PORTFOLIO SAMPLE

Balance Transfer Penetration Test

Voice MFA and session security

Prepared by Dan Gilbert
Sample edition | October 2026

Assessment overview

Testing identified a URL bearer token that enabled an unauthorized Balance Transfer, together with weaknesses in MFA verification, voice challenge issuance, and callback authentication. The highest priority is to restore the server-side authorization boundary around the workflow and transfer action.

HIGH	MEDIUM	LOW	RATED FINDINGS
1	4	1	6

About this sample

This sanitized report presents the assessor's testing approach, evidence, business impact, remediation, and verification criteria. Client identifiers and sensitive values are removed. The report includes redacted assessment photographs and clearly labeled explanatory diagrams.

Sample edition dated October 2026.

Reading guide

Section	Page
Executive assessment and scope	2
Findings and Observations	3
Detailed findings	4 to 8
Remediation and retest	9
Appendix A observations	10
Appendix B controls and references	11

01 EXECUTIVE ASSESSMENT

Executive assessment and scope

The assessor demonstrated an unauthorized Balance Transfer by exploiting a reusable bearer token carried in a URL. Discovery and exploitation occurred through an intercepting proxy; browser testing then confirmed that the copied URL also opened the authenticated workflow without a fresh login or MFA challenge. A tested URL remained usable after logout.

The URL also embedded the member's full Social Security Number. Exposure of the URL therefore combined personal-data disclosure with a reusable authorization secret. The same URL behavior was observed using a production test account and was associated with both voice and SMS MFA.

Remediation priorities

Order	Action	Findings
1	Remove URL secrets and PII. Enforce session, workflow, and transfer authorization on the server; revoke state at logout.	BT-01
2	Enforce MFA attempt limits, control voice challenge issuance, and authenticate Twilio callbacks before accepting code values.	BT-02 to BT-05
3	Apply consistent cookie protection and complete the design and hardening work in Appendix A.	BT-06 to BT-12

Engagement purpose and coverage

The engagement reviewed a new voice MFA option that delivers a code by phone call to the member's number on file. The member enters that code on screen to continue into Balance Transfer, which supports moving a balance from another financial institution to a member line of credit. The objective was to identify vulnerabilities and workarounds in the MFA option and its authentication boundary.

Primary testing covered the QA banking portal at ob-qa.example.com and member center at membercenter-qa.example.com. The production URL observation used a test account at membercenter.example.com. Methods included proxy inspection and replay, parameter mutation, cross-session and logout checks, challenge lifecycle tests, cookie and header inspection, and dependency and TLS review.

The assessor also identified an out-of-scope Twilio callback during diagram review and initiated supplemental live threat modeling with the product team. That review established missing signature validation and the resulting risk of provider impersonation with an attacker-chosen MFA code.

02 FINDINGS REGISTER

Findings and Observations

Six rated findings and six additional observations are indexed below. Remediation priorities appear in the executive assessment; the additional observations are detailed in Appendix A.

ID	Finding or observation	Severity or status	Page
BT-01	URL bearer token enables unauthorized transfer	High	4
BT-02	MFA verification limit not enforced by server	Medium	5
BT-03	Voice challenge issuance insufficiently throttled	Medium	6
BT-04	Voice challenge issuance accepted after logout	Medium	6
BT-05	Twilio callback signature not validated	Medium	7
BT-06	Sensitive cookies omit Secure	Low	8
BT-07	MFA code accepted across sessions	Design review	10
BT-08	Content Security Policy gaps	Hardening	10
BT-09	TLS 1.2 CBC cipher suite supported	Hardening	10
BT-10	Security headers vary by response type	Hardening	10
BT-11	External polyfill dependency review	Follow up	10
BT-12	Failed external resource reference	Follow up	10

Severity approach

Qualitative severity reflects business impact and exploitation prerequisites. Each rated finding includes a concise rationale. Design, hardening, and follow-up observations remain separately identified so remediation effort can be directed toward the demonstrated authentication and authorization weaknesses.

Evidence presentation

BT-01 reflects proxy exploitation and browser confirmation. BT-02 through BT-04 reflect direct verification and request replay. BT-05 was established through architecture review and assessor-led threat modeling. BT-06 reflects response-header inspection.

