paragonie / **awesome-appsec**

Watch 273 | Star 3,137 | Fork 337

<> Code | Issues 5 | Pull requests 2 | 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 resources for learning about application security https://paragonie.com/projects

security-experts reading-list curated application-security security owasp

109 commits | **1** branch | **0** releases | **16** contributors | MIT

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

paragonie-security Add the 2018 PHP Security Guide Latest commit `a3b5059` on Mar 10

data	Add the 2018 PHP Security Guide	2 months ago

img	Add non-free image	3 years ago
src	Add PHP libsodium book	3 years ago
template	Add more resources; added contributing guide	3 years ago
CONTRIBUTING.md	Update CONTRIBUTING.md	3 years ago
LICENSE	Initial commit	3 years ago
README.md	Add the 2018 PHP Security Guide	2 months ago

README.md

Awesome AppSec awesome

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

Maintained by Paragon Initiative Enterprises with contributions from the application security and developer communities. We also have other community projects which might be useful for tomorrow's application security experts.

If you are an absolute beginner to the topic of software security, you may benefit from reading A Gentle Introduction to Application Security.

Contributing

Please refer to the contributing guide for details.

Application Security Learning Resources

- General
  - Articles
    - How to Safely Generate a Random Number (2014)
    - Salted Password Hashing - Doing it Right (2014)
    - A good idea with bad usage: /dev/urandom (2014)
    - Why Invest in Application Security? (2015)
    - Be wary of one-time pads and other crypto unicorns (2015)
  - Books
    - Web Application Hacker's Handbook (2011) 💵
    - Cryptography Engineering (2010) 💵
    - Securing DevOps (2018) 💵
    - Gray Hat Python: Programming for Hackers and Reverse Engineers (2009) 💵
    - The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities (2006) 💵
    - C Interfaces and Implementations: Techniques for Creating Reusable Software (1996) 💵
    - Reversing: Secrets of Reverse Engineering (2005) 💵
    - JavaScript: The Good parts (2008) 💵
    - Windows Internals: Including Windows Server 2008 and Windows Vista, Fifth Edition (2007) 💵
    - The Mac Hacker's Handbook (2009) 💵
    - The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (2008) 💵
    - Internetworking with TCP/IP Vol. II: ANSI C Version: Design, Implementation, and Internals (3rd Edition) (1998) 💵
    - Network Algorithmics,: An Interdisciplinary Approach to Designing Fast Networked Devices (2004) 💵

        - Computation Structures (MIT Electrical Engineering and Computer Science) (1989) 💵
        - Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection (2009) 💵
        - Secure Programming HOWTO (2015)
        - Security Engineering - Second Edition (2008)
        - Bulletproof SSL and TLS (2014) 💵
        - Holistic Info-Sec for Web Developers (Fascicle 0) (2016)
        - Holistic Info-Sec for Web Developers (Fascicle 1)
    - Classes
        - Offensive Computer Security (CIS 4930) FSU
        - Hack Night
    - Websites
        - Hack This Site!
        - Enigma Group
        - Web App Sec Quiz
        - SecurePasswords.info
        - Security News Feeds Cheat-Sheet
        - Open Security Training
        - MicroCorruption
        - The Matasano Crypto Challenges
        - PentesterLab
        - Juice Shop
        - Supercar Showdown
        - OWASP NodeGoat
        - Blogs

      - Crypto Fails
      - NCC Group - Blog
      - Scott Helme
    - Wiki pages
      - OWASP Top Ten Project
    - Tools
      - Qualys SSL Labs
      - securityheaders.io
      - report-uri.io
- Android
  - Books and ebooks
    - SEI CERT Android Secure Coding Standard (2015)
- C
  - Books and ebooks
    - SEI CERT C Coding Standard (2006)
    - Defensive Coding: A Guide to Improving Software Security by the Fedora Security Team (2018)
- C++
  - Books and ebooks
    - SEI CERT C++ Coding Standard (2006)
- C Sharp
  - Books and ebooks
    - Security Driven .NET (2015) 💵
- Go
  - Articles
    - Memory Security in Go - cryptolosophy.io (2017)
- Java

