Vernix

04. august 2026

Sårbarhetsrapport

For Nordvik Regnskap AS (eksempelkunde)

Innhold

Kort fortalt

Denne siden er skrevet for deg som ikke jobber med sikkerhet til daglig. Du trenger ikke lese resten av rapporten for å vite hva som gjelder.

HVA VI FANT

Skanningen av nordvik-regnskap.no viser at **filer som typisk inneholder passord og nøkler kan lastes ned av hvem som helst på internett**, at **en angriper kan lese filer fra serveren utenfra, også filer som ikke er ment å være offentlige**, og at **nettstedet kan brukes til å sende brukere videre til svindelsider i deres navn**.

Dette bør håndteres nå, ikke i neste planlagte utviklingsrunde.

RISIKONIVÅ

52 av 100 betyr forhøyet. Det er ikke akutt, men det bør ned. Ved forrige skann sto det på 71. Gjør dere de to første punktene på neste side, havner dere rundt 30.

STATUS SIDEN FORRIGE SKANN

2	1	6
bekreftet lukket	venter på verifisering	står åpne

ORD DU MØTER I DENNE RAPPORTEN

.env-fil	En fil der utviklere lagrer passord og nøkler applikasjonen trenger. Skal aldri være åpen.
Kritisk / Høy / Middels / Lav	Hvor alvorlig et funn er. Kritisk betyr at vi har bekreftet at det kan utnyttes.
Uløst	Funnet står fortsatt åpent. Andre statuser er «meldt løst» og «bekreftet lukket».
Black-box	Vi testet utenfra, uten passord og uten tilgang til koden — som en utenforstående.
Header	En innstilling nettstedet sender til nettleseren. Flere av funnene handler om manglende headere.
LFI	Local File Inclusion — når en funksjon kan lures til å hente vilkårlige filer fra serveren.

> Denne rapporten beskriver hva som står åpent mot internett i dag. Den vurderer ikke hvor sannsynlig et angrep er, eller hva et angrep ville kostet dere.

Slik kommer du i gang

De tre funnene vi mener bør utbedres først, i rekkefølge. Er dere ikke selv i stand til å gjøre dette, gi denne siden til den som drifter nettsidene deres.

1 **Eksponert .env-fil med passord og nøkler** — Kritisk

Hvor: `https://nordvik-regnskap.no/.env`

Første steg: Finn .env-filen i prosjektmappen.

2 **Filer kan leses fra serveren utenfra** — Kritisk

Hvor: `https://nordvik-regnskap.no/api/dokument?sti=../../../../etc/passwd`

Første steg: Åpne koden for API-ruten som tar imot 'sti'-parameteret.

3 **Nettstedet kan sende brukere videre til andre nettsteder** — Middels

Hvor: `https://nordvik-regnskap.no/gaa?url=//example.org`

Første steg: Finn ruten som håndterer omdirigeringer.

De øvrige 4 funnene er beskrevet i kapittel 2.2, med tiltak og referanser for hvert enkelt.

Trenger dere hjelp til å fikse dette?

Har dere ikke egen utvikler eller driftsleverandør, kan vi sette dere i kontakt med noen som kan utbedre funnene. Send en e-post til hjelp@vernix.no og legg ved denne rapporten.

FOR LEDELSE OG REVISOR

1. Sammendrag

1.1 KONFIDENSIALITETSERKLÆRING

Dette dokumentet er Nordvik Regnskap AS (eksempelkunde) og Vernix' eksklusive eiendom og inneholder konfidensiell og opphavsrettslig beskyttet informasjon. Mangfoldiggjøring, videredistribusjon eller bruk – helt eller delvis – krever samtykke fra Nordvik Regnskap AS (eksempelkunde). Nordvik Regnskap AS (eksempelkunde) kan dele dokumentet med revisorer under taushetsavtale for å dokumentere etterlevelse av krav til sikkerhetstesting.

