

Nye hacks i test

SOCO Frokostseminar, 18. november 2025

AUDUN URKE



Agenda

Hva kan vi lære av hackerne og pentesterne?

- Perspektivet
- Utforskningen
- Viljen og motivasjonen
- Fleksibiliteten

Test

- Teknisk tester
- 13 år i testfaget
- 7 år i SOCO



AUDUN URKE

Pentesting

- Script kiddie

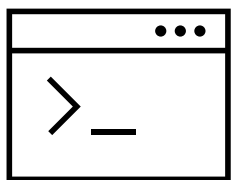
Perspektivet

Et mulig angrepsperspektiv

- Produksjonsmiljø
- Helheten
- Black Box

Verktøyet NMAP

PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	filtered	smtp
80/tcp	open	http
5060/tcp	filtered	sip
9929/tcp	open	nping-echo
31337/tcp	open	Elite



SSH terminal



SMTP epost



HTTP webserver

Operativsystem og versjon

- Windows 11
- Ubuntu

Domenenavn

```
--- http-vhosts script results ---  
• www.example.com  
• api.example.com  
• blog.example.com
```

Databaser

- MySQL version: 5.7.31
- PostgreSQL version: 12.3

Perspektivet

Tester



Pentester/hacker



Fokus

Relevant for release

Alle relevante mangler

Perspektivet

Tester



Pentester/hacker



Hvor

Testmiljø

Produksjon

Perspektivet

Tester



Testtilfeller
ISO-standarder
Beste praksis

Hvordan

Pentester/hacker



Alle typer sårbarheter

Perspektivet

Tester



Pentester/hacker



Hvorfor

Vise tiltak hjelper

Innhente relevant info

Utforskningen

Simultaneously designing and executing tests to learn about the system, using your insights from the last experiment to inform the next.

The
Pragmatic
Programmers

Explore It!

Reduce Risk and
Increase Confidence with
Exploratory Testing



Elisabeth Hendrickson
Edited by Jacquelyn Carter

Utforskningen

Test Charter

Explore input fields
with JavaScript and
SQL injection attacks
to discover
security vulnerabilities

Utforskningen

Explore input fields
with _____ attacks
to discover
security vulnerabilities

Command Injection

Server-Side Request Forgery (SSRF)

File Upload

Server-Side Template Injection (SSTI)

