		238	Today	ANGLE: Almost Native Graphics Layer Engine
☆ aomedia		124	Last 7 days	The open and royalty-free codec for next-generation ultra high definit...
☆ boringssl		223	Yesterday	A fork of OpenSSL that is designed to meet Google's needs
☆ chromedriver		307	Today	WebDriver for Google Chrome
☆ chromium		1115	Today	An open-source project to help move the web forward.

获取一些最新的资讯

[http://www.pcworld.com/category/security/](http://www.pcworld.com/category/security/privacy-for-microsofts-security)

privacy for Microsoft's security



Russia claims it foiled a cyber attack from a foreign spy service

2 days ago in Security



Researchers find a way bypass the iOS activation lock

2 days ago in Security



UPDATED

Severe AirDroid vulnerability threatens tens of millions of Android users

2 days ago in Android



'Distributed guessing' attack lets hackers verify Visa card details


<http://h1.nobbd.de> 非官方 HackerOne 披露时间表。

Nextcloud disclosed a bug submitted by [hackerwahab](#)
BruteForce in to Admin Account

04 Dec 2016 ☹

Shopify disclosed a bug submitted by [shailesh4594](#)
[ecommerce.shopify.com] Invalidated redirection

04 Dec 2016 ☹

Shopify disclosed a bug submitted by [zombiehelp54](#) 
Open redirect in bulk edit

04 Dec 2016 ☹

Nextcloud disclosed a bug submitted by [cr4zyrud](#)
Wordpress Version Disclosure Bug On Nextcloud

04 Dec 2016 ☹

Nextcloud disclosed a bug submitted by [gninrepoli](#)
Reflected XSS in Gallery App

03 Dec 2016 ☹

Nextcloud disclosed a bug submitted by [lukasreschke](#)
\\OCA\\DAV\\CardDAV\\ImageExportPlugin allows serving arbitrary data with user-defined or empty mimetype

03 Dec 2016 ☹

Nextcloud disclosed a bug submitted by [vn-49-d1](#)
IDOR - Disable sharing

03 Dec 2016 ☹

Python disclosed a bug submitted by [artem](#)
Type confusion in FutureIter._throw() which may potentially lead to an arbitrary code execution

03 Dec 2016 ☹

Dropbox disclosed a bug submitted by [fbogner](#)
Subtle Code Injection Vulnerability in Dropbox for Windows

03 Dec 2016 ☹

Badoo disclosed a bug submitted by [tsug0d](#)
Unvalidated redirect on team.badoo.com

03 Dec 2016 ☹

Nextcloud disclosed a bug submitted by [config](#)
Content (Text) Injection at NextCloud Server 9.0.52 - via
http://custom_nextcloud_url/remote.php/dav/files/

02 Dec 2016 ☹

<https://bughunter.withgoogle.com/characterlist>

Google Vulnerability Reward Program

[Home](#)

[Create Profile](#)

[0x0A](#)

[Hall of Fame](#)

Hall of Fame

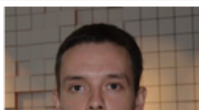
Profile



Tomasz Bojarski



Reginaldo Silva



Google Vulnerability Reward Program

[Home](#)

[Create Profile](#)

[0x0A](#)

[Hall of Fame](#)

Profile

Michał Bentkowski



#12

<http://blog.bentkowski.info>

去年刷过的src

Tsrc | Asrc | JDsrc | Msrc

为什么要刷SRC

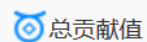


昵称：泳少

主页：<http://>

团队：网络尖刀

签名：在努力奋斗的女白帽



总贡献值

710



安全币

827



有效漏洞/情报

63

泳少的资质认证级别

[了解ASRC资质认证详情](#)



武林高手

资质特权：

- 1 每月安全币最高的1个漏洞可获得**1.5倍**安全币奖励（当月有效漏洞 ≥ 2 个，不与当月其他安全币奖励活动共享）；
- 2 优先参加阿里安全应急响应中心举办的线上线下活动。

