Features Business Explore Marketplace Pricing This repository Search Sign in or Sign up

sergey-pronin / **Awesome-Vulnerability-Research**

Watch 20 Star 271 Fork 54

Code Issues 1 Pull requests 0 Projects 0 Insights

## Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

🦄 A curated list of the awesome resources about the Vulnerability Research

awesome awesome-list vulnerability-research curated reading-list fuzzing exploit-development security-research

**69** commits **1** branch **0** releases **1** contributor

Branch: **master** New pull request Find file Clone or download

**иiиoяꟼ** Merge pull request #2 from insecuritea/master … Latest commit `c78a9c5` on Aug 10, 2017

| | | |
|---|---|---|
| CODE-OF-CONDUCT.md | Update CODE-OF-CONDUCT.md | 10 months ago |

| | | |
|---|---|---|
| CONTRIBUTING.md | Update CONTRIBUTING.md | 10 months ago |
| GLOSSARY.md | Update GLOSSARY.md | 10 months ago |
| LICENSE.md | Update LICENSE.md | 10 months ago |
| README.md | Merge pull request #2 from insecuritea/master | 9 months ago |

**README.md**

# Awesome Vulnerability Research 🕶 awesome

## 🦄 A curated list of the awesome resources about the Vulnerability Research

> First things first: There are no exploits in this project. `Vulnerabilities != Exploits` A Vulnerability resides in the software itself, doing nothing on its own. If you are really curious about then you'll find **your own way** to discover a flow, this list aimed to help you **find it faster**.

Maintained by Serhii Pronin with contributions from the community. Become the next 🌟 stargazer or ✍️ contributor.
In case of emergency gimme a shout 🔑 PGP key fingerprint: `2B56 34F1 51A3 84E0 A039 7815 793A 1A66 A341 8A12`

made with passion license CC-BY-SA-4.0 stars 271

Vulnerability Research is the process of analyzing a product, protocol, or algorithm - or set of related products - to find, understand or exploit one or more vulnerabilities. Vulnerability research can but does not always involve reverse engineering, code review, static and dynamic analysis, fuzzing and debugging.

## Purpose

Currently, there is **way more** insecure code out there than researchers. Much more people looking at code that's deployed in the real world are required by the market. This project exists to share a different awesome sources of information with you and encourage more people to get involved. Here you will find books and articles, online classes, recommended tools, write-ups, methodologies and tutorials, people to follow, and more cool stuff about Vulnerability Research and tinkering with application execution flow in general.

## Contributing

This List is published according to the *"Done is better than Perfect"* approach, so your contributions and suggestions are very valuable and are always welcome! There are two options:

1. Use the standard method of forking this repo, making your changes and doing a pull request to have your content added. Please check the Contributing Guideline for more details.
2. Occasionally, if you just want to copy/paste your content, I'll take that too! Create an "Issue" with your suggestions and I will add it for you.

---

**Legend**:

- 🌟: Most Awesome
- 💰: Costs Money
- 🔥: Hot Stuff
- 🎁: For FREE

---

## Contents

# Advisories

Back to Contents

## Articles

- Super Awesome Fuzzing, Part One - by Atte Kettunen and Eero Kurimo, 2017
- From Fuzzing Apache httpd Server to CVE-2017-7668 and a $1500 Bounty - by Javier Jiménez, 2017
- Root cause analysis of integer flow - by Corelan Team, 2013

Back to Contents

## Books

- 🌟The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities - by Mark Dowd, John McDonald, Justin Schuh - published 2006, ISBN-13: 978-0321444424 / ISBN-10: 9780321444424
- 🌟The Shellcoder's Handbook: Discovering and Exploiting Security Holes - by Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte - published 2007, 2nd Edition, ISBN-13: 978-0470080238 / ISBN-10: 047008023X

Back to Contents

## Classes

- Advanced Windows Exploitation (AWE) - by Offensive Security with complementary OSEE (Offensive Security Exploitation Expert) Certification
- Cracking The Perimeter (CTP) - by Offensive Security, with complementary OSCE (Offensive Security Certified Expert) Certification
- 🎁Modern Binary Exploitation (CSCI 4968) - by RPISEC at Rensselaer Polytechnic Institute in Spring 2015. This was a university course developed and run solely by students to teach skills in vulnerability research, reverse engineering, and binary exploitation.
- Software Security Course on Coursera - by University of Maryland.
- Offensive Computer Security - by W. Owen Redwood and Prof. Xiuwen Liu.