1.2 OVERSIKT

Den 04. august 2026 gjennomførte Vernix en automatisert sikkerhetsvurdering (black-box) av webapplikasjonen for Nordvik Regnskap AS (eksempelkunde). Vurderingen ble utført utenfra, uten legitimasjon og uten tilgang til kildekode — altså med samme utgangspunkt som en ekstern angriper. Formålet var å avdekke svakheter som er synlige fra internett. Omfanget var:

Omfang: nordvik-regnskap.no

Vurderingen resulterte i 2 kritiske, 3 middels og 2 lave funn. Det ble påvist kritiske svakheter som gir en angriper mulighet til å kompromittere applikasjonen eller få tilgang til sensitive data. Disse bør utbedres umiddelbart, før de øvrige funnene.

1.3 UTVIKLING SIDEN FORRIGE SKANN

Ved forrige skann 4. juli 2026 sto 9 funn åpne, og risikonivået var 71. 2 funn er siden bekreftet lukket og 1 er meldt løst av dere og venter på verifisering. 1 tidligere funn er vurdert som falsk positiv og er lukket. Risikonivået er nå 52.

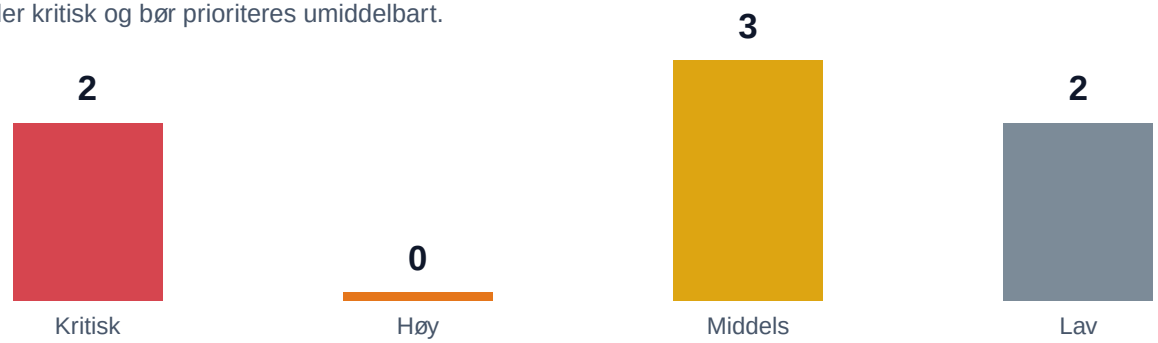
1.4 KONKLUSJON

Sikkerhetstilstanden inneholder svakheter som kan påvirke konfidensialitet, integritet og tilgjengelighet dersom de ikke håndteres. Vi anbefaler å utbedre funnene i prioritert rekkefølge og verifisere rettelsene gjennom en ny skann.

2. Funn

2.1 FORDELING OG SAMLETABELL

Tabellen nedenfor viser hvert identifiserte funn, kategorisert etter alvorlighetsgrad og status. 2 av funnene er gradert høyt eller kritisk og bør prioriteres umiddelbart.



ID	FUNN	STATUS	ALVORLIGHET
F-1	Eksponert .env-fil med passord og nøkler Generic Env File Disclosure	Uløst	Kritisk
F-2	Filer kan leses fra serveren utenfra Local File Inclusion - Linux	Uløst	Kritisk
F-3	Nettstedet kan sende brukere videre til andre nettsteder Open Redirect Detection	Uløst	Middels
F-4	Manglende innholdssikkerhetspolicy Content Security Policy (CSP) Header Not Set	Uløst	Middels
F-5	Utdatert JavaScript-bibliotek med kjente svakheter Vulnerable JS Library	Uløst	Middels
F-6	Mappeinnhold er synlig for alle Directory Listing Enabled	Meldt løst	Lav
F-7	Svake krypteringsmetoder i bruk Weak Cipher Suites Detection	Uløst	Lav

2.2 Detaljerte funn

F-1 — Eksponert .env-fil med passord og nøkler

Kritisk

Generic Env File Disclosure · Status: Uløst · Identifisert 04. august 2026

Innholdet er påvist hentbart. Filen eksponerer en .env-fil, som typisk inneholder databasepassord og API-nøkler. Kritisk er forbeholdt funn der virkningen er bekreftet.

