Mustvedt Sentinel

NORSK SIKKERHETSPLATTFORM

MUSTVEDT SENTINEL · KONFIDENSIELT

Sårbarhets-rapport

eksempelfirma.no

TOTAL	KRITISK	SJEKKET
F	4	107

Levert **23. mai 2026**
Signert **Christer Mustvedt**, Mustvedt Sentinel
Rapport-ID **MS-SR-20260523-6AC0D6**

KONFIDENSIELT · FOR MOTTAKERENS ØYNE

01 · SAMMENDRAG FOR LEDELSEN

Hva vi fant på eksempelfirma.no

Denne rapporten er en sikkerhetsanalyse av **eksempelfirma.no**, kjørt 23. mai 2026. Vi testet domenet mot tusenvis av kjente sårbarhetsmønstre, scannet for åpne tjenester, og samlet inn offentlig OSINT-data. Sammendraget under er skrevet i klartekst slik at ledere uten teknisk bakgrunn skal kunne handle på det.

F

Kritisk

Helse-score 38/100, basert på antall og alvorlighetsgrad av funn.

27 funn · **4** åpne porter · **13** tekniske observasjoner

4	8	8	4	13
KRITISK	HØY	MEDIUM	LAV	OBS.

Hvis du bare har tid til tre ting

Vi vet at lange rapporter er overveldende. Her er de tre viktigste å handle på denne uka:

1. **OpenSSH 8.9p1 Ubuntu eksponert mot Internett med kjent RCE** CRITICAL

   SSH-tjenesten på port 22 kjører OpenSSH 8.9p1 Ubuntu 3ubuntu0.1. Versjonen er sårbar for CVE-2023-38408 (CVSS 9.8), som gir en angriper mulighet til ekstern kjøring av kode under bestemte konfigurasjoner med SSH agent-fo…

2. **Apache 2.4.49 med Path Traversal (CVE-2021-41773)** CRITICAL

   Web-serveren rapporterer Apache 2.4.49. Denne versjonen har en kritisk sårbarhet for path traversal og remote code execution (CVE-2021-41773, CVSS 9.8). En aktivert mod_cgi-modul gjør dette utnyttbart for ekstern kjøring…

3. **SSRF eksponerer AWS instance metadata via /api/url-preview** CRITICAL

   Endepunktet aksepterer en url-parameter og henter inn URL-ens innhold for forhåndsvisning av lenker. Vi sendte http://169.254.169.254/latest/meta-data/iam/security-credentials/ og fikk tilbake et AWS IAM-rolle-token i re…

02 · INNHOLD

Hva ligger i rapporten

INNHOLDSFORTEGNELSE

01	Sammendrag for ledelsen	s. 2
02	Om rapporten og scope	s. 3
03	Åpne tjenester og infrastruktur	s. 4
04	Funn etter kategori (sortert etter alvorlighet)	s. 5+
•	Sårbar programvare (Port 22)	1 funn
•	Web-applikasjon (Nuclei)	1 funn
•	Web-applikasjon (pentest-ai)	8 funn
•	TLS/SSL-konfigurasjon	1 funn
•	Sikkerhets-headers	3 funn
•	Sårbar programvare (Port 80/443)	1 funn
•	Web-applikasjon (Nikto)	2 funn
•	DNS og e-post-konfigurasjon	2 funn
•	Sertifikat (TLS)	1 funn
•	Informasjons-lekkasje	1 funn
•	OSINT (theHarvester)	1 funn
•	OSINT (CT-logs)	1 funn

- Nettverks-rekognosering 1 funn
- Typosquatting (dnstwist) 1 funn
- WAF/Firewall (wafw00f) 1 funn
- Passiv subdomain-recon (subfinder + amass) 1 funn

05 Prioritert handlingsplan

06 Vi tar jobben — Mustvedt Sentinel-tilbud

07 Vedlegg: tekniske observasjoner

Om denne rapporten

Mustvedt Sentinel er en norsk plattform som bruker den samme verktøypakken som internasjonale sikkerhetsteam og bug-bounty-jegere. Hver rapport er resultatet av en fullstendig pen-test-style sikkerhetsanalyse av domenet ditt: Nmap, nuclei, Nikto, testssl.sh, gobuster, theHarvester, subfinder, amass, dnstwist og wafw00f kjøres mot målet i en standardisert prosess. Funnene gjennomgås, kontekstualiseres og prioriteres før de havner i denne PDF-en.

Hvordan lese rapporten

- **Sammendraget** over (side 2) er for ledere uten teknisk bakgrunn. Tre punkter, klartekst, prioritert.
- **Funn etter kategori** grupperer alle observasjoner etter angrepstype. Hver oppføring har severity, lokasjon, beskrivelse og fix-instruksjon.
- **Handlingslisten** er en sortert ToDo etter alvorlighetsgrad. Start på toppen.
- **Vedlegget** bakerst inneholder tekniske observasjoner for IT-personell.

Etisk grunnlag

Alle testene i denne rapporten er kjørt med eksplisitt samtykke fra eieren av eksempelfirma.no. Ingen aktive utnyttelses-forsøk er gjort — vi har kun identifisert mulige risikoer, ikke utnyttet dem. Rådata fra hvert verktøy lagres hos Mustvedt og slettes 90 dager etter rapport-utstedelse.

