True Positives

Welcome to True Positives Managed AppSec Vulnerability Scanning Services!

We are thrilled that you have chosen to evaluate our Service or are ready to begin scanning as a new Subscriber. We are committed to supporting your unrivaled success with brand and asset protection. To ensure safe and effective vulnerability scanning, proactive preparation is crucial.

We suggest you review the following prerequisites and considerations before scanning:

1. **Target Onboarding:** Utilize the Target Onboarding Form to submit your Target to our Service system at your convenience.
2. **Scanning Permission:** Ensure you own or have obtained authorization permission from the scan Target owner to conduct vulnerability scanning.
3. **Target Details**: Have key information readily available to enable vulnerability scanning, such as accurate URLs and Host locations.
4. **Test Credentials:** Where authentication is required, be prepared to provide our Support Team with valid user credentials that allow access to your scan Target(s) when asked. We recommend using "Test" credentials.
    - ➔ **Importance of Authenticated Scanning:** For comprehensive and insightful testing outcomes, we strongly recommend authenticated scanning. This method allows for a more in-depth examination of your web application from a logged-in user's perspective.
    - ➔ **Acquiring Test Credentials:** If specific credentials are necessary for our crawler to perform authenticated scanning and are not readily available or need to be created, engage the appropriate personnel or teams to secure these credentials.
    - ➔ **Multi-Factor Authentication/CAPTCHA:** It is recommended that multiple-factor authentication be disabled for the test. Leaving this enabled will cause testing to take longer and may impact the quality of results.
5. **Pre-Scanning Coordination:** Notify all potentially impacted parties in advance. Effective communication ensures a smooth scanning process without interruptions.
6. **Traffic Alert – Network Permission:** Inform your Network Operations team in advance about upcoming scanning activities to avoid unnecessary alarms or interruptions and to facilitate scanner access. It is recommended that any Web Application Firewall (WAF) be disabled as this will provide a better.

Managed Application Security Vulnerability scan traffic being generated on your behalf by True Positives will originate from here:

IP 54.208.242.36 scanners.acunetix.com
IP 34.194.143.46 online.acunetix.com

7. **Backup Systems:** Back up critical systems and data before the scan.
8. **Off-Peak Scheduling:** Schedule the scan during off-peak hours.
9. **Testing Environment:** It is recommended to test in an environment that is not live. While we are executing non-destructive tests, the very nature of the assessment has the potential to negatively impact the Target.
10. **Prepare for Findings & Remediation:** Be prepared to act on the findings you receive from our Vulnerability Scan Reports and prioritize remediation activities.

These suggested Best Practices for Vulnerability Scanning will ensure the best possible experience and outcomes. Happy Scanning!