BlackFlag Security — Sample Report

Example structure • anonymized content • for evaluation only

Executive summary

• Engagement: Web/API pentest (time-boxed)
• Goal: Identify exploitable risk and attack chains
• Outcome: 1 critical chain, 2 high, 5 medium
• Top risk: Authorization bypass (BOLA/IDOR) enabling account takeover
• Business impact: unauthorized access to customer data exports

Scope & constraints

In scope:
• app.example.com (web)
• api.example.com (REST)
Out of scope:
• Denial of Service, phishing/social engineering
Constraints:
• No destructive actions • Minimal impact evidence only

Finding format (example)

ID: BF-API-001
Title: Broken Object Level Authorization (BOLA)
Severity: Critical
Evidence: Repro steps + request/response snippets
Impact: Account takeover → data export
Recommendation: Centralize authZ checks, add resource-level policies, add tests

BlackFlag Security — Sample Report

Technical detail (example)

Attack chain narrative (example)

1) Obtain low-priv user token
2) Enumerate object IDs via predictable patterns
3) Access /users/{id}/export without ownership check
4) Exfiltrate export file metadata (no full data shown)
5) Demonstrate privilege escalation path (least-impact)

Reproduction steps (snippet)

Request:
GET /v1/users/12345/export
Authorization: Bearer <token>

Expected: 403 Forbidden
Observed: 200 OK (export metadata)

Fix guidance (high level)

• Enforce ownership checks at the service layer
• Deny-by-default authorization policy
• Add tests for object access across roles
• Log and alert on suspicious enumeration patterns