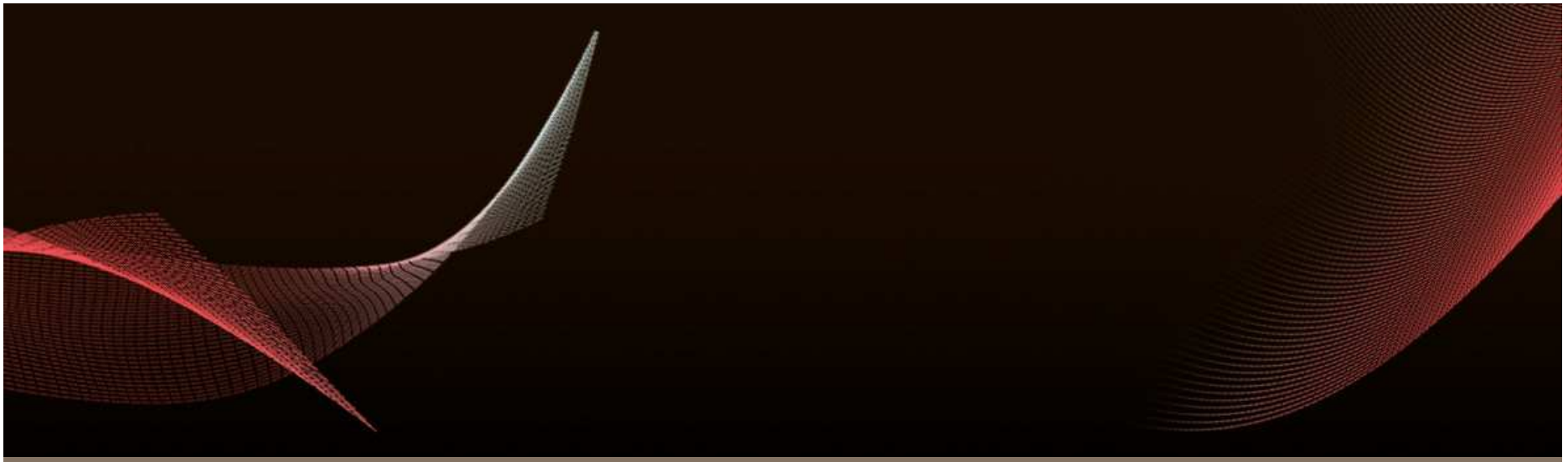


Cross Site Request Forgery

Erlend Oftedal

OWASP, 27.08.08

BEKK

Cross site request forgery - XSRF

- Også kjent som
  - XSRF
  - CSRF
  - Session riding
  - ”Click a link, og to jail”

