Zorroa – ISE Security Partnership

October 5, 2020

Overview

This document summarizes Zorroa's relationship with Independent Security Evaluators (ISE), a security consulting firm that conducts in-depth security assessments of ZVI (Zorroa Visual Intelligence). ZVI is a web application used to facilitate the uploading and processing of cloud data to train machine learning models.

As of this report, ISE has assessed the following components:

- ZVI Web Application
  - Machine Learning portal
  - Admin portal
  - Super-admin portal
- ZVI Platform API

Zorroa initially engaged with ISE in August of 2020. The following table summarizes the project timeline of past and planned assessments:

Revision	Date	Description
1	August 2020	Initial assessment of Zorroa Platform
2	January 2021	Planned Reassessment.
3	July 2021	Planned Reassessment.
4	January 2022	Planned Reassessment.
5	July 2022	Planned Reassessment.
6	January 2023	Planned Reassessment.

Assessment Methodology

ISE specializes in hands-on assessments that consider attack surfaces, permissions, and application logic specific to the target system that a variety of attackers may exploit. ISE uses automated tools to gain an understanding of the system and identify common issues, but the focus of the assessment is manually testing advanced exploits to discover vulnerabilities that scanners will miss. ISE reports all findings with severity ratings based on exploit complexity, impact, and attack chaining.

ISE's threat model considers how a system's assets could be affected by attacks from a variety of sources with different skills and motivation, as summarized below:

- Unauthenticated users (e.g., individual hackers and organized hacker groups) – unauthenticated exploits tend to be rated with critical severity, depending on impact, and the most urgent to mitigate.
- Nation-state adversaries – these groups will have large pools of resources to conduct advanced, targeted attacks that might require access to source code to discover.

- Rogue or former employees, e.g., corporate espionage.
- Insider threats, e.g., current employees and customers – issues pertaining to this group are typically broken access controls within the permission model that lead to privilege escalation.

Building on the threat model to perform the technical assessment, ISE combines (1) knowledge of common types of exploits afflicting technology used in a platform, such as OWASP Top 10 vulnerabilities; (2) hardening opportunities for the technologies in use; (3) security best practices applying to any architecture, such as defense in depth, least privilege, no misplaced trust between components, secure by default, and so on; (4) business context based on knowledge of the industry, review of the product, and discussions with the clients on priorities, and; (5) additional insight based on using the product. To gain and use this knowledge, an assessment typically includes the following activities:

- A kickoff call to coordinate access to the system under testing, review components, receive a demonstration of the product, review the client's priorities or pre-existing security concerns, and identify assets and likely threats.
- A discussion of the product's design and architecture, and walk through of the source code, with the aim of gaining familiarity with the product to a similar level that a new developer joining the development team would desire.
- Reviewing any internal, developer-oriented documentation describing the system's design and architecture, and API documentation (such as name of API call, parameters, required privilege level, and formats of inputs and outputs).
- Reviewing any external, customer-facing documentation explaining how to use or set up the product, configuration choices that may affect security, and optional features.
- Using the product hands-on in order to enumerate its features, gain additional insight into assets and attack surfaces, identify priorities and business limitations to better formulate recommendations to issues we identify later, and overall, gain an understanding of the product's feature set to the level of a power-user or sophisticated customer.
- Where appropriate and effective, running automated scanning tools in order to support the assessment, to both efficiently discover potential vulnerabilities, and also identify high-exposure vulnerabilities that are likely to be discoverable by external adversaries. Scanning tools do not replace manual assessment but supplement it. We review scan results to remove false positives and to investigate correct findings to provide the true context behind the issue, proof of concept steps to reproduce, and recommendations to developers to help resolve the issue.
- The bulk of the assessment consists of on-hands, manual assessment to discover those issues that scanners cannot find, either because of subtle or complicated interactions between components and steps to trigger the issue, and business-level issue that a scanner is simply incapable of finding. This portion of the assessment heavily focuses on authentication and authorization capabilities, to discover both flaws in the design or configuration of these components, but also violations of the expected authentication design. For example, for multi-tenant software-as-a-service architectures, we work with the client to set up ISE as two distinct tenants, and then attempt to use accounts in one tenant to violate tenant boundaries and access data inside another tenant. For systems where a user can be given different levels of access within a tenant, we set the user as a lower-privileged user and attempt to call higher-privileged APIs from that user's account. Other common web attacks include cross-site scripting, cross-site request forgery, SQL injection, XML entity injection, command injection, missing authentication, broken authorization, etc.
- ISE uses the assessment results to write a report including an overview of the system, project logistics (scope, methodology, timeline),, and discovered issues. Each finding includes a high-level description of the issue, attack steps, multiple recommendations (considering difficulty, cost, and limitations based on needed functionality), and additional analysis as needed to provide insight or connections between findings.
- ISE reviews findings with Zorroa, provides interactive guidance on steps to implement fixes, subsequently verifies the fixes manually in the system (referred to as “mitigation” or “remediation” testing).

Below is a general list of the types of vulnerabilities that ISE prioritizes during application assessments. A particular assessment may include a subset of this list or issues outside of this list depending on the defined scope or focus of the assessment.

- Authentication
    - Session management
    - Password policies

    - Account onboarding/offboarding
- Authorization
    - Privilege escalation
    - Broken access controls
- Common application vulnerabilities: XSS, XXE, CSRF, SSRF, etc.
- Injection attacks: SQL injection, command injection, etc.
- Denial of service attacks
- Information disclosure
- Encryption & secrets management
    - Encryption at-rest & in-transit
    - Usage of weak algorithms
    - Key management
- Use of vulnerable third-party software and libraries
- Web hardening measures
    - Cookie protections
    - Security-related headers
- Security configurations
    - Custom application configuration settings
    - AWS security best practices
    - Adherence to secure-by-default principle
- Logging and monitoring capabilities
- Manipulation of custom application logic

About ISE

ISE is an independent security firm headquartered in Baltimore, Maryland. We are dedicated to providing clients proven scientific strategies for defense. On every assessment our team of analysts and developers use adversary-centric approaches to protect digital assets, harden existing technologies, secure infrastructures, and work with development teams to improve our clients' overall security.

Independent Security Evaluators, LLC

4901 Springarden Drive
Suite 200
Baltimore, MD 21209
(443) 270-2296

contact@ise.io
https://www.ise.io/

Relationship with Zorroa

ISE is an independent party to Zorroa and does not have a stake in the outcome of these assessments. ISE does not endorse Zorroa products, or any other product, and is motivated only to improve the security of all products we are engaged to assess. ISE has worked with Zorroa on security assessments since August 2020 at the request of Zorroa and their customers.