FICTIONAL SAMPLE REPORT

# Sample penetration testing report

Illustrative data only. Not actual client findings.

**Report author** · BTNXIO SECURITY · btnxio@gmail.com · btnxiosecurity.com

## Document control

Public illustrative edition · Version 2.0 · Prepared by BTNXIO SECURITY. Target identifiers are reserved examples and scenarios are synthetic.

**Report author** · BTNXIO SECURITY · btnxio@gmail.com · btnxiosecurity.com

# Contents


| | |
|---|---|
| Document control | 2 |
| Executive overview | 3 |
| Scope | 4 |
| Attack surface | 5 |
| DEMO-01 · Cross-account record visibility | 6 |
| DEMO-02 · Missing export permission boundary | 7 |
| DEMO-03 · Inconsistent recovery responses | 8 |
| DEMO-04 · Unsafe profile rendering boundary | 9 |
| DEMO-05 · Incomplete session revocation | 10 |
| DEMO-06 · Insufficient request limits | 11 |
| DEMO-07 · Missing browser security policy | 12 |
| DEMO-08 · Excessive error detail | 13 |
| DEMO-09 · Overly permissive document caching | 14 |
| DEMO-10 · Service ownership documentation gap | 15 |
| Business impact | 16 |
| Remediation | 17 |
| Validation and remediation tracker | 18 |
| Retesting | 19 |

## Executive overview

This example models a scoped review of a fictional customer portal and supporting services. Account isolation and export authorization are the highest remediation priorities. The dashboard reflects only the example findings listed in this report.

Severity is qualitative. No numerical CVSS score was assigned.

**10**
Total findings

### Severity distribution

| | |
|---|---|
| Critical | 0 |
| High | 2 |
| Medium | 4 |
| Low | 3 |
| Informational | 1 |

### Remediation status

| | |
|---|---|
| Open | 3 |
| In progress | 2 |
| Ready for retest | 2 |
| Closed | 3 |

## Assessment objectives

Evaluate account isolation, role enforcement, handling of private records and defensive controls across representative portal and API workflows.

## Scope and limitations

The fictional scope covers the portal, its API, and selected identity and infrastructure controls under example.test. Production, third parties, destructive work, and denial-of-service testing are excluded.

## Testing methodology

Define authorized boundaries, map representative assets, evaluate controls, validate observations, assign qualitative risk and document remediation. This sample models the workflow using synthetic records.

## Discovered inventory

Inventory counts represent modeled assets. The coverage column identifies the portions selected for the sample review.

| | | | |
|---|---|---|---|
| Endpoints | 24 | Representative account, record and export workflows. | |
| Domain | 1 | Reserved fictional domain only. | |
| Subdomains | 2 | Portal and API entry points. | |
| Web services | 3 | Portal, gateway and export service. | |
| APIs | 2 | Records and exports. | |
| Identity components | 2 | Sign-in and recovery controls. | |
| Infrastructure components | 3 | Gateway, cache and routing policy. | |

# DEMO-01 · Cross-account record visibility

High

**Affected component**
Customer portal

**Description**
A record assigned to one test account was visible in a different account in the synthetic model.

**Business impact**
Private records could be disclosed to another customer.

**Remediation**
Evaluate ownership and role policies on the server before returning records.

**Acceptance criteria**
Cross-account requests are denied and authorized users still see their own records.

**Evidence status**
Synthetic observation only

**Classification**
CWE-639 · OWASP A01:2021

**Technical impact**
An inconsistent ownership control could expose account records.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Developer guidance**
Use one authorization policy for list and detail views, defaulting to deny.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Remediation status**
Open

## Synthetic evidence EX-01

**Fictional observation**
A record assigned to one test account was visible in a different account in the synthetic model.

**Simulated observed behavior**
The report model shows a record in a second account.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Expected behavior**
Records stay within their assigned account.

**Interpretation**
An inconsistent ownership control could expose account records.

**Related finding**
DEMO-01

# DEMO-02 · Missing export permission boundary

High

**Affected component**
Export API

**Classification**
CWE-862 · OWASP A01:2021

**Description**
An account marked as a viewer was shown an export intended for authorized operators.

**Technical impact**
A missing permission check could expose bulk data.

**Business impact**
A single export may affect multiple customer records.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Require export permission at initiation and retrieval.

**Developer guidance**
Apply the same policy to queued jobs and stored artifacts.

**Acceptance criteria**
Unauthorized roles cannot initiate or retrieve exports.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
In progress

## Synthetic evidence EX-02

**Fictional observation**
An account marked as a viewer was shown an export intended for authorized operators.

**Expected behavior**
Only users with export permissions can receive exports.

**Simulated observed behavior**
The viewer fixture received an illustrative export descriptor.

**Interpretation**
A missing permission check could expose bulk data.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-02

# DEMO-03 · Inconsistent recovery responses

Medium

**Affected component**
Account recovery

**Classification**
CWE-204 · OWASP A07:2021

**Description**
Simulated recovery feedback differed for two synthetic account states.

**Technical impact**
Observable differences could disclose whether an account exists.

**Business impact**
Account membership may become discoverable.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Standardize public response text and observable behavior.