The photographs included with BT-02 are cropped and permanently redacted copies of supplied assessment evidence. Explanatory diagrams are labeled as illustrations. Example hosts use example.com.

03 DETAILED FINDINGS

URL bearer token enables unauthorized transfer

BT-01 | HIGH | Proxy exploitation and browser confirmation

Finding and exploitation sequence

The application placed a reusable sessionId in a post-authentication URL. The value began with the member's full Social Security Number and included session-specific data. The workflow accepted possession of that value as authorization.

- The assessor inspected the authenticated workflow through an intercepting proxy and identified the session value in the URL.
- Using the captured authorization value in proxy requests, the assessor exploited the session design and demonstrated an unauthorized transfer.
- The assessor then opened the URL in a separate browser context. The authenticated workflow loaded without repeating login or MFA.
- A logout replay check established that a tested URL remained usable after the web session was closed.

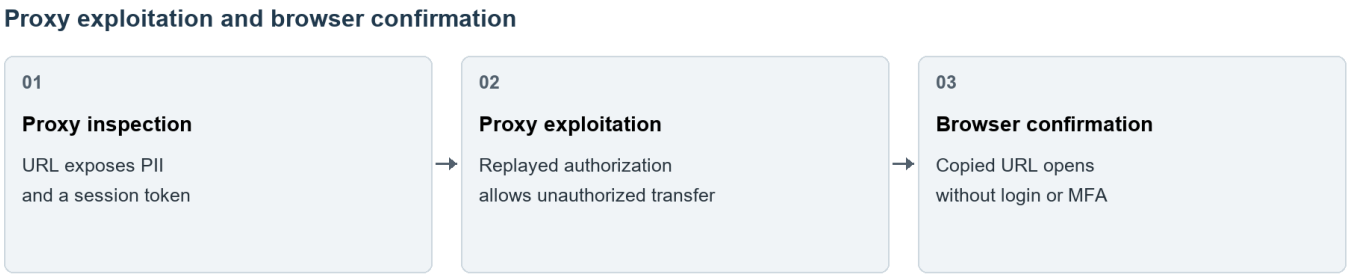


Exhibit 1. Illustrative sequence of proxy exploitation and subsequent browser confirmation.

Business impact and severity

An actor who obtains a valid workflow URL can exercise its bearer authorization. The demonstrated unauthorized transfer establishes financial impact, while the embedded SSN adds sensitive-data exposure. URLs may be copied or retained in browser history, logs, analytics, and monitoring. High severity reflects transfer authorization obtained through a reusable secret outside the normal login and MFA path.

Remediation

Remove PII and reusable authorization secrets from URLs. Use opaque session identifiers in protected cookies and enforce the authenticated member, active session, and allowed workflow state on the server. At transfer submission, validate ownership and permissions and bind the authorization to the approved transfer details; changes to those details must invalidate the prior approval. Revoke related state at logout. Review sensitive URL retention in application and infrastructure logs. See references 1 and 4.

Acceptance criteria

Repeat proxy and browser replay. The copied value cannot establish a fresh authenticated context or authorize a transfer; changing member or transfer details fails authorization. Logout immediately revokes the state. URLs and relevant logging destinations contain no PII or reusable authentication secrets.

03 DETAILED FINDINGS

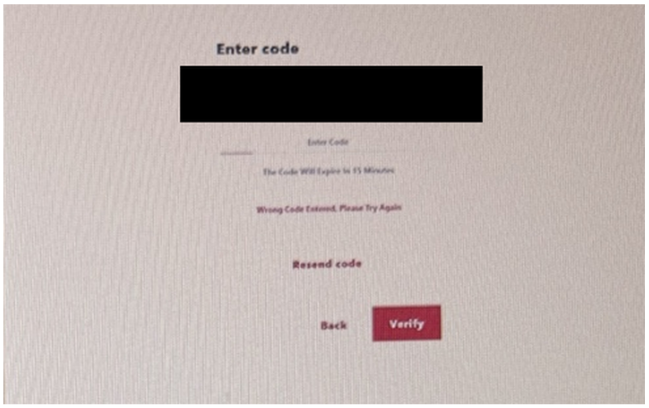
MFA verification limit not enforced by server