Back to Contents

## Conferences

- 🌟DEF CON - Las Vegas, NV, USA
- Black Hat - Las Vegas, NV, USA
- Black Hat Europe - London, UK //🔥Join me this year on Dec 4-7, 2017!
- Black Hat Asia - Singapore
- 🎁BSides - Worldwide //🔥Join me this year in Warsaw on Oct 13-15, 2017!

- BruCON - Brussels, Belgium
- 🌟Chaos Communication Congress (CCC) - Hamburg, Germany
- Code Blue - Tokyo, Japan
- Nullcon - Goa, India
- 44CON - London, UK
- AppSecUSA - Washington DC
- OWASP AppSec EU - Europewide
- Positive Hack Days - Moscow, Russia
- 🌟ZeroNights - Moscow, Russia //🔥Join me this year on Nov 16-17, 2017!
- 🌟WarCon - Warsaw, Poland

Back to Contents

## Conference talks

- 🌟Vulnerabilities 101: How to Launch or Improve Your Vulnerability Research Game - by Joshua Drake and Steve Christey Coley at DEFCON 24, 2016
- Writing Vulnerability Reports that Maximize Your Bounty Payouts - by Kymberlee Price, originally presented at Nullcon, 2016
- Browser Bug Hunting: Memoirs of a Last Man Standing, by Atte Kettunen, presented at 44CON, 2013

Back to Contents

## Intentionally vulnerable packages

- HackSys Extreme Vulnerable Windows Driver

Back to Contents

## Mailing lists and Newsletters

Back to Contents

## Presentations

- 🌟Vulnerabilities 101: How to Launch or Improve Your Vulnerability Research Game [PDF] - by Joshua Drake and Steve Christey Coley at DEFCON 24, 2016
- 🌟Effective File Format Fuzzing [PDF] - by Mateusz “j00ru” Jurczyk presented at BlackHat EU, 2016
- Bootstrapping A Security Research Project [PDF] or Speaker Deck - by Andrew M. Hay at SOURCE Boston, 2016
- Bug Hunting with Static Code Analysis [PDF] - by Nick Jones, MWR Labs, 2016

Back to Contents

## Podcasts and Episodes

### Podcasts

Back to Contents

### Episodes

Back to Contents

## Relevant Standards

- CVE - Common Vulnerabilities and Exposures, maintained by the MITRE Corporation
- CWE - Common Weakness Enumeration, maintained by the MITRE Corporation
- CVSS - Common Vulnerability Scoring System, maintained by FIRST (Forum of Incident Response and Security Teams)

Back to Contents

### Miscellaneous Documents

- 💰ISO/IEC 29147:2014 - Vulnerability Disclosure Standard
- RFPolicy 2.0 - Full Disclosure Policy (RFPolicy) v2.0 by Packet Storm

Back to Contents

## Research Papers

### Whitepapers

- 🔥TSIG Authentication Bypass Through Signature Forgery in ISC BIND [PDF] - Clément BERTHAUX, Synacktiv, CVE-2017-3143

Back to Contents

### Individual researchers

- 🔥Taking Windows 10 Kernel Exploitation to the Next Level – Leveraging WRITE-WHAT-WHERE Vulnerabilities in Creators Update [PDF] - Morten Schenk, originally presented at Black Hat 2017

Back to Contents

## Tools and Projects

- Windbg - The preferred debugger by exploit writers.
- ltrace - Intercepts library calls
- ansvif - An advanced cross platform fuzzing framework designed to find vulnerabilities in C/C++ code.

- Metasploit Framework - A framework which contains some fuzzing capabilities via Auxiliary modules.
- Spike - A fuzzer development framework like sulley, a predecessor of sulley.

