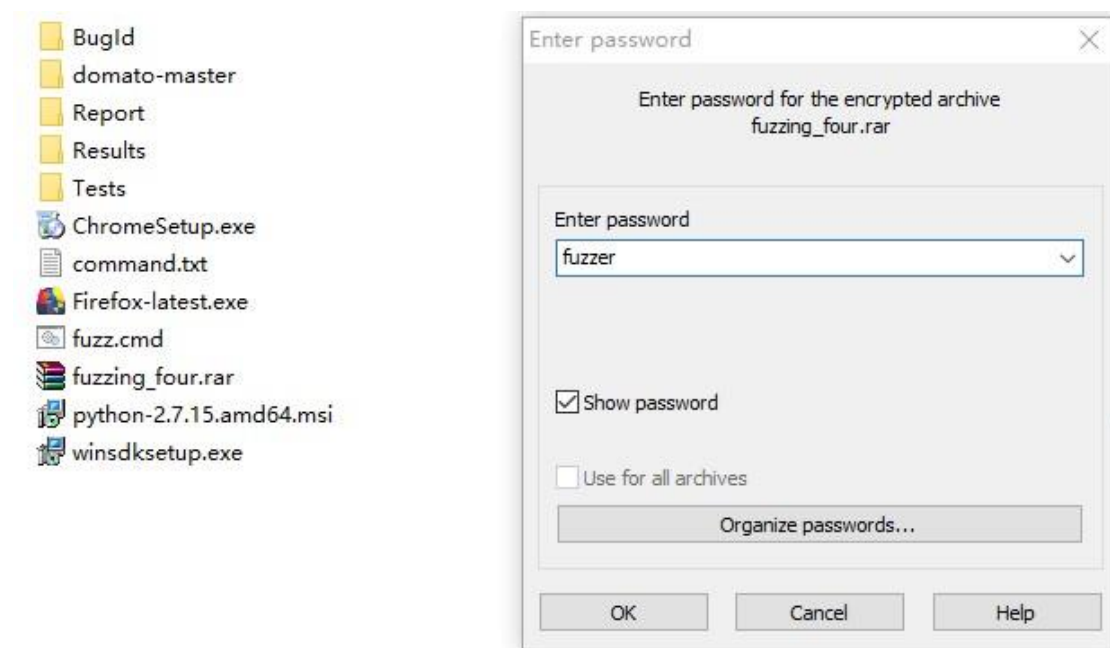


我是如何走进黑客世界的？

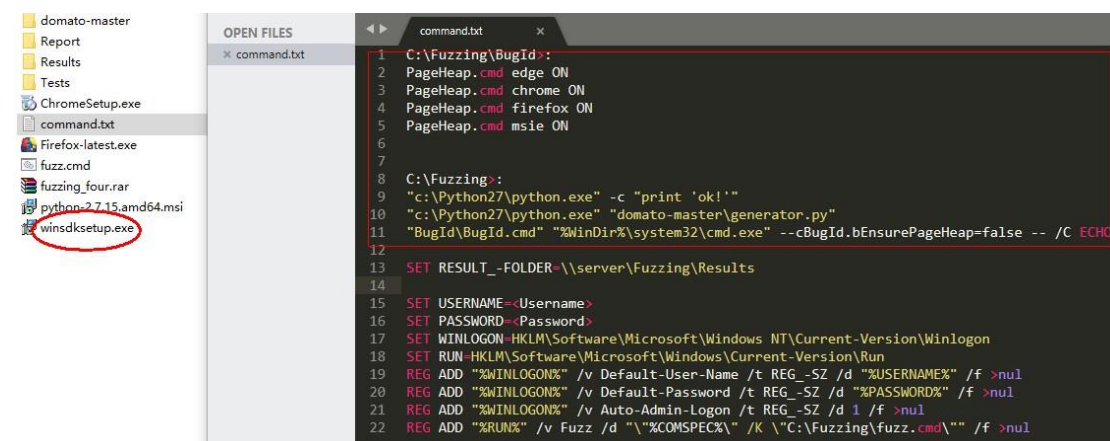
author:myselfexplorer(twitter)&flagellantX(weibo) 11/28-29/2018

我想给你这把钥匙，打开它的大门，你要做的只是静静的聆听一下这些故事。

挖掘零日漏洞，我了解到需要掌握 fuzzing、IDA Pro 反汇编、WinDbg 调试等等这些技巧，当时我最先开始的是学习 fuzzing，它的自动化让我非常着迷，我从网上查询资料，在看到一个关于浏览器的 fuzzing 技巧，我就选中了它(因为我感受过浏览器零日的强大，只要点开一个链接你的设备就被控制了)，我把这个工具包存放好，密码在图片上，你可以直接使用。



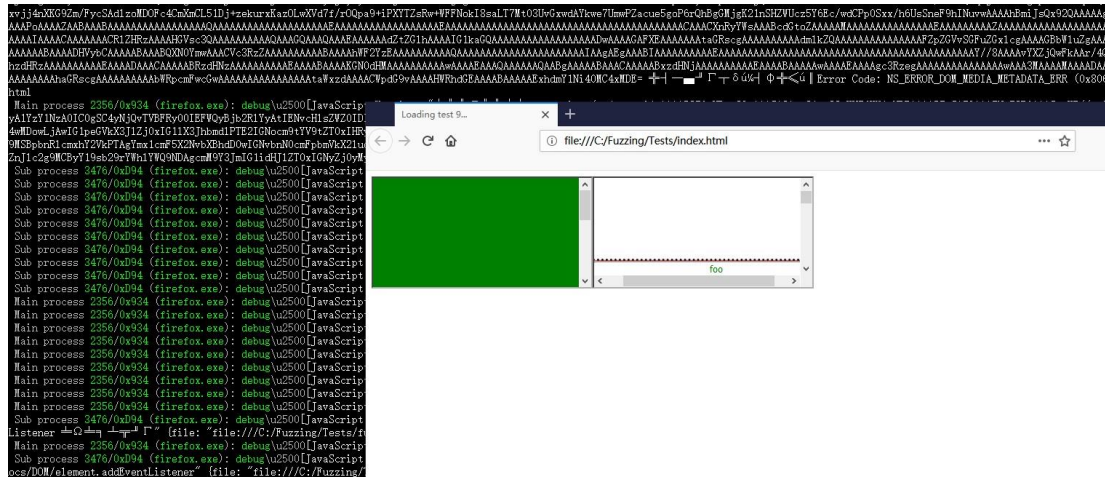
找到正确的路径，按照命令进行输入它们(只要完成方框内的)，当然你要先安装圆圈内的调试器。



完成设置以后它默认的可以帮助你进行尝试找到 firefox,edge,chrome,msie 的 crash，在“fuzz.cmd”里面设置你希望的。

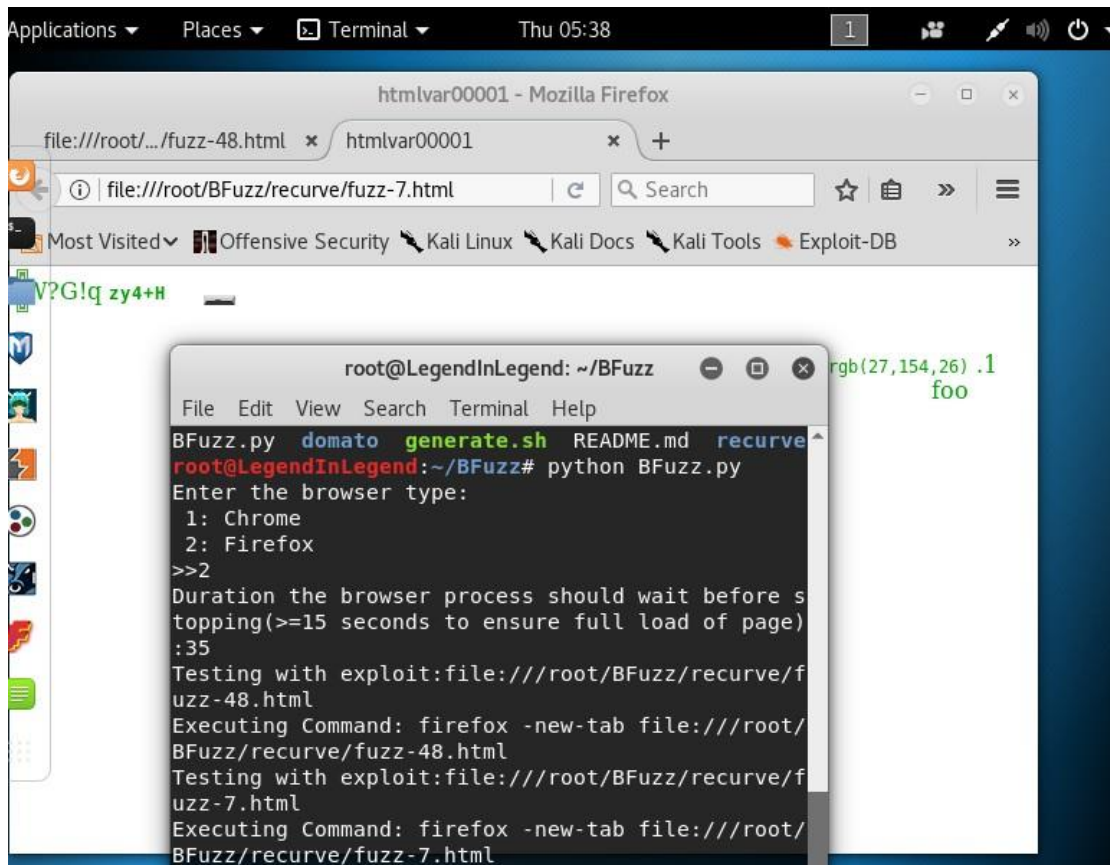
```
fuzz.cmd
1 @ECHO OFF
2 SET BASE_FOLDER=C:\Fuzzing
3 SET PYTHON_EXE=C:\Python27\python.exe
4
5 :: What browser do we want to fuzz? ("chrome" | "edge" | "firefox" | "msie")
6 SET TARGET_BROWSER=firefox
7 :: How many HTML files shall we teach during each loop?
8 SET NUMBER_OF_FILES=100
9 :: How long does it take BugId to start the browser and load an HTML file?
10 SET BROWSER_LOAD_TIMEOUT_IN_SECONDS=30
11 :: How long does it take the browser to render each HTML file?
12 SET AVERAGE_PAGE_LOAD_TIME_IN_SECONDS=2
```