**Developer guidance**
Keep detailed processing outcomes internal.

**Acceptance criteria**
Both fixture states receive equivalent public feedback.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
In progress

## Synthetic evidence EX-03

**Fictional observation**
Simulated recovery feedback differed for two synthetic account states.

**Expected behavior**
Recovery gives equivalent feedback for either account state.

**Simulated observed behavior**
The fixture displayed distinct response classes.

**Interpretation**
Observable differences could disclose whether an account exists.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-03

# DEMO-04 · Unsafe profile rendering boundary

Medium

**Affected component**
Profile display

**Classification**
CWE-79 · OWASP A03:2021

**Description**
A fictional review flagged a plain-text profile field interpreted by a rich rendering component.

**Technical impact**
Untrusted data could be interpreted in a browser context.

**Business impact**
Users may lose trust in the integrity of the portal.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Render the profile field as text.

**Developer guidance**
Use context-appropriate encoding and restrict rich content to approved surfaces.

**Acceptance criteria**
Profile text remains literal across all supported display views.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
Open

### Synthetic evidence EX-04

**Fictional observation**
A fictional review flagged a plain-text profile field interpreted by a rich rendering component.

**Expected behavior**
Display user-controlled values as text.

**Simulated observed behavior**
The model routes the value through a rich rendering surface.

**Interpretation**
Untrusted data could be interpreted in a browser context.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-04

# DEMO-05 · Incomplete session revocation

Medium

**Affected component**
Session service

**Classification**
CWE-613 · OWASP A07:2021

**Description**
The simulated session remained active after an account security event.

**Technical impact**
An obsolete session may retain access.

**Business impact**
Account recovery may fail to contain unauthorized access.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Revoke sessions when the relevant account event completes.

**Developer guidance**
Check revocation consistently across services.

**Acceptance criteria**
Revoked sessions are rejected while valid new sessions still work.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
Ready for retest

## Synthetic evidence EX-05

**Fictional observation**
The simulated session remained active after an account security event.

**Expected behavior**
Sensitive account events revoke related sessions.

**Simulated observed behavior**
The model retained an active session state.

**Interpretation**
An obsolete session may retain access.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-05

# DEMO-06 · Insufficient request limits

Medium

**Affected component**
Records API

**Classification**
CWE-770 · OWASP A04:2021

**Description**
The illustrative policy does not bound request volume in one intensive workflow.

**Technical impact**
Excess usage could exhaust shared capacity.

**Business impact**
Legitimate customers could experience delays or interruption.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Apply limits to the expensive operation.

**Developer guidance**
Budget capacity by identity and define consistent throttling responses.

**Acceptance criteria**
Excess requests are held within defined limits and ordinary usage remains available.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
Open

### Synthetic evidence EX-06

**Fictional observation**
The illustrative policy does not bound request volume in one intensive workflow.

**Expected behavior**
Resource-intensive operations have bounded usage.

**Simulated observed behavior**
The model shows the workflow without a usage limit.

**Interpretation**
Excess usage could exhaust shared capacity.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-06

# DEMO-07 · Missing browser security policy

Low

**Affected component**
Web gateway

**Classification**
CWE-693 · OWASP A05:2021

**Description**
The synthetic configuration lacked an approved browser policy on a document route.

**Technical impact**
Defense in depth is weaker on affected views.

**Business impact**
The impact of a separate browser weakness may be harder to limit.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Publish an approved policy at the gateway.

**Developer guidance**
Manage the header centrally and verify route-specific behavior.

**Acceptance criteria**
Applicable routes receive the policy and ordinary browsing works.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
Closed

### Synthetic evidence EX-07

**Fictional observation**
The synthetic configuration lacked an approved browser policy on a document route.

**Expected behavior**
Applicable document responses include the reviewed policy.

**Simulated observed behavior**
The synthetic response summary omitted the policy.

**Interpretation**
Defense in depth is weaker on affected views.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-07

# DEMO-08 · Excessive error detail

Low

**Affected component**
Error handling

**Classification**
CWE-209 · OWASP A05:2021

**Description**
A simulated error page revealed unnecessary service details.

**Technical impact**
Internal design information may become visible.

**Business impact**
Excessive disclosure can increase follow-up investigation effort.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Return generic user-facing errors.

