> **Dette er et eksempel, ikke en test av noe system**
>
> Funnene under er anonymiserte og satt sammen for å vise formatet. Domener og adresser er hentet fra områdene som er reservert til dokumentasjon i RFC 2606 og RFC 5737, så ingenting her peker på en virkelig kunde eller et virkelig system. En ekte rapport har samme oppbygning og samme detaljnivå.

En rapport fra oss er skrevet for å bli brukt, ikke arkivert. Hvert funn har hvor det er, hvordan det ble funnet, hva det betyr og hva som må endres. Dokumentasjonen står som den var, slik at den kan etterprøves.

Slik er rapporten satt sammen

Sammendrag for ledelsen

Én side uten fagspråk: hva som ble testet, hva som ble funnet, hvor alvorlig det er og hva som bør gjøres først. Den kan videresendes til styret eller til en kunde som spør, uten at du må skrive den om.

Bekreftede funn

Ett oppslag per funn, nummerert F-01 og oppover, med alvorlighetsgrad, berørt ressurs, dokumentasjon på hvordan det ble funnet, hva konsekvensen er og hva som må endres. Der det finnes en relevant standard, står referansen med, for eksempel OWASP API5:2023.

Det som holdt, og hvorfor

En egen del med det som ble angrepet uten å gi etter, og hva dere har gjort bra. Ble et forsøk stoppet, står det hvorfor, og hvilken kontroll som tok det. Kom vi rundt den likevel, står det også, og hvordan. Da vet dere både hva som virker og hvor langt det rekker.

Dekning og gjenstående punkter

Hva som ble rukket, hva som ikke ble det, og hva som krever noe fra dere før det kan testes. Ingenting ligger igjen som en stilltiende antakelse.

Rekkefølge på utbedring

Funnene sortert i den rekkefølgen de bør fikses, ikke bare etter alvorlighetsgrad. Noen ting er raske og fjerner mye risiko; andre er store og kan vente.

Opprydding etter testen

Testdata, kontoer og eventuelle spor vi har lagt igjen, og hva som er fjernet. Du skal slippe å lure på hva som fortsatt ligger i systemet etter at vi er ferdige.

Vedlegg

Kjente CVE-er i komponentene som er i bruk, oversikt over teknologi og versjoner, og kontroll av tredjepartskomponenter. Det som er sjekket automatisk og vist seg å være falske positive, står oppført som nettopp det: avvist, med begrunnelse.

Bekreftede funn

Alvorligste først. Nummereringen følger rapporten, F-01 og oppover.

F-01 KRITISK Innlogget bruker kan hente dokumenter som tilhører andre kunder

`GET /api/v2/documents/{id}` på `app.eksempel.no`

```
# Innlogget som bruker i tenant 1188.
GET /api/v2/documents/8841 HTTP/1.1
Host: app.eksempel.no
Authorization: Bearer <token, tenant 1188>

HTTP/1.1 200 OK
Content-Type: application/json

{"id":8841,"tenantId":"1207","tittel":"Styreprotokoll Q3","eier":"…"}
#                  ^^^^ dokumentet tilhorer en annen kunde
```

HVA DET BETYR

Enhver innlogget bruker kan lese dokumenter på tvers av kunder ved å telle seg gjennom id-ene. Det holder med en vanlig konto. Ingen administratorrettigheter er nødvendig. Dokumentene i miljøet inneholder styrepapirer og personopplysninger.

HVA SOM MÅ ENDRES

Sjekk tilhørighet i endepunktet, ikke i grensesnittet: hent dokumentet med både id og tenant-id i spørringen, og svar 404 når de ikke stemmer overens. Legg samme sjekk i et felles lag som alle dokumentendepunkter går gjennom, og dekk den med en test som forsøker et fremmed dokument.

CWE-639 · OWASP API1:2023

F-02 HØY Domenet ber ikke mottakere gjøre noe med forfalsket e-post

`_dmarc.eksempel.no`

```
$ dig +short TXT _dmarc.eksempel.no
"v=DMARC1; p=none; rua=mailto:dmarc@eksempel.no"

$ dig +short TXT eksempel.no
"v=spf1 include:spf.protection.outlook.com ~all"
```

HVA DET BETYR

SPF finnes, men DMARC står på p=none. Mottakere blir dermed bedt om å ikke gjøre noe med e-post som utgir seg for å komme fra domenet. En faktura sendt i virksomhetens navn fra en fremmed avsender blir levert som vanlig i innboksen til kunder og leverandører.

HVA SOM MÅ ENDRES

Les rapportene som allerede kommer inn på rua-adressen og bekreft at all legitim utsending er dekket av SPF og DKIM. Gå så til p=quarantine med pct=100, og videre til p=reject når rapportene er rene. Sett samtidig SPF til -all i stedet for ~all.

RFC 7489

F-03 MIDDELS Origin-serveren svarer direkte, utenom CDN-et

203.0.113.24:443

```
$ curl -sI https://www.eksempel.no --resolve www.eksempel.no:443:203.0.113.24
HTTP/2 200
server: nginx/1.24.0
x-cache: MISS
x-served-by: origin-01

# Samme forespørsel gjennom CDN-et treffer brannmuren i front.
```

HVA DET BETYR

Origin-adressen er nåbar direkte. Da kan trafikk sendes utenom brannmuren og ratebegrensningen som ligger i CDN-et, og eventuelle blokkeringsregler der får ingen effekt.

HVA SOM MÅ ENDRES

Slipp bare inn trafikk fra CDN-leverandørens adresseområder i brannmuren foran origin, og avvis resten. Krev i tillegg et delt hode eller et klientsertifikat mellom CDN og origin, slik at direkte forespørsler avvises selv om adressen blir kjent.

Om dette eksempelet

Tre funn er tatt med for å vise spennet: ett i forretningslogikken som ingen skanner finner, ett i oppsettet som er lest utenfra, og ett som handler om hvordan tjenesten er satt opp foran. En reell rapport inneholder som regel flere, og den inneholder også delen om hva som holdt.

Vil dere se hva som er synlig utenfra på deres eget domene, ligger den gratis sjekken på glippen.no/scan. Den krever verken innlogging eller e-postadresse.