认证要求：

- 1 最近720天内在阿里安全应急响应中心ASRC平台的贡献值不低于500；
- 2 ASRC实名认证，为人正直。

从低质量到高质量



• burpsuite+Sqlmap

Burp Suite Professional v1.5.18 - licensed to LarryLau

cmd.exe - python sqlmap.py -l .txt --batch -smart

```
SWTneff2zx9Xisw2Y7RZojbPm2MIDAMZSmuU_ZsxIfd17nJ-hadgilqJ5m1caaA/extension_10_66_3.crx?cms_redirect=yes&expire=1472453041&ip=202.100.206.196&ipbits=0&mm=31&mn=sn-13b7kn7r&ms=au&mt=1472438215&mv=m&nh=Igpwcj&zlMhrZzA&Kg0yMDIu0IcuNjluMjEz&pl=21&spams=expire,ip,ipbits,mm,mn,ms,mv,nh,pl&signature=680CF544A356853D89303E056C4205CB252FD68E.1A1CD3979DAFCB5838C359122687D40A141A9960&key=cms1'
```

[17:10:07] [WARNING] provided parameter 'nh' appears to be 'base64' encoded

[17:10:07] [INFO] testing connection to the target URL

[17:10:07] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS

[17:10:07] [INFO] testing if the target URL is stable

[17:10:08] [INFO] target URL is stable

[17:10:08] [INFO] testing if GET parameter 'cms_redirect' is dynamic

[17:10:08] [WARNING] GET parameter 'cms_redirect' does not appear dynamic

[17:10:08] [WARNING] heuristic (basic) test shows that GET parameter 'cms_redirect' might not be injectable

[17:10:09] [INFO] testing for SQL injection on GET parameter 'cms_redirect'

[17:10:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[17:10:10] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'

[17:10:11] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[17:10:12] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[17:10:12] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'

统计和报告

统计 项目 每日报告 每周报告 每月报告

周统计

	当前	项目
已下载:	101.51 MB	118.43 MB
已上传:	22.91 MB	26.73 MB
已上传和下载:	124.42 MB	145.15 MB
拨号连接时间:	无	无

月统计

	当前	项目
已下载:	3.09 GB	3.30 GB
已上传:	4.05 GB	4.33 GB
已上传和下载:	7.14 GB	7.63 GB
拨号连接时间:	无	无

确定

输出(E)

帮助

Type a search term

0 matches

半自动化神器

1.Layer子域名挖掘机 OR subDomainsBrute

Layer子域名挖掘机 V3.1

域名: qq.com 停止 去重 ☒ 服务接口 ☒ 暴力枚举 ☒ 同服挖掘 线程: 3000 过滤: 支持正则

ID	域名	解析IP	CDN列表	WEB服务器	网站状态	来源
704	society.qq.com	2.20.254.129	2.20.254.129, 2.20.254.97	Tencent Login S...	(403) 已禁止	暴力枚举
705	cover.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
706	road.qq.com	203.205.151.215	203.205.151.215, 203.205.151.216	nginx	正常访问	暴力枚举
707	fight.qq.com	203.205.151.216	203.205.151.216, 203.205.151.215	NWS_X2_MID	正常访问	暴力枚举
708	watch.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
709	bear.qq.com	203.205.151.216	203.205.151.216, 203.205.151.215	nginx	正常访问	暴力枚举
710	plant.qq.com	101.226.68.189	可能没有使用CDN	nginx/1.4.1	(403) 已禁止	暴力枚举
711	dark.qq.com	203.205.151.216	203.205.151.216, 203.205.151.215	nginx	正常访问	暴力枚举
712	dance.qq.com	203.205.151.216	203.205.151.216, 203.205.151.215	webserver	请求超时	暴力枚举
713	trade.qq.com	203.205.151.216	203.205.151.216, 203.205.151.215	Apache	(404) 未找到	暴力枚举
714	sign.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
715	food.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
716	origin.qq.com	140.207.54.67	可能没有使用CDN	webserver	请求超时	暴力枚举
717	event.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
718	sale.qq.com	203.205.150.18	203.205.150.18, 203.205.150.1...	NWS_X2_MID	(404) 未找到	暴力枚举
719	vote.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
720	spring.qq.com	10.137.129.173	可能没有使用CDN	webserver	请求超时	暴力枚举
721	science.qq.com	2.20.254.129	2.20.254.129, 2.20.254.97	Tencent Login S...	(403) 已禁止	暴力枚举
722	sing.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
723	heat.qq.com	103.7.31.39	103.7.31.39, 103.7.31.38	HTTP Load Balan...	正常访问	暴力枚举
724	listen.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
725	hall.qq.com	103.7.31.188	可能没有使用CDN	QZHTTP-2.38.20	正常访问	暴力枚举
726	health.qq.com	2.20.254.129	2.20.254.129, 2.20.254.97	squid/3.4.3	正常访问	暴力枚举
727	current.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
728	dream.qq.com	2.20.254.97	2.20.254.97, 2.20.254.129	Tencent Login S...	(403) 已禁止	暴力枚举
729	notice.qq.com	14.17.37.160	可能没有使用CDN	HTTP Load Balan...	正常访问	暴力枚举
730	opinion.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
731	shoot.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
732	scene.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
733	film.qq.com	203.205.151.212	203.205.151.212, 203.205.151...	NWS_UCG_HY	正常访问	暴力枚举
734	rock.qq.com	2.20.254.97	2.20.254.97, 2.20.254.129	Tencent Login S...	(403) 已禁止	暴力枚举
735	recommend.qq.com	14.17.57.225	可能没有使用CDN	webserver	请求超时	暴力枚举
736	lady.qq.com	2.20.254.129	2.20.254.129, 2.20.254.97	squid/3.4.3	正常访问	暴力枚举
737	cross.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
738	block.qq.com	1.1.1.1	可能没有使用CDN	webserver	请求超时	暴力枚举
739	roll.qq.com	125.39.240.46	可能没有使用CDN	webserver	请求超时	暴力枚举
740	trip.qq.com	14.17.57.230	可能没有使用CDN	Apache	正常访问	暴力枚举
741	forward.qq.com	140.207.69.102	140.207.69.102, 140.207.69.101	webserver	请求超时	暴力枚举