看，它工作的样子。



我还发现了类似的工作，在 linux 上你可以更快的做到，

```
1 check:https://github.com/RootUp/BFuzz
2 ~/BFuzz$ ./generate.sh
3 ~/BFuzz$ python BFuzz.py
4 Enter the browser type:
5 1: Chrome
6 2: Firefox
7 >>
```



虽然我们今天的重点不是它们，但是感谢这些朋友的分享，如果拿到了 Crash 就可以尝试报告 CVE，链接上的是成功的案例，可以进行参考填写 Report([CVE-2018-11396: https://bugzilla.gnome.org/show\\_bug.cgi?id=795740](https://bugzilla.gnome.org/show_bug.cgi?id=795740))。

所以我要说的是，我是如何学到这些的？

[Twitter]:

我要告诉你的第一件事情就是它，twitter 是你在黑客世界的好伙伴，学会去使用它。我在 twitter 上面搜索"fuzzing","fuzz","fuzzer"这些关键词，当然你也可以加上一个"#”，像是"#fuzzing”，这会是一个话题，是发布者希望你能看到的相关，接着我就找到了上面的两个技巧，

Home Notifications Messages fuzz 1337

**Trends for you** · Change

- #언니\_로\_시작하는\_자동완성\_글쓰기 2,910 Tweets
- Julia Banks 4,166 Tweets
- Manafort 133K Tweets
- Thanksgiving 413K Tweets
- #UnlikelyPlacesToMeditate 3,486 Tweets
- Biloxi 9,833 Tweets
- #IveBeenAroundLongEnoughTo 2,263 Tweets
- #GothamAwards 2,827 Tweets
- Toni Collette 13.3K Tweets
- #TENvsHOU

© 2018 Twitter About Help Center Terms Privacy policy Cookies Ads info

Abdulrhman Alqabandi and 1 other Retweeted

**SkyLined** @berendjanwever · Oct 18

Always wanted to **fuzz** browsers but never had the time to figure out how? In this blog post I show how to get started quickly without having to know much about anything. This should be a useful read for both n00bs and **1337** h4x0rs.

**Fuzz in sixty seconds**  
Use publicly available tools to quickly start fuzzing browsers.  
bugid.skylined.nl

10 332 597

**David Gomes** @david\_l3n · Sep 6

Replying to @Pink\_P4nthor

@revdev1337 just said that he's bringing the bot back if you now SE the OSCP team to find out what software they use to open the report, **fuzz** the shit out of it and find a 0 day RCE vuln to get a shell and hack your points to **1337**. It's in your hands!

Home Notifications Messages fuzzing

35 572 1.8K

**Binni Shah** @binitamshah · Nov 3

BFuzz : **Fuzzing** Browsers : [github.com/RootUp/BFuzz](https://github.com/RootUp/BFuzz) cc @mishradhiraj\_

**RootUp/BFuzz**  
Fuzzing Browsers. Contribute to RootUp/BFuzz development by creating an account on GitHub.  
[github.com](https://github.com)

1 68 142

**Tavis Ormandy** @taviso · Nov 2

There is now preliminary support for macOS in halfempty 🍷, if you're **fuzzing** complex files and want them reduced fast, try it out! Thanks to Matthew Fernandez for the PR.

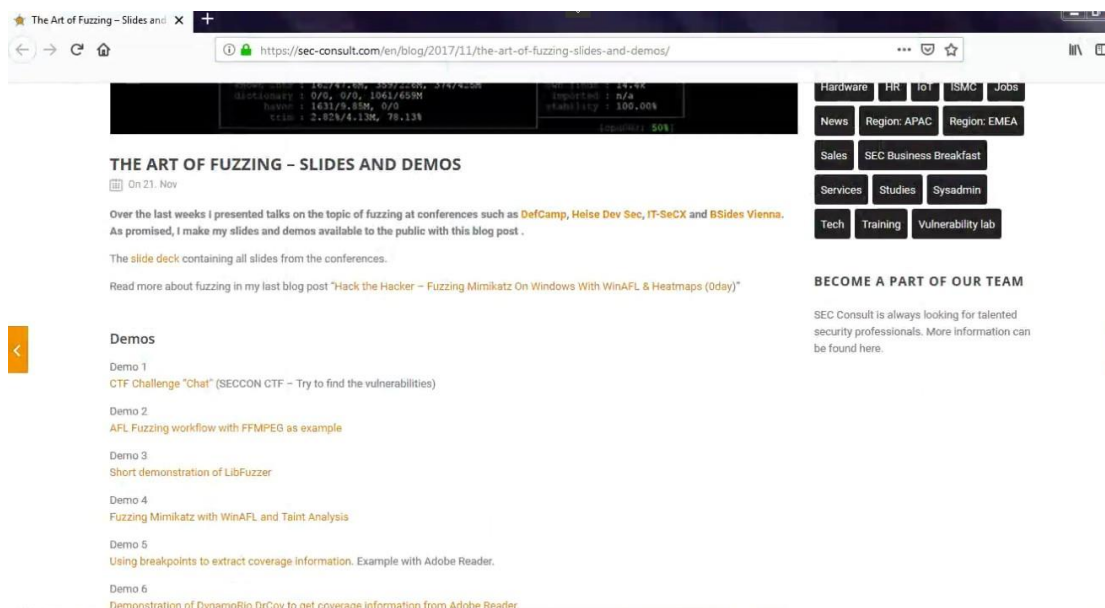
**googleprojectzero/halfempty**  
A fast, parallel testcase minimization tool. Contribute to googleprojectzero/halfempty development by creating an account on GitHub.  
[github.com](https://github.com)

1 58 162

**John Regehr** @johnregehr · Nov 1

类似的关键词有太多，去寻找你想要的。

我在寻找文章的同时也希望找到一些录像，这样可以更直观的对进行帮助，



点进去看，我找到了什么？  
是的，我要向你介绍你的第二个黑客帮手。

[Youtube]:



是的，就是它，在右下角有一个设置的按钮，里面可以帮助你进行翻译，如果视频里面并不是使用你的母语的话，这样做可以帮助你解决一些语言上的问题。  
知道了这些，你就可以泡一杯咖啡，开始像欣赏电影一般的，观看来自全世界的黑客分享的经验，一些会议，像是“Defcon”、“BlackHat”、“OWASP”、“CernerEng”、“hacktivity”、“Bugcrowd”有 bugcrowd university,“hackerone”的 hacker101 是教你做“bugbounty”的，就是 web 方面的漏洞挖掘，你可以找到漏洞获得赏金，例如我对 APT 方面非常感兴趣，我在 Defcon 里面搜索“APT”，看一下我找到了什么？



DEFCONConference  
133,964 subscribers

HOME VIDEOS PLAYLISTS COMMUNITY CHANNELS ABOUT 🔍 apt

**DEF CON 23 - Ian Latter - Remote Access the APT**  
DEFCONConference • 2K views • 2 years ago  
ThruGlassXfer (TGXF) is a new and exciting technique to steal files from a computer through the screen. Any user that has screen and keyboard access to a shell (CLI, GUI or browser) in an enterpri...