**Developer guidance**
Keep diagnostic detail in access-controlled logs.

**Acceptance criteria**
Public errors stay generic and operators can trace incidents internally.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
Ready for retest

## Synthetic evidence EX-08

**Fictional observation**
A simulated error page revealed unnecessary service details.

**Expected behavior**
Public errors return a brief message and reference.

**Simulated observed behavior**
The example view showed internal service labels.

**Interpretation**
Internal design information may become visible.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-08

# DEMO-09 · Overly permissive document caching

Low

**Affected component**
Portal cache

**Description**
The fictional configuration treated a private page as broadly cacheable.

**Business impact**
On shared devices, private content may remain visible.

**Remediation**
Set cache policy according to information sensitivity.

**Acceptance criteria**
Private document responses use the approved restrictive cache directive.

**Evidence status**
Synthetic observation only

**Classification**
CWE-525 · OWASP A05:2021

**Technical impact**
Private response content might survive beyond the intended context.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Developer guidance**
Keep public and authenticated route rules separate.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Remediation status**
Closed

## Synthetic evidence EX-09

**Fictional observation**
The fictional configuration treated a private page as broadly cacheable.

**Simulated observed behavior**
The model flagged an overly broad cache rule.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Expected behavior**
Private document responses follow a restrictive cache policy.

**Interpretation**
Private response content might survive beyond the intended context.

**Related finding**
DEMO-09

# DEMO-10 · Service ownership documentation gap

Informational

**Affected component**
Asset catalog

**Description**
The sample catalog omitted an owner for a support service.

**Technical impact**
An unclear owner may delay maintenance decisions.

**Business impact**
Issue routing may take longer during an incident.

**Assessment limitations**
Limited to the representative component and conditions modeled for this example.

**Remediation**
Record the accountable team and review cadence.

**Developer guidance**
Include ownership fields in asset onboarding and review.

**Acceptance criteria**
Catalog entry includes a designated owner and a review schedule.

**Retesting requirements**
Confirm the acceptance criteria and verify intended behavior against the same approved sample scenario.

**Evidence status**
Synthetic observation only

**Remediation status**
Closed

## Synthetic evidence EX-10

**Fictional observation**
The sample catalog omitted an owner for a support service.

**Expected behavior**
Each service has an accountable owner.

**Simulated observed behavior**
The catalog listed the service without a maintenance contact.

**Interpretation**
An unclear owner may delay maintenance decisions.

**Evidence limitations**
Model output only. No live request, response, customer account or independently verified evidence is represented.

**Related finding**
DEMO-10

## Business impact

Account isolation and export control weaknesses carry the greatest modeled confidentiality impact. Address those first, then reduce the likelihood of service disruption and operational delays.

- DEMO-01 · Private records could be disclosed to another customer.
- DEMO-02 · A single export may affect multiple customer records.

## Conclusion

The model supports a staged remediation effort. Close only after the agreed checks demonstrate both control effectiveness and normal user functionality.

## Remediation roadmap

Priorities are recommendations for this scenario. Implementation and verification schedules depend on impact, dependencies and the agreed engagement.

**Critical**

Immediate attention

**High**

Prioritized remediation

**Medium**

Planned remediation

**Low**

Scheduled hardening

**Informational**

Routine review

## Security recommendations

Centralize authorization, cover security boundaries in regression tests, and assign teams to maintain monitoring and documentation.

## Validation and remediation tracker

| Finding ID | Finding | Severity | Responsible team | Priority | Remediation status | Retesting status |
|---|---|---|---|---|---|---|
| **DEMO-01** | Cross-account record visibility | High | Application | Prioritized remediation | Open | Awaiting fix |
| **DEMO-02** | Missing export permission boundary | High | API Engineering | Prioritized remediation | In progress | Awaiting fix |
| **DEMO-03** | Inconsistent recovery responses | Medium | Identity | Planned remediation | In progress | Awaiting fix |
| **DEMO-04** | Unsafe profile rendering boundary | Medium | Application | Planned remediation | Open | Awaiting fix |
| **DEMO-05** | Incomplete session revocation | Medium | Identity | Planned remediation | Ready for retest | Queued |
| **DEMO-06** | Insufficient request limits | Medium | API Engineering | Planned remediation | Open | Awaiting fix |
| **DEMO-07** | Missing browser security policy | Low | Platform | Scheduled hardening | Closed | Passed in simulation |
| **DEMO-08** | Excessive error detail | Low | Platform | Scheduled hardening | Ready for retest | Queued |
| **DEMO-09** | Overly permissive document caching | Low | Platform | Scheduled hardening | Closed | Passed in simulation |
| **DEMO-10** | Service ownership documentation gap | Informational | Application | Routine review | Closed | Passed in simulation |

## Retesting plan

Record the remediation version and environment, repeat the approved checks with synthetic accounts, verify acceptance criteria and normal workflows, and document outstanding limitations.

## Conclusion

The model supports a staged remediation effort. Close only after the agreed checks demonstrate both control effectiveness and normal user functionality.

## Technical appendix

Identifiers beginning DEMO- and EX- link fictional findings and evidence. CWE references describe weakness classes. OWASP references use the 2021 edition. Qualitative ratings consider possible impact and likelihood in the modeled scope.

**Report author** · BTNXIO SECURITY · btnxio@gmail.com · btnxiosecurity.com