域名总数: 1178 进度: 服务接口模式运行中 枚举状态: (11790/26073) eiq.qq.com 作者: Seay 访问博客

3.对生成好的IP进行获取title

```
#coding=utf-8
import re
import urllib2
import threading

def htmlurl():
    url=open("test.txt","r")
    f=open("url.txt","w")
    for urlt in url:
        try:
            urlt="http://"+urlt
            html=urllib2.urlopen(urlt,timeout=1)
            html=html.read()
            title=r'<title>(.)</title>'
            title_user=re.compile(title)
            title_list=re.findall(title_user,html)
            for line in title_list:
                f.write(urlt.replace("\n","\t")+line)
                print urlt.replace("\n","\t")+line
                time.sleep(1)
        except:
            pass

def main():
    threads=[]
    t=threading.Thread(target=htmlurl)
    threads.append(t)
    for tt in threads:
        tt.start()
    tt.join()

if __name__ == '__main__':
    main()
```

223.252.197.210	中国大学MOOC<慕课>_最好的在线课程学习平台
223.252.197.227	LOFTER (乐乎) - 记录生活,发现同好
223.252.197.229	校园云
223.252.197.230	网之易智能云主页
223.252.197.233	网易云音乐2015全国校园歌手大赛
223.252.197.239	Welcome to nginx on Debian!
223.252.197.249	中国好声音
223.252.197.252	中国好声音
61.135.254.10	OpenId transaction in progress
106.2.32.71	Welcome to nginx!
106.2.32.136	phpMyAdmin
106.2.32.143	程序设计类实验辅助教学平台
106.2.32.175	味央
106.2.32.180	网之易智能云主页
106.2.32.181	网之易智能云主页
106.2.32.226	check-up
106.2.32.227	check-up
106.2.32.229	我的订单
106.2.32.238	Welcome to nginx!
106.2.32.252	网易财经-收银台
106.2.32.253	网易财经-收银台
61.145.121.77	盈世企业邮箱登录 (原尚易企业邮箱)
61.145.121.82	盈世企业邮箱登录 (原尚易企业邮箱)
61.145.121.200	金羊网-华南地区最出色的新闻网站
61.145.121.202	金羊网-华南地区最出色的新闻网站

渗透工具功能

1. 智能爬虫，过滤相似性 URL，获取攻击向量，及时跟踪。
2. 自动 SQLi 注入工具。
3. XSS scanner 基于 Dom 的 XSS scanner，可以挖掘反射型和 DOM 型的 XSS
4. 弱口令扫描器。FTP，HTTP，SMTP 等20多种协议的弱口令爆破
5. 社工库。
6. 简单指纹识别

谢谢

Thank you for listening