**DEF CON 19 - Lai, Wu, and Chiu - PK Balancing The Pwn Trade Deficit APT Secrets in Asia**  
DEFCONConference • 92 views • 5 years ago  
Anthony Lai, Benson Wu, Jeremy Chiu and PK - Balancing The Pwn Trade Deficit - APT Secrets in Asia  
<https://www.defcon.org/images/defcon-19/dc-19-presentations/Lai-Wu-Chiu-PK/DEFCON-19-Lai-Wu->

**DEF CON 26 PACKET HACKING VILLAGE = Sen and Sinturk - Normalizing Empires Traffic to Evade IDS**  
DEFCONConference • 483 views • 2 weeks ago  
Perimeter defenses are holding an important role in computer security. However, when we check the method of APT groups, a single spear-phishing usually enough to gain a foothold on the network. The...

**DEF CON 22 - Christopher Campbell - The \$env:PATH less Traveled**  
DEFCONConference • 2.2K views • 3 years ago  
Slides here: <https://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-Path-Less-Traveled.pdf> The \$env:PATH less Traveled is Full of Easy Privilege

讲述者分享了一个叫做“TGXF”还有“TKXF”/“TCXF”的技术，它可以实现在没有网络的情况下，对文件进行传输，通过扫描二维码，在手机和电脑之间进行，在后面还有更酷的，利用镜头完成电脑和电脑之间的传输；这项技术在我的国家不是很普及，虽然它是 15 年的，但是在 17 年仍然有人在社交软件上展示，到现在也丝毫不影响这个技巧的实战意义，可以用来窃密或者保护文件之类的。

在最开始我说过 Oday 的问题，所以我尝试搜索“how to find bug”这样的关键词，

DEFCONConference  
133,966 subscribers

HOME VIDEOS PLAYLISTS COMMUNITY CHANNELS ABOUT 🔍 how to find bug

**DEF CON 23 - Jason Haddix - How to Shot Web: Web and mobile hacking in 2015**  
DEFCONConference • 15K views • 2 years ago  
2014 was a year of unprecedented participation in crowdsourced and static bug bounty programs, and 2015 looks like a trendmaker. Join Jason as he explores successful tactics and tools used by himse...

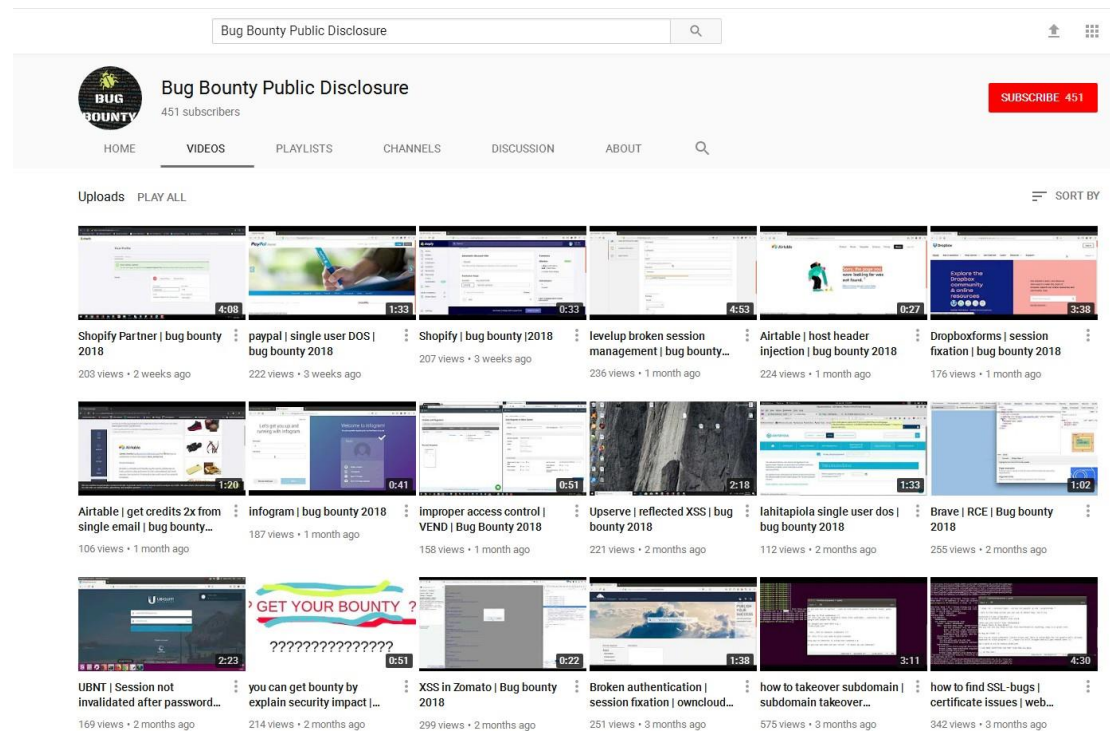
**DEF CON 16 - Mati Aharoni: BackTrack Foo - From bug to Oday**  
DEFCONConference • 1.4K views • 5 years ago  
DEF CON 16 - Mati Aharoni: BackTrack Foo - From bug to Oday As pentesters and hackers we often find the need to create our exploits on the fly. Doing this always presents a challenge. But one chall...

**DEF CON 26 RECON VILLAGE - Anshuman Bhartiya, Glenn Grant - Bug Bounty Hunting on Steroids**  
DEFCONConference • 433 views • 2 weeks ago  
Bug bounty programs are a hot topic these days. More and more companies are realizing the benefits of running a program, and researchers are jumping at the opportunity to grab some swag and make so...

显然我又找到了我要的东西，作者完整的演示了如何调试出一个零日漏洞，开始到结尾，一

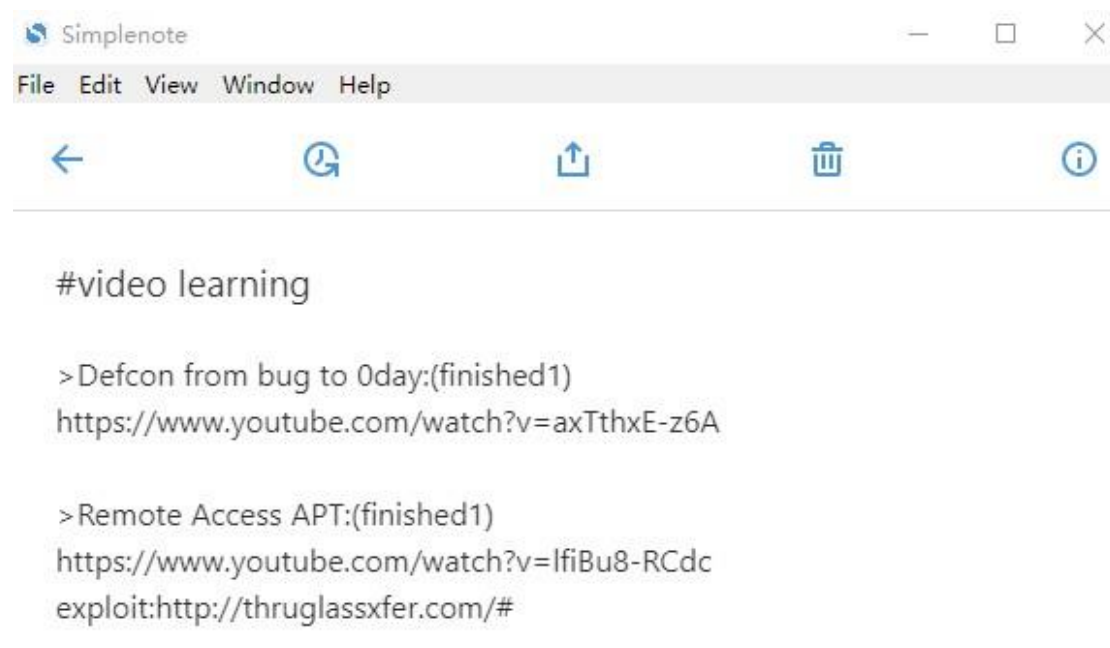
一个新的 Oday 的诞生，获得了全场的掌声。

对于 bugbounty，除了看书的学习，你可以通过其他人的实战来学习更多的捉虫技巧，你可以查看“Bug Bounty Public Disclosure”，虽然他们是 fixed 的漏洞，但是对你的帮助是不影响的，不是吗？当然你也可以直接搜索“bugbounty”在 Youtube，这样的话会有很多视频，你需要进行筛选最适合你的。



一些建议:

我用 simplenote 这款软件进行我的简单笔记，分别是 video & paper learning,用来记录我通过文章和视频的学习过程，“finished”表示我学习了全部，“1”表示我进行了一次学习，

