

Secure code review evidence (SAMPLE)

Fernbrook Systems

Period	Q2 2025, 1 April 2025 to 30 June 2025
Produced	31 August 2026 by the sample report
Export reference	sample-py-q2
Named detail	Open: named per-person detail is included for the roles entitled to it.
Plan	Team

NOT EVIDENCE. This is a sample document produced from invented data so that a buyer can read one before paying. Every name, score and date in it was made up, and it is not recorded against any organisation.

What this is

Each exercise is a staged merge request against a working codebase: a browser, its commits and the diff a reviewer would actually open, written to look like ordinary feature work.

Findings are planted in that diff by hand, each with a CWE id number, the exact lines, and a written explanation.

Grading runs on the server against a prepared answer that is never sent to the browser. The reviewer submits one finding at a time, the lines they flagged and the weakness they think it is, and each is marked as it is submitted. The score is worked out on the server, so a submission cannot be forged.

A weakness is found when the reviewer's selection overlaps the lines it was planted on and the weakness they name is the answer's own, an alternative the answer accepts or one in the same family. Each weakness is worth 10 points, so a challenge with three weaknesses planted in it is out of 30.

Every wrong try costs 1 point: a try on lines with nothing wrong in them, or on the right lines naming the wrong weakness. The score is the points for the weaknesses found less what the wrong tries cost, and never below nought. A weakness never found scores nothing. In an assessment, a weakness closes after 3 tries on its lines that name the wrong weakness, and scores nothing from then on.

A challenge is passed at 80 per cent of its full marks, rounded up to whole points: 24 of 30 with three weaknesses. The score recorded for it is the percentage of its full marks it reached.

Assessment work is kept separate from training in the database. Everything in this report comes from assessments an administrator set. Practice a seat holder does on their own account never reaches it.

The grading policy is published in full and does not change per customer. It is at justappsec.com/docs/how-a-review-works.

What this record does not establish

What this record establishes: that the account named against each result was signed in, submitted those findings in the window shown, and was marked on our server against a prepared answer the browser never receives. The exercise is never published, so it cannot be practised beforehand. Hints are off unless an administrator switched them on, which is stated on each row. No assessment shows a walkthrough or a video, whatever its switches say.

What it does not establish: who was at the keyboard. The sitting is not invigilated. Nothing here shows whether the named person worked alone, whether someone was helping, or whether the diff was pasted into another tool. We only see what the product offered and what was submitted to it.

Read a result as evidence of work done under this account, in this window, under the stated settings. Where a role needs more than that, run the sitting under your own supervision and record that alongside this document.

Who is in this document: everybody who was assigned an assessment in the period and held a seat when they sat it. That is not necessarily everybody who writes code here. This record cannot say how many engineers the organisation has or how the people assigned were chosen. An auditor who needs that should ask for it.

Summary

Assessments	People assessed	Assignments	Submitted
1	10	13	10
In progress	Not started	Not completed in window	Reviews recorded
0	0	3	40
Team catch rate	Team median score		
51%	Not published		

Withheld: 10 people have graded work in this period, counting anyone part way through an assessment. A median needs 20.

An aggregate is only published when at least 10 people are in it, and a median when at least 20 are, because with fewer than that you could work out who is who.

Coverage by CWE category

Dimension	People	Findings	Caught	Missed	Catch rate
Access control	10	40	21	19	53%
Cryptography	10	30	15	15	50%
Injection	10	30	15	15	50%

Coverage by language

Dimension	People	Findings	Caught	Missed	Catch rate
TypeScript	10	40	21	19	53%
Python	10	30	15	15	50%
Ruby	10	30	15	15	50%

Track records

Seat holder	Seat	Submitted	Caught	Missed	Catch rate	Find the fix	Median score	Status	Last submission
Rafferty Quinn	No	4	3	7	30%	Not asked	31.5	Well below	18 June 2025
Callum Peverell	Yes	4	3	7	30%	Not asked	30	Well below	16 June 2025

Seat holder	Seat	Submitted	Caught	Missed	Catch rate	Find the fix	Median score	Status	Last submission
Oisin Farrelly	Yes	4	5	5	50%	Not asked	45	Needs work	14 June 2025
Tomasz Wierzbicki	No	4	5	5	50%	Not asked	44.5	Well below	13 June 2025
Mirela Antonescu	Yes	4	4	6	40%	Not asked	31.5	Well below	12 June 2025
Idris Kalunga	Yes	4	6	4	60%	Not asked	56.5	Needs work	11 June 2025
Aiko Matsubara	Yes	4	6	4	60%	Not asked	58	Needs work	10 June 2025
Bethan Craddock	Yes	4	7	3	70%	Not asked	64.5	Needs work	9 June 2025
Nkechi Adeyemi	Yes	4	5	5	50%	Not asked	44.5	Well below	7 June 2025
Saoirse Lenehan	Yes	4	7	3	70%	Not asked	63	Needs work	5 June 2025

Status is the product's own grade, on the same pass mark it uses for every submission: a median score of 80 or more is a pass. Below the mark reads Needs work, and Well below where the score is also under the median of the people listed here. That median is for this table only; a published team figure needs to be shorter before the report states one. Somebody who has not finished their assessment is not graded yet: they are In progress, or Not finished once its window has closed, with their figures so far.

