Khoros™

Introduction

Khoros Customers are welcome to conduct their own automated or manual security testing on approved staging sites after signing the Khoros External Security Assessment Agreement or EXSAA.

Why is testing not allowed on production sites?

Conducting security tests against the production site is strictly prohibited for the following reasons:

1. **Shared Multi-Tenant Platform**: Khoros operates a shared multi-tenant SaaS platform where any disruptive activity could negatively impact other customers.
2. **Resource and Performance Concerns**: Automated security scanners can generate huge amounts of traffic in a short period of time and pose the threat of impacting performance of other customer sites.
3. **Security Monitoring**: Monitoring tools generate alerts to respond to suspected attacks. Most security scanners and security testing will generate traffic that is virtually indistinguishable from malicious attack traffic and will likely result in a large number of false alarms being generated.
4. **Test Data Injection**: Application testing usually involves injecting test data. This can confuse users and/or cause unnecessary workload to clean up the test entries.
5. **Application Workflow Triggers**: Some application features may generate operation workflows such as creating a service request ticket for support, resulting in wasted time and resources.

Testing Restrictions

Testers shall not do the following:

1. Test against any other server, IP or URL other than what has been formally approved by Khoros
2. Attempt any type of Denial of Service attack
3. Attempt to reboot servers
4. Install bots, viruses, trojans, rootkits or other harmful executables
5. Attempt to access, modify or delete information without authorization from Khoros

Note: SQL injection testing is permitted as long as it doesn't involve the use of destructive methods.

Scanning Recommendations

1. **Low Speed**: Use the lowest possible speed/settings for your security scanner.
2. **Targeted Whitelist Approach**: By using a targeted whitelist approach, you can make sure that all the pages and features that you are most concerned about get properly scanned.
3. **Prevent Information Overload**: Limit the maximum number of links to test to a reasonable size. Automated scans can sometimes take days to complete and generate reports that are hundreds of pages long.
4. **Create a Security Baseline**: Automated scanners often generate a large number of false positives. Creating a baseline will allow you to compare tests with previous results and speed up the process.

Getting Started

Contact your sales or support representative or email Support@Khoros.com to get a copy of the Khoros External Security Assessment Agreement and to start the process.