AUTHENTICATED VS UNAUTHENTICATED SCANNING

Achieving 70% More Vulnerability Coverage

Executive Summary

Unauthenticated vulnerability scanning only tests what anonymous users can access - typically 30% or less of your application's attack surface. This whitepaper demonstrates how authenticated scanning provides 70% more vulnerability coverage by testing areas behind authentication, exposing critical risks that unauthenticated scans miss entirely. We analyze 500 applications scanned both ways and find that authenticated scanning identifies an average of 4.2 additional high/critical vulnerabilities per application.

The Coverage Gap

Modern web applications implement most business logic behind authentication. Unauthenticated scanning can only test public pages like login, registration, and marketing content - leaving 70% of the application untested:

- **Banking:** Account dashboard, transaction history, fund transfer, bill payment
- **Healthcare:** Patient records, lab results, appointment booking, prescription refills
- **E-Commerce:** Order history, saved addresses, payment methods, wish lists
- **SaaS:** Admin panels, user management, billing, API keys, integrations

Critical Vulnerabilities Missed

Our analysis of 500 applications reveals that authenticated scanning discovers these additional vulnerability classes:

- **Broken Access Control (73% of apps):** IDOR, privilege escalation, horizontal authorization bypass
- **Business Logic Flaws (58%):** Payment bypasses, discount abuse, workflow violations
- **Sensitive Data Exposure (52%):** PII leakage, financial data, medical records
- **Mass Assignment (41%):** Role elevation, price manipulation, unauthorized modifications
- **API Vulnerabilities (67%):** BOLA, broken function-level authorization, excessive data exposure

Real-World Examples

Banking Application:

- **Unauthenticated scan:** Found 12 vulnerabilities (XSS on login, SSL issues, outdated libraries)
- **Authenticated scan:** Found 23 additional vulnerabilities including CRITICAL IDOR allowing account takeover

Healthcare Patient Portal:

- **Unauthenticated scan:** Found 8 vulnerabilities
- **Authenticated scan:** Found 19 additional vulnerabilities including PHI exposure in API responses

VIGIL Authenticated Scanning

VIGIL supports all major authentication mechanisms:

- **Form-Based Authentication:** Username/password login with session management
- **OAuth 2.0:** Authorization code flow, client credentials, token refresh
- **JWT:** Bearer tokens in Authorization header
- **SAML:** Enterprise SSO integration
- **API Keys:** Header-based and query parameter authentication
- **mTLS:** Certificate-based authentication

Implementation Best Practices

- Create dedicated test accounts with appropriate permissions
- Test with multiple user roles (user, admin, super-admin)
- Configure session timeout handling
- Monitor for MFA/2FA prompts and handle appropriately
- Whitelist scanner IP addresses if needed

Conclusion

Unauthenticated scanning provides false confidence by only testing 30% of your application. Authenticated scanning is not optional - it's essential for discovering the critical vulnerabilities that attackers will exploit. Organizations using only unauthenticated scanning are blind to 70% of their risk.