No retake was granted or sat in this period. Everyone here above is a first sitting.

The record for each person, broken down by CTFE category and by language, is in the CSV exported alongside this document, one row per person per category and per language.

Results

Each challenge submitted in this period, with the score and grade it was given. These are the results the figures above are taken from.

Seat holder	Assessment	Challenge	Score	Grade	Caught	Submitted
Aiko Matsubara	The first round access control and cryptography review, 2025	Reports readable across tenants	95	Passed	2 of 2	6 June 2025
Aiko Matsubara	The first round access control and cryptography review, 2025	An account switch that keeps the old session	50	Needs work	1 of 2	7 June 2025
Aiko Matsubara	The first round access control and cryptography review, 2025	A search filter assembled by hand	66	Needs work	2 of 3	9 June 2025
Aiko Matsubara	The first round access control and cryptography review, 2025	Balances signed with a shared secret	33	Needs work	1 of 3	10 June 2025

Seat holder	Assessment	Challenge	Score	Grade	Caught	Submitted
Bethan Craddock	The first round access control and cryptography review, 2025	Reports readable across tenants	90	Passed	2 of 2	6 June 2025
Bethan Craddock	The first round access control and cryptography review, 2025	An account switch that keeps the old session	50	Needs work	1 of 2	7 June 2025
Bethan Craddock	The first round access control and cryptography review, 2025	A search filter assembled by hand	63	Needs work	2 of 3	8 June 2025
Bethan Craddock	The first round access control and cryptography review, 2025	Balances signed with a shared secret	66	Needs work	2 of 3	9 June 2025
Callum Peverell	The first round access control and cryptography review, 2025	Reports readable across tenants	0	Needs work	0 of 2	12 June 2025
Callum Peverell	The first round access control and cryptography review, 2025	An account switch that keeps the old session	5	Needs work	1 of 2	14 June 2025
Callum Peverell	The first round access control and cryptography review, 2025	A search filter assembled by hand	30	Needs work	1 of 3	15 June 2025
Callum Peverell	The first round access control and cryptography review, 2025	Balances signed with a shared secret	30	Needs work	1 of 3	16 June 2025
Idris Kalunga	The first round access control and cryptography review, 2025	Reports readable across tenants	45	Needs work	1 of 2	7 June 2025
Idris Kalunga	The first round access control and cryptography review, 2025	An account switch that keeps the old session	50	Needs work	1 of 2	8 June 2025
Idris Kalunga	The first round access control and cryptography review, 2025	A search filter assembled by hand	66	Needs work	2 of 3	10 June 2025
Idris Kalunga	The first round access control and cryptography review, 2025	Balances signed with a shared secret	63	Needs work	2 of 3	11 June 2025
Mirela Antonescu	The first round access control and cryptography review, 2025	Reports readable across tenants	95	Passed	2 of 2	8 June 2025

Seat holder	Assessment	Challenge	Score	Grade	Caught	Submitted
Mirela Antonescu	The first round access control and cryptography review, 2025	An account switch that keeps the old session	0	Needs work	0 of 2	9 June 2025
Mirela Antonescu	The first round access control and cryptography review, 2025	A search filter assembled by hand	30	Needs work	1 of 3	11 June 2025
Mirela Antonescu	The first round access control and cryptography review, 2025	Balances signed with a shared secret	33	Needs work	1 of 3	12 June 2025
Nkechi Adeyemi	The first round access control and cryptography review, 2025	Reports readable across tenants	100	Passed	2 of 2	2 June 2025
Nkechi Adeyemi	The first round access control and cryptography review, 2025	An account switch that keeps the old session	0	Needs work	0 of 2	4 June 2025
Nkechi Adeyemi	The first round access control and cryptography review, 2025	A search filter assembled by hand	30	Needs work	2 of 3	5 June 2025
Nkechi Adeyemi	The first round access control and cryptography review, 2025	Balances signed with a shared secret	33	Needs work	1 of 3	7 June 2025
Oisin Farrelly	The first round access control and cryptography review, 2025	Reports readable across tenants	50	Needs work	1 of 2	9 June 2025
Oisin Farrelly	The first round access control and cryptography review, 2025	An account switch that keeps the old session	40	Needs work	1 of 2	11 June 2025
Oisin Farrelly	The first round access control and cryptography review, 2025	A search filter assembled by hand	33	Needs work	1 of 3	12 June 2025
Oisin Farrelly	The first round access control and cryptography review, 2025	Balances signed with a shared secret	66	Needs work	2 of 3	14 June 2025
Rafferty Quinn	The first round access control and cryptography review, 2025	Reports readable across tenants	0	Needs work	0 of 2	15 June 2025
Rafferty Quinn	The first round access control and cryptography review, 2025	An account switch that keeps the old session	40	Needs work	1 of 2	16 June 2025

