Zarco

Sample report, illustrative

PENETRATION TEST REPORT

Security posture assessment with application and API penetration test

Example Ltd

Testing window	1 to 12 September 2026	Report issued	19 September 2026
Retest	30 September 2026	Version	v1.1, updated after retest

Example Ltd is fictional: a 60-person software company with a customer portal, a Microsoft 365 tenant and a small AWS footprint. This sample is illustrative and contains no client data.

CONTENTS

1 Executive summary
2 Posture at a glance
3 Findings at a glance
4 Scope and approach
5 Attack path
6 Findings in detail
7 Retest record
A Coverage and limitations
B Letter of attestation

1 Section

Executive summary

THE QUESTION

Where is the business exposed, and is the customer portal secure?

Overall posture AT RISK → GOOD, WITH TWO ITEMS IN PROGRESS

Example Ltd asked a simple question: where is the business exposed, and is the customer portal secure? Over two weeks, our AI agents examined everything Example Ltd shows the internet, its Microsoft 365 tenant and its customer portal, and our testers confirmed twelve findings.

Four were high risk. An old admin portal was still online with outdated software. Three administrator accounts were not protected by multi-factor authentication. In the customer portal, two weaknesses combined to let one customer download another customer's exports, and sessions stayed active after a password change.

All four were fixed and verified on retest by 30 September. Two lower-risk items are in progress, and one is an accepted risk.

WHAT'S WORKING

- Production and staging are well separated.
- The main website and email service are patched promptly.
- Clear ownership: urgent findings were fixed within two days of being raised.

PRIORITIES NOW

- Finish the invitation fix on the bulk-invite path (ZP-06).
- Move email protection from quarantine to reject (ZP-10).
- Keep an inventory of internet-facing systems and review it quarterly.

> RECOMMENDED NEXT STEP
>
> The customer portal ships weekly. Regular retesting would re-check these fixes and test new releases as they ship.

2 Section

Posture at a glance

How exposed each area was when testing started, and where it stands after the retest.

AREA	BEFORE	AFTER RETEST	WHAT CHANGED
Internet-facing systems	AT RISK	GOOD	The forgotten admin portal is offline. Older encryption on one site is an accepted risk.
Customer portal and API	AT RISK	NEEDS ATTENTION	All high-severity issues fixed. The bulk-invite path still accepts a role from the browser.
Microsoft 365	AT RISK	GOOD	Multi-factor authentication now covers every administrator.
Cloud storage	NEEDS ATTENTION	GOOD	Public listing disabled and internal files moved.
Code and secrets	NEEDS ATTENTION	GOOD	The leaked key is revoked and secret scanning is on.
Email and domain	NEEDS ATTENTION	NEEDS ATTENTION	Spoofed email is now quarantined; blocking is planned.

Findings at a glance

0	4	4	3	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

ID	FINDING	AREA	SEVERITY	AFTER RETEST
ZP-01	Forgotten admin portal online with outdated software	Internet-facing systems	HIGH	Fixed
ZP-02	Three administrator accounts without multi-factor authentication	Microsoft 365	HIGH	Fixed
ZP-03	Cross-workspace access to exports	Customer portal	HIGH	Fixed
ZP-04	Sessions survive a password change	Customer portal	HIGH	Fixed
ZP-05	Sequential export identifiers	Customer portal	MEDIUM	Fixed
ZP-06	Invitation role accepted from the browser	Customer portal	MEDIUM	Partially fixed
ZP-07	Storage container lists file names publicly	Cloud storage	MEDIUM	Fixed
ZP-08	Email-service key in a public repository still valid	Code and secrets	MEDIUM	Fixed
ZP-09	Detailed error messages	Customer portal	LOW	Open
ZP-10	Email domain not fully protected against spoofing	Email and domain	LOW	Partially fixed
ZP-11	Password reset links last seven days	Customer portal	LOW	Fixed
ZP-12	Older encryption protocols accepted	Internet-facing systems	INFO	Accepted risk

Scope and approach

IN SCOPE

- example.com, its subdomains and the services they expose
- The customer portal (app.example.com) and its API (api.example.com): staging environment, three roles and two test workspaces
- The Microsoft 365 tenant, as a read-only configuration review
- Public code repositories and sources linked to example.com
- Storage buckets in the AWS account that serve the website

OUT OF SCOPE

- The internal office network
- Staff phishing and physical security
- Denial-of-service testing
- The third-party payment provider

RULES OF ENGAGEMENT

- Written authorisation from Example Ltd for every system in scope
- Testing on weekdays, 08:00 to 18:00 UK time
- Portal traffic limited to 4 requests per second
- Anything that could change or delete data held for approval
- A named stop contact on both sides

HOW WE TESTED

AI agents mapped and tested the scope in parallel, with every action checked against the agreed scope before it ran. Experienced testers steered the work, confirmed every finding and rated its severity for Example Ltd's business. References: the OWASP Web Security Testing Guide and ASVS for the portal, and the CIS Microsoft 365 Foundations Benchmark for the tenant.