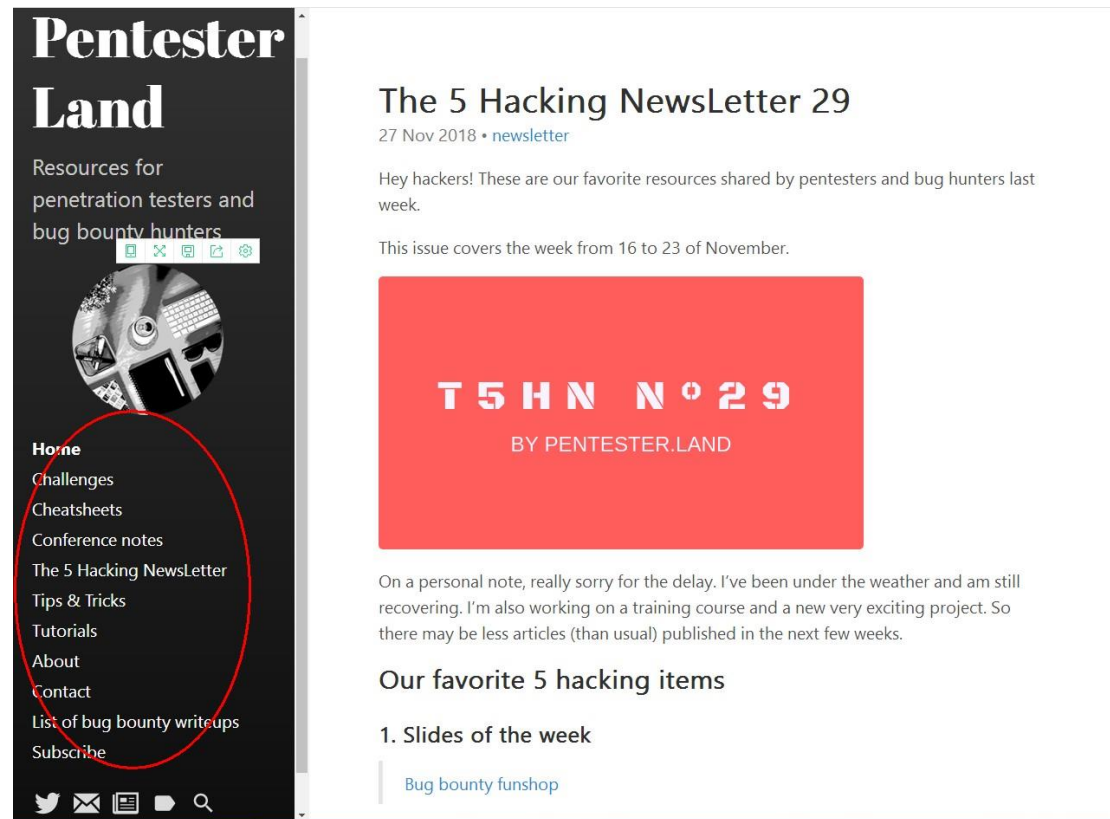


Write-up:

它的意思可以理解成一些经验之谈:

Pentester land:<https://pentester.land/>

pentesterland 的优秀当你点进去就知道，你真的能在里面学到太多,如果你是一个渗透测试人员，那么它对你的帮助无疑是巨大的；



Bug Bounty Reference:<https://github.com/ngalongc/bug-bounty-reference>

它告诉你了几乎所有在 web 安全上的技巧:



- XSSI
- Cross-Site Scripting (XSS)
- Brute Force
- SQL Injection (SQLi)
- External XML Entity Attack (XXE)
- Remote Code Execution (RCE)
  - Deserialization
  - Image Tragick
- Cross-Site Request Forgery (CSRF)
- Insecure Direct Object Reference (IDOR)
- Stealing Access Token
  - Google Oauth Login Bypass
- Server Side Request Forgery (SSRF)
- Unrestricted File Upload
- Race Condition
- Business Logic Flaw
- Authentication Bypass
- HTTP Header Injection
- Email Related
- Money Stealing
- Miscellaneous

如果你想看实际的案例，还是到这个岛上面

<https://pentester.land/list-of-bug-bounty-writeups.html>

## List of bug bounty writeups

### Table of contents

- [Bug bounty writeups published in 2018](#)
- [Bug bounty writeups published in 2017](#)
- [Bug bounty writeups published in 2016](#)
- [Bug bounty writeups published in 2015](#)
- [Bug bounty writeups published in 2014](#)
- [Bug bounty writeups published in 2013](#)
- [Bug bounty writeups published in 2012](#)
- [Bug bounty writeups with unknown publication date](#)

### Bug bounty writeups published in 2018

Title & URL	Author	Bug bounty program	Vulnerability	Reward \$\$\$	Publication date	Link 2 / Archived content
<a href="#">From CTFs to Bug Bounty Booty</a>	Benji Tobias	Tailor Store	Information disclosure	\$200	11/26/2018	
<a href="#">XML XSS in *.yandex.ru by Accident</a>	Oktavandi (@Oktavandi)	Yandex	XSS	\$160	11/26/2018	
<a href="#">My Journey To The Google Hall Of Fame</a>	Abartan Dhakal (@imhaxormad)	Google	Open redirect, XSS	-	11/25/2018	
<a href="#">Bypassing Scratch Cards On</a>	Pratheesh P	Google	Logic flaw	\$0,	11/22/2018	

它帮助你收集了过去到现在的所有经典的挖洞过程。

最后的是 PayloadsAllThings:

<https://github.com/swisskyrepo/PayloadsAllTheThings>

不管你是红队，渗透，ctf 玩家，你都可以在里面获得全部你想要的。

[NEWS]:

作为黑客，你肯定要了解最新的新闻，国内外我推荐两个

Thehackernews:

<https://thehackernews.com/>

Freebuf:

<https://www.freebuf.com/>

它们同样能给你很多帮助，例如文章不是我们的母语非常吃力的时候，可以在 freebuf 找到小编翻译好的，icloud 经常翻译挖洞经验的文章，你可以直接的进行学习。

在 thehackernews 里面，我看到了"sandboxescaper"的新闻，虽然在她的 twitter 上大部分时间在骂人（哈哈,lol~），但是她分享了逆向挖掘 ALPC 零日的技巧，

# Hacker Discloses Unpatched Windows Zero-Day PoC)

August 27, 2018 Swati Khandelwal



A security researcher has publicly disclosed the details of a previously unknown zero-day vulnerability in the Microsoft's Windows operating system that could help a local user or malicious program obtain system privileges on the targeted machine.

And guess what? The zero-day flaw has been confirmed working on a "fully-patched 64-bit Windows 10 system."

The vulnerability is a privilege escalation issue which resides in the Windows' task scheduler program and occurred due to errors in the handling of Advanced Local Procedure Call (ALPC)

# Bye

[Disclosures](#)[About me](#)[Travel photos](#)[Completed trails](#)[PGP](#)

Wednesday, October 31, 2018

## Reversing ALPC: Where are your windows bugs and sandbox escapes?

### Introduction

While I don't profess to be a Windows Internals expert, my usual approach to bug hunting is as follows:

1. Finding and watching interesting attack surface videos on YouTube
2. After finding a topic of interest, I Google everything I possibly can about the subject
3. Analyze the minimal knowledge to get started and experiment kinesthetically

The goal of this post is to understand my process for finding bugs (which are generally done through any means necessary), so it's important to note they aren't indicative of mastery in any given subject. As always, if you find any errors, or corrections, feel free to contact me. This is a personal hobby of mine and do not profess to being a professional vulnerability researcher.

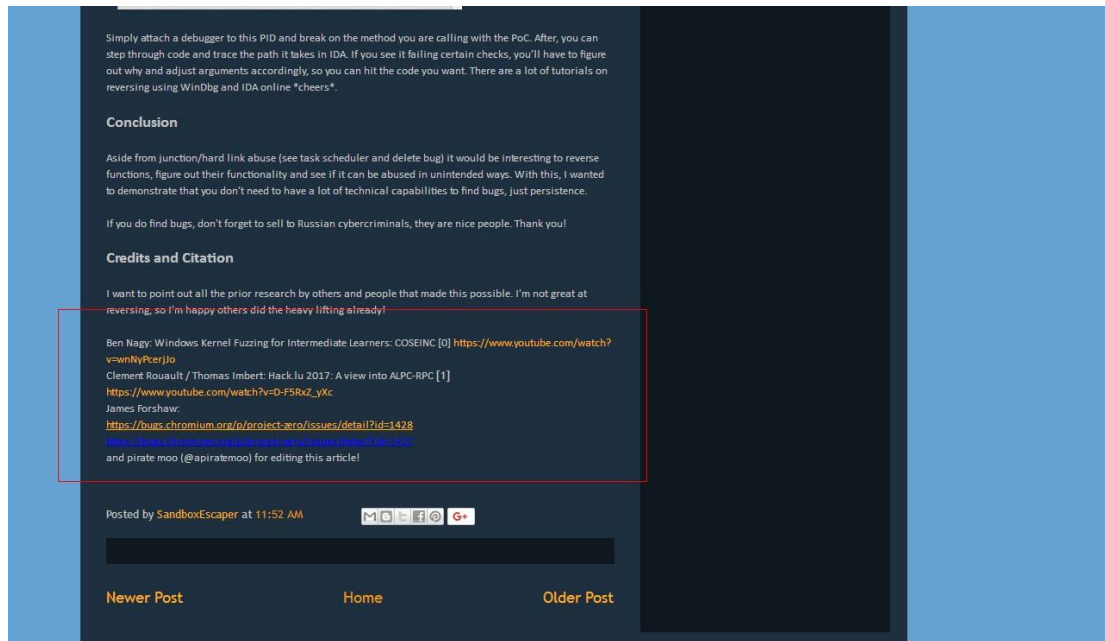
With that said: Where are your windows bugs and sandbox escapes? ☺

Bier since watching the video by Ben Nagy (Windows Kernel Fuzzing for Intermediate Learners), I was really interested in ALPC (Advanced Local Procedure Call). It wasn't until after a Hack.lu talk from 2017, by Clement Rouault and Thomas Imbert however (A view into ALPC-RPC), that I managed to piece enough together to get started. Before the talk was published, I had done some work hooking NtAlpcSendWaitReceivePort without much results :).