XSRF

- Demo

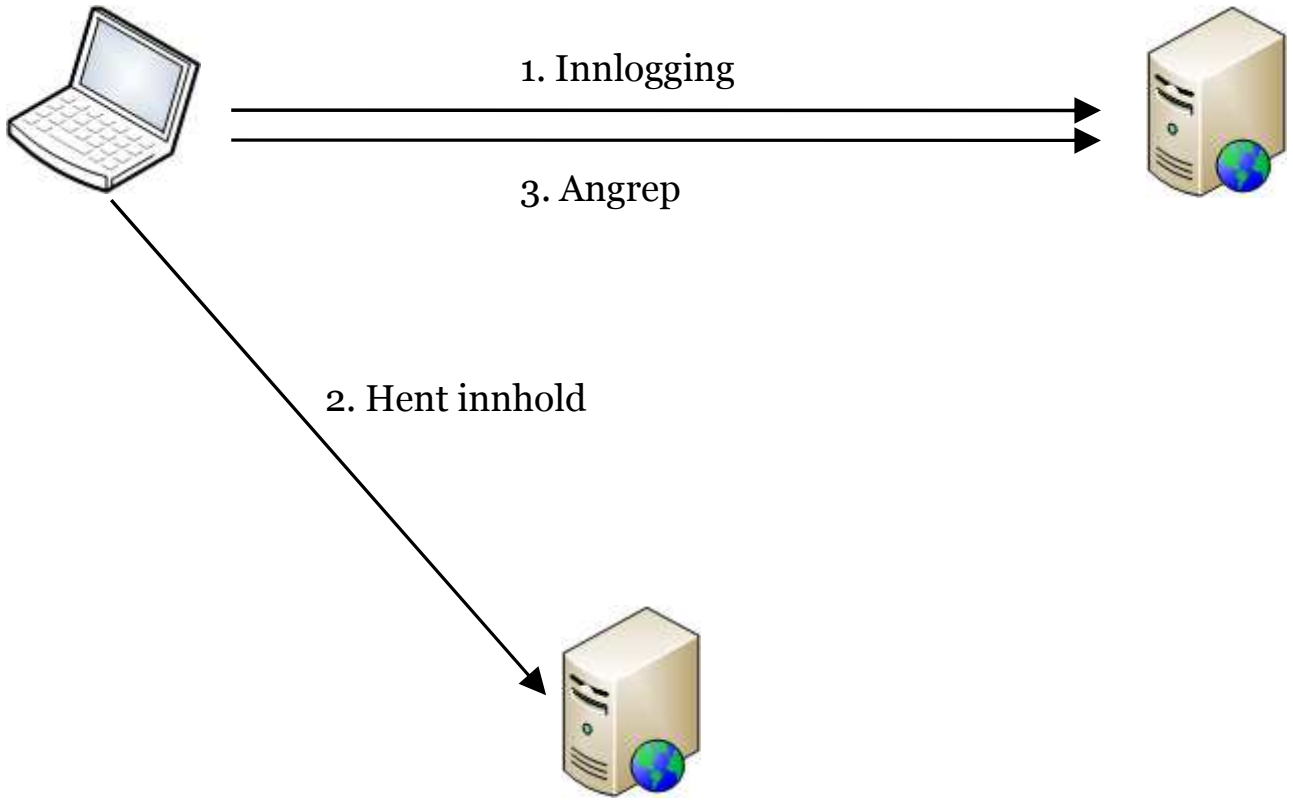
Angrepet

- Angriper gjør forespørsler i browser på vegne av bruker
  - Utnytter at bruker er logget inn på eller har tilgang til en applikasjon
- Indirekte og ofte et blindt angrep
- Angrepene må skreddersys mot bestemte mål

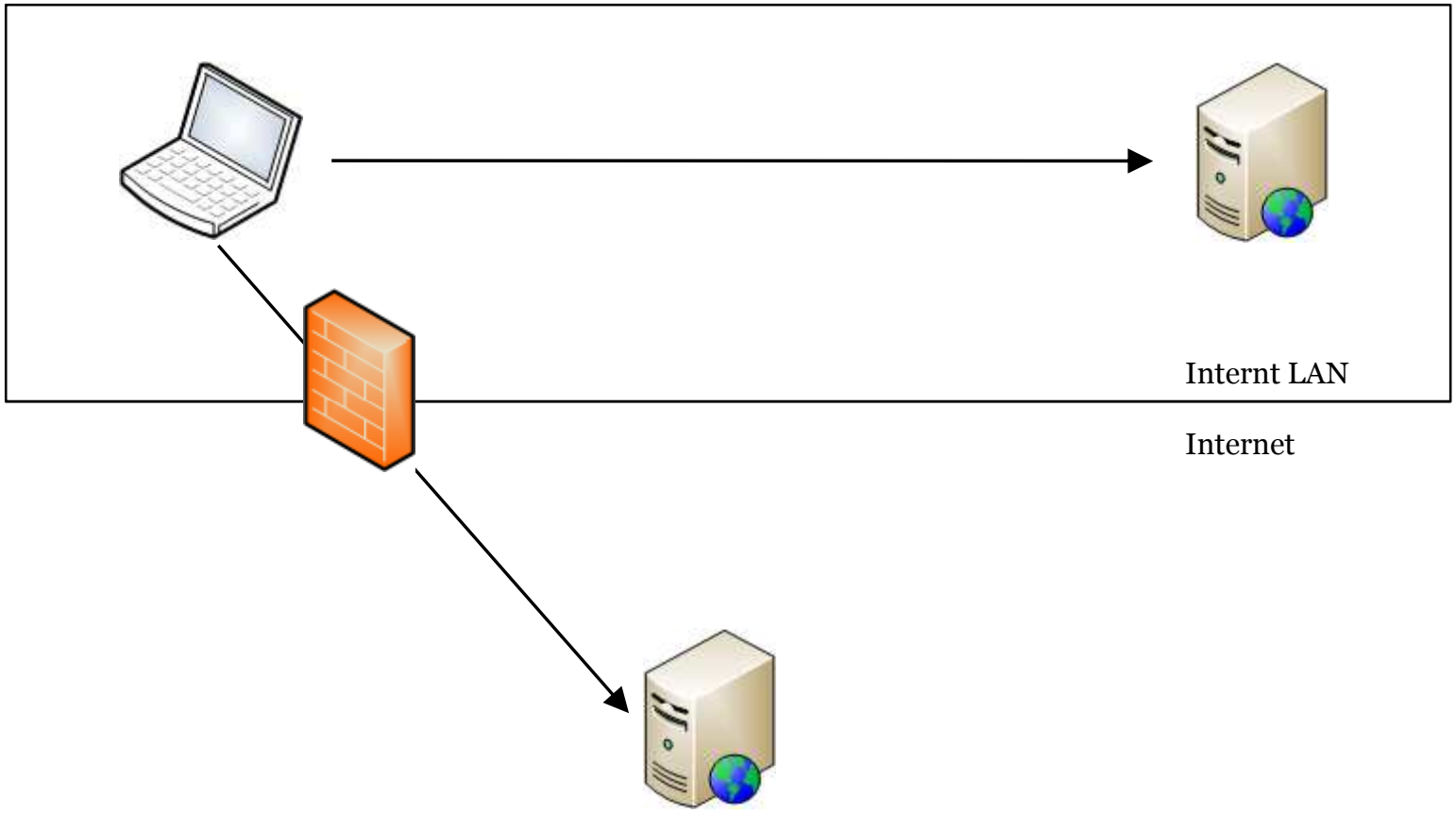
Typisk angrep

- Siden inneholder samme skjema som siden som skal angripes
- Skjemaet er allerede ferdig utfylt med angripers verdier
- Javascript brukes for å submitte formet (skjult)
- Offeret besøker siden fra:
  - En populær side som mange brukere besøker
  - Url fra mail

XSRF - Oversikt



XSRF – Interne applikasjoner



XSRF - Angrep

- Utfører operasjon på vegne av user
- Angripe interne applikasjoner
  - Gjøre endringer på router dersom default passord
  - Finne andre webapplikasjoner
  - Utføre XSS angrep mot interne applikasjoner

Drive-By Pharming: How Clicking on a Link Can Cost You Dearly

02-15-2007 12:00 AM Zulfikar Ramzan write

I wanted to talk about a recent new attack, called Driv
Stamm and Markus Jakobsson of the Indiana Universi
a Web page that, simply when *viewed*, results in subs
broadband router or wireless access point. As a result
which you surf the Web, allowing them to direct you t
you direct your Web browser to).
I believe this attack has serious widespread implicatio
Fortunately, this attack is easy to defend against as v
mention some prior related work, and then go over bes

How the attack works:

I'll start with a high-level real-world analogy of this attack. Imagine that whenever you wanted to go to your bank, you picked up your phone directory, looked up the bank's address, and then went there. Our attack

Ny type angrep kaprer hjemme-rutere

Av **Eirik Rossen**, tirsdag 20. feb 2007 kl 10:14

annonse

Symantec sier det er lett å kapre hjemmerutere med standard brukernavn og passord.

Angrep mot router – Drive-by-pharming

- Gjøre endringer i router

```
<img src="http://admin:@192.168.0.1/?angreps-parametere">
```

- Slå av brannmur (Linksys WRT54GL):

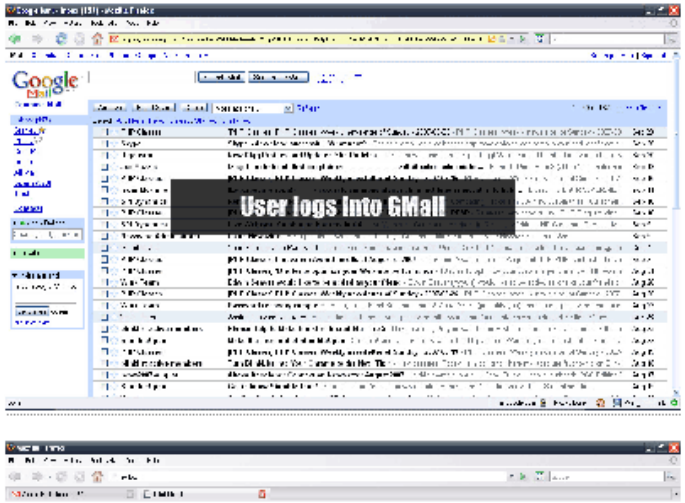
```
https://192.168.1.1/apply.cgi?submit_button=Firewall&change_action=&action=A
pply&block_wan=1&block_loopback=0&multicast_pass=0&ident_pass=0&block_cookie
=0&block_java=0&block_proxy=0&block_activex=0&filter=off&_block_wan=1&_block
_multicast=0&_ident_pass=1
```