Attack path

Individual findings matter less than what they lead to. This path shows how two findings combined.

AP-01

A Viewer in workspace A reads workspace B's documents

START

Viewer role, workspace A

Agreed test identity

ZP-05, MEDIUM

Export IDs are sequential

Valid IDs for other workspaces are predictable

ZP-03, HIGH

No ownership check on export

The API trusts the ID it is given

OBJECTIVE

Workspace B documents

Metadata and signed download links

Two individually moderate weaknesses combine into one high-impact path. Fixing ZP-03 closes it; fixing ZP-05 alone doesn't.

Findings in detail

ZP-01

HIGH

Forgotten admin portal online with outdated software

Area	Internet-facing systems
Affected	admin-old.example.com
Weakness	CWE-1104: Use of unmaintained third-party components

WHAT WE FOUND

An administration portal replaced in 2024 is still reachable from the internet. It runs a version of its software with a published high-severity vulnerability.

WHY IT MATTERS

The old portal still holds customer contact records. An outsider who used the vulnerability could reach them, and nobody was watching the system.

ROOT CAUSE

Decommissioning removed the portal from use but not from the internet, and there is no owned inventory of internet-facing systems.

HOW TO FIX IT

Take the portal offline and remove its DNS record. Keep an inventory of internet-facing systems and review it every quarter.

ev_1a04 certificate record | ev_1a05 version check | ev_1a06 screenshots

Retest: Fixed. Portal offline; hostname no longer resolves.

ZP-02

HIGH

Three administrator accounts without multi-factor authentication

Area	Microsoft 365
Affected	Conditional access policy, global administrators
Weakness	CWE-308: Use of single-factor authentication

WHAT WE FOUND

Three of five global administrator accounts were excluded from the policy that requires multi-factor authentication.

WHY IT MATTERS

A stolen or guessed password for any of these accounts would give full control of email, files and every user account.

ROOT CAUSE

The accounts were excluded during a 2025 migration and never added back.

HOW TO FIX IT

Require phishing-resistant multi-factor authentication for every administrator, keep two monitored emergency accounts, and review policy exclusions monthly.

`ev_2b11 policy export` `ev_2b12 sign-in log extract`

Retest: Fixed. All administrators now covered; exclusions reviewed.

ZP-03

HIGH

Cross-workspace access to exports

Area	Customer portal
Affected	GET /api/v2/exports/{exportId}
Weakness	CWE-639: Authorization bypass through user-controlled key
CVSS 4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

WHAT WE FOUND

Signed in as a Viewer in one customer's workspace, we could download exports belonging to another customer.

WHY IT MATTERS

Any customer could read other customers' documents, which is likely to be a reportable personal data breach.

ROOT CAUSE

Workspace ownership is enforced in the interface but not in the export service.

HOW TO FIX IT

Scope every export lookup to the caller's workspace in the service layer, and add a regression test that fails if it ever isn't.

EVIDENCE: REQUEST AND RESPONSE

```
GET /api/v2/exports/10482 HTTP/1.1
Host: api.example.com
Authorization: Bearer eyJhbGciOi... # viewer, workspace A

HTTP/1.1 200 OK
content-type: application/json

{ "id": 10482, "workspace": "ws_b", "name": "Q3 contracts.zip",
  "download_url": "https://files.example.com/...[redacted]" }
```

ev_0f3a request and response | ev_0f3b screenshot | trace e81f

Retest: Fixed. Cross-workspace export IDs now return 404.

Other findings

In a full engagement report, each of these has the same write-up as above.