The way I approach step three is simple: I try to reiterate everything in my head and ask questions without getting overly technical.

### Blog Archive

- ▼ 2018 (19)
  - November (4)
  - ▼ October (1)
    - Reversing ALPC: Where are your windows bugs and sa...
  - August (8)
  - July (1)
  - June (2)
  - February (1)
  - January (2)
- 2017 (5)



你可以看到，她分享的学习过程，通过 **youtube** 观看视频，**google** 查询一些细节，然后实现具体的操作，在文章的最后，又给了你技术的来源，这些有价值的东西是不是就向你跑来了，没错吧？

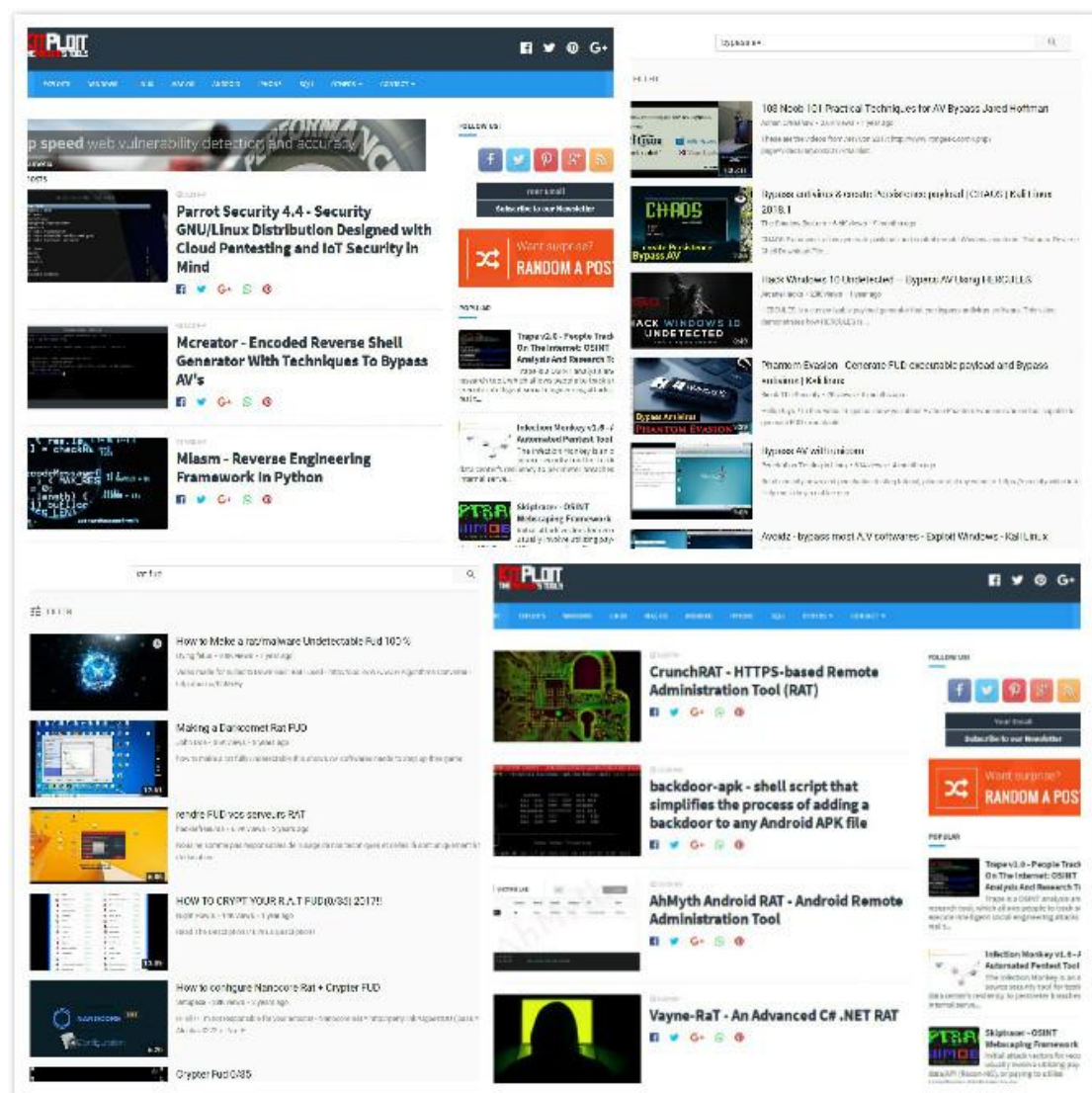
[Tools]:

不要相信“脚本小子论”，除了尽快的学习最新的 **1/nday**，利用工具也可以帮助你飞快的成长；

**Kitloit**: <https://www.kitloit.com/>

你可以在推特关注它，如果但看文章你并不知道怎么操作，可以去 **youtube** 搜索工具的关键词，获得使用的过程，也可以帮助你找到很多教你使用黑客工具的分享者，像这样的找 **RAT** 关键词，你可以尝试每一款是否能逃避杀毒软件，当然也可以在 **Youtube** 上搜索“**rat fud**”，“**bypass av**”这些你希望找的关键词，太多了，





只要对你有帮助的，你都尽快的记录下来，不要在意太多，如果你想提高自己可以通过阅读工具的源代码(它们大部分是 python,ruby,perl 这些)，也可以通过学习编程，计算机科学提高，后面我会讲到。

Connect-trojan:

<http://www.connect-trojan.net/>

windows 平台下的 hacker tools，太多了，就像之前有朋友问我找 RAT，你只要一搜基本上都会有，扫描、暴力破解、间谍软件、利用包这些，我只能举例一下，就好比下载这个 RAT 下载器，可以获得 A-Z 大概几百款国外 RAT，有的 APT 组织的就是这儿来的，当然不乏源码，可以二次开发一些：



