Web App Hacking: Cookie Attacks

INTRODUCTION

Dawid Czagan
SECURITY INSTRUCTOR

@dawidczagan

Overview

Importance of secure cookie processing

Cookie attacks

Cookie processing fundamentals

Cookies store sensitive data (session ID, ...)

Leakage of cookie with session ID = user impersonation

Two-factor authentication will not help!

Importance of Secure Cookie Processing

Common Cookie Attacks

Leakage of cookie with sensitive data

Cookie hijacking

Weaknesses in cookie lifecycle:

- Log in
- Log out

More Advanced Cookie Attacks

Underestimated risk: XSS via cookie

Remote cookie tampering

Cookie Processing Fundamentals

Cookie:

- Name
- Value
- Optional attribute(s)

Web app → browser
(Set-Cookie)

Browser → web app
(automatically appended)