Seat holder	Assessment	Challenge	Score	Grade	Caught	Submitted
Rafferty Quinn	The first round access control and cryptography review, 2025	A search filter assembled by hand	30	Needs work	1 of 3	17 June 2025
Rafferty Quinn	The first round access control and cryptography review, 2025	Balances signed with a shared secret	33	Needs work	1 of 3	18 June 2025
Saoirse Lenehan	The first round access control and cryptography review, 2025	Reports readable across tenants	50	Needs work	1 of 2	1 June 2025
Saoirse Lenehan	The first round access control and cryptography review, 2025	An account switch that keeps the old session	90	Passed	2 of 2	2 June 2025
Saoirse Lenehan	The first round access control and cryptography review, 2025	A search filter assembled by hand	60	Needs work	2 of 3	3 June 2025
Saoirse Lenehan	The first round access control and cryptography review, 2025	Balances signed with a shared secret	66	Needs work	2 of 3	5 June 2025
Tomasz Wierzbicki	The first round access control and cryptography review, 2025	Reports readable across tenants	100	Passed	2 of 2	9 June 2025
Tomasz Wierzbicki	The first round access control and cryptography review, 2025	An account switch that keeps the old session	0	Needs work	0 of 2	10 June 2025
Tomasz Wierzbicki	The first round access control and cryptography review, 2025	A search filter assembled by hand	26	Needs work	1 of 3	12 June 2025
Tomasz Wierzbicki	The first round access control and cryptography review, 2025	Balances signed with a shared secret	63	Needs work	2 of 3	13 June 2025

Assessment records

Assessment	Set on	Switches	Assigned	Submitted	Window
The first round access control and cryptography review, 2025	20 May 2025	On: hints, the number of findings	13	10	Closed 20 June 2025

The switches are stated because they change what the score means: an assessment sat with hints available is not the same exercise as one sat without. They are taken from each sitting's own record, written when the sitting was opened, or from the assessment as set where a sitting predates that record. The number of findings is taken from the assessment as set, which

cannot change once anybody has started it. A walkthrough or video switch is recorded as it was set. No assessment shows a walkthrough or a video, so the seat holder saw neither.

Assignments still outstanding

Assessment	Name	Email	State	Assigned	Seat held
The first round access control and cryptography review, 2025	Domhnall Kearney	domhnall.kearney@fernbrook.example	Not completed in window	1 June 2025	Yes
The first round access control and cryptography review, 2025	Priti Raval	priti.raval@fernbrook.example	Not completed in window	1 June 2025	Yes
The first round access control and cryptography review, 2025	Jun-ho Baek	jun-ho.baek@fernbrook.example	Not completed in window	1 June 2025	Yes

Seat integrity

Seats purchased today	Assigned now	Seats held at least once in period	Assignments and releases
50	48	48	2 and 1

A seat is assigned to a named individual and can move to someone else once a calendar month. 50 seats are paid for as things stand today, and 48 seats were held one during this period, counted from the seat assignments and releases in the audit log. A number well above the number purchased means seats were passed between people, which changes what the results above cover.

Where this fits

This is one layer of an evidence pack, not the whole of one. It shows that named people were measured against planted weaknesses, on dated exercises, under stated settings, and how they did. It does not cover your policies, your pipeline controls, your penetration testing or your vulnerability management, and it is not a certification.

PCI DSS v4.0.1, 6.2.2 and 6.2.3.1

Software development personnel are to be trained at least annually in secure design and coding for the languages and tools they use, and bespoke code is to be reviewed before release by someone other than its author, knowledgeable in secure coding. The graded records here double as the training record 6.2.2 asks for, and evidence that reviewers can do what 6.2.3.1 requires of them.

DORA (EU) 2022/2554, Article 13(6), and the ICT risk management RTS, Article 16(3)

Financial entities are to run ICT security awareness programmes and digital operational resilience training for staff, and to apply secure coding practices with a proportionate review of the code they produce. This report evidences the second half of that: that the people writing the code were measured against real weaknesses.

ISO/IEC 27001:2022, clause 7.2 and Annex A 8.28

Clause 7.2 asks for competence to be determined, achieved and evidenced, and A.8.28 asks for secure coding principles to be applied. A dated, per-person record of what a seat holder caught and missed is the kind of evidence of competence clause 7.2 asks for.

EU AI Act (EU) 2024/1689, Article 4

Providers and deployers are to take measures to ensure a sufficient level of AI literacy among staff dealing with AI systems. Where the exercises cover AI-assisted code and AI-specific weaknesses, this record speaks to that obligation.

Integrity of this file

NOT EVIDENCE. This is a sample document produced from invented data so that a buyer can read one before paying. Every name, score and date in it was made up, and it is not recorded against any organisation.

The underlying rows are exported alongside this document as a CSV, so the figures above can be recomputed.

SAMPLE