03 · SCOPE OG SCORING

Det vi testet

Helse-score, slik vi regner

Score-en starter på 100. Vi trekker fra basert på funn:

- Hvert **kritisk** funn: −20 poeng
- Hvert **høyt** funn: −10 poeng
- Hvert **medium** funn: −4 poeng
- Hvert **lavt** funn: −1 poeng

Letter-grade-en (F) er en oversettelse av score til en SSL-Labs-stil karakter (A+ til F).

Verktøys-matrise — hva ble faktisk kjørt

Verktøys-matrise ikke tilgjengelig for denne rapporten (eldre rapport-format).

Åpne porter / eksponerte tjenester

Vi fant **4 åpne porter** som lytter mot internett. Dette er angrepsflaten din.

PORT	TJENESTE	VERSJON
22/	**ssh**	8.9p1 Ubuntu 3ubuntu0.1
25/	**smtp**	3.6.4
80/	**http**	2.4.49
443/	**https**	2.4.49

Offentlig fotavtrykk (OSINT)

theHarvester samlet passive data fra åpne kilder (Bing, crt.sh, OTX, m.fl.):

- **12** offentlig kjente e-postadresser
- **8** subdomener oppdaget
- **2** tilknyttede IP-adresser

03B · RECON & ANGREPS-OVERFLATE

Hva en angriper ser

Passiv rekognosering uten å treffe målet. Disse dataene er offentlig tilgjengelige — en angriper kan samle dem på 30 minutter.

Subdomener (subfinder + amass)

Sammenslått resultat fra 2 enumerator-verktøy som spør **40 datakilder** (crt.sh, Bing, OTX, Censys, HackerTarget, AlienVault m.fl.):

- **23** subdomener identifisert totalt
- **3** aktive og eksponerte uten autentisering

SUBDOMENE
mail.eksempelfirma.no
dev.eksempelfirma.no
staging.eksempelfirma.no
test.eksempelfirma.no
autodiscover.eksempelfirma.no
ftp.eksempelfirma.no
beta.eksempelfirma.no
gamle-sider.eksempelfirma.no
vpn-old.eksempelfirma.no
jenkins.eksempelfirma.no
elk.eksempelfirma.no
git.eksempelfirma.no
… og 11 til

Typosquatting (dnstwist)

Genererte **1 834** stave-varianter av domenet. **3** av disse er allerede registrerte og kan brukes til phishing:

DOMENE	REGISTRAR	RISIKO	MX
eksempelfirrma.no	private/RO	MEDIUM	nei
eksempelfirna.no	namesilo	LOW	nei
eksempelfirma-no.com	GoDaddy	HIGH	JA — kan motta e-post

Web Application Firewall (wafw00f)

Testet **22 WAF-signaturer** mot domenet (Cloudflare, AWS WAF, Imperva, Akamai, Sucuri, F5 BIG-IP m.fl.).

Status: **INGEN WAF — applikasjonen er direkte eksponert**

Uten en WAF kan en angriper iterere mot kjente sårbarhets-mønstre uten å bli filtrert. Cloudflare gratis-tier dekker SQL-injection, XSS og DDoS-beskyttelse og kan settes opp på ~1 time.

04 · FUNN ETTER KATEGORI

Sårbar programvare (Port 22) (1 funn)

OpenSSH 8.9p1 Ubuntu eksponert mot Internett med kjent RCE

KRITISK · FIKS I DAG

CVE-2023-38408 · CVSS 9.8

`ssh.eksempelfirma.no:22`

SSH-tjenesten på port 22 kjører OpenSSH 8.9p1 Ubuntu 3ubuntu0.1. Versjonen er sårbar for CVE-2023-38408 (CVSS 9.8), som gir en angriper mulighet til ekstern kjøring av kode under bestemte konfigurasjoner med SSH agent-forwarding. To andre CVE-er i samme versjon er klassifisert som høy: CVE-2023-28531 (CVSS 9.8, autorisasjons-omgåing) og CVE-2024-6387 (regreSSHion, CVSS 8.1). Selv om CVE-2024-6387 i praksis krever lang race-condition-tid, betyr eksponering mot Internett at en motivert angriper kan forsøke dette.

> **Slik fikser du:** Steg 1: Oppgrader OpenSSH til siste pakkeversjon: 'sudo apt update && sudo apt upgrade openssh-server'. Verifiser med 'ssh -V'. Steg 2: Begrens SSH-tilgang til kjente IP-er via brannmur, eventuelt sett opp VPN eller bastion-host. Steg 3: Slå av agent-forwarding hvis det ikke er strengt nødvendig (sett 'AllowAgentForwarding no' i sshd_config).

DETEKTERT AV: NMAP + VULNERS

04 · FUNN ETTER KATEGORI

Web-applikasjon (Nuclei) (1 funn)

Apache 2.4.49 med Path Traversal (CVE-2021-41773)

KRITISK · FIKS I DAG

CVE-2021-41773 · CVSS 9.8

https://eksempelfirma.no/

Web-serveren rapporterer Apache 2.4.49. Denne versjonen har en kritisk sårbarhet for path traversal og remote code execution (CVE-2021-41773, CVSS 9.8). En aktivert mod_cgi-modul gjør dette utnyttbart for ekstern kjøring av kommandoer. Vi fant dette via en POC-sjekk som returnerte filinnhold fra utenfor document-root.