HVA DETTE ER

.env-fil: Dette betyr at konfigurasjonsfilen for applikasjonen er offentlig tilgjengelig. Dette kan føre til at sensitive opplysninger, som passord, blir eksponert.

HVA EN ANGRIPER KAN GJØRE MED DET

Med innholdet i denne filen kan en angriper logge inn i databasen deres og lese eller endre kundedata — uten å måtte bryte seg inn noe sted.

BERØRTE ADRESSER

`https://nordvik-regnskap.no/.env`

BEVIS

```
DB_PASSWORD=***
APP_KEY=base64:***
```

FOR DEN SOM FIKSER

Hvor: Flytt .env-filen ut av webroot, slik at den ikke kan nås via nettleseren.

1. Finn .env-filen i prosjektmappen.
2. Flytt filen til en sikker plassering utenfor webserverens rotmappe.
3. Oppdater applikasjonen til å referere til den nye plasseringen av .env-filen.
4. Endre alle eksponerte legitimasjoner som er nevnt i filen.

SLIK BEKREFTER DU AT DET ER FIKSET

```
curl -s -o /dev/null -w '%{http_code}\n' https://nordvik-regnskap.no/.env
```

Kommandoen skal skrive ut 403 eller 404. Skriver den 200, er filen fortsatt tilgjengelig — og en omdirigering (301/302) er ikke nok, siden innholdet kan være tilgjengelig på det nye stedet.

REFERANSER

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/03-Test_File_Extensions_Handling_for_Sensitive_Information
https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html

F-2 — Filer kan leses fra serveren utenfra

Kritisk

Local File Inclusion - Linux · Status: Uløst · Identifisert 04. august 2026

Utnyttelsen er aktivt verifisert i denne skanningen, ikke utledet fra en template — virkningen er dermed påvist og ikke antatt.

HVA DETTE ER

Local File Inclusion: Dette betyr at applikasjonen kan inkludere filer fra serveren uten tilstrekkelig kontroll. Utnyttelse kan gi tilgang til sensitive systemfiler.

HVA EN ANGRIPER KAN GJØRE MED DET

En angriper kan hente ut filer fra serveren, blant annet konfigurasjonsfiler og brukerlister, og bruke dem til å komme seg videre inn i systemene deres.

BERØRTE ADRESSER

`https://nordvik-regnskap.no/api/dokument?sti=../../../../etc/passwd`

FOR DEN SOM FIKSER

Hvor: Kontroller API-ruten som håndterer parameteret 'sti'.

1. Åpne koden for API-ruten som tar imot 'sti'-parameteret.
2. Implementer en liste over tillatte stier (allowlist) for å validere inndata.
3. Sørg for at filene som kan inkluderes, ligger i en forhåndsdefinert mappe.
4. Test endringen for å sikre at kun tillatte filer kan inkluderes.

SLIK BEKREFTER DU AT DET ER FIKSET

```
curl -s 'https://nordvik-regnskap.no/api/dokument?sti=../../../../etc/passwd' | grep -c 'root:'
```

Kommandoen sender samme forespørsel som skanningen og skal skrive ut 0. Et tall over 0 betyr at serveren fortsatt leverer innholdet i /etc/passwd.

REFERANSER

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion

F-3 — Nettstedet kan sende brukere videre til andre nettsteder

Middels

Open Redirect Detection · Status: Uløst · Identifisert 04. august 2026

HVA DETTE ER

Åpen omdirigering: Dette betyr at applikasjonen kan omdirigere brukere til eksterne nettsteder uten kontroll. Dette kan føre til phishing-angrep.

HVA EN ANGRIPER KAN GJØRE MED DET

En angriper kan sende ut e-poster med lenker som starter på deres eget domene, men ender på en svindelside. Mottakeren ser deres navn i lenken og stoler på den.