  - Books and ebooks
    - SEI CERT Java Coding Standard (2007)
    - Secure Coding Guidelines for Java SE (2014)
- Node.js
  - Articles
    - Node.js Security Checklist - Rising Stack Blog (2015)
  - Books and ebooks
    - Essential Node.js Security (2017) 💵
  - Training
    - Security Training by ^Lift Security 💵
    - Security Training from BinaryMist 💵
- PHP
  - Articles
    - It's All About Time (2014)
    - Secure Authentication in PHP with Long-Term Persistence (2015)
    - 20 Point List For Preventing Cross-Site Scripting In PHP (2013)
    - 25 PHP Security Best Practices For Sys Admins (2011)
    - PHP data encryption primer (2014)
    - Preventing SQL Injection in PHP Applications - the Easy and Definitive Guide (2014)
    - You Wouldn't Base64 a Password - Cryptography Decoded (2015)
    - A Guide to Secure Data Encryption in PHP Applications (2015)
    - The 2018 Guide to Building Secure PHP Software (2017)
  - Books and ebooks
    - Securing PHP: Core Concepts 💵
    - Using Libsodium in PHP Projects

    - Useful libraries
        - defuse/php-encryption
        - ircmaxell/password_compat
        - ircmaxell/RandomLib
        - thephpleague/oauth2-server
        - paragonie/random_compat
        - psecio/gatekeeper
        - openwall/phpass
    - Websites
        - websec.io
        - Blogs
            - Paragon Initiative Enterprises Blog
            - ircmaxell's blog
            - Pádraic Brady's Blog
        - Mailing lists
            - Securing PHP Weekly
- Perl
    - Books and ebooks
        - SEI CERT Perl Coding Standard (2011)
- Python
    - Books and ebooks
        - Python chapter of Fedora Defensive Coding Guide
        - Black Hat Python: Python Programming for Hackers and Pentesters 💵
        - Violent Python 💵
    - Websites

    - OWASP Python Security Wiki (2014)
- Ruby
  - Books and ebooks
    - Secure Ruby Development Guide (2014)

General

Articles

How to Safely Generate a Random Number (2014)

Released: February 25, 2014

Advice on cryptographically secure pseudo-random number generators.

Salted Password Hashing - Doing it Right (2014)

Released: August 6, 2014

A post on Crackstation, a project by Defuse Security

A good idea with bad usage: /dev/urandom (2014)

Released: May 3, 2014

Mentions many ways to make `/dev/urandom` fail on Linux/BSD.

Why Invest in Application Security? (2015)

Released: June 21, 2015

Running a business requires being cost-conscious and minimizing unnecessary spending. The benefits of ensuring in the security of your application are invisible to most companies, so often times they neglect to invest in secure software development as a cost-saving measure. What these companies don't realize is the potential cost (both financial and to brand reputation) a preventable data compromise can incur.

The average data breach costs millions of dollars in damage.

Investing more time and personnel to develop secure software is, for most companies, worth it to minimize this unnecessary risk to their bottom line.

Be wary of one-time pads and other crypto unicorns (2015)

Released: March 25, 2015

A **must-read** for anyone looking to build their own cryptography features.

Books

💵 Web Application Hacker's Handbook (2011)

Released: September 27, 2011

Great introduction to Web Application Security; though slightly dated.

💵 Cryptography Engineering (2010)

Released: March 15, 2010

Develops a sense of professional paranoia while presenting crypto design techniques.

💵 Securing DevOps (2018)

Released: March 1, 2018

Securing DevOps explores how the techniques of DevOps and Security should be applied together to make cloud services safer. This introductory book reviews state of the art practices used in securing web applications and their infrastructure, and teaches you techniques to integrate security directly into your product.

💵 Gray Hat Python: Programming for Hackers and Reverse Engineers (2009)

Released: May 3, 2009

💵 The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities (2006)

Released: November 30, 2006

💵 C Interfaces and Implementations: Techniques for Creating Reusable Software (1996)

Released: August 30, 1996

💵 Reversing: Secrets of Reverse Engineering (2005)

Released: April 15, 2005

💵 JavaScript: The Good parts (2008)

Released: May 1, 2008

💵 **Windows Internals: Including Windows Server 2008 and Windows Vista, Fifth Edition (2007)**

Released: June 17, 2007

💵 **The Mac Hacker's Handbook (2009)**

Released: March 3, 2009

💵 **The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (2008)**

Released: August 22, 2008

💵 **Internetworking with TCP/IP Vol. II: ANSI C Version: Design, Implementation, and Internals (3rd Edition) (1998)**

Released: June 25, 1998

💵 **Network Algorithmics,: An Interdisciplinary Approach to Designing Fast Networked Devices (2004)**

Released: December 29, 2004

💵 **Computation Structures (MIT Electrical Engineering and Computer Science) (1989)**

Released: December 13, 1989

💵 **Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection (2009)**

Released: August 3, 2009

Secure Programming HOWTO (2015)

Released: March 1, 2015

Security Engineering - Second Edition (2008)

Released: April 14, 2008

💵 Bulletproof SSL and TLS (2014)

Released: August 1, 2014

Holistic Info-Sec for Web Developers (Fascicle 0) (2016)

Released: September 17, 2016

The first part of a three part book series providing broad and in-depth coverage on what web developers and architects need to know in order to create robust, reliable, maintainable and secure software, networks and other, that are delivered continuously, on time, with no nasty surprises.