> **Slik fikser du:** Oppgrader til Apache 2.4.51 eller nyere umiddelbart: 'sudo apt install apache2'. Verifiser ny versjon med 'apache2 -v'. Restart tjenesten. Hvis kontroll på mod_cgi-konfigurasjonen er begrenset, vurder å skifte til Nginx for offentlige endepunkter.

DETEKTERT AV: NUCLEI + MANUELL VERIFIKASJON

04 · FUNN ETTER KATEGORI

Web-applikasjon (pentest-ai) (8 funn)

SSRF eksponerer AWS instance metadata via /api/url-preview

KRITISK · FIKS I DAG

`POST https://eksempelfirma.no/api/url-preview`

Endepunktet aksepterer en url-parameter og henter inn URL-ens innhold for forhåndsvisning av lenker. Vi sendte http://169.254.169.254/latest/meta-data/iam/security-credentials/ og fikk tilbake et AWS IAM-rolle-token i responsen. Tokenet ga oss tilgang til S3-buckets med kundedata og delvis EC2-rettigheter under testen. Dette er en klassisk Server-Side Request Forgery mot sky-metadata-tjenesten.

> **Slik fikser du:** Steg 1: Aktiver IMDSv2 (session-token-basert) på alle EC2-instanser — det krever et innledende PUT-kall som SSRF-angrep typisk ikke kan utføre. Steg 2: Valider og whitelist URL-er i /api/url-preview — kun https-skjema, og blokker private og link-local IP-rom (10/8, 172.16/12, 192.168/16, 169.254/16, 127/8). Steg 3: Konfigurer http-proxy på applikasjonsserveren slik at alle uthentinger passerer gjennom en proxy som blokkerer metadata-IP-er.

DETEKTERT AV: PENTEST-AI · WEB.SSRF_CLOUD_METADATA (AUTORISERT)

Usikker deserialisering i /api/import gir RCE

KRITISK · FIKS I DAG

`POST https://eksempelfirma.no/api/import`

Import-endepunktet aksepterer en base64-kodet pickle-payload i data-feltet. Vi sendte en payload med __reduce__-metoden som kaller os.system og kjørte id-kommandoen på serveren. Returnverdien uid=33(www-data) gid=33(www-data) groups=33(www-data) kom direkte tilbake i responsen. Dette er en full Remote Code Execution som www-data-bruker, og er en av de mest alvorlige sårbarhetene som finnes i web-applikasjoner.

> **Slik fikser du:** Steg 1: Aldri deserialiser ubetrodd input med pickle. Bytt til JSON med streng schema-validering (jsonschema eller pydantic). Steg 2: Hvis binær-format kreves, bruk msgpack eller protobuf med whitelist over godkjente typer. Steg 3: Kjør applikasjonen som en bruker uten skrive-tilgang utenfor sitt eget arbeidsområde, og pakk den i en container med read-only rotfilsystem. Steg 4: Aktiver audit-logging og varsler ved suspekt deserialiserings-aktivitet.

DETEKTERT AV: PENTEST-AI · WEB.DESERIALIZATION

IDOR — bruker kan hente andre brukeres ordrer

HØY · DENNE UKA

`GET https://eksempelfirma.no/api/orders/{id}`

Endepunktet returnerer ordre-detaljer basert på en numerisk ID i URL-en. Det sjekkes at brukeren er innlogget, men ikke at ordren faktisk tilhører brukerens konto. Vi logget inn med en testkonto og hentet ordre 1, 2, 3 osv. — fikk tilgang til ordre-detaljer (kundenavn, leveringsadresse, totalbeløp, betalt-status) for andre kunder uten begrensning. Differensiell autorisasjon (differential authz) er en variant av Insecure Direct Object Reference.

> **Slik fikser du:** Steg 1: Legg til en eksplisitt sjekk i ordre-controllers: WHERE order.id = :id AND order.user_id = :session_user_id. Steg 2: Bytt fra sekvensielle ID-er til UUID-er. Det stopper enkel enumerering, men IKKE autorisasjons-feilen i seg selv. Steg 3: Gjør en bredere audit av alle /api/{resource}/{id}-endepunkter og verifiser eierskap-sjekk i hvert tilfelle. Steg 4: Logg alle ordre-oppslag for å oppdage masse-enumerering i ettertid.

DETEKTERT AV: PENTEST-AI · WEB.IDOR_AUTHZ_DIFFERENTIAL (AUTENTISERT)

CORS reflekterer enhver Origin og tillater credentials

HØY · DENNE UKA

`OPTIONS https://api.eksempelfirma.no/v1/*`

API-en responderer på CORS preflight med Access-Control-Allow-Origin satt til verdien av Origin-headeren i requestet, kombinert med Access-Control-Allow-Credentials: true. Det betyr at en ondsinnet nettside (f.eks. https://angriper.no) som en innlogget bruker besøker, kan sende autentiserte CORS-kall til API-en og lese svaret. I praksis er dette tilsvarende en CSRF-sårbarhet med tilgang til hele API-overflaten.

> **Slik fikser du:** Steg 1: Erstatt Origin-refleksjon med en streng whitelist over godkjente origins (kun https://eksempelfirma.no og evt. https://app.eksempelfirma.no). Steg 2: Hvis du må støtte mange under-domener, bygg en regex og test grundig — wildcards (*) tillates IKKE sammen med credentials. Steg 3: Vurder om Access-Control-Allow-Credentials i det hele tatt er nødvendig — fjern det hvis API-en kan bruke Bearer-tokens i stedet for cookies.

