

SAMMANSTÄLLD RAPPORT / VERSION 1.0

Formkurvan Live

Säkerhetsrapport

Kodgranskning, verifierade rättningar och kvarvarande risker
Granskningsdatum och rapportdatum: 13 oktober 2026

Slutsats

Inga blockerande fynd kvar i de granskade rättningarna, med den dokumenterade riskacceptansen nedan. De rapporterade felen i SÄK-02 till SÄK-08 är verifierat rättade i de kontrollerade fallen. SÄK-01 är delvis rättat; möjligheten att i vissa förlopp härleda startplatsen kvarstår och har accepterats enligt projektets beslut.

Version som slutsatsen gäller

Slutligt granskat: grenen server, commit

e0556aedfa2f5726834ab50d18ba413373ef63a2

Ursprunglig granskning: grenen integration, commit

3805f93a8539bd4181d30f154417478922fe3718

Rapporten sammanför den ursprungliga granskningen och tre omgranskningar av säkerhetsrättningarna. Den innebär inte en ny totalgranskning av all kod som skiljer grenarna åt.

Resultat i korthet

Kontroll	Slutligt utfall
Rapporterade fynd	7 verifierat rättade; 1 delvis rättat med accepterad kvarvarande risk.
Sista provomgången	502 prov: 500 godkända, 2 underkända. De två röda visar den accepterade startplatsrisken.
Beroenden	DOMPurify uppdaterat och kontrollerat. En uuid-varning i mobilbyggets beroenden kvarstår som underhåll.
Drift	Ingen verifiering av driftsatt version eller provning mot dev/produktion.

Rapport-id: G-FKL-2026-10-13-R1

Utförd av: G - AI-assisterad granskare (Codex), på Pers uppdrag.

Dokumentets karaktär: tekniskt granskningsunderlag, inte en ackrediterad certifiering.

RAPPORT / 02

Omfattning och metod

Granskningen är riktad mot säkerhetsrelevanta funktioner i Formkurvan Live. Den kombinerar läsning av källkod, lokala reproduktioner, befintliga regressionsprov, egna kompletterande prov, webbläsarkontroller och en beroendekontroll. Den omfattar inte varje kodrad i applikationen.

Granskat område	Vad som kontrollerades
Identitet och behörighet	Inloggning, sessionsversioner, lösenordsbyte/återställning, telefonnycklar, ägarskap och delning.
Platsintegritet	Live-telemetri, integritetszoner, baninformation och kombinationer av publika fält.
Träning och externa tjänster	AI-API:er, användningsbokföring, träningslagring, Strava-händelser och notiser. Filimport och externa anrop lästes också.
Klient och beroenden	Säkerhetsrelevanta webbflöden, HTML-rening, Python-krav och npm-beroenden. Mobilkonfigurationen lästes översiktligt.

Angriparscenarier

Kontrollerna utgick från en anonym besökare, en person med giltig delningslänk eller följaråtkomst, ett inloggat konto, någon med en tidigare stulen cookie eller telefonnyckel samt förfalskade eller upprepade webhook-händelser. För AI-svar-id prövades ett redan känt främmande id; möjligheten att upptäcka ett sådant id har inte belagts.

Isolerad provning

Exakta kodversioner exporterades till separata lokala kopior. Proven använde tillfälliga databaser och syntetiska konton. AI, Strava och push ersattes av attrapper. Inloggning, HTML-rening och integritetsvarning provades även i Chrome med separata testprofiler. Inga verkliga användardata, notiser eller AI-kostnader ingick.

Utanför granskningen

Driftsatt kod och konfiguration, nginx, TLS, brandvägg, produktionsdatabas, säkerhetskopior, systempaket och mobilappen på hårdvara kontrollerades inte. Ingen belastningsattack, fullständig historisk hemlighetssökning, juridisk GDPR-bedömning eller fullständig serversvit ingick. Faktisk leverantörsdebitering och alla webbläsarvarianter provades inte.

Hur resultaten ska läsas: "Verifierat rättat" avser det rapporterade felet och de provade fallen. Ett grönt prov är stöd för en viss egenskap, inte bevis för att hela funktionen eller applikationen saknar säkerhetsbrister.

RAPPORT / 03

Fynd och slutlig status

Nivåerna nedan är den ursprungliga rapportens bedömningar, inte CVSS-poäng och inte kvarvarande risknivå efter rättning. Praktiska förutsättningar anges för att inte jämföra exempelvis kontostörning med kontokapning.

