

Live demo: XSS

Hvorfor er phishing og XSS så giftig?

Speaker: Jakob Bo Møller

wingmen | wingmen SECURITY

Agenda

- Hvorfor er XSS stadig relevant?
- Kort intro til demo
- Demo
- Hvad kan aktøren opnå med XSS
- Learnings / hvordan forsvarer vi os?







wingmen part of springboardnetwork | wingmen SECURITY

Hvorfor er XSS stadig relevant?

- XSS = Cross-Site Scripting (Første CVE-1999-1167)
  - OWASP top 10 i ALLE udgivelser (8 gange)
  - Ondsindet kode injected på en ellers legitim hjemmeside
- AI finder hurtigt XSS
- AI gør phishing “nemt” for ondsindede aktører



WordPress core (~40% af alle websider)

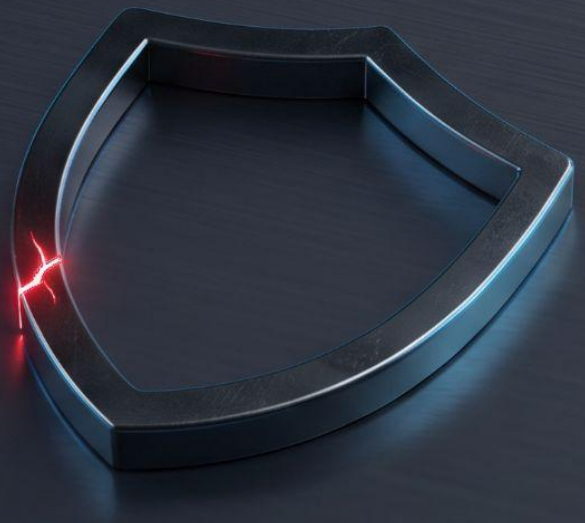
- XSS2Shell (CVE-2026-64638, CVSS score: 8.9)

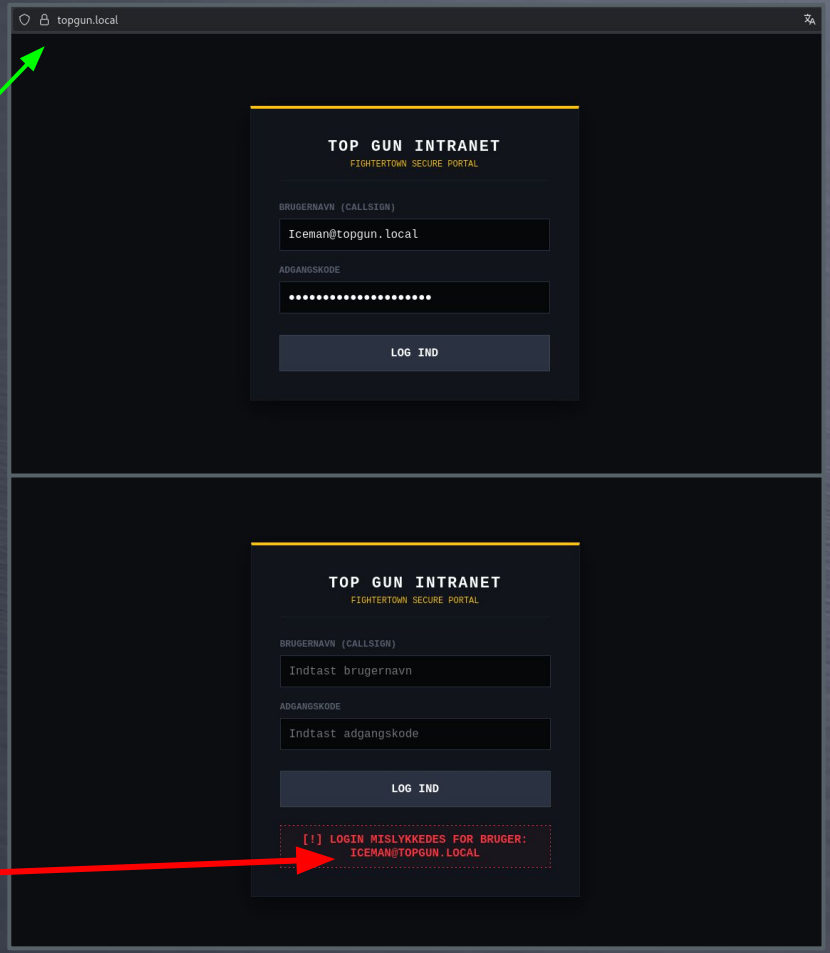
WordPress plugins

- WooCommerce (CVE-2026-93836, CVSS score: 7.1) (20% af WordPress)
- Ninja Forms (CVE-2026-94504, CVSS score: 7.1)

Kort intro til demo

- Reflected XSS -> brugernavn reflected





wingmen | wingmen SECURITY

Demo


SYSTEM HEALTHY
SECURED
LOGS ACTIVE
NETWORK · STABLE
ALERT:
ANOMALY DETECTED
- ZONE 7
CYBER COMMAND

Hvad kan aktøren opnå med XSS

- Credential harvest
- Scraping af data gemt bag login
- Password reset
- Session hijack - Gør alt hvad brugeren kan
- Skjult persistence (usynlige users, magic login URL mm.)
- Remote code execution (RCE) - WordPress plugin install
- Next step med credentials / RCE
    - Login cloud / onprem som standard bruger



Learnings / hvordan forsvarer vi os?



- XSS er fortsat en trussel
- Kendte domæne navne er ikke sikkerhed
- Sikker forbindelse er ikke sikkerhed
- Mouse over - svær at gennemskue

- Tech som forsvar —>
  - Same-Origin Policy (SOP) -> Begrænser script adgang
  - Content Security Policy (CSP) -> Stopper extern scripts
  - HttpOnly Cookies -> Forhindre cookie adgang for scripts
  - Input Sanering -> Renser ondsindet input
  - Context-Aware Output Encoding -> Renser output
  - Web Application Firewall (WAF) -> Skjold udenom websiden
  - **2-factor authentication!**

- Er du i tvivl, så er du ikke i tvivl
  - Skriv adressen manuelt
  - Bookmarks

Tak for nu



jakobbomoeller

jbm@wingmen.security

wingmen
part of springboard network

wingmen
SECURITY