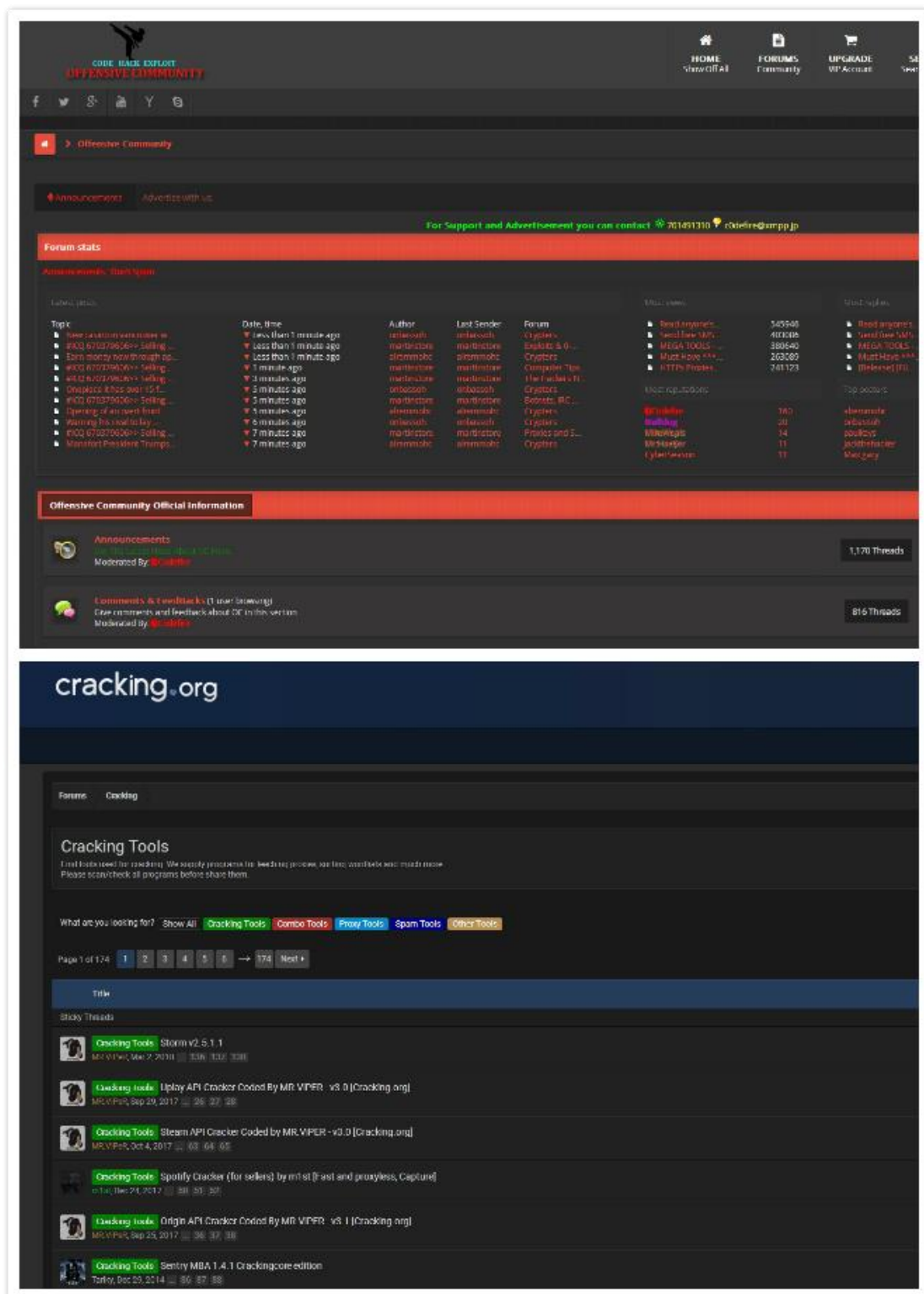
SSH R.A.T 1.3 [ RAT / Keylogger / Crypter ]
Kronus RAT By Kronus Team
Revenge-RAT v0.0.3.5 BETA By N A P O L E O N
Wayne Rat v1.3 (SRC) By TheM4hd1
Anti-Humanity RAT - Plugin Incubator [njRAT v0.7d] (SRC) By Hazem
Loki.Rat (SRC)
C-Sharp R.A.T (SRC) By Advanced Hacker 101
Hac Tool Crypter Server Revenge-RAT v0.3 (SRC) By Hac Tool
SpyNet RAT (SRC) By XilluX
Orcus RAT 1.9.1 + 13 Plugins
Screenshot RAT (SRC) By Jhassan Aly
AhMyth - Android RAT (SRC)
Darktrack RAT v4.1 Alien+ By LuckyDuck
Download RAT 0.3 RC1 (SRC) By SOOFT T
Download RAT 0.3 RC1 By SOOFT T
AhMyth - Android RAT [ User - Windows / Linux ]

Offensive Community:

<http://offensivecommunity.net/>

Cracking:

<https://cracking.org/forums/cracking-tools.16/>



这是两个黑客论坛，关于各方面的讨论，不要去百度上搜索“黑客”，“黑客教学”，“黑客论坛”，“黑客排行榜”，“黑客教父”这些东西，它害了多少中国热爱 hacker 的孩子，让他们还不知道什么是 hacker 精神的时候，就迷失在了恶作剧、违法、金钱、虚荣、交智商税的怪圈里，严厉的打击这些混蛋(不要成为那样的狗屎)。

[1/nday&Exploit]:

Metasploit 是最快最好的，

<https://github.com/rapid7/metasploit-framework/pulls>

在这里能获得最新的漏洞利用

rapid7 / metasploit-framework

Watch

1,550

Star

14,251

Fork

7,455

<> Code

Issues 548

Pull requests 66

Projects 6

Wiki

Insights

is:pr is:open

Labels

Milestones

New pull request

66 Open

8,192 Closed

Author

Labels

Projects

Milestones

Reviews

Assignee

Sort

Compatible with REG\_MULTI\_SZ when set value. ✓ **meterpreter**

#11038 opened 4 hours ago by Green-m

improve fingerprinting for Cisco ASA VPN scanner ✓ **bug** **module**

#11035 opened 14 hours ago by busterb 0 of 4

WIP Xorg x11 suid server modulepath ✓ **delayed** **module** **needs-docs**

#11025 opened 3 days ago by aringo 0 of 3

11

Add linux bpf local privilege escalation module ✗ **delayed** **module** **needs-docs**

#11013 opened 5 days ago by RootUp

Fix file suffix error, add multiple path download ✗ **enhancement** **library** **module**

#11005 opened 7 days ago by SmallTashi • Changes requested

8

Port msmtp(Nick Powers) + Cleanup for GO bridge ✓ **external modules**

#10964 opened 15 days ago by cleer7 • Changes requested 0 of 9

17

Added WordPress Duplicator <= 1.2.40 and documentation ✓ **docs** **module**

#10960 opened 15 days ago by hypn0s • Changes requested 0 of 10

39

Add exploit module for apache spark unauth rce. ✓ **docs** **module**

#10954 opened 16 days ago by Green-m

30

WP GDPR Compliance plugin exploit - privsec to admin registering ✓ **docs** **module**

#10952 opened 17 days ago by thomas-lab • Changes requested 0 of 5

17

CVE-2017-12557: HPE Intelligent Management Center Java Deserialization RCE ✓ **docs** **module**

#10947 opened 19 days ago by carmaa 0 of 6

29

在 twitter 上搜索一些#exploit,或者#0day 以外，你也可以在 Youtube 上搜索 cve+年份



[Top](#) [Latest](#) [People](#) [Photos](#) [Videos](#) [News](#) [Broadcasts](#)

Trends for you · [Change](#)

#ThrowbackThursday  
7,689 Tweets

© 2018 Twitter About Help Center Terms  
Privacy policy Cookies Ads info

🔄 Hacker Fantastic and 2 others Retweeted

**raptor** @0xdea · Nov 25  
I was investigating another **0day**, when I noticed that Solaris 11 is also affected by the recent Xorg local privilege escalation vulnerability (CVE-2018-14665).

Here's my fresh exploit:  
[github.com/0xdea/exploits...](https://github.com/0xdea/exploits)

Please read comments carefully before running it.

[illegible]

5 153 241

[Show this thread](#)

**Dan Kaminsky**  @dakami · Nov 26  
Hawaii 5-0day

2 2 9

**Kelly Shortridge** @swagjtda\_ · Nov 26  
"We stop advanced APT **0day** THREATS with MACHINE LEARNING and ARTIFICIAL INTELLIGENCE and unit 8200-trained BEES who SWARM attackers because the best defense is a good BEE ARMY."

cve 2018



FILTER



### Libssh - Authentication Bypass - CVE-2018-10933

HackerSploit • 11K views • 1 month ago

Hey guys! HackerSploit here back again with another video, in this video, I will be demonstrating how to exploit the Libssh ...



### CVE-2018-12613 - phpMyAdmin - Remote Code Execution (Metasploit) Kali linux

Minute hacking • 1.6K views • 4 months ago

CVE-2018-12613 - explain the newly found vulnerability in phpMyAdmin. We will demonstrate the vulnerability. An issue was ...



### CVE 2018 0802

Vu Duc Quan • 6.1K views • 10 months ago

CVE-2018-0802.



### libSSH Authentication Bypass Exploit (CVE-2018-10933) Demo

Ethical Hackers Club • 6.2K views • 1 month ago

In this demo, we will be exploiting the libSSH Authentication Bypass Vulnerability (CVE-2018-10933) to execute commands ...



### Exploiting CVE-2018-0802 : Microsoft Office Memory Corruption Vulnerability | Lucideus Research

Lucideus • 4.9K views • 9 months ago

A new Zero-Day Vulnerability has been founded on 8th January 2018 in the Microsoft Office Software which is a Remote Code ...