Id / ursprunglig nivå			Risk och viktig förutsättning	Status vid e0556aed
SÄK-01			Plats kan härledas trots integritetszon. Kräver delningslänk/följaråtkomst och användbar bangeometri.	Delvis rättat. Direkta läckor stängda. Härledning av startplats accepterad.
SÄK-02			Stulen telefonnyckel fortsätter fungera efter lösenordsbyte eller återställning.	Verifierat rättat.
SÄK-03			Besök på främmande sida kan ge inloggning på fel konto. Begränsad praktisk konsekvens; inget lösenord stjäls.	Verifierat rättat i provad Chrome och ursprungskontroller.
SÄK-04			AI-förbrukning vid avbrott bokförs som noll. Kostnadsrisk, inte kontoåtkomst.	Rapporterat fel rättat. Kostnadstaket är inte en hård garanti.
SÄK-05			Eget histogram kan växa utan sammanlagt tak. Kvot- och belastningsrisk för inloggat konto.	Verifierat rättat.
SÄK-06			Tidigare giltig cookie kan koppla bort nya telefoner. Störning, inte återvunnen läsåtkomst.	Verifierat rättat.
SÄK-07			Främmande AI-svar-id kan användas utan ägarkontroll. Kräver redan känt/läckt id.	Verifierat rättat med leverantörsattrapp.
SÄK-08			Förfalskade händelser kan påverka lokal Strava-cache; dubletter kan ge notiser. Kräver aktiverad webhook.	Rapporterade fel rättade. Driftaktivering ej kontrollerad.

SÄK-id är granskningens egna beteckningar, inte GR-ärenden. SÄK-04 och SÄK-05 handlar främst om resurskontroll och robusthet. SÄK-07 och SÄK-08 är villkorade fynd, inte belägg för pågående angrepp mot tjänsten.

Vad användare märker

Efter lösenordsbyte/återställning är gamla telefonnycklar ogiltiga; den egna appen kan koppla om automatiskt enligt projektets dokumentation. Integritetsvyn visar en tydligare varning. Följare får mindre positionsinformation inom zonen. Ogiltiga eller för stora histogram avvisas. Övriga rättningar påverkar främst skyddet i bakgrunden.

RAPPORT / 04

SÄK-01: integritetszon och startplats

Status: delvis rättat, kvarvarande risk accepterad.

En integritetszon döljer de direkta positionsfälten, men garanterar inte att startplatsen inte kan härledas ur annan information.

Ursprungligt fel och rättningar

I grundversionen doldes latitud och longitud, men banläget `match_s` fanns kvar. Samma delningslänk gav banans geometri, så ett banläge kunde översättas till kartposition. Det reproducerades med syntetiska data inne i en zon med 500 meters radie.

`a14b5a67` utökade filtreringen av positions- och sträckfält inne i zonen, även i sammanfattningen. En första omprovning visade att det upprepade startfältet `match_start_missed_m` fortfarande syntes i senare rader utanför zonen. `c48c4876` döljer nu även det fältet på alla publika rader när en zon finns. Ägaren behåller åtkomsten till sina egna uppgifter.

Vad som fortfarande går att härleda

Ett senare prov kombinerade en publik rad utanför zonen med den delade banan. I testet var `match_s` 3 336 meter och `distance_m` 2 224 meter. Skillnaden, 1 112 meter längs banan, gav den dolda startpunkten. `match_total_m` gav samma resultat. Att enbart ta bort det uttryckliga startfältet stänger alltså inte denna väg.

Förloppet kräver att passet startat på den kända banan och följt den framåt utan extra varv eller avstickare. De idealiska testvärdena gav exakt startpunkt; verklig GPS och vägmätare innebär osäkerhet. Ingen slutsats om exakt adressprecision för alla pass dras. Konsekvensen kan ändå vara betydande när starten avslöjar hem eller annan känslig plats.

Dokumenterat beslut och användarinformation

Projektets beslut, tillskrivet Per den 13 oktober 2026, accepterar denna kvarvarande risk för att behålla följares distansinformation. `ebb434d7` lägger till en varning i integritetsvyn: startar passet i zonen på en bana kan följaren räkna ut ungefärlig startplats; användaren rekommenderas att starta utanför zonen. Varningen har verifierats synlig via Jag → Integritet i Chrome med mobilbredd.

Detta är information och riskacceptans, inte en teknisk spärr mot härledning. Rådet att starta utanför zonen är en riskminskning, ingen garanti mot alla sätt att uppskatta plats.