DETEKTERT AV: PENTEST-AI · WEB.CORS_REFLECTION

JWT-verifisering aksepterer alg: none

HØY · DENNE UKA

`POST https://eksempelfirma.no/api/auth/verify`

Tokens som sendes til /api/auth/verify aksepteres selv når alg-feltet i JWT-headeren er satt til none og signaturen er tom. Vi konstruerte en token med {alg:none, typ:JWT} og payload {user_id: 1, role: admin}, sendte den uten signatur, og fikk en gyldig sesjon med admin-rettigheter. Dette er en velkjent JWT-validerings-feil som typisk skyldes at biblioteket aksepterer alle algoritmer som standard.

> **Slik fikser du:** Steg 1: Hardkod tillatt algoritme i token-verifiseringen: kun HS256 eller RS256 — aldri none. Steg 2: Sjekk at JWT-biblioteket ditt har spesifikk versjon uten kjente alg-confusion-feil (eks: jsonwebtoken < 9.0.0 i Node hadde dette). Steg 3: Roter signing-key umiddelbart siden alle eksisterende tokens nå er kompromittert. Steg 4: Implementer kort gyldighet (15 min) + refresh-token-flow for å begrense skadeomfanget av lekkede tokens.

DETEKTERT AV: PENTEST-AI · WEB.JWT_ALG_NONE

Mass assignment lar bruker promote seg selv til admin

HØY · DENNE UKA

`PATCH https://eksempelfirma.no/api/users/me`

Endepunktet for å oppdatere egen profil aksepterer hele bruker-objektet uten å filtrere bort sensitive felter. Vi sendte PATCH /api/users/me med body {"display_name":"test","role":"admin","is_verified":true}. Serveren tok inn alle feltene og oppdaterte vår testkonto til admin-rolle. Etter neste login fikk vi tilgang til admin-dashboard og kunne se alle brukere.

> **Slik fikser du:** Steg 1: Definer en eksplisitt allowlist over felter en bruker får oppdatere via /api/users/me: typisk display_name, avatar_url, preferred_language. Steg 2: Bruk strict-input-DTO-er (data transfer objects) i stedet for å mappe hele kropps-objektet direkte til database-entiteten. Steg 3: Audit hvilke brukere som har blitt promotert til admin den siste 90 dagene — sårbarheten kan ha vært aktivt utnyttet. Steg 4: Logg alle role-endringer permanent og varsle ved manuelle endringer.

DETEKTERT AV: PENTEST-AI · WEB.MASS_ASSIGNMENT (AUTENTISERT)

API-nøkler lekket i JavaScript source maps

MEDIUM · DENNE MÅNEDEN

`https://eksempelfirma.no/static/app.bundle.js.map`

Frontend-bundle inkluderer source maps som er offentlig tilgjengelig. I source-mapen fant vi en hardkodet Stripe test-nøkkel (sk_test_...), en Mapbox access token og en Sentry DSN. Mapbox-tokenet brukes fra frontend (det er per definisjon offentlig), men Stripe-nøkkelen og Sentry-DSN'en bør ikke ligge i klient-side kode. Source maps er gjerne ufortolket av angripere, men de gir også fullstendig innsyn i hele applikasjonens logikk og struktur.

> **Slik fikser du:** Steg 1: Rotér de eksponerte API-nøklene umiddelbart, selv om de er 'test'-nøkler. Steg 2: Slå av source maps i produksjon, eller server dem kun via en autentisert intern proxy for utviklere. Steg 3: Bruk environment-variabler og en build-time-secret-prosess (eks: Vite/Webpack DefinePlugin) for å holde private nøkler ute av bundlen. Steg 4: Kjør hemmelig-scan (gitleaks, trufflehog) på dist-folderen før hver deploy.

DETEKTERT AV: PENTEST-AI · WEB.LEAKED_CREDENTIALS (SOURCE MAPS)

Open redirect i return-parameter på login

LAV · VURDER

`GET https://eksempelfirma.no/login?return=`

Login-endepunktet aksepterer en return-parameter som styrer hvor brukeren sendes etter vellykket innlogging. Vi fant at parameteren ikke valideres mot en whitelist over interne URL-er — vi kunne sette return=https://angriper.no/phish og brukeren ble redirected dit etter login. Selv om dette ikke gir direkte tilgang til serveren, brukes open redirects ofte i phishing-kampanjer for å gi en pålitelig avsender-URL i e-poster (https://eksempelfirma.no/login?return=...) som ender på et angriper-domene.

> **Slik fikser du:** Steg 1: Tillat kun relative URL-er (starter med /) som return-parameter. Avvis alle absolutte URL-er. Steg 2: Alternativt, ha en whitelist over godkjente eksterne URL-er hvis det er bevisst design. Steg 3: Hvis du må videresende eksternt, vis først en mellom-side med 'Du sendes nå til [URL] — er dette riktig?' og en eksplisitt klikk.