### Apache Struts2 rce CVE-2018-11776

除了大会上的分享，Youtube 上也需要筛选，不要搜索什么黑客教程，那样有好多傻子在黑“hacker”这个东西，知识来自于网络世界，服务于网络世界，因为是知识所以需要你花费努力才能获得结果，不要相信不劳而获的东西，不然你会上当的。

再加一点什么，我试试

LiveOverflow Binary Hacking(二进制黑客的入门):

<https://www.youtube.com/playlist?list=PLhixgUqwRTjxgllswKp9mpkfPNfHkzyeN>

有一个列表的功能，我们尝试搜索一下“reverse engineering”(逆向工程):

[https://www.youtube.com/results?sp=EglQAw%253D%253D&search\\_query=reverse+engineering](https://www.youtube.com/results?sp=EglQAw%253D%253D&search_query=reverse+engineering)

reverse engineering

FILTER

**Lecture 1 - Reverse Engineering Intro x86(32bit)**  
Kevin Eze  
Day 1 Part 1: Introductory Intel x86: Architecture, Assembly, Applications • 1:26:50  
Day 1 Part 2: Introductory Intel x86: Architecture, Assembly, Applications • 1:25:05  
VIEW FULL PLAYLIST (11 VIDEOS)

**Reverse Engineering**  
Andelkader Belcaid  
SECCON 2016 Online CTF | #Reverse | Anti-Debugging 100 Points • 3:04  
EKOPARTY CTF 2016 | #Reverse | F#ck 50 Points • 1:42  
VIEW FULL PLAYLIST (20 VIDEOS)

**Intro Reverse Engineering**  
Open SecurityTraining  
Day 1 Part 1: Intro to Software RE (Reverse Engineering) • 57:36  
Day 1 Part 2: Intro to Software RE (Reverse Engineering) • 1:17:18  
VIEW FULL PLAYLIST (10 VIDEOS)

**Linux reverse engineering 1**  
yuduki iseki  
Reverse Engineering 1 • 1:21:01  
Reverse engineering techniques to find security bugs: A... • 1:01:22  
VIEW FULL PLAYLIST (3 VIDEOS)

**macOS reverse engineering**  
Florica Florin  
Intro to Hopper • 12:03  
Reverse Engineering Dictation in OS X Mavericks • 36:46  
VIEW FULL PLAYLIST (17 VIDEOS)

**introduction to Reverse Engineering**

这些都是太好的课程，“linux”、“macos”的逆向，也有 101 to master 系统的学习。

像这个 Browser Fuzzing:

<https://www.youtube.com/playlist?list=PL00QFekqLCCLvF4iaP8FLuUuot2OIsiqg>

毫无疑问是挖掘浏览器漏洞的 fuzzing 技术，我还没有看完，我当然是在“fuzzing”关键词的表单功能(playlist)找到它们的:

FILTER



### The Art of Fuzzing - Demos

SEC Consult

The Art of Fuzzing - Demo 1: Find flaws in CTF Chat binary • 6:01

The Art of Fuzzing - Demo 2: AFL workflow with FFMPEG • 12:23

VIEW FULL PLAYLIST (12 VIDEOS)



### BROWSER FUZZING

Bruno Eligio Pavesi

Fuzzing Browsers for Bugs • 56:06

Use After Free Exploitation - OWASP AppSecUSA 2014 • 47:13

VIEW FULL PLAYLIST (18 VIDEOS)



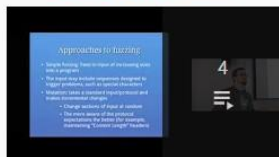
### Fuzzing Rare 60's Trashers

Pangár Finn

the riats run run run • 3:12

The Banana-There She Goes Again • 2:29

VIEW FULL PLAYLIST (12 VIDEOS)



### Fuzzing/Exploit Dev

holomatic

Bug Hunting and Exploit Development 2: Finding Flaws Using Fuzzing 1 • 14:38

Windows Kernel Fuzzing For Beginners - Ben Nagy • 58:00

VIEW FULL PLAYLIST (4 VIDEOS)



### Fuzzing & Exploit

hckguja

From Fuzzing to Metasploit, Part 1/3 • 8:56

SEH Exploits Part 1 • 9:33

VIEW FULL PLAYLIST (6 VIDEOS)



### Fuzzed Out!: 60's Garage/Psych Gems

[China number 1]:

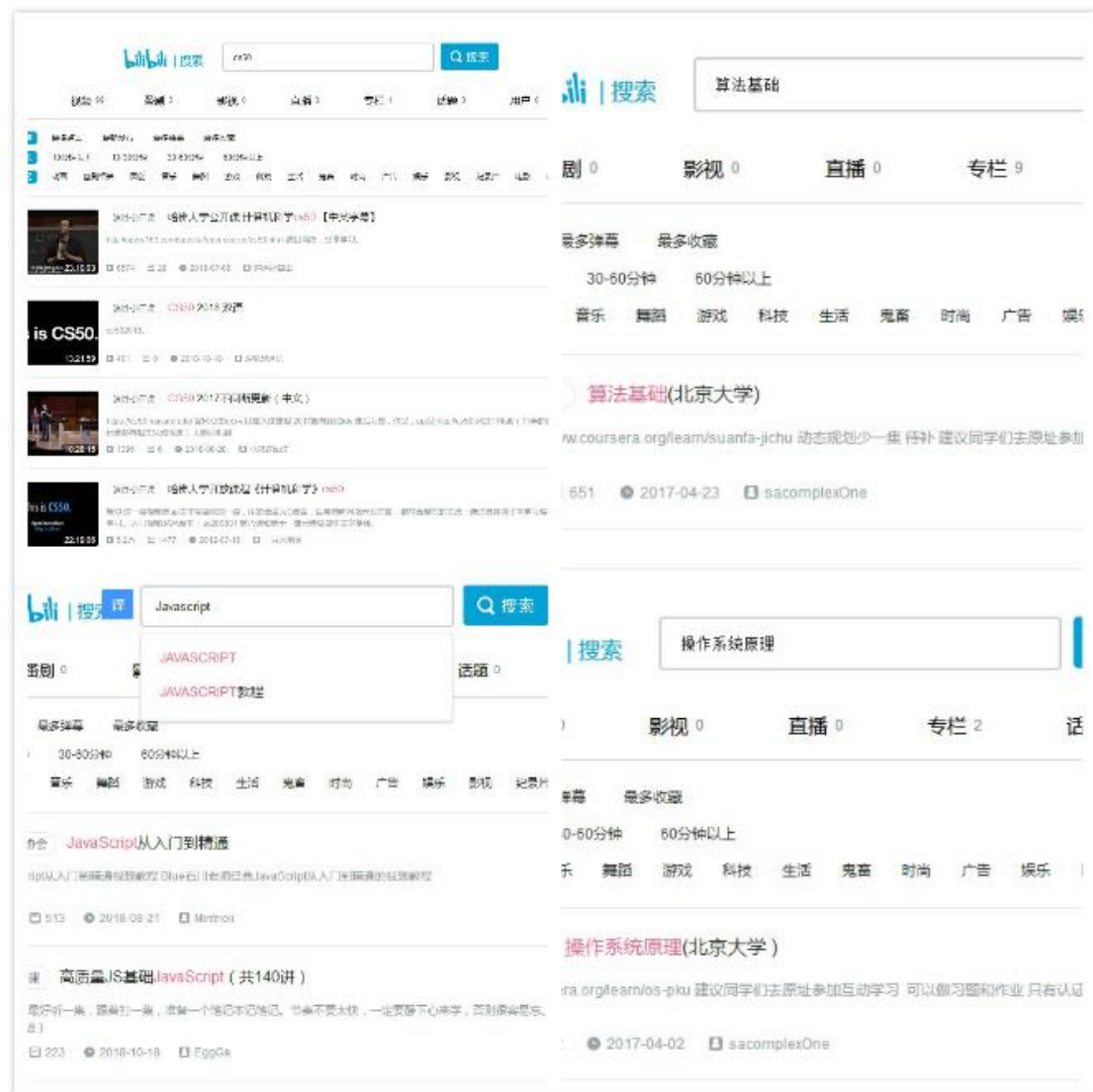
你要是觉得母语外的东西看不懂，比较排斥，那我上面的岂不是都对你没有帮助？  
当然我告诉你另一个地方，它也可以帮助你成为强大的黑客，

Bilibili:

<https://www.bilibili.com/>

尝试的找一些“操作系统原理”、“编程语言”、“计算机科学”、“算法基础”这些你想要的，里面有太多优秀的课程，甚至国外的知识，都是翻译好的，你只要坐下来学习就行了。





汇编、C、Python、Javascript，这些你都能在里面找到，底层的原理，哈佛的 cs50，计算机科学，就像内功一样，它们太重要了，当你看透二进制世界的时候，可能不仅仅限于 hacking 了，人工智能，大数据，还有更多的东西，你都可以在里面找到，非母语的问题到此可以解决了。

[Add-On]:

“我们不是凡人，需要一点魔法”-诺兰三部曲

Instagram: <https://www.instagram.com/>

我非常喜欢摄影，你可以在这里找到太多优秀的图像作品，搜你要的，甚至 hacking, hacker, exploit 都是可以的，能找到很多黑客元素的东西，为什么不呢？

Vsco: <https://vSCO.co/>

如果你喜欢摄影，但平时用手机，希望图片可以变成摄影作品

Appstore 上的:

Huji, 能拍出胶片感, 年代感  
轻颜,妹(汉?)子会喜欢的, 你总要找女(男)朋友的吧

#### Basketball:

运球, 投篮, 弹跳, 球商("ball IQ"),很多热爱 hacker 的也是球手, 上 youtube, 当然包括最好的关于 nba 的东西, the professor, ballislife, in the lab 等等 check it!

