



Demo Allergy Diary (synthetic test customer)

Security readiness assessment

Observed on 2026-10-15 | Version 1.0

Prepared for

Demo Allergy Diary (synthetic test customer)

Prepared by

Amadis Consultancy Ltd

Veydr assessment team

Draft: not approved for release

CONFIDENTIAL

Contents

Section	Title
1	Summary
2	Scope and depth
3	Findings by severity
4	OWASP Top 10 (2025)
5	OWASP API Security Top 10 (2023)
6	OWASP MASVS (v2)
7	Access-control results
8	UK GDPR and data-security checklist
9	Fixes and retest status
10	Limits of this assessment
11	What this report is and is not
12	Sources and attribution
13	Review and approval

Document control

Version	Date	Change
Draft	2026-10-16	Reviewed by Amadis

1. Summary

Between 1 and 15 October 2026 we scanned four repositories in the customer's own CI, reviewed every automated result by hand, tested access control on the beta environment with two test accounts, and ran passive checks of the public API host.

The most serious observation is F04: a signed-in test account could read another account's allergy profile by changing an id in the request.

What to fix first

F04: One account can read another account's allergy profile Critical

Check on the server that the profile requested belongs to the signed-in account before returning it.

F02: An API key is committed to the repository High Revoke the key with its issuer, issue a new one held in the CI secret store, and remove the value from the file.

F03: Search query built by string formatting High Pass the search term as a query parameter instead of formatting it into the SQL.

Demo Allergy Diary (synthetic test customer): readiness observations at 2026-10-15 within the agreed scope (2026-10-01). Report version 1.0.

Final severity	Open	Fix reported, not yet retested	Not detected (not proof of a fix)	Verified fixed (fix observed on retest)	Accepted risk
Critical	0	1	0	1	0
High	2	0	0	0	0
Medium	0	0	0	0	0
Low	0	0	0	0	1

Areas not assessed or only partly assessed: 11 (listed in section 2).

Not looked at: the payment provider's hosted pages, staff laptops and email.

FINDINGS

Critical	2
High	2
Medium	0
Low	1

STATUS

Open	2
Fix reported, not yet retested	1
Verified fixed (fix observed on retest)	1
Accepted risk	1

DATES

Scope agreed	2026-10-01
Observed	2026-10-15

2. Scope and depth

Agreed scope (2026-10-01):

Asset	Kind	Internet-facing	Special category data	What was covered
demo-api	web API for the mobile app	yes	yes	repository main (kit), passive outside-in checks of api.demo.example.test, manual access-control tests
demo-reports	internal reporting job	no	yes	repository main (kit)
demo-ops	deployment configuration	no	no	repository main (kit)
demo-mobile	iOS app source	no	yes	repository main (kit), configuration and source only; the app was not built

Excluded from scope: the payment provider's hosted pages, staff laptops and email.

Repository: main at commit 0123456789abcdef0123456789abcdef01234567; kit version 0.2.0, run 2026-10-15T09:12:00Z.

Area	Status	Not assessed or partial, with the reason
Dependencies	partial: direct dependencies only for some manifests	mobile/ios/Podfile: not assessed
Code flaws (javascript, njsscan)	partial, depth baseline	JSX and TypeScript files are not read by njsscan
Code flaws (python, bandit)	assessed, depth partial	none
Code flaws (swift, no module)	not assessed, depth none	no code-flaw module for this language yet
Infrastructure configuration	assessed	git::https://example.test/modules/vpc.git: remote terraform modules not assessed
Mobile configuration	partial: some mobile files could not be read	mobile/ios/App/Info.plist: not assessed
Backend rules	assessed	none
.NET build	assessed	none
NuGet Audit (.NET packages)	not assessed	ops/tools/Tools.csproj: dotnet restore failed (exit 1); NuGet Audit did not run on it
Engines that did not complete	mobsfscan	see the depth rows above

Area	Status	Not assessed or partial, with the reason
Suppressions found in the repository	3	.gitleaksignore reports/export.py line 19 # nsec ops/tools/Directory.Build.props (.NET suppression settings: NoWarn, rule severity or analysis switched off)
Manual tests	listed in section 7	two test accounts created by the customer for Amadis (account A and account B), 2026-10-14

3. Findings by severity

Ordered Critical, High, Medium, Low; within a level, open before fixed.