Directory Traversal

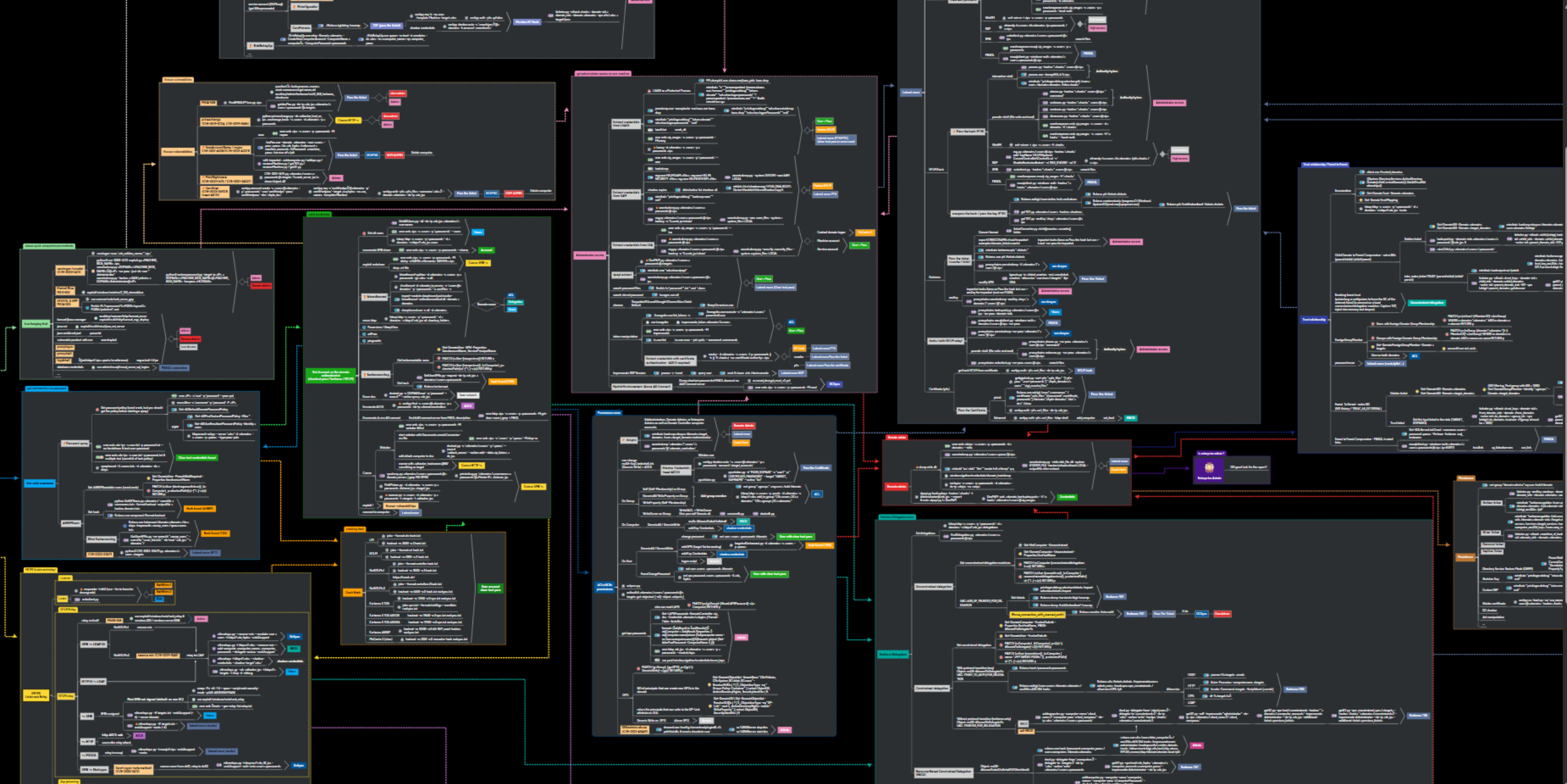
Insecure Direct Object Reference

Hvordan?

Explore input fields
with XSS attacks
to discover
security vulnerabilities

Event handlers that do not require user interaction

Event:	Description:	Tag:	Code:
onafterscriptexecute			
Compatibility:	Fires after script is executed	custom tags ▼	<xss onafterscriptexecute=alert(1)> <script>1</script>
  			
onanimationcancel			
Compatibility:	Fires when a CSS animation cancels	custom tags ▼	<style>@keyframes x{from {left:0;}to {left: 1000px;}}:target {animation:10s ease-in-out 0s 1 x;}</style><xss id=x style="position:absolute;" onanimationcancel="print()"></xss>
  			
onanimationend			
Compatibility:	Fires when a CSS animation ends	custom tags ▼	<style>@keyframes x{}</style><xss style="animation-name:x" onanimationend="alert(1)"></xss>
  			
onanimationiteration			
Compatibility:	Fires when a CSS animation repeats	custom tags ▼	<style>@keyframes slidein {}</style><xss style="animation-duration:1s;animation-name:slidein;animation-iteration-count:2" onanimationiteration="alert(1)"></xss>
  			



Utforskningen

***running out of time
is probably the **worst criterion**
to use to determine
when to stop exploring***

Viljen og motivasjonen



Fleksibilitet

Tester



Hacker



Verktøy

Pentester

Kommersielle lisenser
Sikkerhetspolicy
Personvernpolicy

Kraftige angrepsverktøy
Egne scripts/angrepskode
Github o.l

Fleksibilitet

Tester



Hacker



Datagrunnlag

Pentester

Syntetisk testdata
Strengt regler for behandling

Brukere er et mål

Fleksibilitet

Tester



Tid

Hacker



Avgrenset release-syklus

Potensielt lange perioder

Mulige take aways

- ✓ Prøv nye perspektiver, teste i Prod og let etter info
- ✓ Sette av tid til mer utforskende testing
- ✓ Motivasjon kan påvirke
- ✓ Nye fremgangsmåter, verktøy og data

Komme i gang med pentesting

- ✓ TryHackMe
<https://tryhackme.com>
- ✓ TCM
<https://academy.tcm-sec.com/p/practical-ethical-hacking-the-complete-course>
- ✓ HackTheBox
<https://www.hackthebox.com/hacker>
- ✓ PortSwigger Web Academy
<https://portswigger.net/web-security>
- ✓ OWASP
<https://owasp.org/www-project-web-security-testing-guide/latest/>

Vårt bidrag

- ✓ Observere
- ✓ Melde fra
- ✓ Spørre
- ✓ Teste



Q&A



Neste SOCO Frokostseminar



Lansering Testinnsikt 2026!

KI i test og testing av KI

Tirsdag 4. februar. august

Hotel Continental

www.soco.no