Holistic Info-Sec for Web Developers (Fascicle 1)

The second part of a three part book series providing broad and in-depth coverage on what web developers and architects need to know in order to create robust, reliable, maintainable and secure software, VPS, networks, cloud and web applications, that are delivered continuously, on time, with no nasty surprises.

Classes

Offensive Computer Security (CIS 4930) FSU

A vulnerability research and exploit development class by Owen Redwood of Florida State University.

Be sure to check out the lectures!

Hack Night

Developed from the materials of NYU Poly's old Penetration Testing and Vulnerability Analysis course, Hack Night is a sobering introduction to offensive security. A lot of complex technical content is covered very quickly as students are introduced to a wide variety of complex and immersive topics over thirteen weeks.

Websites

Hack This Site!

Learn about application security by attempting to hack this website.

Enigma Group

Where hackers and security experts come to train.

Web App Sec Quiz

Self-assessment quiz for web application security

SecurePasswords.info

Secure passwords in several languages/frameworks.

Security News Feeds Cheat-Sheet

A list of security news sources.

Open Security Training

Video courses on low-level x86 programming, hacking, and forensics.

MicroCorruption

Capture The Flag - Learn Assembly and Embedded Device Security

The Matasano Crypto Challenges

A series of programming exercises for teaching oneself cryptography by Matasano Security. The introduction by Maciej Ceglowski explains it well.

PentesterLab

PentesterLab provides free Hands-On exercises and a bootcamp to get started.

Juice Shop

An intentionally insecure Javascript Web Application.

Supercar Showdown

How to go on the offence before online attackers do.

OWASP NodeGoat

Purposly vulnerable to the OWASP Top 10 Node.JS web application, with tutorials, security regression testing with the OWASP Zap API, docker image. With several options to get up and running fast.

Blogs

Crypto Fails

Showcasing bad cryptography

NCC Group - Blog

The blog of NCC Group, formerly Matasano, iSEC Partners, and NGS Secure.

Scott Helme

Learn about security and performance.

Wiki pages

OWASP Top Ten Project

The top ten most common and critical security vulnerabilities found in web applications.

Tools

Qualys SSL Labs

The infamous suite of SSL and TLS tools.

securityheaders.io

Quickly and easily assess the security of your HTTP response headers.

report-uri.io

A free CSP and HPKP reporting service.

Android

Books and ebooks

SEI CERT Android Secure Coding Standard (2015)

Released: February 24, 2015

A community-maintained Wiki detailing secure coding standards for Android development.

C

Books and ebooks

SEI CERT C Coding Standard (2006)

Released: May 24, 2006

A community-maintained Wiki detailing secure coding standards for C programming.

Defensive Coding: A Guide to Improving Software Security by the Fedora Security Team (2018)

Released: March 10, 2018

Provides guidelines for improving software security through secure coding. Covers common programming languages and libraries, and focuses on concrete recommendations.

C++

Books and ebooks

SEI CERT C++ Coding Standard (2006)

Released: July 18, 2006

A community-maintained Wiki detailing secure coding standards for C++ programming.

C Sharp

Books and ebooks

💵 Security Driven .NET (2015)

Released: July 14, 2015

An introduction to developing secure applications targeting version 4.5 of the .NET Framework, specifically covering cryptography and security engineering topics.

Go

Articles

Memory Security in Go - cryptolosophy.io (2017)

Released: August 3, 2017

A guide to managing sensitive data in memory.

Java

Books and ebooks

SEI CERT Java Coding Standard (2007)

Released: January 12, 2007

A community-maintained Wiki detailing secure coding standards for Java programming.

Secure Coding Guidelines for Java SE (2014)

Released: April 2, 2014

Secure Java programming guidelines straight from Oracle.

Node.js

Articles

Node.js Security Checklist - Rising Stack Blog (2015)

Released: October 13, 2015

Covers a lot of useful information for developing secure Node.js applications.

Books and ebooks

💵 Essential Node.js Security (2017)

Released: July 19, 2017

Hands-on and abundant with source code for a practical guide to Securing Node.js web applications.