BT-02 | MEDIUM | Direct verification through the intercepting proxy | QA

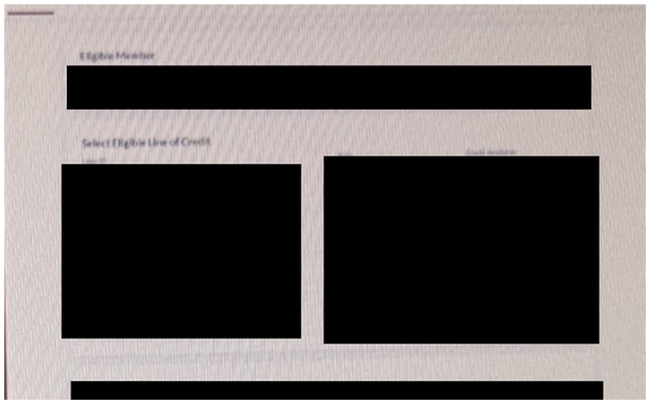
Finding and evidence

The interface indicated a five-attempt limit, but direct requests to /BalanceTransfer/Loan/MfaVerifyCode exceeded it. After nine invalid submissions, the valid code was accepted on attempt 10 and the authenticated workflow continued. Separate high-volume testing triggered upstream HTTP 403 and CAPTCHA protection at approximately 1,100 attempts.

A Invalid code response



B Protected workflow after verification



SUPPLIED EVIDENCE PHOTOGRAPHS | Cropped and permanently redacted

Original evidence content retained; black areas conceal identifiers and sensitive values.

Exhibit 2. Redacted photographs from the assessment show the invalid-code response and the protected transfer form reached after verification. The recorded test sequence contained nine failures followed by successful verification.

Business impact and severity

A caller with an eligible challenge can submit more guesses than the interface allows. Medium severity reflects a demonstrated server-side control failure that expands the online guessing opportunity within an active MFA workflow. Upstream traffic protection does not enforce the challenge's intended attempt budget.

Remediation

Maintain the failure counter on the server against the challenge and relevant authentication context. Invalidate the challenge at the approved threshold, and reject exhausted, expired, replaced, or completed challenges. Enforce counters atomically and apply account-level controls so reissue cannot reset the effective failure budget. See reference 2.

Acceptance criteria

Reach the configured failure limit with direct requests, then submit the valid code. The server rejects the exhausted challenge. Concurrent verification and repeated reissue cannot bypass the limit.

03 DETAILED FINDINGS

Voice challenge issuance and logout

BT-03 | MEDIUM | Voice challenge issuance insufficiently throttled | QA

Finding and evidence

Repeated replay of a call-initiation request generated outbound calls. A request sent during an active call interrupted it, invalidated the prior code, and initiated another call. No effective application resend throttle was apparent during testing.

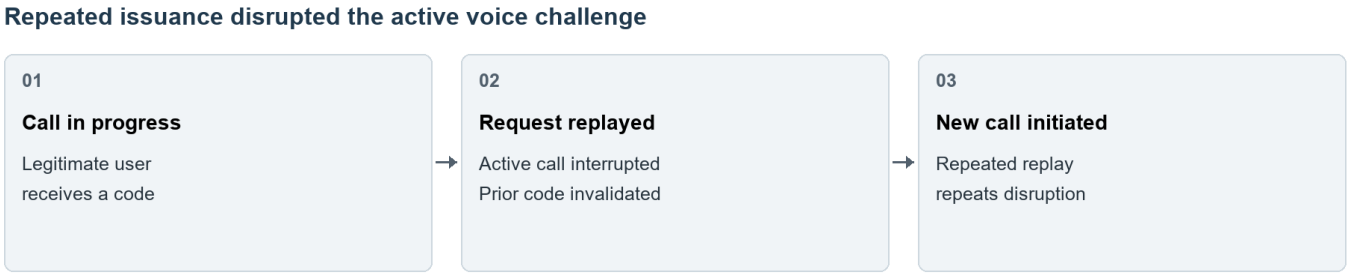


Exhibit 3. Illustrative sequence of repeated issuance disrupting the active voice challenge.

Impact and corrective action

Medium severity reflects the ability to disrupt authentication repeatedly, generate nuisance calls, and increase telephony use. Enforce resend intervals and rolling caps by account, destination, and relevant session context. Control replacement of active challenges and alert on abnormal issuance.