ID	Final severity	Title	Asset	Status
F04	Critical	One account can read another account's allergy profile	demo-api	Fix reported, not yet retested
F01	Critical	Log4j 2.14.1 allows remote code execution (Log4Shell)	demo-api	Verified fixed
F02	High	An API key is committed to the repository	demo-ops	Open
F03	High	Search query built by string formatting	demo-reports	Open
F05	Low	The deployment image runs as root	demo-ops	Accepted risk

Each finding below gives its location, evidence, impact, fix and how its severity was reached.

F04: One account can read another account's allergy profile

Severity Critical	Status open: fix reported by the customer, not yet retested	Asset demo-api
Location GET /api/profiles/{id}	Frameworks A01:2025, API1:2023	Rubric 2 (EPSS off)

What we observed

Signed in as account B, changing the profile id in the request returned account A's profile.

Evidence

```
GET /api/profiles/1041 HTTP/1.1
Host: beta.api.demo.example.test
Authorization: Bearer [redacted: account B's session]

HTTP/1.1 200 OK
{"id": 1041, "owner": "veydr-test-a", "allergies": ["[synthetic test values, redacted]"]}
```

Impact

Any signed-in user could read every other user's allergies, which is special category health data.

Fix

Check on the server that the profile requested belongs to the signed-in account before returning it.

How the severity was reached

Medium (default); internet-facing +1: demo-api is reachable from the public internet; special-category-data +1: the profile holds allergy (health) data; rubric 2 (EPSS off)

Base Medium (default)

internet-facing +1

special-category-data +1

Critical

F01: Log4j 2.14.1 allows remote code execution (Log4Shell)

Severity Critical	Status verified fixed: retest on 2026-10-15 (kit rerun at the fix commit no longer reports it; the lockfile holds log4j-core 2.17.1)	Asset demo-api
Location api/pom.xml, org.apache.logging.log4j:log4j-core 2.14.1 (fixed in 2.15.0)	Frameworks A03:2025, API8:2023	Rubric 2 (EPSS off)

What we observed

The API's build pulls in log4j-core 2.14.1, a version with a published remote code execution flaw that is being exploited.

Impact

Anyone who can get a crafted string logged by the API could run their own code on the server and read the allergy records it holds.

Fix

Upgrade log4j-core to 2.17.1 or later.

Advisory

GHSA-jfh8-c2jp-5v3q <https://github.com/advisories/GHSA-jfh8-c2jp-5v3q>

How the severity was reached

Critical (cvss3, 10.0); kev +1: CVE-2021-44228 is in the CISA KEV catalog; internet-facing +1: demo-api is reachable from the public internet; special-category-data +1: demo-api holds allergy (health) data; rubric 2 (EPSS off)

Base Critical (cvss3)

kev +1

internet-facing +1

special-category-data +1

Critical

F02: An API key is committed to the repository

Severity High	Status open	Asset demo-ops
Location ops/config/settings.py line 7, fingerprint sha256:5f1d2c0e9b7a4c3d2e1f0a9b8c7d6e5f4a3b2c1d0e9f8a7b6c5d4e3f2a1b0c9d	Frameworks A04:2025, A02:2025	Rubric 2 (EPSS off)

What we observed

A value shaped like an API key is stored in a tracked configuration file.

Impact

Anyone who can read the repository gets whatever that key grants until it is revoked.

Fix

Revoke the key with its issuer, issue a new one held in the CI secret store, and remove the value from the file.