Verifiering och spårbarhet

De tidigare publik- och ägarproven är gröna. Två oförändrade prov för härledning via `distance_m` respektive `match_total_m` är fortsatt röda och redovisas öppet. Denna härledning fanns före `c13a4eb3` och missades i den första omprovningen; den infördes inte av rättningen.

Källor: `server/live.py`; `server/templates/settings.html` (varning, rad 366-375); [U3], [U4]. Riskbeslutet finns i serverns säkerhetsrapport, avsnitt "SÄK-01, accepterad risk: startplatsen".

RAPPORT / 05

Identitet och sessioner

SÄK-02: telefonnycklar efter lösenordsbyte

Orsak: lösenordsbyte/återställning återkallade webbsessioner genom sessionsversionen, men telefonernas separata bearer-nycklar förblev giltiga. Någon med en tidigare stulen nyckel kunde behålla dess API-åtkomst.

Rättning: 69fbb146 återkallar telefonnycklar i samma transaktion som lösenordsändringen. **Verifierat:** gamla telefonnycklar får 401 vid både läsning och ändring efter byte respektive återställning. En gammal webbsession avvisas efter återställning. Klockans separat kopplade nyckel fungerar fortfarande enligt den avsedda policyn. Detta är alltså inte ett löfte om att alla typer av enhetsnycklar återkallas.

SÄK-03: påtvingad inloggning

Orsak: en främmande webbsida kunde skicka ett inloggningsformulär med angriparens kontouppgifter och få besökaren inloggad på fel konto. Den praktiska risken är att senare uppladdning sker till det kontot, inte att besökarens lösenord avslöjas.

Rättning: 0a18bbad kontrollerar Origin och Sec-Fetch-Site. **Verifierat:** den tidigare reproduktionen i Chrome får 403 och skapar ingen inloggad session; den egna inloggningssidan fungerar. Begäranden som saknar båda ursprungshuvudena accepteras fortfarande. Äldre webbläsare och alla inbäddade webbvisare är inte provade. Slutsatsen gäller det rapporterade angreppet och de testade klienterna.

SÄK-06: gammal cookie och nykopplade telefoner

Orsak: utloggningen använde användar-id från en signerad men återkallad cookie utan att först kontrollera aktuell sessionsversion. En tidigare stulen cookie kunde därför koppla bort en ny telefon.

Rättning: 69fbb146 gör giltighetskontrollen före kontoändringen. **Verifierat:** en gammal cookie efter "logga ut alla" kan inte återkalla en telefon som kopplats därefter. Fyndet avsåg störning av telefonåtkomsten, inte återställd läsrätt eller full kontokapning.

Samlad bedömning: SÄK-02, SÄK-03 och SÄK-06 är rättade i de kontrollerade fallen.

Telefonåterkallandet är den användarsynliga policyförändringen. Något generellt löfte om stöd och skydd för alla äldre klienter lämnas inte.

Källor: [server/auth.py](#); [server/shared.py](#); [server/pairing.py](#). Rättningsprov och resultat: [U2], upprepade i [U3] och [U4].

RAPPORT / 06

Kostnad och lagring

SÄK-04: AI-förbrukning vid avbrott

Ursprungligt fel: användningen bokfördes först när hela svarströmmen lästs. Om anslutningen avbröts efter att leverantören börjat arbeta blev den interna kostnaden noll. Timgränserna gällde fortfarande; fyndet gav inte ett obegränsat antal anrop.

Rättning: 652a7d15 säkerställer bokföring även vid avbrott och leverantörsfel. När slutlig användning saknas används en uppskattning. **Verifierat:** åtta kombinationer av analys/chatt, Anthropic/OpenAI och anslutningsavbrott/leverantörsfel bokför positiv kostnad en gång. Befintliga prov täcker fullständiga svar och cacheträffar.

Kvarvarande begränsning: uppskattningen är varken exakt debitering eller ett bevisat övre tak. Ingen budget reserveras före anropet; samtidiga anrop kan därför överskrida ett önskat dygnstak. De granskade timgränserna är fem analyser och tjugo chattfrågor. Leverantörsfakturer och avbrott genom produktionsproxyn har inte provats.

Bedömning: det rapporterade bokföringsfelet är rättat. Ett hårt, garanterat kostnadstak är en annan egenskap och ska inte påstås vara verifierad. Det är en kostnads- och robusthetsfråga, inte en belagd väg till andra användares data.

