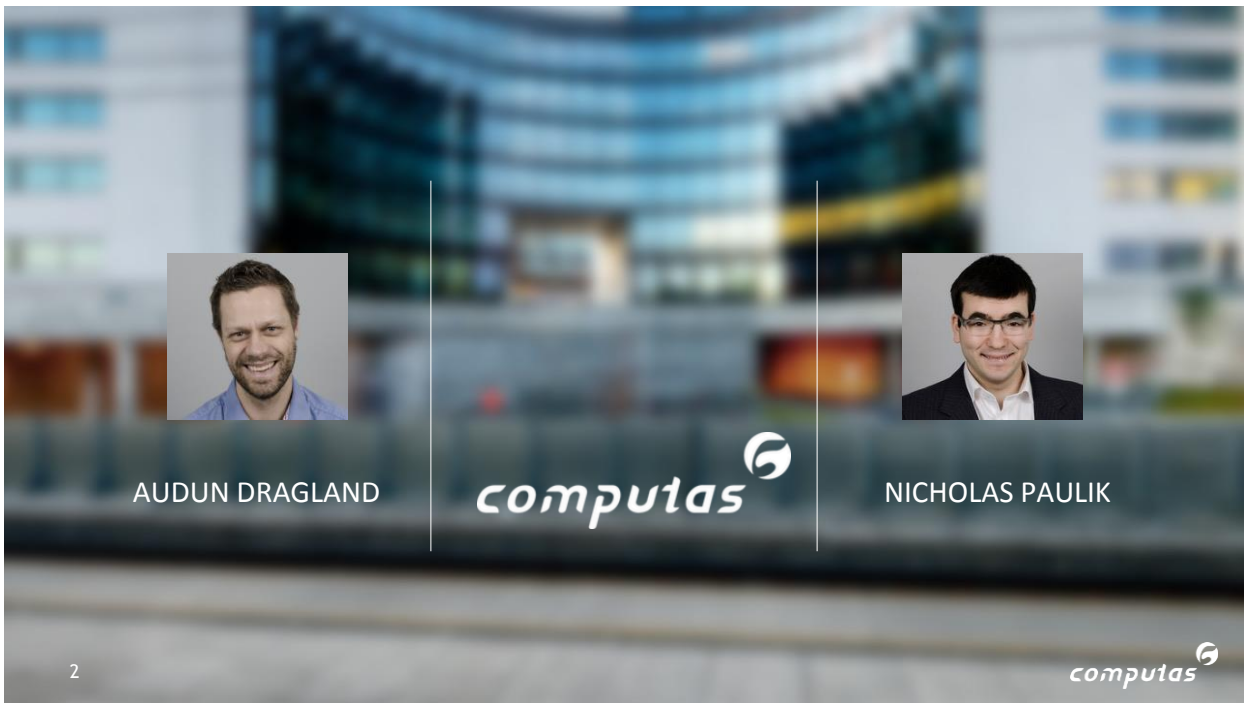
HACKING OWASP Top 10

computas



OWASP

Open Web Application Security Project

computas

The OWASP Top 10 - 2013:

- A1 - Injection
- A2 - Broken Authentication and Session Management
- A3 - Cross-Site Scripting (XSS)
- A4 - Insecure Direct Object References
- A5 - Security Misconfiguration
- A6 - Sensitive Data Exposure
- A7 - Missing Function Level Access Control
- A8 - Cross-Site Request Forgery (CSRF)
- A9 - Using Components with Known Vulnerabilities
- A10 - Unvalidated Redirects and Forwards

computas

A10 - UNVALIDATED REDIRECTS AND FORWARDS

5

A10 – Unvalidated Redirects and Forwards

Original URL:
https://lovligside.no/login?redirect=https://lovligside.no/profile

Phishing-URL:
https://lovligside.no/login?redirect=http://scamside.info

6

computas

A7 - MISSING FUNCTION LEVEL ACCESS CONTROL

7

A8 - CROSS-SITE REQUEST FORGERY (XSRF)

8

Cross-site request forgery (XSRF)

Klassisk eksempel:

```
<b>Hei Alex!</b>

Fint vær i dag! Håper du har det bra!
<img
src="http://bank.no/transfer?from=alex&to=martin&sum=1
000000" />

Med vennlig hilsen
Martin
```

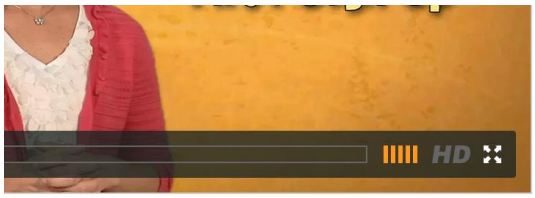
9

computas

<script>

A3 - CROSS-SITE SCRIPTING (XSS)

10



me basic info to setup your account.

* Nicho

* Paulik<script>function evilhack(death

mail *

Password *

REGISTER NOW

Cross-site scripting (XSS)

Reflektert

- URL inneholder den ondsinnede koden
- Bruker klikker på URL

Lagret

- Angriperen lagrer koden på nettstedet
- Brukere som går til nettstedet får koden kjørt

11

A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

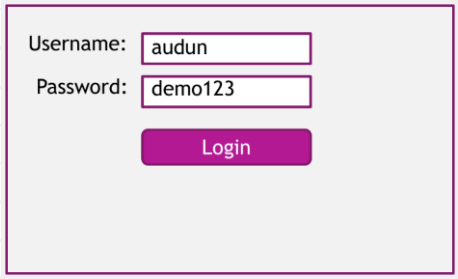
12

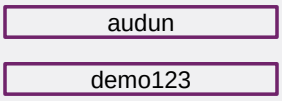
A5 - SECURITY MISCONFIGURATION

A1 - INJECTION FLAWS

Injection Flaws - eksempel

```
cmd.CommandText = "SELECT * FROM Users WHERE
                  Username ='" + txtUsername.Text + "' AND
                  Password='" + txtPassword.Text + "'";
```





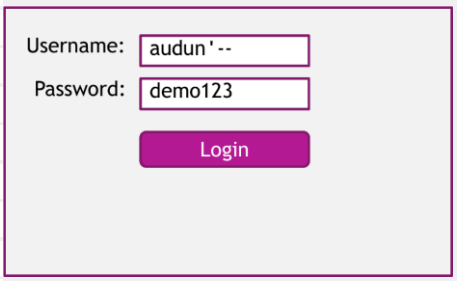

```
SELECT * FROM Users WHERE Username ='audun' AND Password='demo123'
```

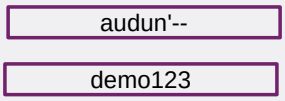
15

computas

Injection Flaws - eksempel

```
cmd.CommandText = "SELECT * FROM Users WHERE
                  Username ='" + txtUsername.Text + "' AND
                  Password='" + txtPassword.Text + "'";
```






```
SELECT * FROM Users WHERE Username ='audun'--' AND Password='demo123'
```

16

computas

Vær i forkant

- Mange sårbarheter er enkle å oppdage – enkle å teste/utnytte
- Kom tidlig i gang med sikkerhetstesting og trusselmodell
- Utpek sikkerhetsildsjel blant utviklerne – bygg sikkerhetskultur
- Forsøk å trene kunden i sikkerhetstesting - ikke bare testing
- Kjør automatiserte verktøy og scannere regelmessig

computas