How the severity was reached

High (secret); no adjustments; rubric 2 (EPSS off)

Base High (secret)

High

F03: Search query built by string formatting

Severity High	Status open	Asset demo-reports
Location reports/allergy_search.py line 41	Frameworks A05:2025	Rubric 2 (EPSS off)

What we observed

The report job builds an SQL query by inserting a search term into the query text.

Impact

If the search term can come from a user, they could read or change records beyond their own.

Fix

Pass the search term as a query parameter instead of formatting it into the SQL.

How the severity was reached

Medium (label); special-category-data +1: demo-reports reads allergy (health) data; rubric 2 (EPSS off)

Base Medium (label)

special-category-data +1

High

F05: The deployment image runs as root

Severity Low	Status accepted risk until 2027-04-15 (owner: the customer's engineering lead): the image runs only on an internal build host	Asset demo-ops
Location ops/Dockerfile line 1	Frameworks A02:2025	Rubric 2 (EPSS off)

What we observed

The Dockerfile sets no non-root user.

Impact

A flaw in the service would give an attacker root inside the container, making it easier to go further.

Fix

Add a USER line with an unprivileged account.

How the severity was reached

Low (label); no adjustments; rubric 2 (EPSS off)

Base Low (label)

Low

Kit results reviewed and not reported, with the reason:

Kit result

Reason

gitleaks generic-api-key
api/tests/fixtures/client.json 3

a placeholder in a test fixture; the customer showed it is not accepted by
any service

4. OWASP Top 10 (2025)

Item	Name	Result	Evidence
A01:2 025	Broken Access Control	not met	F04
A02:2 025	Security Misconfiguration	not met	F02, F05
A03:2 025	Software Supply Chain Failures	not met	F01
A04:2 025	Cryptographic Failures	not met	F02 (a credential in plain text)
A05:2 025	Injection	not met	F03
A06:2 025	Insecure Design	not assessable	design is not examined by scanning; no design review was agreed
A07:2 025	Authentication Failures	met	sign-in, session expiry and password reset tried with both test accounts (section 7)
A08:2 025	Software or Data Integrity Failures	not assessable	dependency lockfiles and CI configuration read; no finding (shown as not assessable: dependencies is partial: direct dependencies only for some manifests)
A09:2 025	Security Logging and Alerting Failures	not assessable	logging and alerting run outside the repository
A10:2 025	Mishandling of Exceptional Conditions	not assessable	error handling under load or fault was not tested

Source: OWASP Top 10:2025, <https://owasp.org/Top10/>.

5. OWASP API Security Top 10 (2023)

Item	Name	Result	Evidence
API1:2 023	Broken Object Level Authorization	not met	F04
API2:2 023	Broken Authentication	met	section 7, sign-in and session tests
API3:2 023	Broken Object Property Level Authorization	met	section 7, property update test
API4:2 023	Unrestricted Resource Consumption	not assessable	no load or rate tests were agreed
API5:2 023	Broken Function Level Authorization	met	section 7, admin route test
API6:2 023	Unrestricted Access to Sensitive Business Flows	not assessable	business flows were not tested
API7:2 023	Server Side Request Forgery	not assessable	code-flaw rules for outbound requests ran on the Python code; no finding (shown as not assessable: code is partial: some languages not assessed or not fully read)
API8:2 023	Security Misconfiguration	not met	F01
API9:2 023	Improper Inventory Management	not assessable	no API inventory was in scope
API10: 2023	Unsafe Consumption of APIs	not assessable	third-party APIs the service calls were not in scope

Source: OWASP API Security Top 10 2023, <https://owasp.org/API-Security/editions/2023/en/0x11-t10/>.