SÄK-05: histogram utan sammanlagt tak

Ursprungligt fel: API:t slog ihop godtycklig JSON med tidigare data. En gräns per anrop hindrade inte att samma databaspost växte över många anrop. Tre syntetiska uppladdningar lagrade cirka 3 MB samtidigt som lagringsredovisningen visade noll.

Rättning: 16231924 validerar histogrammens verkliga format, begränsar antalet staplar och inför ett sammanlagt tak på 5 MiB. Histogramdata räknas nu in i träningslagringen. **Verifierat:** båda legitima formaten fungerar; godtycklig text avvisas med 400 och överskridande med 413 utan att tidigare giltiga data skrivs över.

Bedömning: den rapporterade tillväxtvägen är rättad. Ett inloggat konto kunde påverka sin egen post, med potentiell belastning på den gemensamma tjänsten. Ingen faktisk överbelastning eller driftstörning framkallades, vare sig före eller efter rättningen.

Avgränsning: proven verifierar hanteringen av enskilda anrop och den lagrade posten. De mäter inte applikationens totala kapacitet, alla resurskvoter eller produktionskostnaden under belastning.

Källor: `server/traning_ai.py`; `server/traning_api.py`; `server/lagring.py`. Evidens: [U1], [U2], [U4].

RAPPORT / 07

AI-ägarskap och Strava-händelser

SÄK-07: ägarskap för AI-svar-id

Ursprungligt fel: klientens `previous_response_id` skickades till OpenAI utan kontroll av vilket konto som ägde det. Ett syntetiskt konto kunde få ett annat kontos kända id vidarebefordrat. Att angriparen kunde upptäcka id:t eller få ut verkligt innehåll från leverantören visades inte.

Rättning: 30995bea knyter både första och efterföljande svar-id till ägaren, med stöd för den tidigare analyscachen. **Verifierat:** eget id tillåts; främmande id går inte vidare. Utan egen analys returneras 400 före leverantörsanropet. Med egen analys skapas en separat konversation. Schema- och kontorelaterade prov är gröna. Bedömningen gäller kontokontrollen; leverantören var en attrapp.

SÄK-08: förfalskning, återspelning och samtidighet

Ursprungligt fel: en konfigurerad webhook-token aktiverade POST-vägen men autentiserade inte avsändaren. När funktionen aktiverades i testet kunde ett anonymt falskt raderingsmeddelande ta bort en post ur den lokala Strava-cachen. Aktiviteten hos Strava raderades inte.

Rättning av radering: 1582efba behandlar meddelandet som en signal som måste kontrolleras mot Strava med användarens nyckel. En aktivitet som finns kvar (200) raderas inte; ett leverantörsfel (500) raderar inte heller. Ett bekräftat 404-svar tillåter radering. Dessa fall är verifierade med attrapper.

Rättning av dubletter: en första kontroll före lagring hindrade sekventiella, men inte samtidiga dubletter. Åtta samtidiga händelser gav fem notiser i den sparade mellanversionens prov. 5962ab97 låter nu databasen avgöra förstahandsinsättningen atomiskt med INSERT OR IGNORE och nyckeln (`user_id`, `activity_id`). Reservation och ifyllning sker i samma transaktion; endast den som skapar raden får skicka notisen.

Verifierat i slutversionen: åtta samtidiga händelser ger en rad och en notis. Sekventiella dubletter ger ingen ny notis. Ett framkallat lagringsfel återställer transaktionen utan ofullständig rad eller notis; nästa försök lyckas med komplett rad och en notis.

Status: de rapporterade raderings- och dubblettproblemen är rättade. Webhooken är fortfarande inte autentiserad och upprepade anrop kan orsaka externa kontroller. Den uppges vara avstängd i projektets dokumentation; faktisk driftinställning är inte verifierad. Detta är inte belägg för ett aktivt angrepp eller en total överbelastningsgaranti.

Källor: `traning_ai.py`; `strava_webhook.py` (rad 76-91); `strava.py` (444-483); `db_schema.py` (1052-1067). Evidens: [U2]-[U4].

RAPPORT / 08

Beroenden och befintliga skydd

DOMPurify: uppdaterat och verifierat

Den incheckade versionen har uppdaterats från 3.1.6 till 3.4.17 i 712ee401. Den nya filen jämfördes byte för byte med den officiella npm-utgåvan och är identisk. Den sparade kontrollen av 105 publika npm-paketnamn/versioner gav ingen varning för den nya DOMPurify-versionen.