Training

💵 Security Training by ^Lift Security

Learn from the team that spearheaded the Node Security Project

💵 Security Training from BinaryMist

We run many types of info-sec security training, covering Physical, People, VPS, Networs, Cloud, Web Applications. Most of the content is sourced from the book series Kim has been working on for several years. More info can be found here

PHP

Articles

It's All About Time (2014)

Released: November 28, 2014

A gentle introduction to timing attacks in PHP applications

Secure Authentication in PHP with Long-Term Persistence (2015)

Released: April 21, 2015

Discusses password policies, password storage, "remember me" cookies, and account recovery.

20 Point List For Preventing Cross-Site Scripting In PHP (2013)

Released: April 22, 2013

Padriac Brady's advice on building software that isn't vulnerable to XSS

25 PHP Security Best Practices For Sys Admins (2011)

Released: November 23, 2011

Though this article is a few years old, much of its advice is still relevant as we veer around the corner towards PHP 7.

PHP data encryption primer (2014)

Released: June 16, 2014

@timoh6 explains implementing data encryption in PHP

Preventing SQL Injection in PHP Applications - the Easy and Definitive Guide (2014)

Released: May 26, 2014

TL;DR - don't escape, use prepared statements instead!

You Wouldn't Base64 a Password - Cryptography Decoded (2015)

Released: August 7, 2015

A human-readable overview of commonly misused cryptography terms and fundamental concepts, with example code in PHP.

If you're confused about cryptography terms, start here.

A Guide to Secure Data Encryption in PHP Applications (2015)

Released: August 2, 2015

Discusses the importance of end-to-end network-layer encryption (HTTPS) as well as secure encryption for data at rest, then introduces the specific cryptography tools that developers should use for specific use cases, whether they use libsodium, Defuse Security's secure PHP encryption library, or OpenSSL.

The 2018 Guide to Building Secure PHP Software (2017)

Released: December 12, 2017

This guide should serve as a complement to the e-book, PHP: The Right Way, with a strong emphasis on security and not general PHP programmer topics (e.g. code style).

Books and ebooks

💵 Securing PHP: Core Concepts

Securing PHP: Core Concepts acts as a guide to some of the most common security terms and provides some examples of them in every day PHP.

Using Libsodium in PHP Projects

You shouldn't need a Ph.D in Applied Cryptography to build a secure web application. Enter libsodium, which allows developers to develop fast, secure, and reliable applications without needing to know what a stream cipher even is.

Useful libraries

defuse/php-encryption

Symmetric-key encryption library for PHP applications. (**Recommended** over rolling your own!)

ircmaxell/password_compat

If you're using PHP 5.3.7+ or 5.4, use this to hash passwords

ircmaxell/RandomLib

Useful for generating random strings or numbers

thephpleague/oauth2-server

A secure OAuth2 server implementation

paragonie/random_compat

PHP 7 offers a new set of CSPRNG functions: `random_bytes()` and `random_int()`. This is a community effort to expose the same API in PHP 5 projects (forward compatibility layer). Permissively MIT licensed.

psecio/gatekeeper

A secure authentication and authorization library that implements Role-Based Access Controls and Paragon Initiative Enterprises' recommendaitons for secure "remember me" checkboxes.

openwall/phpass

A portable public domain password hashing framework for use in PHP applications.

Websites

websec.io

websec.io is dedicated to educating developers about security with topics relating to general security fundamentals, emerging technologies and PHP-specific information

Blogs

Paragon Initiative Enterprises Blog

The blog of our technology and security consulting firm based in Orlando, FL

ircmaxell's blog

A blog about PHP, Security, Performance and general web application development.

Pádraic Brady's Blog

Pádraic Brady is a Zend Framework security expert

Mailing lists

Securing PHP Weekly

A weekly newsletter about PHP, security, and the community.

Perl

Books and ebooks

SEI CERT Perl Coding Standard (2011)

Released: January 10, 2011

A community-maintained Wiki detailing secure coding standards for Perl programming.

Python

Books and ebooks

Python chapter of Fedora Defensive Coding Guide

Lists standard library features that should be avoided, and references sections of other chapters that are Python-specific.

💵 Black Hat Python: Python Programming for Hackers and Pentesters

Black Hat Python by Justin Seitz from NoStarch Press is a great book for the offensive security minds

💵 Violent Python

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation.

Websites

OWASP Python Security Wiki (2014)

Released: June 21, 2014

A wiki maintained by the OWASP Python Security project.

Ruby

Books and ebooks

Secure Ruby Development Guide (2014)

Released: March 10, 2014

A guide to secure Ruby development by the Fedora Security Team. Also available on Github.