6. OWASP MASVS (v2)

Item	Name	Result	Evidence
MASVS-STORAGE	Storage	not assessable	Info.plist could not be read (section 2)
MASVS-CRYPTO	Cryptography	not assessable	Swift has no code-flaw module yet (section 2)
MASVS-AUTH	Authentication and Authorization	not assessable	the app was not built or run
MASVS-NETWORK	Network Communication	not assessable	Info.plist could not be read (section 2)
MASVS-PLATFORM	Platform Interaction	not assessable	the app was not built or run
MASVS-CODE	Code Quality	not assessable	Swift has no code-flaw module yet; Podfile not read (section 2)
MASVS-RESILIENCE	Resilience Against Reverse Engineering and Tampering	not assessable	needs a manual test of the built app
MASVS-PRIVACY	Privacy	not assessable	the app was not built or run

Source: OWASP Mobile Application Security Verification Standard v2, <https://mas.owasp.org/MASVS/>.

7. Access-control results

Test	Accounts used	Request	Result	Evidence	Finding
Account B reads account A's profile by changing the id	A, B	GET /api/profiles/{id}	not met	response held account A's profile (kept in Amadis's records)	F04
Account B changes its own role field in a profile update	B	PATCH /api/profiles/{id}	met	the role field was ignored	none
A normal account calls an admin route	B	GET /api/admin/users	met	answered 403	none
Sign-in, session expiry and password reset	A, B	POST /api/session, POST /api/password-reset	met	sessions ended after 30 minutes idle; reset links expired after one use	none

8. UK GDPR and data-security checklist

Answers are **self-declared** by the customer (synthetic) on 2026-10-13; Amadis has not verified them. This section is not legal advice.

Item	Question	What good looks like	Self-declared answer	Evidence	Source
G01	Does the app record health information about people, such as their allergies, reactions or medication?	You know which fields hold health data and treat them as special category data (allergy details are health data).	yes	internal document g01-record (synthetic)	UK GDPR Article 9(1), https://www.legislation.gov.uk/eur/2016/679/article/9
G02	Have you written down the Article 6 lawful basis for each purpose you use personal data for, and has your data protection adviser confirmed it? (to confirm with your adviser)	Each purpose is written down with its lawful basis and the adviser's confirmation.	unsure	none	UK GDPR Article 6(1), https://www.legislation.gov.uk/eur/2016/679/article/6 ; ICO, lawful basis for processing, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/
G03	Have you written down the Article 9(2) condition you rely on for the health data (for example explicit consent, Article 9(2)(a)), and has your adviser confirmed it applies? (to confirm with your adviser)	The condition is written down for each use of health data, with the adviser's confirmation and any extra condition the Data Protection Act 2018 Schedule 1 requires.	unsure	none	UK GDPR Article 9(2), https://www.legislation.gov.uk/eur/2016/679/article/9 ; Data Protection Act 2018 Schedule 1, https://www.legislation.gov.uk/ukpga/2018/12/schedule/1
G04	If you rely on explicit consent, is it asked for in a separate, clearly worded statement the person actively agrees to, recorded with the date and wording shown, and as easy to withdraw as to give, in wording your adviser has confirmed? (to confirm with your adviser)	A consent record per person (what they saw, when, how) and a working withdraw option in the app.	yes	internal document g04-record (synthetic)	UK GDPR Articles 7 and 9(2)(a), https://www.legislation.gov.uk/eur/2016/679/article/7 ; ICO, consent, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/

Item	Question	What good looks like	Self-declared answer	Evidence	Source
G05	Have you completed a DPIA for processing health data in the app, before the processing started?	A dated DPIA that describes the processing, its risks to people and the measures taken, reviewed when the app changes.	no	none	UK GDPR Article 35, https://www.legislation.gov.uk/eur/2016/679/article/35 ; ICO, DPIAs, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
G06	Has your organisation paid the data protection fee to the ICO, and is the registration current?	A current entry on the ICO's register of fee payers, with its reference number and renewal date.	yes	internal document g06-record (synthetic)	The Data Protection (Charges and Information) Regulations 2018, https://www.legislation.gov.uk/uksi/2018/480 ; ICO, data protection fee, https://ico.org.uk/for-organisations/data-protection-fee/
G07	Do you have a list of every supplier that handles personal data for you (hosting, database, email, analytics, crash reporting, support tools), and does each have a signed data processing agreement?	A list of every processor, what data each sees, and a signed contract with the Article 28(3) terms for each.	unsure	none	UK GDPR Article 28, https://www.legislation.gov.uk/eur/2016/679/article/28
G08	Is each transfer of personal data outside the UK (stored or accessed there) covered by a written transfer mechanism (answer yes if no personal data is stored or accessed outside the UK)?	Each transfer listed with its mechanism (UK adequacy regulations, the IDTA or the UK Addendum) and a transfer risk assessment where needed.	yes	internal document g08-record (synthetic)	UK GDPR Articles 44 to 49, https://www.legislation.gov.uk/eur/2016/679/article/44 ; ICO, international transfers, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/
G09	Have you set a written retention period for each kind of personal data, including backups and logs, and a step that deletes it once that period is up?	A written retention period per kind of data, and a deletion step (automatic where possible) that is checked.	no	none	UK GDPR Article 5(1)(e), https://www.legislation.gov.uk/eur/2016/679/article/5