Ett Chrome-prov kontrollerade att normal Markdown-formatering behålls och att provens script, javascript-länkar och händelsehanterare tas bort. Detta stödjer rättningen men är inte ett fullständigt bevis mot alla XSS-varianter.

SHA-256 för den kontrollerade DOMPurify-filen:

```
cd37898f9782adf54820c413191b5691803f0  
f137c799d6edcfd38523b4c2c31
```

Officiellt underlag: [npm](#), [DOMPurify 3.4.17](#). Kontrollresultat: [U5].

uuid: kvarvarande beroendeunderhåll

uuid 7.0.3 via mobilbyggets xcode-beroende har en registervarning för vissa UUID-funktioner med medskickad utmatningsbuffert. Någon exploaterbar väg i den körande Formkurvan-tjänsten har inte belagts. Hantera detta som planerat beroendeunderhåll, inte som ett bevisat pågående intrång.

Referens: [GHSA-w5hq-g745-h8pq](#). Uppgiften återges från den sparade beroendekontrollen, inte en ny sökning vid dokumentskapandet.

Python och kontrollens giltighet

pip-audit mot serverns kravfil gav inga kända sårbarheter i de versioner som löstes vid grundgranskningen. Alla transitiva beroenden är inte fullständigt låsta. Resultatet gäller den sparade upplösningen, inte automatiskt en annan installation eller produktionsserverns systempaket. Ingen ny beroendesökning gjordes i den sista omgranskningen eftersom beroendena inte hade ändrats.

Grundskydd som observerades

Sessionscookies använder Secure, HttpOnly och SameSite=Lax. Vanlig sessionskontroll jämför sessionsversion mot databasen; lösenord lagras med Werkzeugs lösenordshashning. Gemensamma ägarskapskontroller finns för banor och flera andra resurser. OAuth använder state-kontroll. Storleks- och anropsgränser, HTML-rening och säkerhetsrubriker finns i de granskade vägarna.

Ingen bekräftad SQL-injektion, sökvägstraversering, kommandoinjektion eller generell åtkomst mellan konton hittades i dessa vägar. Det är en observation inom granskningens omfattning, inte ett påstående att sådana fel saknas överallt.

RAPPORT / 09

Provresultat och granskningshistorik

Kodversion / omgång	Prov	Utfall och betydelse
3805f93a Grundgranskning	421 befintliga 10 reproduktioner	Alla körningar gröna. De 10 reproduktionerna bekräftade brister; grönt betydde här inte säker funktion.
badc2f1b Första omprovning	495	492 gröna, 3 röda: två publikvägar för startfältet och en notisdublett.
c13a4eb3 Andra omprovning	499	496 gröna, 3 röda: två nya startplatshärledningar och samtidiga notisdubletter.
e0556aed Slutlig omprovning	502	500 gröna, 2 röda. Samtidighetsfelet rättat; startplatshärledningen kvarstår enligt accepterad risk.

Omgångarna återanvänder många prov. Antalen ska inte summeras till ett mått på unika säkerhetsegenskaper eller täckning.

Slutomgångens 502 prov

Provgrupp	Godkända	Underkända
Befintliga säkerhets-, API- och databasprov	475	0
Tidigare oberoende omprov	22	0
Kompletteringar: samtidighet och två integritetsfall	1	2
Nya kontroller: transaktionsåterställning och synlig mobilvarning	2	0
Totalt	500	2

De två röda proven är kvar oförändrade. De kontrollerar att dold startplats inte går att härleda via distance_m respektive match_total_m. Den egenskapen uppfylls inte av slutversionen och ingår i det dokumenterade riskbeslutet. Proven är inte överhoppade eller omskrivna för att bli gröna.

Reproducerbarhet

Resultaten är sparade som JUnit XML tillsammans med provkoden. Slutomgångens retest-results.xml innehåller 500 prov, varav två underkända; extra-results.xml innehåller ytterligare två godkända. Antalen i denna rapport har stämts av mot dessa filer. För återkörning används en isolerad export av den exakta committen, serverns testberoenden, tillfällig databas samt de tre granskningsfilerna i [U4].

Miljö: lokal macOS, Python 3.12.14 och pytest 9.1.1; Chrome för webbläsarproven. Ingen fullständig serversvit eller produktionsprovning utfördes. Dokumentsammanställningen innebar inte ytterligare en körning av hela provurvalet.

