CASE STUDY #1

Critical Account Takeover & Advanced File Upload Exploitation

Web Application & Partner API Security Assessment

WEB APPLICATION PARTNER API PRIVILEGE ESCALATION

⬡ ENGAGEMENT AT A GLANCE

2	5+	1-2 wks	100%
Critical Vulnerabilities	High & Medium Findings	Engagement Duration	Manual Validation Rate

⬡ CLIENT BACKGROUND

A growing technology company approached IVASTA Security after releasing several new features within their web application and partner API ecosystem. With upcoming enterprise engagements and increasing reliance from integration partners, they required an independent penetration test to validate the security of the newly deployed functionality.

The primary objective was to assess whether the recent changes introduced exploitable vulnerabilities that could impact user accounts, partner integrations, or overall system integrity.

⬡ SCOPE OF ENGAGEMENT

The assessment covered all major surfaces of the client's technology stack:

- Authenticated and unauthenticated testing of the web application
- Security testing of partner-facing API endpoints
- Role-based access control validation
- File upload functionality
- Cross-endpoint logic validation
- Exploit chaining across multiple components

A manual, adversarial testing approach was applied throughout the assessment — no automation-only shortcuts.

⬡ METHODOLOGY

APPROACH	KEY FOCUS AREAS
▸ Business logic testing across multiple workflows	▸ File upload validation bypass attempts ▸ Chaining medium-severity findings into high-impact paths

- Horizontal and vertical privilege escalation attempts
- Token manipulation and session handling analysis
- Multi-step exploitation scenarios
- Identifying meaningful compromise scenarios
- Cross-endpoint request chaining analysis

⬡ KEY FINDINGS

The assessment uncovered two critical vulnerabilities, each requiring complex, multi-step exploitation paths that would go undetected by automated scanning tools.

FINDING 01 | CRITICAL

Account Takeover Leading to Administrative Compromise

- Abuse of inconsistent authorization logic across application endpoints
- Manipulation of multi-step authentication and session workflows
- Leveraging medium-severity issues as escalation pivot points
- Cross-endpoint request chaining to bypass access controls
- Final impact: Full administrative access, user management control, and potential system takeover

⚠ IMPACT SUMMARY

Once escalated to administrative access, the impact was severe: full control over user management, access to sensitive application data, ability to modify critical configurations, and potential for full system compromise and operational takeover.

FINDING 02 | CRITICAL

Advanced Malicious File Upload Bypass

- Bypassing layered server-side and client-side validation logic
- Exploiting inconsistencies between frontend and backend validation
- Manipulation of request structures across different endpoints
- Combining multiple individually subtle weaknesses into one exploit chain
- Final impact: Dangerous system-level file execution achieved

⚠ IMPACT SUMMARY

This vulnerability would not have been detected through automated scanning. It required deep manual analysis, chaining of business logic flaws, and cross-endpoint manipulation — the hallmark of real-world adversarial testing.

⬡ ADDITIONAL FINDINGS

HIGH SEVERITY

- Authorization inconsistencies across user roles
- Improper rate limiting on sensitive endpoints
- Token handling weaknesses in API flows

MEDIUM SEVERITY

- Input validation gaps in form fields
- Security misconfigurations in API endpoints
- Partner API exposure risks identified

While individually less severe, these findings contributed to strengthening both the core application and partner-facing integrations.

⬡ RETESTING & VALIDATION

Following remediation, IVASTA Security conducted a structured retest to validate that all critical and high-severity vulnerabilities were fully resolved.

✓	✓	✓	✓
Critical exploits fully remediated	**Validation logic** hardened	**Authorization** handling improved	**Attack surface** reduced

The retest was considered a crucial part of the engagement, providing assurance that fixes were not only applied, but correctly implemented.

⬡ DELIVERABLES & OUTCOME

📄 **Comprehensive Technical Report** — Detailed reproduction steps, evidence, and full vulnerability documentation

🎯 **Business Impact Analysis** — Risk-prioritized findings with remediation guidance tailored to the client

🔄 **Formal Retest Validation Report** — Structured confirmation that all critical and high-severity vulnerabilities were resolved

🏆 **Digital Security Validation Certificate** — Independent third-party security certification used with enterprise clients and partners

⬡ BUSINESS IMPACT

The engagement significantly strengthened the client's security posture.

The client expressed strong satisfaction with the depth of testing, clarity of communication, and the structured retest process.

- Eliminated critical account compromise risk
- Prevented a severe file upload exploitation scenario
- Improved partner API resilience and security posture
- Provided independent security validation for enterprise engagement readiness

Ready to find out what attackers could do to your systems?

hello@ivasta-security.com | ivasta-security.com