Item	Question	What good looks like	Self-declared answer	Evidence	Source
G10	Is health data encrypted in transit (TLS on every connection) and at rest (database, file storage, backups and device storage in the app)?	TLS on every endpoint, encryption at rest switched on for each store, keys held apart from the data, and the app keeps tokens in the platform's protected storage.	yes	internal document g10-record (synthetic)	UK GDPR Article 32(1)(a), https://www.legislation.gov.uk/eur/2016/679/article/32
G11	Is access to users' health data, in your organisation and at your suppliers, limited to the roles that need it, does every account use multi-factor sign-in, and have those access rights been reviewed in the last year?	Access limited to named roles that need it, multi-factor sign-in for staff and admin accounts, and a dated access review at least yearly.	yes	internal document g11-record (synthetic)	UK GDPR Articles 5(1)(f) and 32, https://www.legislation.gov.uk/eur/2016/679/article/32
G12	Do you have a written process to assess a personal data breach, report it to the ICO within 72 hours where required, tell affected people where the risk is high, and log every breach?	A short written process with named roles, the ICO reporting route, a template message for users, and a breach log (kept even for breaches not reported).	no	none	UK GDPR Articles 33 and 34, https://www.legislation.gov.uk/eur/2016/679/article/33 ; ICO, personal data breaches, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-data-breaches/
G13	Do you keep a record of processing activities, listing the personal data you hold, its purposes, the recipients and the retention period?	A record with the Article 30 details, kept up to date when the app changes.	yes	internal document g13-record (synthetic)	UK GDPR Article 30, https://www.legislation.gov.uk/eur/2016/679/article/30
G14	Does the app show a privacy notice, before data is collected, that explains the health data, its purposes, the lawful basis and condition, processors, retention and people's rights?	A notice reachable from the sign-up screen and the app's settings, matching what the app really does.	yes	internal document g14-record (synthetic)	UK GDPR Articles 12 and 13, https://www.legislation.gov.uk/eur/2016/679/article/13
G15	Can you find, export, correct and delete one user's data on request, and answer within one month?	A tested way to handle access, correction and deletion requests, including data held by processors and in backups.	unsure	none	UK GDPR Articles 12 and 15 to 22, https://www.legislation.gov.uk/eur/2016/679/article/12

