DAST Executive Summary

Sample packaged PDF artifact based on a ZAP-style reporting workflow

Target	staging.app.example.com
Method	authenticated web and API scan
Window	2026-03-24 to 2026-03-25
Tools	OWASP ZAP, OpenAPI import, authenticated context

Scope summary

The scan covered authenticated user flows, selected admin-adjacent routes, and the exported OpenAPI surface. The review intentionally excluded destructive admin endpoints and third-party callback paths.

Risk area	Status	Comment
TLS and security headers	Pass with notes	Headers present; CSP still broader than necessary
Authentication coverage	Needs follow-up	Authenticated context worked, but one export path was only partially exercised
Authorization checks	Needs manual review	Scanner signal suggests object-level checks require targeted manual validation
Input validation and injection	No direct evidence	Continue code-side and contract-side verification
Rate limiting and abuse telemetry	Partially evident	Headers and 429 behavior observed on login and export flows

Recommended next actions

- Tighten CSP and reduce unused script sources before production promotion.
- Run one focused manual authorization review against export and bulk-object workflows.
- Retain this scan in CI as a tuned signal source rather than expanding it into an untuned full-scan gate.
- Attach the HTML/XML scanner output to DefectDojo or the release evidence pack for traceability.

Interpretation notes

This sample PDF is intentionally concise. It demonstrates how a scanner-oriented report can be turned into a human-readable artifact with scope, status, and next actions rather than a raw dump of alerts.

Good reporting habits

Do this	Avoid this
State what was in and out of scope	Pretend the scan covered every meaningful workflow
Translate alerts into engineering decisions	Ship raw findings with no prioritization
Keep auth/debug notes with the report	Make future reviewers rediscover context from scratch