DETEKTERT AV: PENTEST-AI · WEB.OPEN_REDIRECT

04 · FUNN ETTER KATEGORI

TLS/SSL-konfigurasjon (1 funn)

TLS 1.0 og TLS 1.1 fortsatt aktivert

HØY · DENNE UKA

`https://eksempelfirma.no/ (port 443)`

TLS 1.0 og TLS 1.1 er aktivert på web-serveren. Begge er offisielt utdatert og deprecated av IETF (RFC 8996, mars 2021). De har kjente svakheter som BEAST, POODLE og er sårbare for downgrade-angrep. PCI-DSS, NSM og Datatilsynet anbefaler å bare støtte TLS 1.2 og 1.3. Tilstedeværelsen av eldre protokoller indikerer feilkonfigurasjon og senker den totale sikkerhetsscoren.

> **Slik fikser du:** Apache: legg til 'SSLProtocol -all +TLSv1.2 +TLSv1.3' i ssl.conf. Nginx: 'ssl_protocols TLSv1.2 TLSv1.3;'. Test resultatet på https://www.ssllabs.com/ssltest/ – målet er karakter A eller A+.

DETEKTERT AV: TESTSSL.SH

04 · FUNN ETTER KATEGORI

Sikkerhets-headers (3 funn)

Manglende HSTS-header

HØY · DENNE UKA

https://eksempelfirma.no/

HTTP Strict Transport Security (HSTS) er ikke konfigurert. Uten denne headeren kan en angriper i samme nettverk gjennomføre SSL-strip-angrep og lure brukeren til å sende sensitive data over ukryptert HTTP. Dette er spesielt risikofylt på åpne Wi-Fi-nettverk. HSTS er en av de billigste sikkerhets-mekanismene å aktivere og bør være på plass.

> **Slik fikser du:** Legg til følgende header i web-server-konfigurasjonen: 'Strict-Transport-Security: max-age=63072000; includeSubDomains; preload'. Etter at dette er testet i produksjon i noen uker, vurder å legge domenet på HSTS-preload-listen via https://hstspreload.org/.

DETEKTERT AV: NIKTO + NUCLEI

Manglende X-Content-Type-Options

MEDIUM · DENNE MÅNEDEN

https://eksempelfirma.no/

Headeren 'X-Content-Type-Options: nosniff' er ikke satt. Uten denne kan eldre nettlesere forsøke å MIME-sniffe innholdstype og kjøre filer som JavaScript selv om de er ment som data. Dette muliggjør XSS via opplastede filer.

> **Slik fikser du:** Legg til 'X-Content-Type-Options: nosniff' som en global respons-header. Apache: 'Header always set X-Content-Type-Options "nosniff"' i konfigurasjonen.

DETEKTERT AV: NUCLEI + NIKTO

Manglende X-Frame-Options

MEDIUM · DENNE MÅNEDEN

https://eksempelfirma.no/

Headeren 'X-Frame-Options' (eller den nyere 'Content-Security-Policy: frame-ancestors') er ikke satt. Dette gjør at siden kan iframes av tredjepartsdomener, hvilket åpner for clickjacking-angrep der en angriper plasserer din side som et usynlig overlay på en angripers side og lurer brukeren til å klikke på elementer.

> **Slik fikser du:** Sett enten 'X-Frame-Options: SAMEORIGIN' eller den moderne ekvivalenten 'Content-Security-Policy: frame-ancestors self'. Den siste er mer fleksibel og dekker flere browsere konsistent.

DETEKTERT AV: NUCLEI

04 · FUNN ETTER KATEGORI

Sårbar programvare (Port 80/443) (1 funn)

PHP 7.4 (utgått versjon)

HØY · DENNE UKA

https://eksempelfirma.no/

X-Powered-By-headeren avslører PHP 7.4. Denne versjonen nådde end-of-life 28. november 2022 og mottar ikke lenger sikkerhetsoppdateringer. Kjente CVE-er som ikke vil bli rettet inkluderer CVE-2022-31626 (CVSS 8.8) i mysqlnd-driveren.

> **Slik fikser du:** Oppgrader til PHP 8.2 eller 8.3 (begge støttet med sikkerhetsoppdateringer). Test alle aktive plugins og applikasjoner først - PHP 8 har breaking changes mot 7.4. Som midlertidig tiltak: fjern X-Powered-By-headeren via 'expose_php = Off' i php.ini, det reduserer informasjons-lekkasje men løser ikke den underliggende risikoen.

DETEKTERT AV: NIKTO

04 · FUNN ETTER KATEGORI

Web-applikasjon (Nikto) (2 funn)

Cookie XSRF-TOKEN uten HttpOnly-flagg

MEDIUM · DENNE MÅNEDEN

https://eksempelfirma.no/

Cookie-en XSRF-TOKEN settes uten HttpOnly-flagget. Dette gjør at JavaScript-kode på siden kan lese verdien, noe som øker risikoen ved en eventuell XSS-sårbarhet (en angriper kan eksfiltrere tokenet).

Slik fikser du: Sett HttpOnly-flagget på cookien. I PHP: 'setcookie($name, $value, [..., "httponly" => true])'. I rammeverk som Laravel: konfigurer i config/session.php. Test deretter at applikasjonen fortsatt fungerer (CSRF-tokens leses normalt server-side, ikke fra JavaScript).