古典乐方面(也许有一天也会用上):

肖邦:<https://www.youtube.com/channel/UCSTXol20Q01Uj-U5Yp3lqFg/videos>

爱乐:<https://www.youtube.com/playlist?list=PLYiZl0A2kNDU-JMqvdBh-hjP6W-DTvNa8>

霍罗威茨:<https://www.youtube.com/watch?v=8ELwCdGQLQ>

"Skr Wu"的"auto-tune"(它前段日子太火了):

AdobeAudition[https://www.youtube.com/results?sp=EglQAw%253D%253D&search\\_query=Adobe+Audition](https://www.youtube.com/results?sp=EglQAw%253D%253D&search_query=Adobe+Audition) 记得安装插件,录音后期这些东西可比你学 hacker 来的容易

Magic,我知道很多喜欢 hacker 的都喜欢 magic, 社工, 钓鱼, 浏览器攻击, 黑客的很多技巧何尝不是魔术师呢, youku 或许比油管更适合学习魔术, 尝试的找这种, 不要直接搜索, 魔术教程, 你可以试试那会找到哪些, 就好比搜索黑客教程在百度上, 教你 ping? :P

[https://v.youku.com/v\\_show/id\\_XMzcyNjU3MDAw.html?spm=a2h0j.11185381.listitem\\_page1.5!12~A](https://v.youku.com/v_show/id_XMzcyNjU3MDAw.html?spm=a2h0j.11185381.listitem_page1.5!12~A)

说了那么多, 我重新注册回了 github,这是今天的最后一份礼物, 我想不起更多的东西暂时, 但我爱你们, 人生不仅仅是 hacker, 在有限的日子中活出更多的可能吧

>hacking Library:

<https://github.com/MyselfExplorer>

>Data hunter:

<https://cdn.databases.today/>

我在尝试数据猎人时期收集到的一个地方, 你可以下载它们, 也可以在搜索栏目找你想要的, 也可以把它做成一个 havebeenpwd, 不要花钱去购买, 它们都是老的东西, 不要用在违法上, 它们还是有危害性的, 不要卖到类似 deepweb 上换得一些酬劳, 我见过有人这么做, 但这些东西可以放在好事上, 比如保护家人朋友的隐私, 去做这个。

---

## Index of /

---

../		
random/		
17.Media.rar	775184173	22-May-2017 12:35 AM
PS3Hax.net.txt.gz	32544874	22-May-2017 12:59 AM
patreondump.tar.gz	3997819699	22-May-2017 01:41 AM
Experian.7z	1089324780	22-Mar-2018 12:05 AM
Ashley_Madison_users.7z	1773584384	22-May-2017 12:47 AM
xat.7z	227685739	22-May-2017 01:12 AM
7dc58-ngp-van.7z	711396436	22-May-2017 12:33 AM
investbank.ae.7z	263716864	22-May-2017 12:47 AM
linkedin_all.7z	4535170532	22-May-2017 01:41 AM
Libero.it 900k.zip	42068740	22-May-2017 12:52 AM
index.nginx-debian.html	612	09-Nov-2018 06:40 AM
MPGH.net_vb_April_2015.txt.7z	191805283	22-May-2017 12:54 AM
STRATFOR EMAIL HACK.7z	96631480	22-May-2017 01:01 AM
Ubisoft.com forum.sql	80917457	22-May-2017 01:08 AM
neopets_2013_68M.7z	1446757824	22-May-2017 01:13 AM
ClixSense.com_2.2M_08_2016.rar	181536745	22-May-2017 12:28 AM
000webhost_13mil_plain_Oct_2015.7z	300075885	22-Mar-2018 12:13 AM
kaixin001.com.7z	98443782	22-May-2017 12:54 AM
fling.com_40M_users.sql.7z	2594113915	10-Apr-2018 09:26 AM
modbsolutions.rar	2799583102	22-May-2017 01:35 AM
Arma3Life.sql	105118884	22-May-2017 12:26 AM
comcast.7z	21199935	22-May-2017 12:27 AM
Myspace.com.txt.7z	13117982617	22-May-2017 01:47 AM
DayZ.com_Forum.txt	19995139	22-May-2017 12:27 AM
lastfm-thesle3p.rar	2162247227	22-May-2017 01:22 AM
ovh_kimsufi_2015.7z	51938554	22-May-2017 12:58 AM
index.php	3318	04-Jun-2018 11:01 PM
AndroidForums.com_VB_26-12-2013.sql.7z	43635621	22-May-2017 12:24 AM
taobao.7z	158520312	22-May-2017 01:03 AM
exploit.in.zip	872448000	22-May-2017 12:47 AM
NaughtyAmerica.7z	299009564	22-May-2017 12:59 AM
blackhatworld.7z	67100270	22-May-2017 12:25 AM
forbes-wp_users.txt.zip	66406889	22-May-2017 12:36 AM
Adobe 152M.tar.gz	1457520640	22-May-2017 12:47 AM
Badoo.com_June2016.rar	1286209536	22-May-2017 12:47 AM
Gamevn.com.txt	137100507	22-May-2017 12:38 AM

我不知道多少掌握技巧的“坏人”可以轻轻敲击几下键盘查看所有人的情况，并且利用，各个地方的信息都在传输到隐私的海里，我们已经在海上，如果拒绝上传无法保护你的隐私，你只能尝试着变成一滴水，混在这片海里(破了洞已经堵不住，那就应该造一面镜子)。

>Exploiting fastest:

sploitius :<https://sploitius.com/>

漏洞搜索引擎，可以帮你最快的找到公开漏洞



SPLOITUS

☐ Title only

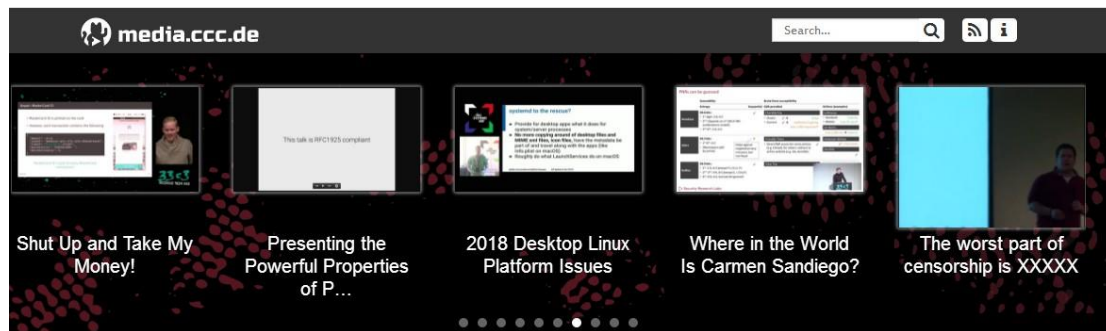
### Exploits of the week

1. Xorg X11 Server SUID Privilege Escalation
2. Joomla Admin 3.7.4 Database Disclosure
3. Joomla MacGallery Database Disclosure
4. WordPress Absolutely Glamorous Custom Admin 6.4.1 Database Disclosure
5. Consona Password Reset Security Bypass
6. WordPress Universal Post Manager 1.5.0 Database Disclosure
7. WordPress Pods 2.7.9 Database Disclosure
8. Cory Support 1.0 SQL Injection
9. Oracle Secure Global Desktop Administration Console 4.4 Cross Site Scripting
10. Unitrends Enterprise Backup bpserved Privilege Escalation

>media.ccc.de

<https://media.ccc.de/>

伟大的平台，去找你需要的东西，获得知识



4 767 hours of content in 29 393 files of 6 118 recordings at 168 events

- Popular
- Recent
- Browse
- All Events

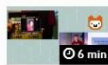
### Recently added

[More recent videos](#)

#### Jugend Hackt 2018



Lightning Talk: Animatronics  
14 min  
2018-11-24



Lightning Talk: Foodrush  
6 min  
2018-11-24

#### Rustfest 2018 Rome

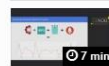


Declarative programming in Rust  
32 min  
2018-11-24



Increasing Rust's Reach Project Highlight  
19 min  
2018-11-24

#### DENOG 10



Using Streaming Telemetry with Prometheus  
7 min  
2018-11-22



DENOG10 closing  
5 min  
2018-11-22



>跟安全人员交流:

在推特上, 开放私信的安全研究人员, 以至于名头很大粉丝巨多, 或者一些安全公司甚至某些专家, 黑客书籍的作者等, 只要开放了, 发送你确切具体的问题, 90%都会答复你, 不管是出名的大牛还是一些不著名独立的 **bughunter**, 不要害怕交流和询问, 你会获得帮助。

>Ending:

“心能转物, 即同如来”

在任何困难的时候, 别无他法的情况下, 改变自己的心境, 才能改变现状;

“天上天下, 唯我独尊”

你已经来到这个世界, 便是独一的, 别人的成功与否与你关系并不大, 不要羡慕和追捧它人, 那只是消磨你的时间, 而要专注于完成你自己的生命修行, 遵照你的内心, 更少的不受外物所扰, 活成一个传奇。