ID	FINDING	SEVERITY	FIX
ZP-04	**Sessions survive a password change** Changing a password did not sign out the account's other sessions.	HIGH	End every other session when a password changes, and offer users a "sign out everywhere" option.
ZP-05	**Sequential export identifiers** Export identifiers are sequential, so valid identifiers for other workspaces are easy to predict.	MEDIUM	Use random, unguessable identifiers for exports and other shared objects.
ZP-06	**Invitation role accepted from the browser** When inviting a colleague, the role sent from the browser was trusted, so an Editor could invite an Admin.	MEDIUM	Check on the server that the inviter can grant the requested role, on every invitation path.
ZP-07	**Storage container lists file names publicly** A storage bucket for website images let anyone list its contents, including two internal price lists.	MEDIUM	Block public listing, move internal files to private storage, and serve images through the website.
ZP-08	**Email-service key in a public repository still valid** A key for the email-sending service was committed to a public repository in 2023 and still worked.	MEDIUM	Revoke and replace the key, and turn on secret scanning for every repository.
ZP-09	**Detailed error messages** Some errors return internal details, including software versions.	LOW	Return generic errors to users and log the detail internally.
ZP-10	**Email domain not fully protected against spoofing** The domain's email policy only monitors spoofed messages rather than blocking them.	LOW	Move the policy to quarantine, then reject, once legitimate senders are confirmed.
ZP-11	**Password reset links last seven days** Reset links remain valid for seven days and can be used more than once.	LOW	Expire reset links after an hour and after first use.
ZP-12	**Older encryption protocols accepted** The marketing site still accepts TLS 1.0 and 1.1 alongside modern versions.	INFO	Disable TLS 1.0 and 1.1 at the hosting provider.

7 Section

Retest record

Every finding re-tested against the deployed fix on 30 September 2026, with the original evidence as the baseline.

ID	FINDING	RESULT	NOTE
ZP-01	Forgotten admin portal online with outdated software	Fixed	Portal offline; hostname no longer resolves.
ZP-02	Three administrator accounts without multi-factor authentication	Fixed	All administrators now covered; exclusions reviewed.
ZP-03	Cross-workspace access to exports	Fixed	Cross-workspace export IDs now return 404.
ZP-04	Sessions survive a password change	Fixed	Original scenario no longer reproduces.
ZP-05	Sequential export identifiers	Fixed	Original scenario no longer reproduces.
ZP-06	Invitation role accepted from the browser	Partially fixed	Single invites fixed; the bulk-invite path still accepts a role.
ZP-07	Storage container lists file names publicly	Fixed	Original scenario no longer reproduces.
ZP-08	Email-service key in a public repository still valid	Fixed	Original scenario no longer reproduces.
ZP-09	Detailed error messages	Open	Scheduled by Example Ltd for the October release.
ZP-10	Email domain not fully protected against spoofing	Partially fixed	Moved to quarantine; reject planned.
ZP-11	Password reset links last seven days	Fixed	Original scenario no longer reproduces.
ZP-12	Older encryption protocols accepted	Accepted risk	Accepted until the site moves host in December.

A Appendix

Coverage and limitations

REF	AREA	STATUS
EXT	Internet-facing discovery and testing	Tested
M365	Microsoft 365 configuration Read-only review	Tested
WSTG-ATHN	Portal authentication	Tested
WSTG-ATHZ	Portal authorisation	Tested
WSTG-SESS	Portal session management	Tested
WSTG-INPV	Portal input validation	Tested
WSTG-BUSL	Portal business logic	Tested
WSTG-APIT	API testing	Tested
AWS	Cloud storage serving the website Storage only; no full cloud test	Partial
–	Internal network and phishing	Out of scope
–	Denial of service Excluded in rules of engagement	Out of scope

This report describes what was tested during the testing window, against the agreed scope. It does not certify that no other vulnerabilities exist, and a clean result in an area is evidence of what was examined, not a guarantee.

Findings separate what was observed, what was suspected but not confirmed, and what was not tested and why.

B Appendix

Letter of attestation

To whom it may concern,

Zarco carried out an authorised security posture assessment with application and API penetration test for Example Ltd, under written rules of engagement agreed with Example Ltd.

Scope	example.com, app.example.com, api.example.com and the Microsoft 365 tenant
Testing window	1 to 12 September 2026
Method	Agent-assisted testing with tester validation, against OWASP WSTG and ASVS and the CIS Microsoft 365 benchmark
Results	0 critical, 4 high, 4 medium, 3 low, 1 info
Retest	All four high-severity findings fixed and verified on 30 September 2026

This is a point-in-time assessment of the agreed scope. It does not certify that the systems are free of vulnerabilities.

Lead tester, Zarco

1 October 2026