DETEKTERT AV: NIKTO

BREACH-sårbar compression med dynamisk innhold

MEDIUM · DENNE MÅNEDEN

https://eksempelfirma.no/

Content-Encoding: deflate er aktivert sammen med dynamisk innhold som inkluderer auth-tokens. Dette gjør applikasjonen potensielt sårbar for BREACH-angrep, der en angriper i samme nettverk kan utlede CSRF-tokens via compression-ratio-analyse over tid.

Slik fikser du: Slå av HTTP-compression for endepunkter som returnerer dynamisk innhold med auth-tokens, eller masker CSRF-tokens per request (bytt verdi for hvert respons). Apache: 'SetEnvIfNoCase Request_URI "^/api/" no-gzip'.

DETEKTERT AV: NIKTO

04 · FUNN ETTER KATEGORI

DNS og e-post-konfigurasjon (2 funn)

Svak DMARC-policy (p=none)

MEDIUM · DENNE MÅNEDEN

_dmarc.eksempelfirma.no

DMARC er satt opp, men med 'p=none' som betyr at policy ikke håndheves. Mottakere som Gmail, Outlook og Proton vil rapportere brudd til deg, men ikke avvise forfalskede e-poster. Det betyr at en angriper kan sende falske e-poster i ditt navn som ofte når frem til mottakeren.

> **Slik fikser du:** Etter en periode med p=none og analyse av rapporter, gå gradvis over til 'p=quarantine; pct=25' (25 prosent av falske e-poster havner i søppelpost). Etter 1-2 måneder uten falske positive, gå til 'p=quarantine; pct=100' og deretter 'p=reject'. Bruk verktøy som dmarcanalyzer.com for å overvåke rapportene.

DETEKTERT AV: DNS + EMAIL-CHECKS

SPF-policy bruker ~all (softfail) ikke -all (fail)

LAV · VURDER

eksempelfirma.no TXT

SPF-recorden ender på '~all' (softfail). Det betyr at mottakere får råd om å sortere ikke-godkjente avsendere til søppelpost, men ikke avvise dem. En strengere '-all' (hardfail) gir bedre beskyttelse mot forfalskning.

> **Slik fikser du:** Etter at du har verifisert at alle legitime utsendelser går via SPF-godkjente kilder (egen mail-server, Brevo, Stripe, Google Workspace, og lignende), endre SPF-recorden til '-all'. Test med https://mxtoolbox.com/.

DETEKTERT AV: DNS + EMAIL-CHECKS

04 · FUNN ETTER KATEGORI

Sertifikat (TLS) (1 funn)

TLS-sertifikat utløper innen 30 dager

LAV · VURDER

https://eksempelfirma.no/

Let's Encrypt-sertifikatet utløper 18. juni 2026 (27 dager). Selv om auto-fornyelse antakelig fungerer, er det god praksis å verifisere at certbot eller tilsvarende kjører som forventet, da et utløpt sertifikat fører til at hele siden blir utilgjengelig for brukere.

> **Slik fikser du:** Verifiser at 'certbot renew --dry-run' kjører uten feil. Sjekk at certbot.timer er aktiv: 'systemctl status certbot.timer'. Sett opp varsling 14 dager før utløp via UptimeRobot eller egen monitorering.

DETEKTERT AV: TESTSSL.SH

04 · FUNN ETTER KATEGORI

Informasjons-lekkasje (1 funn)

Server-versjon eksponert i HTTP-header

LAV · VURDER

https://eksempelfirma.no/

Server-headeren returnerer 'Apache/2.4.49 (Ubuntu)'. Selv om versjonen i seg selv ikke er en sårbarhet, gir den en angriper rask vei til kjente exploit-databaser, og fjerner ett hinder fra rekognoserings-fasen.

> **Slik fikser du:** Apache: 'ServerTokens Prod' og 'ServerSignature Off' i konfigurasjonen. Nginx: 'server_tokens off;' i http-blokken. Test deretter ved å se på Server-headeren med 'curl -I https://eksempelfirma.no/'.

DETEKTERT AV: HTTP-HEADERS

04 · FUNN ETTER KATEGORI

OSINT (theHarvester) (1 funn)

12 ansatte-e-poster funnet via offentlige kilder

INFO

Crawled fra Bing, crt.sh, GitHub

Vi fant 12 e-postadresser knyttet til eksempelfirma.no på offentlige steder (LinkedIn, GitHub-commits, gamle nyhetsbrev). Dette i seg selv er ikke et angrep, men er nettopp den informasjonen en angriper bruker som grunnlag for phishing-kampanjer (BEC, lønn-bytte-svindel og lignende).

> **Slik fikser du:** Gjennomgå hvilke ansatte-e-poster som er offentlig synlige, og vurder om noen kan maskeres (firmapost@ i stedet for navn@). Tren ansatte i hvordan de gjenkjenner BEC-mønstre. Bestill MAILSCAN-monitoring fra Mustvedt Sentinel for kontinuerlig overvåking av lekkasjer.

DETEKTERT AV: THEHARVESTER + CRT.SH

04 · FUNN ETTER KATEGORI

OSINT (CT-logs) (1 funn)

8 subdomener identifisert via Certificate Transparency

INFO

crt.sh-lookup

Vi fant 8 subdomener knyttet til eksempelfirma.no: mail, autodiscover, ftp, dev, staging, test, gamle-sider, beta. 'dev' og 'staging' returnerer 200 OK uten autentisering og inneholder full kopi av produksjon med test-data.