BERØRTE ADRESSER

`https://nordvik-regnskap.no/gaa?url=//example.org`

FOR DEN SOM FIKSER

Hvor: Se på koden som håndterer 'url'-parameteret.

1. Finn ruten som håndterer omdirigeringer.
2. Legg til en sjekk som bare tillater omdirigeringer til stier innenfor ditt eget domene.
3. Test for å sikre at eksterne omdirigeringer ikke er tillatt.

SLIK BEKREFTER DU AT DET ER FIKSET

```
curl -sI 'https://nordvik-regnskap.no/gaa?url=//example.org' | grep -i '^location'
```

Kommandoen skal ikke vise en Location-header som peker på example.org. Gjør den det, sender nettstedet fortsatt brukere videre til en adresse angriperen styrer.

REFERANSER

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/04-Testing_for_Client-side_URL_Redirect

F-4 — Manglende innholdssikkerhetspolicy

Middels

Content Security Policy (CSP) Header Not Set · Status: Uløst · Identifisert 04. august 2026

HVA DETTE ER

Mangler Content Security Policy (CSP): Dette betyr at serveren ikke har en sikkerhetspolicy for innhold. Uten denne kan applikasjonen være mer utsatt for angrep.

HVA EN ANGRIPER KAN GJØRE MED DET

Uten denne innstillingen har nettleseren ingen sperre mot skadelig skript som eventuelt slipper inn på siden.

BERØRTE ADRESSER

`https://nordvik-regnskap.no/`

FOR DEN SOM FIKSER

Hvor: Legg til CSP-header i serverens respons.

1. Åpne konfigurasjonen for serveren (f.eks. Nginx eller Apache).
2. Legg til 'add_header Content-Security-Policy "default-src 'self';"' i Nginx eller 'Header set Content-Security-Policy "default-src 'self';"' i Apache.
3. Lagre endringene og start serveren på nytt.
4. Test for å bekrefte at CSP-headeren er lagt til i responsene.

SLIK BEKREFTER DU AT DET ER FIKSET

```
curl -sI https://nordvik-regnskap.no/ | grep -i 'Content-Security-Policy'
```

Kommandoen skal skrive ut en linje med Content-Security-Policy. Ingen utskrift betyr at headeren fortsatt mangler.

F-5 — Utdatert JavaScript-bibliotek med kjente svakheter

Middels

Vulnerable JS Library · Status: Uløst · Identifisert 04. august 2026

HVA DETTE ER

Sårbart JS-bibliotek: Dette betyr at den identifiserte jQuery-versjonen 1.12.4 har kjente sårbarheter. Utnyttelse kan føre til sikkerhetsproblemer.

HVA EN ANGRIPER KAN GJØRE MED DET

En angriper kan utnytte kjente svakheter i biblioteket til å kjøre kode i nettleseren til de som besøker siden deres.

BERØRTE ADRESSER

`https://nordvik-regnskap.no/static/js/jquery-1.12.4.min.js`

FOR DEN SOM FIKSER

Hvor: Finn jQuery-biblioteket i prosjektet.

1. Åpne filen som refererer til jQuery (f.eks. static/js/jquery-1.12.4.min.js).
2. Oppgrader jQuery til versjon 3.5.0 eller nyere.
3. Test applikasjonen for å sikre at alt fungerer som forventet etter oppgraderingen.

REFERANSER

https://www.cve.org/CVERecord?id=CVE-2020-11022

F-6 — Mappeinnhold er synlig for alle

Lav

Directory Listing Enabled · Status: Meldt løst · Identifisert 04. august 2026

HVA DETTE ER

Kataloglisting aktivert: Dette betyr at serveren viser innholdet i en mappe. Dette kan gi uønsket informasjon om filene på serveren.

HVA EN ANGRIPER KAN GJØRE MED DET

En angriper kan bla gjennom filene i mappen og finne dokumenter som ikke var ment å være offentlige.

