

# Web Application Security Guide

---

[Edit Intro \(https://en.wikibooks.org/w/index.php?title=Web\\_Application\\_Security\\_Guide/Intro&action=edit\)](https://en.wikibooks.org/w/index.php?title=Web_Application_Security_Guide/Intro&action=edit)

This guide attempts to provide a comprehensive overview of web application security. Common web application security issues and methods how to prevent them are explained. Web server and operating system security are not covered. The guide is intended mainly for web application developers, but can also provide useful information for web application reviewers.

The [checklist](#) gives a short summary containing only the individual guidelines. It is recommended to take the time and read the full version, where the guidelines are explained in detail, especially if any questions arise.

Most web application developers probably (hopefully) already know some or even most of the points mentioned in this guide. However, there will probably be something new for every developer. Remember, as a developer it is your responsibility to develop your application securely, and a single mistake may be enough to allow an attack.

## Contents

---

- [Checklist](#)
- [Topics](#)
  1. [Miscellaneous points](#)
  2. [File inclusion and disclosure](#)
  3. [File upload vulnerabilities](#)
  4. [SQL injection](#)
  5. [Cross-site scripting \(XSS\)](#)
  6. [XML and internal data escaping](#)
  7. [XML, JSON and general API security](#)
  8. [\(Un\)trusted input](#)
  9. [Cross-site request forgery \(CSRF\)](#)
  10. [Clickjacking](#)
  11. [Insecure data transfer](#)
  12. [Session fixation](#)
  13. [Session stealing](#)
  14. [Truncation attacks, trimming attacks](#)
  15. [Password security](#)
  16. [Comparison issues](#)
  17. [PHP-specific issues](#)
  18. [Prefetching and Spiders](#)
  19. [Special files](#)
  20. [SSL, TLS and HTTPS basics](#)
- [Further reading](#)
- [Authors](#)

The [print version](#) provides the entire book on a single page.

## Web Application Security Guide

[Main book page](#) | [Introduction](#) | [Checklist](#)

[Miscellaneous points](#) | [File inclusion and disclosure](#) | [File upload vulnerabilities](#) | [SQL injection](#) | [Cross-site scripting \(XSS\)](#) | [XML and internal data escaping](#) | [XML, JSON and general API security](#) | [\(Un\)trusted input](#) | [Cross-site request forgery \(CSRF\)](#) | [Clickjacking](#) | [Insecure data transfer](#) | [Session fixation](#) | [Session stealing](#) | [Truncation attacks, trimming attacks](#) | [Password security](#) | [Comparison issues](#) | [PHP-specific issues](#) | [Prefetching and Spiders](#) | [Special files](#) | [SSL, TLS and HTTPS basics](#)

[Further reading](#) | [Authors](#) | [Print version](#)

---

Retrieved from "[https://en.wikibooks.org/w/index.php?title=Web\\_Application\\_Security\\_Guide&oldid=3470463](https://en.wikibooks.org/w/index.php?title=Web_Application_Security_Guide&oldid=3470463)"

---

This page was last edited on 24 September 2018, at 00:47.

Text is available under the Creative Commons Attribution-ShareAlike License.; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy.