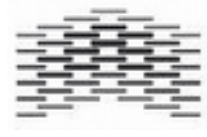
Hvordan skal arkivaren tenke sikkerhet i en endrende teknologisk landskap?

Thomas Sødring
Oslo - Met



Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata

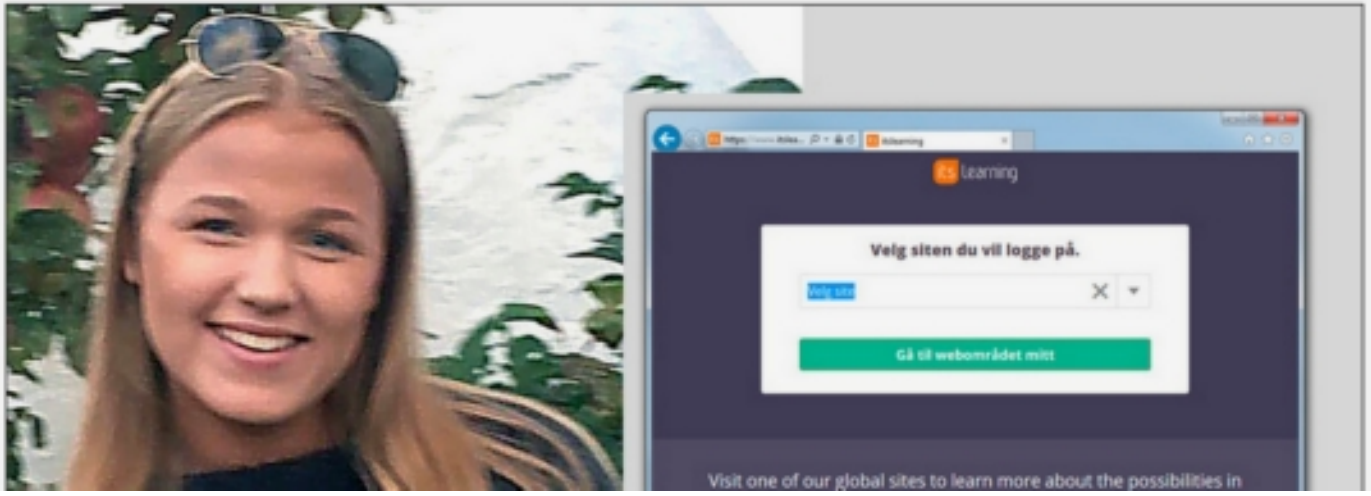
De siste ukene har titalls IT-arbeidere i Asia og Øst-Europa hatt tilgang og utvidete rettigheter til datasystemet til Helse Sø har hatt mulighet til å hente ut pasient

VG NYHETER

< Nyheter

Innenriks | Utenriks | Siste 48t | Meninger

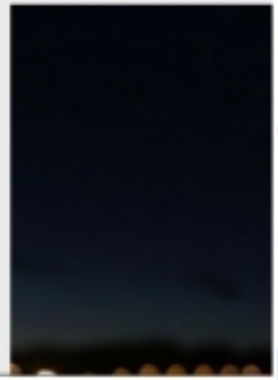
Problemer for skoler i Rogaland: Elever fikk tilgang til hverandres personlige informasjon



https://www.vg.no/nyheter/innenriks/teknologi/problemer-for-skoler-i-rogaland-elever-fikk-tilgang-til-hverandres-personlige-informasjon/a/23952236/
https://www.nrk.no/norge/helse-sor-ost_-innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443

Irenes private helseopplysninger lå åpent ute på nett: – Sjokkerende og ekkelt

En rekke dokumente
ligget åpent og søkb
private helseopplysn



UNIVERSITETET I OSLO

Universitet la ut hundrevis av fødselsnumre på nett

Var tilgjengelige for uvedkomne i månedvis.

NTB | JUSS OG SAMFUNN | PUBLISERT: 18. AUG. 2015 - 07:20

Facebook Twitter

Oslo (NTB): En feil hos Universitetet i Oslo førte til at fødselsnummeret til over 900 studenter i månedsvis ble liggende tilgjengelig på nett.

Feilen i skolens vitenarkiv, som ligger åpent på internett, ble oppdaget torsdag 6. august, og all sensitiv informasjon ble umiddelbart slettet, opplyser universitetet i en pressemelding.

https://www.nrk.no/nordland/irenes-private-helseopplysninger-la-apent-ute-pa-nett_-_-sjokkerende-og-ekkelt-1.13693173
https://www.digi.no/artikler/universitet-la-ut-hundrevis-av-fodselsnumre-pa-nett/208910

Nyheter

Studenters vitnemål lå åpent på nett

Av **Jørgen Svarstad** - 11. august 2017

Slik ser et vitnemål i Vitnemålportalen ut. Det er ikke først gang det skjer en personverntabbe ved Universtetet i Oslo.

Del på Fa

Ved hjelp vitnemål.

OLJEDOKUMENTER: I forbindelse med artikkelserien «Null CTRL» har Dagbladet funnet fem åpne og søkbare servere med detaljerte, tek
norsk oljebransje. Arkivfoto: Eirik Helland Urke / Dagbladet

Sensitive oljedokumenter lå åpent på nett

http://www.forskerforum.no/studenters-vitnemal-la-apent-pa-nett/
https://www.dagbladet.no/nyheter/sensitive-oljedokumenter-la-apent-pa-nett/61876897

Driftet norsk nødnett fra India

OPPSUMMERT

Politiets sikkerhetstjeneste har henlagt saken etter NRKs avsløringer om at indiske IT-arbeidere driftet det norske nødnettet uten sikkerhetsklarering. Årsaken til henleggelsen er at Sikkerhe

6. februar 20

nødnettsake

(Nkom) gir tel

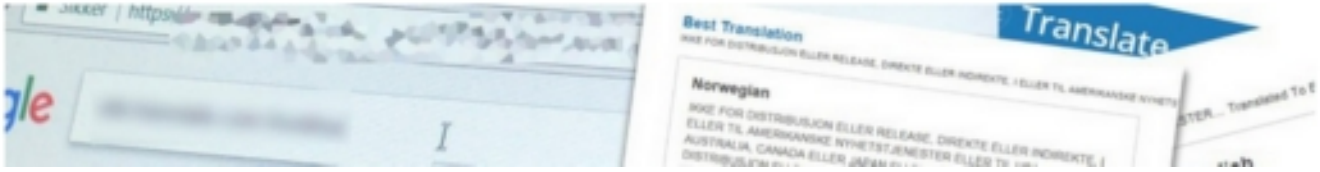
etter at det ble

systemer som

nettet driftet a

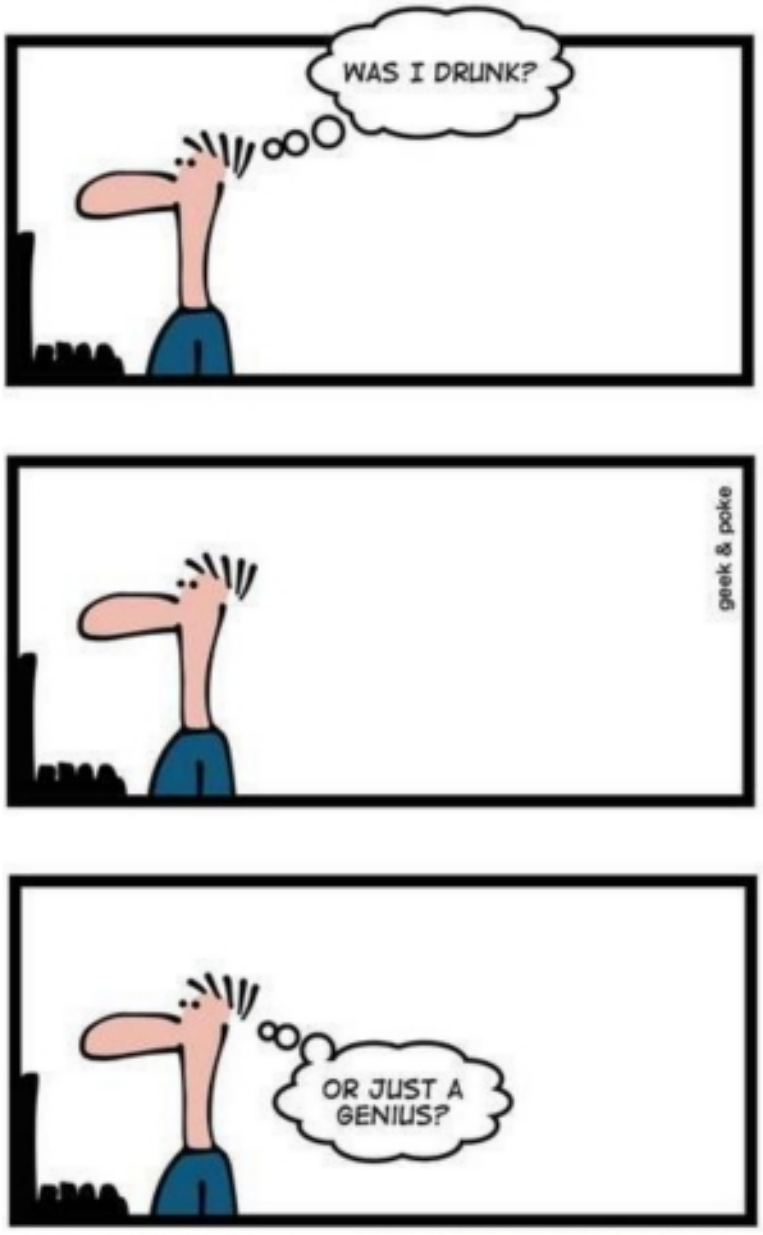
Slår alarm om oversettingsside: Passord og kontrakter ligger åpent på nettet

Sensitiv informasjon som har blitt oversatt i en populær digital oversettingstjeneste har blitt lagret i nettskyen og dermed vært søkbar i Google. Tekna advarer norske myndigheter, selskaper og privatpersoner mot naiv bruk av nettstedet.



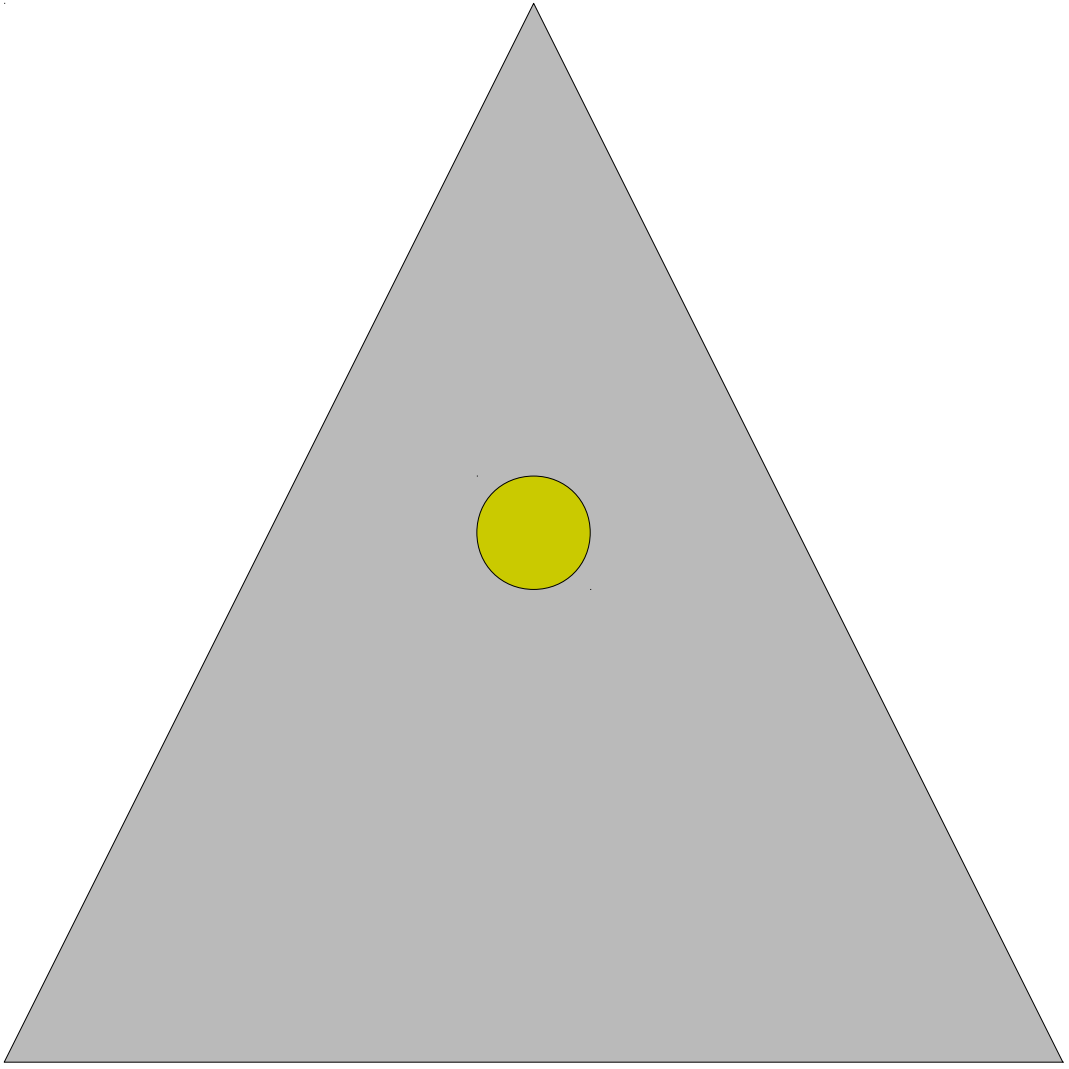
Line Tomter
Journalist

Martin Herman Wiedswang Zondag
Journalist



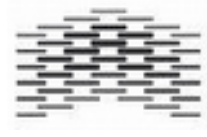
http://geek-and-poke.com/geekandpoke/2013/12/3/yesterdays-regex

Velg 2 ...



Arkivfaglig informasjonssikkerhet

- Begrepet informasjonssikkerhet er ofte definert i henhold til ***konfidensialitet***, ***kvalitet og integritet***, og ***tilgjengelighet***
  - Men disse begrepene betyr også noe for en arkivar
- I et arkivfaglig perspektiv har vi et anderledes horisont basert på tid. Sett eksempel på
  - dokumenter som forsvinner
    - Av 300 000 dokumenter er 120 borte. Problem?
  - uttrekk med kryptert informasjon
  - Uttrekk hvor 50% av dokumentene manglet



