True Positives

Vulnerability Scan Preparation

Pre-Scan Checklist

Complete the following items before your scheduled DAST assessment to ensure accurate results and minimize operational disruption.

1. Define Scan Scope

- **Target URLs and environments —** Provide all web application URLs including domain and starting page to be tested. Specify whether scanning production, staging, or development.
- **API endpoints —** Provide OpenAPI/Swagger, RAML, or WSDL specification files where available.
- **Scope boundaries and additional hosts —** Confirm in-scope vs. excluded domains. List any additional subdomains or API hosts (e.g., api.yourapp.com) the application relies on.

2. Configure Network Access

- **Trustlist Invicti scanner IPs —** Whitelist scanner IPs in firewalls, IDS/IPS, and WAFs. IPs are region-specific:
  - US: docs.invicti.com/ip/trustlist-us
  - EU: docs.invicti.com/ip/trustlist-eu
  - CA: docs.invicti.com/ip/trustlist-ca
- **Cloud provider authorization —** If hosted on AWS, Azure, or GCP, verify your provider permits external vulnerability scanning and complete any required authorization forms.
- **Internal applications —** For non-public apps, an Invicti scan agent must be installed on a server with port 80/443 connectivity to the targets. Verify the agent can reach each target application.

3. Provide Authentication Credentials

- **Dedicated scan account —** Provide credentials with access to authenticated functionality (forms, workflows, data entry). The account must allow concurrent sessions.
- **Disable or bypass CAPTCHA —** Disable any CAPTCHA or Bot Protections

- **Extend session lifetimes —** Ensure tokens and session cookies remain valid for at least 24 hours.
- **Complex or API authentication —** For SSO/IdP flows, document the login steps or provide Selenium recordings. For OAuth 2 APIs, provide the client ID, client secret, token endpoint, and scopes.

4. Provide Scan Preferences

- **Excluded endpoints —** List pages or paths that should not be tested: logout, password reset, payment processing, destructive actions, or third-party integrations.
- **Rate limits and scanning hours —** Specify max requests per second if performance-sensitive, and any time windows when scanning must not occur.
- **Required headers, cookies, or form values —** Provide any headers, cookies (feature flags, tenant IDs, API keys), or custom form field values needed. The scanner defaults to invicti@example.com for email fields.
- **Application type —** Note if the app is a single-page application (React, Angular, Vue.js) or relies heavily on JavaScript rendering.

5. Notify Stakeholders and Prepare

- **Internal teams —** Inform IT operations, SOC, application owners, and development teams of the scan window. Scanning traffic can trigger IDS/IPS alerts and WAF rules. Brief executive or compliance leadership if required by policy.
- **External providers —** Coordinate with hosting providers, CDN vendors, and managed infrastructure providers to prevent automatic IP blocking.
- **Backup your environment —** Snapshot applications, databases, and configurations before the assessment. Verify rollback procedures have been tested. If scanning staging, seed with representative non-sensitive test data.

6. Schedule the Assessment

- **Select scan window / Freeze Window —** Identify windows of time for testing or when testing is not allowed. Typical scans can range from 8-10 hours. It is best to have no deployments during that time frame..
- **Provide escalation contact —** Name and contact method (phone, Slack, email) for the person to reach if the scan needs to be paused.