BERØRTE ADRESSER

`https://nordvik-regnskap.no/vedlegg/`

FOR DEN SOM FIKSER

Hvor: Endre konfigurasjonen for webserveren.

1. Åpne konfigurasjonsfilen for webserveren (f.eks. Nginx eller Apache).
2. Finn innstillingen for kataloglisting.
3. Deaktiver kataloglisting ved å sette 'autoindex off' i Nginx eller 'Options -Indexes' i Apache.
4. Test for å bekrefte at kataloglisting ikke lenger er aktivert.

SLIK BEKREFTER DU AT DET ER FIKSET

```
curl -s https://nordvik-regnskap.no/vedlegg/ | grep -c 'Index of'
```

Kommandoen skal skrive ut 0. Et tall over 0 betyr at mappelisten fortsatt vises.

REFERANSER

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/04-Review_Old_Backup_and_Unreferenced_Files_for_Sensitive_Information

F-7 — Svake krypteringsmetoder i bruk

Lav

Weak Cipher Suites Detection · Status: Uløst · Identifisert 04. august 2026

HVA DETTE ER

Svake krypteringsmetoder oppdaget: Dette betyr at serveren støtter metoder med utilstrekkelig nøkkellengde. Dette kan gjøre kommunikasjonen mindre sikker.

HVA EN ANGRIPER KAN GJØRE MED DET

En angriper med tilgang til nettverkstrafikken kan i teorien bryte krypteringen og lese det som sendes mellom besøkende og nettstedet.

BERØRTE ADRESSER

`https://nordvik-regnskap.no:443/`

FOR DEN SOM FIKSER

Hvor: Endre TLS-konfigurasjonen på serveren.

1. Åpne konfigurasjonen for TLS/SSL.
2. Identifiser svake krypteringsmetoder og deaktiver dem.
3. Oppdater konfigurasjonen for å bare tillate sterke krypteringsmetoder.
4. Test for å bekrefte at svake metoder ikke lenger er tilgjengelige.

SLIK BEKREFTER DU AT DET ER FIKSET

```
openssl s_client -connect nordvik-regnskap.no:443 -tls1 2>&1 | grep -c 'Cipher is'
```

Kommandoen skal skrive ut 0. Et tall over 0 betyr at TLS 1.0 fortsatt godtas.

2.3 Observasjoner

Punktene under er observasjoner fra skanningen, ikke sårbarheter. De er ikke gradert og teller ikke med i funntallet, men er verdt å være klar over.

X-Content-Type-Options mangler
Serveren hindrer ikke nettleseren i å gjette innholdstype på filer den mottar.
`https://nordvik-regnskap.no/`

Tidsstempel eksponert
En fil på nettstedet avslører tidsstempler fra systemet.
`https://nordvik-regnskap.no/static/js/app.js`

GraphiQL-konsoll tilgjengelig
Et utviklerverktøy for GraphQL-API-et er åpent tilgjengelig. Vurder om det bør være i produksjon.
`https://nordvik-regnskap.no/graphql`

2.4 Ikke gjenfunnet i denne skanningen

Funnene under ble rapportert ved forrige skanning, men ble ikke gjenfunnet denne gangen. Det betyr ikke nødvendigvis at de er utbedret: enkelte tester er avhengige av tidsavhengige tilbakekall og gir ikke treff hver gang. Kontroller hvert punkt før det regnes som lukket.

Middels Missing Anti-clickjacking Header — sett 04. juli 2026

2.5 Løst siden sist

Funn som er lukket siden forrige rapport. Dette er dokumentasjonen dere kan vise til ved revisjon eller når en kunde spør hva dere har gjort.

FUNN	STATUS	BEKREFTET
Eksponert sikkerhetskopi av database Exposed Database Backup	Bekreftet lukket	28. juli 2026 · skanner
Manglende HSTS-header Strict-Transport-Security Missing	Bekreftet lukket	2. august 2026 · skanner
Mistenkt SQL-injeksjon i søkefelt SQL Injection - heuristic	Bekreftet falsk positiv	19. juli 2026 · manuell

TEKNISK

Vedlegg A — Omfang og metodikk

Vurderingen er en automatisert black-box-skann utført utenfra, uten legitimasjon og uten tilgang til kildekode. Testtilfellene er forankret i OWASP Web Security Testing Guide (WSTG) v4.2 — for utvalget av testtilfeller som lar seg automatisere.

