Summary

Dawid Czagan
SECURITY INSTRUCTOR

@dawidczagan

Summary

Importance of secure cookie processing

Cookie attacks:

- Leakage of cookie with sensitive data
- Cookie hijacking
- Weaknesses in cookie lifecycle
- Underestimated risk: XSS via cookie
- Remote cookie tampering

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

HTTP: insecure

HTTPS: secure

Secure attribute: cookie sent over HTTPS

Leakage of Cookie with Sensitive Data

XSS: stealing cookie with session ID

HttpOnly attribute: cookie can't be read (XSS)

Cookie Hijacking

Regenerate cookies with sensitive data

Remember about server-side invalidation

Weaknesses in Cookie Lifecycle

XSS via cookie

≠

local exploitation

Cross-origin exploitation

Sanitize special characters

Underestimated Risk: XSS via Cookie

Browser dependent exploitation

↓

More powerful attacks

Comma-separated list of cookies

↓

Remote cookie tampering

Remote Cookie Tampering