> **Slik fikser du:** Sett opp HTTP basic-auth eller IP-restriksjon på dev/staging/test-subdomener. Vurder å bruke .private-subdomener som ikke føres i CT-logs (sjeldnere brukt mønster). Som langsiktig tiltak: bruk Sentinel CT-monitorering for å fanges opp nye subdomener fortløpende.

DETEKTERT AV: CERTIFICATE TRANSPARENCY

04 · FUNN ETTER KATEGORI

Nettverks-rekognosering (1 funn)

Eksponering på Shodan

INFO

shodan.io-treff

Shodan har indeksert eksempelfirma.no med fingerprint: Apache 2.4.49, Ubuntu, port 22 og 443 åpne, sist sett 17. mai 2026. Det betyr at hele Internett enkelt kan finne domenet ditt i sårbarhets-søk basert på programvare-versjon.

> **Slik fikser du:** Skjul programvare-versjon (se 'Server-versjon eksponert'-funn). Vurder å sette opp WAF (Web Application Firewall) som Cloudflare for å skjule reell server-versjon og IP. Som Sentinel PLUSS-kunde: aktiver kontinuerlig overvåking av Shodan-fingerprint via Sentinel.

DETEKTERT AV: SHODAN + THEHARVESTER

04 · FUNN ETTER KATEGORI

Typosquatting (dnstwist) (1 funn)

3 registrerte typosquatting-domener funnet

HØY · DENNE UKA

Nær-stavinger av eksempelfirma.no

dnstwist genererte 1834 mulige stavefeil/forvekslinger av eksempelfirma.no. Av disse er 3 allerede registrerte og kan brukes til phishing mot dine ansatte eller kunder: eksempelfirrma.no (registrert hos privat aktør i Romania), eksempelfirna.no (hos namesilo, peker til parking), og eksempelfirma-no.com (hos GoDaddy, ny registrering 2026-04-12). En av disse, eksempelfirma-no.com, har MX-record satt og kan motta e-post som ser ut til å være fra deg.

> **Slik fikser du:** 1. Registrer kritiske staveformer defensivt (typisk 5-10 nær-domener, ~150 kr/år per domene). 2. Sett opp DMARC med p=reject for å forhindre at falske e-poster fra disse når mottakerne dine. 3. Aktiver Sentinel sin phishing-radar for kontinuerlig overvåking av nye typosquatting-registreringer.

DETEKTERT AV: DNSTWIST

04 · FUNN ETTER KATEGORI

WAF/Firewall (wafw00f) (1 funn)

Ingen Web Application Firewall (WAF) detektert

MEDIUM · DENNE MÅNEDEN

https://eksempelfirma.no/

wafw00f kjørte 22 detektor-signaturer mot domenet uten å finne tegn til en WAF som Cloudflare, AWS WAF, Imperva eller Akamai. Det betyr at applikasjons-laget eksponeres direkte mot internet, og en angriper kan iterere mot kjente sårbarhets-mønstre uten å bli filtrert. For en bedrift med kundedata bør dette være obligatorisk.

> **Slik fikser du:** Sett opp Cloudflare gratis WAF (gratis tier dekker SQL-injection, XSS, og DDoS-beskyttelse) eller AWS WAF hvis du allerede er på AWS. Cloudflare gratis-konto er tilstrekkelig for de fleste SMB-er og kan settes opp på en time ved å bytte nameservers til Cloudflare sine.

DETEKTERT AV: WAFW00F

04 · FUNN ETTER KATEGORI

Passiv subdomain-recon (subfinder + amass) (1 funn)

23 subdomener identifisert via passiv recon

MEDIUM · DENNE MÅNEDEN

`subfinder + amass kombinert mot 40+ datakilder`

Vi fant 23 subdomener knyttet til eksempelfirma.no via passiv enumeration (Bing, crt.sh, OTX, AlienVault, Censys, HackerTarget, og 35+ andre datakilder). 8 av disse er ikke nevnt i selskapets offentlige web-tilstedeværelse, og 3 lytter på port 80/443 uten autentisering: vpn-old.eksempelfirma.no (utdatert OpenVPN admin-portal), jenkins.eksempelfirma.no (Jenkins CI med default-login fortsatt aktiv), og elk.eksempelfirma.no (Kibana 7.10 åpen for hele internet, viser interne logger).

> **Slik fikser du:** 1. Avregistrer eller intern-rute alle ikke-aktive subdomener. 2. Sett opp HTTP basic-auth eller IP-allowlist på utviklings-/intern-verktøy som Jenkins og Kibana. 3. Inkluder subdomain-monitorering i Sentinel slik at nye subdomener (via Certificate Transparency-logs) fanges opp innen 24 timer.

DETEKTERT AV: SUBFINDER + AMASS

05 · HANDLINGSPLAN

Slik tar du tak

Jobb deg ovenfra og nedover. Hvert punkt med kritisk eller høy alvorlighet bør være fikset innen kort tid — ellers tar du på deg unødvendig risiko.