Back to Contents

### GitHub repos

- Google Sanitizers - A repo with extended documentation, bugs and some helper code for the AddressSanitizer, MemorySanitizer, ThreadSanitizer, LeakSanitizer. The actual code resides in the LLVM repository.
- 🔥FLARE VM - FLARE (FireEye Labs Advanced Reverse Engineering) a fully customizable, Windows-based security distribution for malware analysis, incident response, penetration testing, etc.
- hackers-grep - The hackers-grep is a tool that enables you to search for strings in PE files. The tool is capable of searching strings, imports, exports, and public symbols (like woah) using regular expressions.
- Grinder - Grinder is a system to automate the fuzzing of web browsers and the management of a large number of crashes.
- Choronzon - An evolutionary knowledge-based fuzzer
- boofuzz - A fork and successor of Sulley framework
- sandsifter - The x86 processor fuzzer

Back to Contents

## Tutorials

Back to Contents

## Videos

Back to Contents

## Vendor’s bug databases

- Google Chrome issue tracker - The Chromium Project. *Google Account Required*

Back to Contents

## Vulnerability databases

Back to Contents

## Wargames and CTFs

Back to Contents

## Websites

- Corelan Team
- FuzzySecurity by b33f
- Fuzzing Blogs - by fuzzing.info

Back to Contents

### Blogs

- 🌟j00ru//vx tech blog - Coding, reverse engineering, OS internals covered one more time

Back to Contents

## Who to Follow

### GitHub

- FuzzySecurity
- jksecurity
- MortenSchenk

Back to Contents

### Mastodon

Back to Contents

### Medium

- the grugq (@thegrugq)

Back to Contents

### Slack

Back to Contents

### SlideShare

Back to Contents

### Speaker Deck

Back to Contents

### Telegram

Back to Contents

### Twitter

- 🌟Joshua Drake (@jduck)
- 🌟Steve Christey Coley (@sushidude)
- Andrew M. Hay (@andrewsmhay)
- the grugq (@thegrugq)
- b33f (@FuzzySec)
- Tim Strazzere (@timstrazz)
- Wojciech Pawlikowski (@wpawlikowski)
- Atte Kettunen (@attekett)
- Pawel Wylecial (@h0wlu)
- Hooked Browser (@antisnatchor)
- Kymberlee Price (@Kym_Possible)
- Michael Koczwara (@MichalKoczwara)
- Mateusz Jurczyk (@j00ru)
- Project Zero Bugs (@ProjectZeroBugs) - Cheks for new bug reports every 10 minutes. Not affiliated with Google.
- Hack with GitHub (@HackwithGithub) - Open source hacking tools for hackers and pentesters.

Back to Contents

## Miscellaneous Advisories

Back to Contents

# Companies and Jobs

Back to Contents

# Coordinated Disclosure

- SecuriTeam Secure Disclosure (SSD) - SSD provides the support you need to turn your experience uncovering security vulnerabilities into a highly paid career. SSD was designed by researchers, for researchers and will give you the fast response and great support you need to make top dollar for your discoveries.
- The Zero Day Initiative (ZDI) - ZDI is originally founded by TippingPoint, is a program for rewarding security researchers for responsibly disclosing vulnerabilities. Currently managed by Trend Micro.

Back to Contents

# Common Lists

## Awesome Lists

- Awesome AppSec - A curated list of resources for learning about application security. Contains books, websites, blog posts, and self-assessment quizzes.
- Awesome Web Security - A curated list of Web Security materials and resources.

Back to Contents

## Other Lists

- Hack with Github - Open source hacking tools for hackers and pentesters.

- Movies for Hackers - A list of movies every cyberpunk must watch.
- SecLists - SecLists is the security tester's companion.

Back to Contents

## Thanks

- Joshua Drake (@jduck) and Steve Christey Coley (@sushidude) for the inspiration!
- *@yournamehere* for the most awesome contributions
- And sure everyone of you, who has sent the pull requests or suggested a link to add here!

Thanks a lot!

Back to Contents

## License

Back to Contents