XSRF – Cross site printing

- XSRF mot web-interfacet til en skriver

[Cross site printing, Aaron Weaver, 2007]

XSRF - Eksempel



WARNING: Google's GMail security failure leaves my business sabotaged

David Airey | 7:58 am | December 24, 2007 | Domain hijack

[http://www.davidairey.co.uk/google-gmail-security-hijack/]

”Click a link, go to jail”

- Websiten angripes ikke direkte
- Fra webservers side kommer angrepet fra offerets IP
- Angrepet kan være en bilde-URL på en populær side

http://ha.ckers.org/blog/20080320/click-a-link-go-to-jail/

Hvordan løse?

- Referer?
- HTTP POST istedenfor GET?

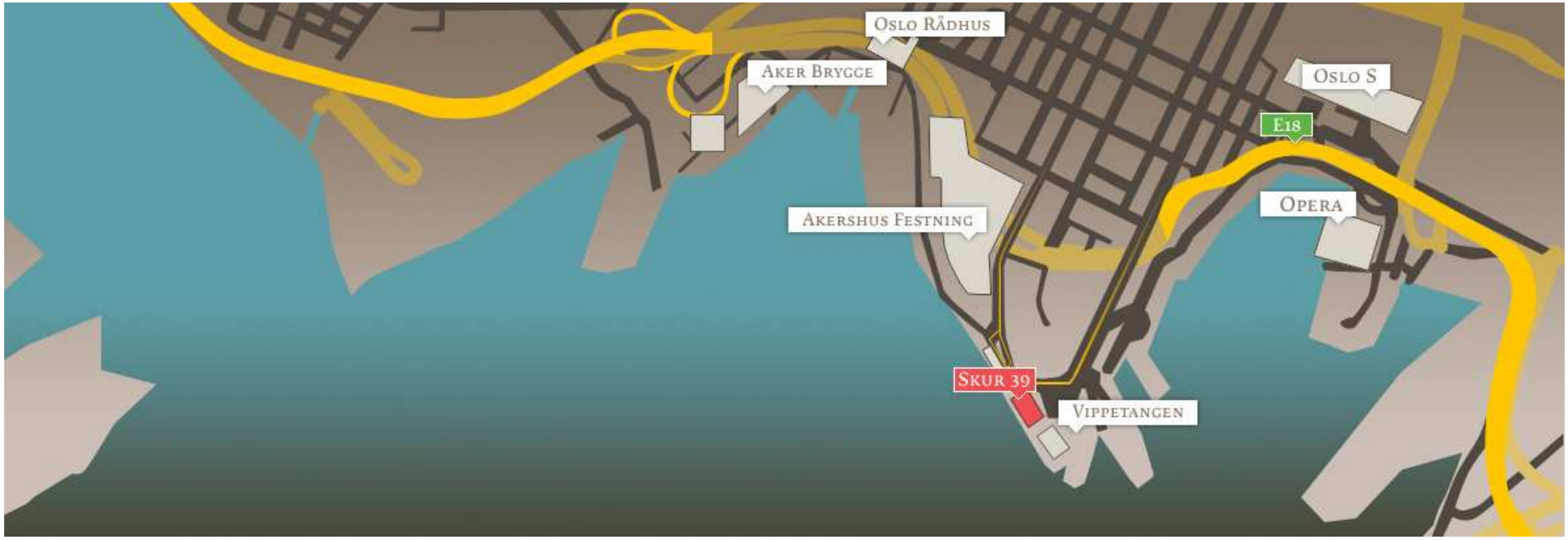
XSRF - Løsning

- Legg en unik verdi (nonce) i siden som sendes til klient, for eksempel i et skjult felt (NB! Ikke i cookie)
- Sjekk at verdien er den samme når siden postes tilbake

- Mulig løsning i ASP.NET
  - Legg verdien i Viewstate og på sesjon
  - Sjekk at verdien er den samme ved postback

Spørsmål?

- http://www.owasp.org/
- http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)



BEKK

BEKK CONSULTING AS
SKUR 39, VIPPETANGEN. P.O. BOX 134 SENTRUM, 0102 OSLO, NORWAY. WWW.BEKK.NO