#	ALVOR	HVA	TIDSFRIST
1	CRITICAL	OpenSSH 8.9p1 Ubuntu eksponert mot Internett med kjent RCE	I dag
2	CRITICAL	Apache 2.4.49 med Path Traversal (CVE-2021-41773)	I dag
3	CRITICAL	SSRF eksponerer AWS instance metadata via /api/url-preview	I dag
4	CRITICAL	Usikker deserialisering i /api/import gir RCE	I dag
5	HIGH	IDOR — bruker kan hente andre brukeres ordrer	Denne uka
6	HIGH	CORS reflekterer enhver Origin og tillater credentials	Denne uka
7	HIGH	JWT-verifisering aksepterer alg: none	Denne uka
8	HIGH	Mass assignment lar bruker promote seg selv til admin	Denne uka
9	MEDIUM	API-nøkler lekket i JavaScript source maps	Denne mnd
10	LOW	Open redirect i return-parameter på login	Når du har tid
11	HIGH	TLS 1.0 og TLS 1.1 fortsatt aktivert	Denne uka
12	HIGH	Manglende HSTS-header	Denne uka
13	HIGH	PHP 7.4 (utgått versjon)	Denne uka
14	MEDIUM	Cookie XSRF-TOKEN uten HttpOnly-flagg	Denne mnd
15	MEDIUM	Manglende X-Content-Type-Options	Denne mnd
16	MEDIUM	Manglende X-Frame-Options	Denne mnd
17	MEDIUM	BREACH-sårbar compression med dynamisk innhold	Denne mnd
18	MEDIUM	Svak DMARC-policy (p=none)	Denne mnd

#	ALVOR	HVA	TIDSFRIST
19	LOW	TLS-sertifikat utløper innen 30 dager	Når du har tid
20	LOW	Server-versjon eksponert i HTTP-header	Når du har tid
21	LOW	SPF-policy bruker ~all (softfail) ikke -all (fail)	Når du har tid
22	INFO	12 ansatte-e-poster funnet via offentlige kilder	Valgfritt
23	INFO	8 subdomener identifisert via Certificate Transparency	Valgfritt
24	INFO	Eksponering på Shodan	Valgfritt
25	HIGH	3 registrerte typosquatting-domener funnet	Denne uka
26	MEDIUM	Ingen Web Application Firewall (WAF) detektert	Denne mnd
27	MEDIUM	23 subdomener identifisert via passiv recon	Denne mnd

06 · VI TAR JOBBEN

La oss fikse funnene for deg

DONE-FOR-YOU · TIMEBASERT ELLER FASTPRIS

Mustvedt Sentinel kan ta utbedringene

Du slipper å bruke uker på å forstå hva som må gjøres — vi har sett mønstrene før, og vi har verktøyene som trengs. Når du vil ha hjelp til å rette opp i funnene fra denne rapporten, så stiller vi opp.

HVA	HVORDAN	PRIS
Konkrete fikser av sårbarhetene i denne rapporten. Vi setter opp WAF, oppdaterer SSL-konfigurasjon, lukker eksponerte filer, oppgraderer utdatert programvare.	Direkte arbeid på dine servere og DNS-konfig, eller veiledning til ditt IT-team. Vi rapporterer hva som er gjort med før/etter-skann som bevis.	Time-basert konsulent-honorar eller fastpris per kategori. Tilbud etter samtale, og du betaler først når jobben er gjort og verifisert.

Ta kontakt: Christer Mustvedt · **Christer@mustvedt.net** · **mustvedt.net**

Andre Mustvedt Sentinel-tjenester

- **Sentinel PLUSS-abonnement (179 kr/mnd):** Kontinuerlig overvåkning av domener og e-poster mot lekkasje-databaser, daglig sikkerhets-skann, varsler ved nye sårbarheter, og selvbetjent skanne-dashboard med 17 verktøy.
- **Engangs Sårbarhetsrapport (1 990 kr):** Denne rapport-typen, levert som signert PDF innen 3 arbeidsdager. Bra for årlig sikkerhetsrevisjon eller før compliance-audit.
- **Custom enterprise-avtaler:** For større organisasjoner med spesielle behov. Ta kontakt for tilbud.

07 · VEDLEGG

Tekniske observasjoner

Disse er ikke sårbarheter, men informasjon om stack-en din som ble oppdaget under skannen. Inkludert for fullstendighet og for IT-personell.

KATEGORI	OBSERVASJON	STED
Web-server	**Server: Apache/2.4.49 (Ubuntu)**	HTTP-header
Web-server	**Powered by PHP 7.4.21**	HTTP-header
DNS	**DNSSEC ikke signert**	eksempelfirma.no
DNS	**Ingen CAA-record satt**	eksempelfirma.no
OSINT	**Subdomain identifisert: mail.eksempelfirma.no**	crt.sh
OSINT	**Subdomain identifisert: dev.eksempelfirma.no**	crt.sh
OSINT	**Subdomain identifisert: staging.eksempelfirma.no**	crt.sh
TLS	**Sertifikat utstedt av Let's Encrypt**	https://eksempelfirma.no/
Web-applikasjon	**ETag-header eksponerer inode-info**	https://eksempelfirma.no/
Web-applikasjon	**OPTIONS HTTP-metode aktivert**	https://eksempelfirma.no/
Web-applikasjon (pentest-ai)	**61 web-prober kjørt via pentest-ai**	engagement #437263d9
Deteksjon	**Sigma-, SPL- og KQL-regler generert for alle utnyttede teknikker**	vedlagt rapport.tar.gz
Angreps-kjede	**1 kritisk angreps-kjede oppdaget på tvers av funn**	automatisk korrelering