Item	Question	What good looks like	Self-declared answer	Evidence	Source
G16	Has your adviser confirmed whether you must appoint a data protection officer, given that processing health data at scale may be a core activity? (to confirm with your adviser)	A recorded decision, with the adviser's reasoning, and the officer's contact details published if one is needed.	unsure	none	UK GDPR Article 37(1)(c), https://www.legislation.gov.uk/eur/2016/679/article/37
G17 a	Has your adviser said whether UK GDPR Article 8 and the ICO's Age Appropriate Design Code apply to the app, counting both children using it and parents recording a child's allergies in it? (to confirm with your adviser)	A recorded decision, with the adviser's reasoning, covering both children using the app and parents recording a child's data.	yes	internal document g17a-record (synthetic)	UK GDPR Article 8, https://www.legislation.gov.uk/eur/2016/679/article/8 ; ICO, Age Appropriate Design Code, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/
G17 b	If your adviser says the code applies, has its assessment been done and does the DPIA cover children's data (answer yes if your adviser has recorded that it does not apply)? (to confirm with your adviser)	The code's standards assessed and applied, and the DPIA covering children's data, or the adviser's record that the code does not apply.	yes	internal document g17b-record (synthetic)	UK GDPR Article 8, https://www.legislation.gov.uk/eur/2016/679/article/8 ; ICO, Age Appropriate Design Code, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/
G18	Are backups taken, kept encrypted, and restored in a test at least once a year, and are your security measures tested regularly?	Dated restore tests and a regular test of the measures (this readiness report can be one part of that).	not answered	none	UK GDPR Article 32(1)(c) and (d), https://www.legislation.gov.uk/eur/2016/679/article/32

9. Fixes and retest status

Finding	Fix	Fix reported by	Retested on	Retest result	Status
F04	Check on the server that the profile requested belongs to the signed-in account before returning it.	the customer	none	not yet retested	open: fix reported by the customer, not yet retested
F01	Upgrade log4j-core to 2.17.1 or later.	Veydr fix pull request merged by the customer	2026-10-15	fix observed	verified fixed: retest on 2026-10-15 (kit rerun at the fix commit no longer reports it; the lockfile holds log4j-core 2.17.1)
F02	Revoke the key with its issuer, issue a new one held in the CI secret store, and remove the value from the file.	none	none	not yet retested	open
F03	Pass the search term as a query parameter instead of formatting it into the SQL.	none	none	not yet retested	open
F05	Add a USER line with an unprivileged account.	none	none	not yet retested	accepted risk until 2027-04-15 (owner: the customer's engineering lead): the image runs only on an internal build host

10. Limits of this assessment

What automated scanning cannot find:

- Flaws in business logic and multi-step flows (paying less than the price, skipping a step, abusing a refund).
- Authorisation between users and roles, beyond the manual tests listed in section 7.
- Anything outside the agreed scope, and anything the depth table marks not assessed or partial.
- Weaknesses with no published advisory or rule yet, and code-flaw patterns beyond the rules each engine runs.
- How the running systems are configured and operated: hosting, cloud accounts, staff access, backups, monitoring.
- People and process: phishing, lost devices, how a breach would really be handled.

The iOS app was not built, so its compiled binary was not examined. Remote Terraform modules were not fetched.

When a manual penetration test, or a CREST-accredited one, is worth buying:

- Before launch, or before a large change, of a service holding special category data (such as health or allergy data) or payments.
- When a customer, insurer, regulator or contract asks for a penetration test report by a named, CREST-accredited tester.
- When this report shows areas not assessed, or access-control and business-logic risks that only a tester working through the live system can explore.
- After a serious incident, to look for what an attacker could still do.

11. What this report is and is not

This report records observations at 2026-10-15 within the agreed scope set out in section 2. Systems change: it describes what was observed then, not how they are now.

It is a readiness report. It is not an accreditation or a certification, and it does not say that any system is secure or compliant with any law or standard.

It is not a guarantee: where nothing was observed, that means nothing was found at the depth shown in section 2, not that nothing is there.

It is not legal advice. The UK GDPR checklist records the customer's own self-declared answers; lawful basis and other legal duties are for the customer's own adviser to confirm.

It is not a penetration test, except for the manual tests listed in section 7, and only for those tests.

12. Sources and attribution

Contains data from the GitHub Advisory Database, licensed under CC BY 4.0 (<https://creativecommons.org/licenses/by/4.0/>).

Uses the CISA Known Exploited Vulnerabilities catalog.

13. Review and approval

Reviewed by Amadis on 2026-10-16.

Draft: not approved for release

Inputs SHA-256: 7acd9e89b0bda016647a6ddb40e1b09990dac9ea6a7cd8fccfd17f2e8406772a