	Black box (utført)	Grey box	White box
Tilgangsnivå	Ingen tilgang eller intern info	Noe intern tilgang og info	Full åpen tilgang
Fordeler	Mest realistisk; angriperperspektiv	Mer effektiv; sparer tid	Mest grundig
Ulemper	Lettere å overse skjulte forhold	Flere skjulte svakheter kan overses	Krever mer info og tid

FASER SOM BLE KJØRT

FASE	STATUS	RESULTAT
Kartlegging av subdomener	Fullført	4 verter funnet
DNS-oppslag	Fullført	4 verter slo opp
Sjekk av levende tjenester	Fullført	3 tjenester svarte
Portskanning	Fullført	2 åpne porter
Kjente sårbarheter (templatebasert)	Fullført	4 funn i rapporten
Gjennomgang av nettstedet	Fullført	0 funn i rapporten
Aktiv testing av parametre (fuzzing)	Fullført	0 funn i rapporten
Aktiv sikkerhetstesting (ZAP)	Fullført	3 funn i rapporten

Tallene viser hva hver fase bidro med til denne rapporten, etter at funn er deduplisert og sortert. Oppdagelsesfasene kartlegger flate og teller derfor verter og tjenester, ikke funn. En fase som fullførte uten funn betyr ikke at området er trygt — bare at denne skanningen ikke påviste noe der.

TEKNISK / REVISOR

Vedlegg B — Sårbarhetsdekning

En automatisert black-box-skann kan påvise mange sårbarhetsklasser, men ikke alle. Tabellen under viser hva denne vurderingen dekker, og hva som krever manuell testing med legitimasjon og kjennskap til applikasjonens forretningslogikk. Funn utenfor venstre kolonne kan ikke utelukkes på grunnlag av denne rapporten.

Dekket av denne vurderingen	Krever manuell testing — utenfor omfang
Eksponerte filer og kataloger (.env, .git, konfigfiler, kataloglisting)	Feil tilgangskontroll mellom brukere (krever to kontoer å sammenligne)
Kjente sårbarheter i komponenter (versjonsbaserte CVE-treff)	IDOR — usikre direkte objektreferanser (krever gyldig sesjon)
Injeksjon mot synlige parametre (XSS, SQLi, SSTI, LFI, kommandoinjeksjon)	Brutt eller mangelfull autentisering (krever innlogging og sesjonshåndtering)
SSRF og åpne videresendinger	Forretningslogikkfeil (krever kjennskap til hva appen skal gjøre)
TLS-, HTTP- og sikkerhetsheadere	Rettighetseskalering og flerstegs-angrepskjeder
Eksponerte tjenester og subdomener	Feil i JWT-validering og øktshåndtering

Vedlegg C — Ordliste

Autentisering
Å bekrefte hvem en bruker er, før tilgang gis.

Autorisasjon
Å avgjøre hva en innlogget bruker har lov til å gjøre.

Black-box
Testing utenfra, uten passord og uten tilgang til kildekoden.

Header
En innstilling nettstedet sender til nettleseren sammen med innholdet.

IDOR
Når man kan endre en referanse i adressen og få tilgang til andres data.

LFI
Local File Inclusion — når en funksjon kan lures til å hente vilkårlige filer fra serveren.

PII
Personopplysninger — data som kan identifisere en bestemt person.

SQL-injeksjon
Når inndata kan manipulere spørringene mot databasen.

TLS
Krypteringen som gjør at trafikk til nettstedet ikke kan avlyttes.

XSS
Cross-Site Scripting — når skadelig skript kan kjøres i besøkendes nettleser.

WSTG
OWASP Web Security Testing Guide — metodikken testtilfellene bygger på.