Acceptance: normal, burst, and concurrent requests obey the configured limits. Rejected requests generate no call and leave the legitimate active challenge usable.

Voice challenge issuance after logout

BT-04 | MEDIUM | Captured issuance request replay | QA

Captured call-initiation requests generated calls for approximately 10 minutes after web logout. Results varied across replays; a later replay at approximately 60 minutes failed.

Medium severity reflects continued use of stale authorization to initiate an external action after logout. This extends the disruption opportunity in BT-03. Revoke all session and workflow artifacts that authorize issuance, and check current authorization on every request.

Acceptance: replay immediately after logout is denied and generates no call, including requests submitted concurrently with logout. See reference 1.

03 DETAILED FINDINGS

Twilio callback signature not validated

BT-05 | MEDIUM | Architecture review and assessor-led threat modeling

Discovery and evidence

The assessor identified a Twilio callback while reviewing a diagram provided by the product team. Because it was outside the original test scope, the assessor paused to initiate live dialogue and threat model the integration as a supplemental review. During the discussion, the assessor identified the callback signature header and questioned its validation. The review established that the application did not validate that signature.

Affected authentication flow

For voice MFA, the member requests a call to the phone number on file and enters the delivered code on the Balance Transfer screen. In the reviewed integration, Twilio calls back into member center with the MFA code value. The receiving application trusts that input without verifying the provider signature.

Evidence method: architecture review and live threat modeling.

Business impact and severity

A correctly formatted request can impersonate Twilio within this workflow and supply an MFA code chosen by the attacker. That undermines the integrity of the second factor: the code supplied to the workflow is no longer authenticated as originating from the expected provider. Medium severity reflects attacker control of a security-relevant input within the voice MFA integration.

Remediation

- Validate X-Twilio-Signature before accepting the code value or invoking callback logic. Use the supported SDK with the exact external URL and request inputs required for validation.
- Associate accepted callbacks with the expected pending challenge and member workflow. Reject unexpected, duplicate, expired, or mismatched callbacks; code values must not replace unrelated challenge state.
- Reject missing, malformed, or invalid signatures before processing. Protect the verification secret and verify reverse-proxy handling of the external URL.

Acceptance criteria

A valid signed callback for the expected challenge succeeds. A request carrying an attacker-chosen code without a valid signature is rejected and cannot set or replace the challenge code. Tampered, duplicate, and mismatched callbacks fail without altering authentication state. See reference 3.

03 DETAILED FINDINGS

Sensitive cookies omit Secure

BT-06 | LOW | Response-header inspection | QA

Finding and evidence

Responses to POST /BalanceTransfer/Loan/Sso issued application cookies without the Secure attribute. Two reviewed responses omitted Secure on .AspNetCore.Session; one also omitted it on .AspNetCore.Antiforgery.[SUFFIX]. Authentication and upstream protection cookies in the same responses included Secure.

Cookie class	Secure attribute
.AspNetCore.Session	Absent in two reviewed responses
.AspNetCore.Antiforgery.[SUFFIX]	Absent in one reviewed response
Authentication cookie	Present in the same responses
Upstream protection cookies	Present in the same responses

Business impact and severity

An affected cookie can be sent over HTTP if the browser reaches a cleartext connection within its scope. Low severity reflects this conditional exposure path and the mitigating HSTS observed on normal application responses. Explicit cookie protection should be consistent across the authentication flow.

Remediation

- Require Secure on session, authentication, antiforgery, and other sensitive cookies across SSO and subsequent workflow responses.
- Use HttpOnly where script access is unnecessary. Configure SameSite, Domain, and Path for the intended authentication flow and required scope.
- Verify application and proxy behavior together so TLS termination does not weaken the cookie attributes issued by the application.

Acceptance criteria

Inspect Set-Cookie responses during login, SSO, MFA, renewal, and navigation. Sensitive cookies consistently carry Secure and the intended HttpOnly, SameSite, Domain, and Path settings. Legitimate authentication continues to work. See reference 1.

04 REMEDIATION AND RETEST

Remediation and verification

Assign an accountable owner and target date to each rated finding. Resolve the transfer authorization defect first, then the MFA lifecycle and callback weaknesses. Use the criteria below to verify deployed behavior before closing the findings.