Kvarvarande risk och uppföljning

Fråga	Bedömning och lämplig uppföljning
Startplats, SÄK-01	Accepterad risk enligt projektbeslut. Behåll den synliga varningen och pröva beslutet igen om publik telemetri, delning eller integritetslöften ändras. Markera inte fyndet som helt tekniskt rättat.
Motstridig dokumentation	server/docs/sakerhetsgranskning-2026-10-13.md, rad 324, säger fortfarande "Ingen risk är accepterad." Det motsäger den nya status Tabellen och riskbeslutet. Rätta meningen; detta är inte ett blockerande kodfel.
uuid i mobilbygget	Planera uppdatering eller verifierad avgränsning av beroendet. Ingen exploaterbar produktväg är påvisad i granskningen.
Strava före aktivering	Kontrollera faktisk konfiguration och driftsbeteende. De lokala proven ersätter inte ett kontrollerat end-to-end-prov med den riktiga prenumerationen.
AI-kostnad	Beskriv gränsen som en uppskattad kontroll, inte garanterat hårt dygnstak. Följ upp verklig debitering och avbrott om kostnadstaket är ett verksamhetskrav.
Drift och senare versioner	Verifiera att rätt kodversion och avsedda inställningar används vid release. Nya säkerhetsrelevanta ändringar kräver ny bedömning; denna rapport gäller inte automatiskt senare commits.

Ingen ny acceptans eller driftsättning genom rapporten

Rapporten återger det befintliga beslutet om startplatsrisken; G fattar inget nytt riskbeslut åt Per. Inga produktfiler, driftinställningar eller data har ändrats under granskningen. G har inte mergat, deployat eller godkänt en driftsatt version genom detta dokument.

Intygets innebörd

Det separata granskningsintyget G-FKL-2026-10-13-I1 styrker att den redovisade AI-assisterade granskningen genomförts och sammanfattar dess resultat för exakt e0556aed. Det är inte en ackrediterad säkerhetscertifiering, en oberoende mänsklig revisors signatur, en GDPR-/ISO-bedömning eller en garanti om frånvaro av sårbarheter. Det ska läsas tillsammans med denna rapport.

Den konsoliderade rapporten är styrande för sammanfattad slutstatus. Äldre rapporter behålls som historik: deras öppna fynd och tidigare slutsatser ska läsas mot respektive kodversion, inte som oförändrad slutstatus.

RAPPORT / 11

Underlag och spårbarhet

Underlagen finns i den lokala granskningsmappen sakerhetsgranskning-3805f93a. Här anges relativa sökvägar inom den mappen. De ursprungliga rapporterna och proven bevaras; denna sammanställning skriver inte över dem.

Referens	Underlag
U1 Grundgranskning	rapport.md underlag/test_audit_review.py underlag/existing-tests.xml underlag/audit-reproductions.xml
U2 Första omprovning	omprovning-badc2f1b/rapport.md underlag/test_audit_retest.py samt existing-tests.xml, schema-tests.xml och independent-tests.xml i samma omprovningsmapp.
U3 Andra omprovning	omprovning-c13a4eb3/rapport.md underlag/test_audit_followup.py underlag/retest-results.xml och followup-results.xml i samma omprovningsmapp.
U4 Slutlig omprovning	omprovning-e0556aed/rapport.md underlag/test_audit_retest.py underlag/test_audit_followup.py underlag/test_audit_e0556aed.py underlag/retest-results.xml och extra-results.xml i samma omprovningsmapp.
U5 Beroenden	underlag/dependency-audit.json och npm-advisories.json omprovning-badc2f1b/underlag/dependency-retest.json Kontrollskripten finns intill respektive resultat.

Versionsankare

Grundversion (integration):

3805f93a8539bd4181d30f154417478922fe3718

Slutligt granskad version (server):

e0556aedfa2f5726834ab50d18ba413373ef63a2

Källkod: [öppna den slutligt granskade kodversionen på Bitbucket](#). Länkarna i rapporten pekar på denna version om inget annat anges. Åtkomst till det privata repot kan kräva inloggning.

Viktiga rättningscommits

SÄK-01: a14b5a67, c48c4876, ebb434d7 (information/riskbeslut).
SÄK-02/06: 69fbb146. SÄK-03: 0a18bbad. SÄK-04: 652a7d15.
SÄK-05: 16231924. SÄK-07: 30995bea.
SÄK-08: 1582efba, 47ebc476, 5962ab97. DOMPurify: 712ee401.

En manifestfil intill PDF-dokumentet innehåller SHA-256 för rapport, intyg och bevarade lokala underlagsfiler. Kontrollsummorna visar filidentitet, inte en digital signatur eller extern certifiering.