Utviklingsmodeller over tid

Brukergrensesnitt
og programvarelogikk

Database

Utviklingsmodeller over tid

Brukergrensesnitt
og programvarelogikk

Database

Brukergrensesnitt

Programvarelogikk

Database

Utviklingsmodeller over tid

Brukergrensesnitt
og programvarelogikk

Database

Brukergrensesnitt

Programvarelogikk

Database

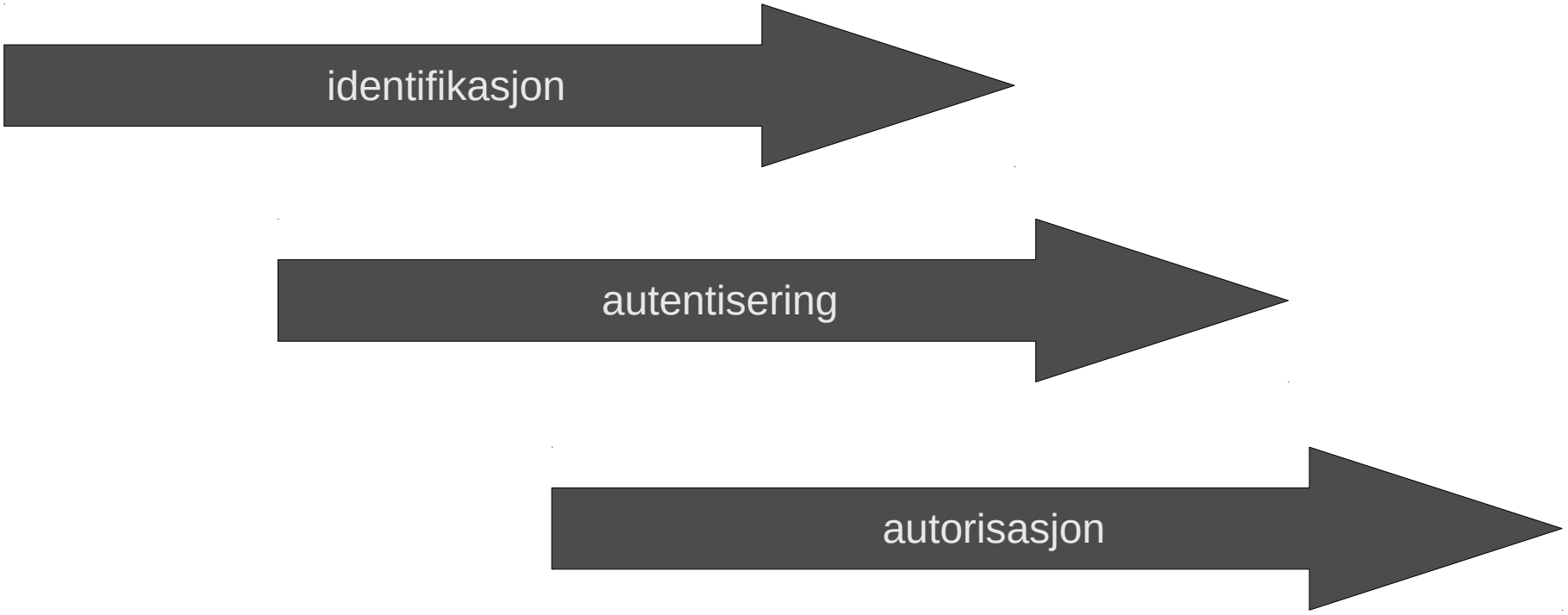
Brukergrensesnitt

Grensesnitt

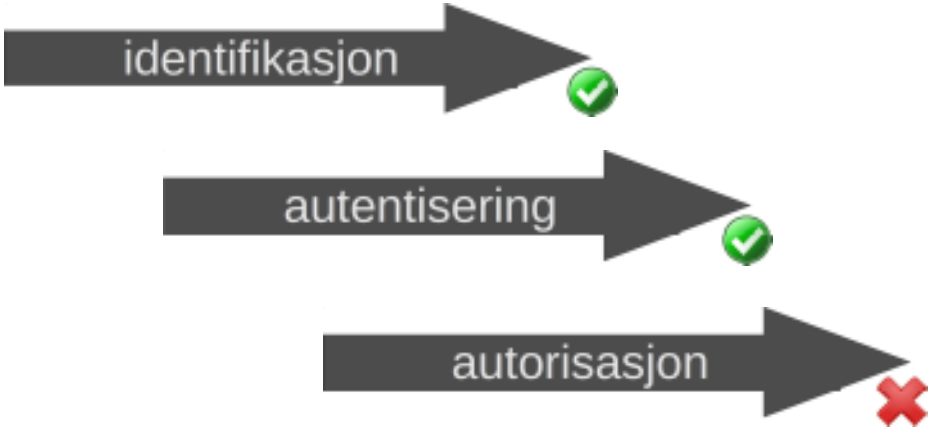
Programvarelogikk

Database

Rolle og tilgangstyring



Korrupsjonssaken i Drammen



Korrupsjonstiltalt innrømmet løgner og uheldig rolleblanding

Hva kjennetegner denne modellen?