ID	Verification required for closure
BT-01	Proxy replay cannot authorize a transfer. Copied URLs cannot establish a fresh session. Ownership and transfer-detail checks hold; logout revokes access. Review URLs and logging destinations for sensitive data.
BT-02	At the configured failure limit, a subsequent valid code is rejected. Concurrency and challenge reissue cannot bypass the effective failure budget.
BT-03	Burst and concurrent issuance obey limits without extra calls or uncontrolled challenge replacement.
BT-04	Captured issuance requests fail immediately after logout and generate no call.
BT-05	Unsigned or tampered callbacks carrying a chosen code cannot alter challenge state. Valid callbacks are bound to the expected pending workflow.
BT-06	Sensitive cookies carry approved attributes throughout the authentication lifecycle.

Ownership and evidence

Application and identity owners should address session, transfer, and MFA enforcement together. Integration owners should verify callback validation through the deployed route, including proxy behavior. Platform owners should confirm cookie and transport settings and coordinate provider-controlled changes.

For each retest, record the deployed build, environment, time and timezone, tester, owner, sanitized evidence, expected result, actual result, and disposition. Capture the original failure condition and the corresponding protected behavior after the fix.

Regression coverage

Recheck legitimate MFA completion, existing-code behavior, code expiration, challenge replacement, destination integrity, IVR termination, and upstream traffic protection alongside the fixes. Record any accepted residual risk with its responsible owner.

Additional observations

Resolve BT-07 through BT-12 using the checks in Appendix A. Design decisions and provider-controlled exceptions should have an owner and a documented disposition.

APPENDIX A ADDITIONAL OBSERVATIONS

Design review and hardening

MFA code accepted across sessions

BT-07 | Design review

A code issued in Session A was accepted through the existing-code option in Session B for the same authentication context. Session B entered the workflow while Session A remained at code entry. Confirm the intended session boundary, bind the challenge to the required user and action, and verify single-use acceptance.

Content Security Policy gaps

BT-08 | Hardening

CSP was absent on selected authentication and mobile-support pages. Define a policy for application-controlled responses, monitor in report-only mode where needed, and enforce it after confirming legitimate resources continue to load.

TLS cipher configuration

BT-09 | Hardening

The QA banking endpoint supported TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 under TLS 1.2. Prefer TLS 1.3 and approved TLS 1.2 AEAD suites. Remove CBC suites where compatibility permits and verify effective ingress configuration.

Security headers by response type

BT-10 | Hardening

Header behavior varied across OPTIONS, discovery, error, and provider-managed responses. Normal authentication pages included framing restrictions, nosniff, HSTS, and cache restrictions. Define a baseline by response sensitivity and rendering behavior; document provider-controlled exceptions.

External polyfill dependency review

BT-11 | Follow up

Authentication and mobile-support pages loaded a provider-hosted polyfill version 2.1.0. Verify provenance, support, applicable vulnerabilities, and integrity controls. Remove unused dependencies and restrict permitted script sources.

Failed external resource reference

BT-12 | Follow up

An external resource failed to load on the QA Balance Transfer page. Identify the complete reference, confirm ownership, and remove or correct the dependency. Verify expected content from an approved location.

APPENDIX B SUPPORTING INFORMATION

Preserved controls and references

Controls observed during testing

Control	Observed behavior
Code expiration	Codes became invalid after 15 minutes.
Challenge replacement	A newly issued code invalidated the previous code.
Destination integrity	Attempts to replace the destination phone number were rejected.
IVR handling	The voice session ended after three invalid selections.
Upstream protection	Sustained automation triggered HTTP 403 and CAPTCHA at approximately 1,100 attempts.
Transport headers	Normal application responses included HSTS.

Technical references

1 OWASP Session Management Cheat Sheet

Session handling, cookie attributes, and server-side invalidation.

2 NIST SP 800 63B 4 Digital Identity Guidelines

Authentication secret verification, rate limiting, and one-time acceptance.

3 Twilio Security and Request Validation

Provider signature validation and supported verification libraries.

4 OWASP Transaction Authorization Cheat Sheet

Server-side transaction authorization and protection of approved transaction details.

Sample handling

This is a portfolio work sample. Example hosts use example.com. Client and account identifiers, session values, and phone details are omitted or permanently redacted. Supplied evidence photographs retain the underlying visible test results; explanatory diagrams remain labeled illustrations.