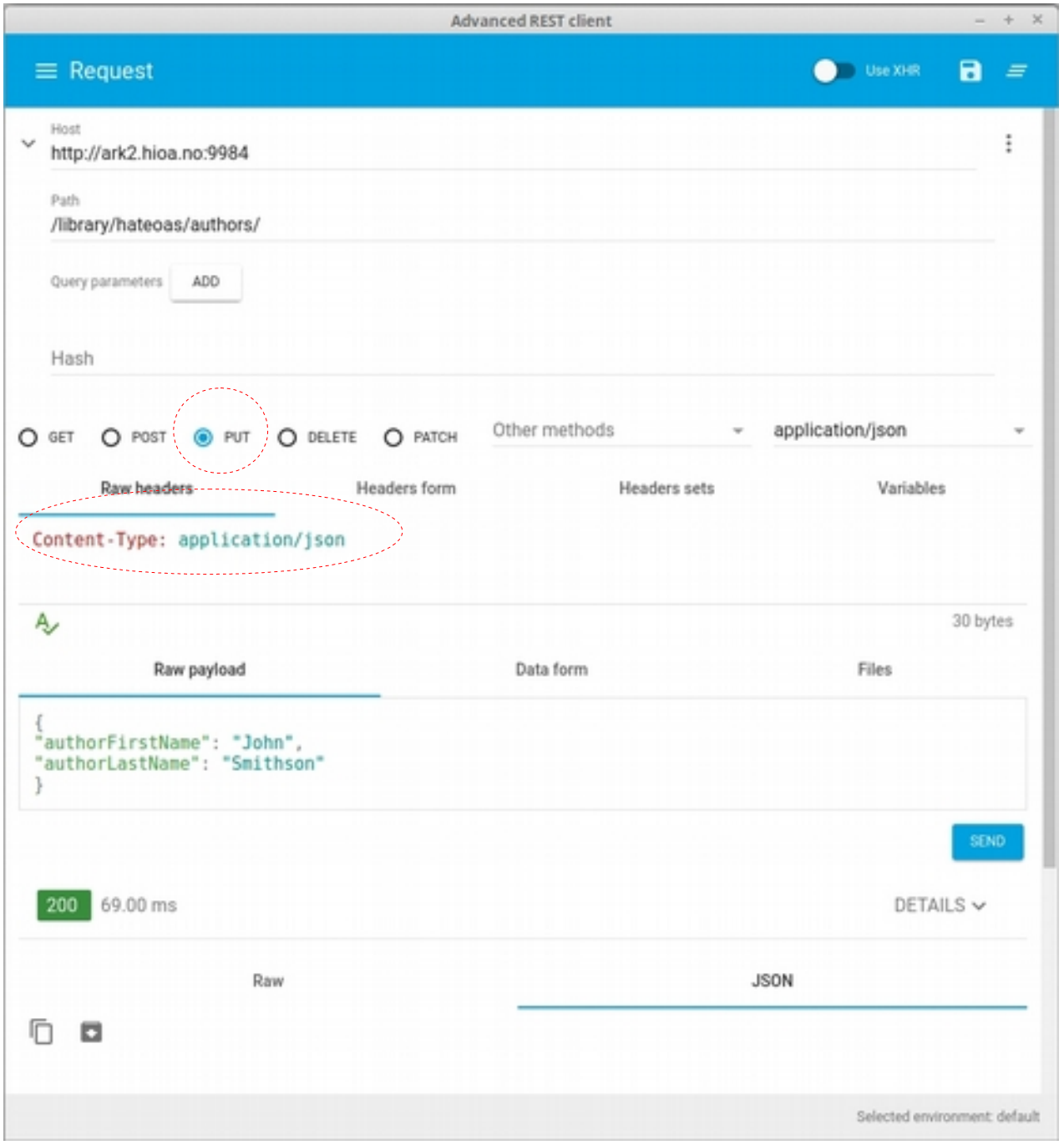
Brukergrensesnitt

Grensesnitt

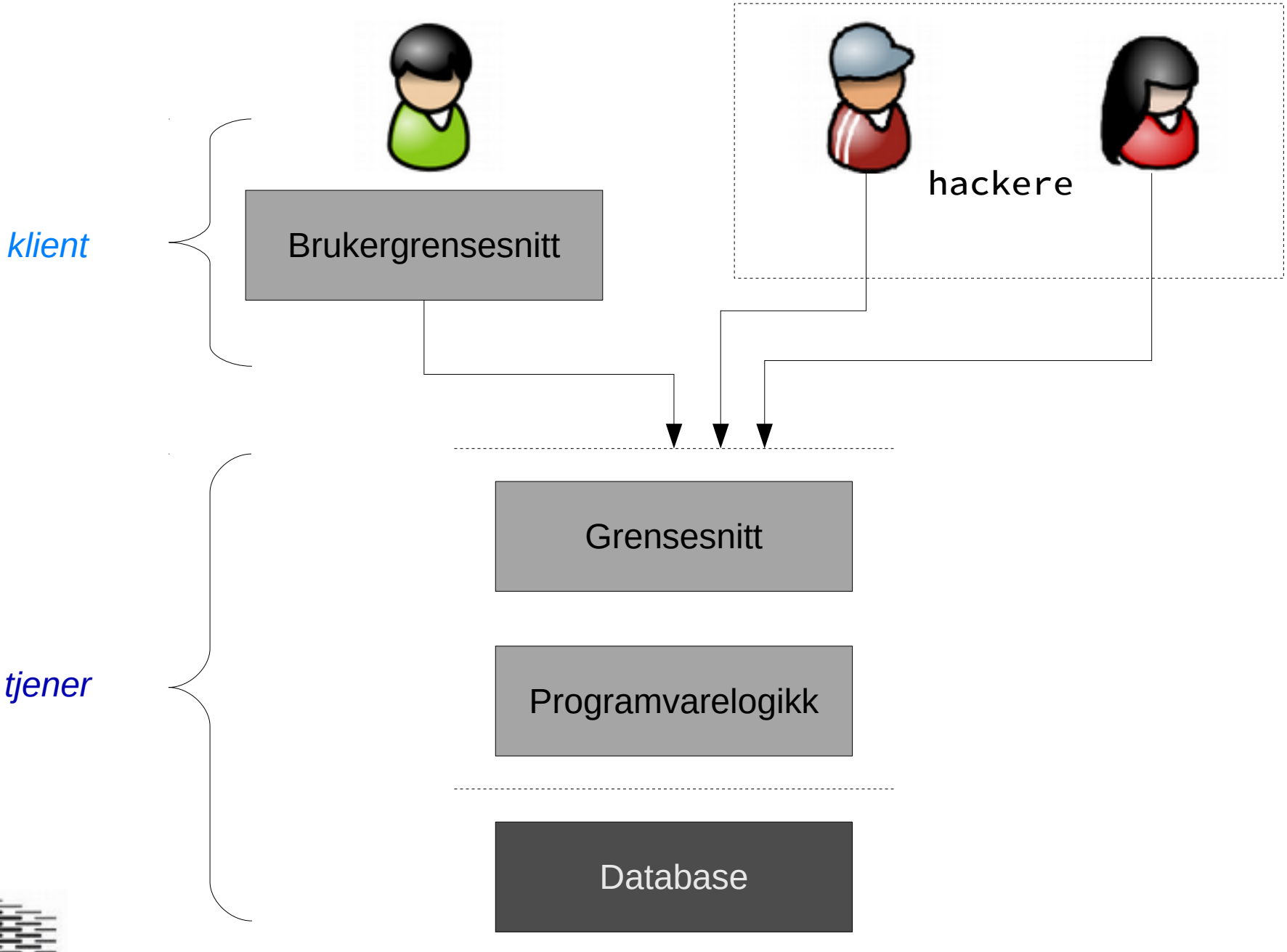
Programvarelogikk

Database

- Bruker internett
- Bruk av HTTPS standarden
- Payloads i JSON


Advanced REST client
Request
Use XHR
Host
http://ark2.hioa.no:9984
Path
/library/hateoas/authors/
Query parameters
ADD
Hash
GET
POST
PUT
DELETE
PATCH
Other methods
application/json
Raw headers
Headers form
Headers sets
Variables
Content-Type: application/json
30 bytes
Raw payload
Data form
Files
{
"authorFirstName": "John",
"authorLastName": "Smithson"
}
SEND
200
69.00 ms
DETAILS
Raw
JSON
Selected environment: default

Tilgjengelighet kontra sikkerhet



Autentisering og autorisasjon

Company Thanks Guy Who Alerted Them To Big Security Flaw By Sending The Cops... And The Bill

from the *this-is-why-white-hats-go-black* dept

We've seen before that organizations don't seem to react well to outside security folks pointing out vulnerabilities in their systems. They very often take a "blame the messenger" approach -- as if pointing out a flaw suddenly makes that flaw come into existence. But one company seems to be taking it to another level. **That Anonymous Coward** points us to a story in which a security professional found a *big* and ridiculously obvious bug in the website of an Australian investment fund, First State Superannuation. Apparently you could see other people's accounts by merely changing the account numbers in the URL. Increase the number by one, and see the next user in line. This is the kind of extraordinarily basic mistake that I thought had been eradicated a decade ago. Apparently not.

But the company that runs the fund, Pillar, went quite crazy about this. While the company did fix the security hole, it also **sent the police to interrogate** the security researcher, Patrick Webster. Pillar also **sent a letter to customers** (pdf) in which it suggests that Webster *created* this massive security flaw, rather than their own dreadful programming:

> *It has come to our attention that a member of First State Super, who has online access to their account, devised a way to view an image of your statement.*

And then, to add insult to injury, Pillar sent Webster a letter **saying he broke the law, they were closing his account, and may seek money from him to fix the vulnerability**:

https://banken.no/kunde=1234

https://banken.no/kunde=1235

- Det er mye programvare som er skrevet i forhold til en «desktop»-paradigme framfor en «nett»-paradigme
- Kjennetegnes med manglende evne å skille mellom autentisering og autorisasjon

https://www.techdirt.com/articles/20111015/20563516374/company-thanks-guy-who-alerted-them-to-big-security-flaw-sending-cops-bill.shtml