Synoptek

Case Study

Vulnerability Assessment Helps Software Company Identify and Fix Security Loopholes

Customer Overview

Customer

A private IT security software company

Profile

The client specializes in Data and IT Security, IT Compliance, Information Governance, IT Risk Assessment, Insider Threat Detection, User Behavior Analysis, Change Auditing, and Content Services.

Industry

Software

Services

Vulnerability Testing

Business Need

The client empowers information security and governance professionals to reclaim control over sensitive, regulated, and business-critical data, regardless of where it resides.

While the client could always successfully identify and resolve any security loopholes, Open Bug Bounty Researcher found a security vulnerability affecting the website and its users. They identified XSS (Cross-Site Scripting) and other vulnerabilities and disclosed information related to XSS vulnerability on Open Bug Bounty site.

To get detailed insight into the security gaps identified, the client was looking to partner with a security consulting firm that could look into the gaps and provide a complete vulnerability report. The client also wanted the firm to provide a list of preventive/corrective action items for their infected website.

Approach and Solution

Synoptek partnered with the client to understand their issues and offered the required Vulnerability Testing Services. Synoptek took the following actions for the Open Bug Bounty issue(s) and vulnerabilities assessment testing activities:

- Carried out manual exploration of the website and suggested necessary preventive actions.
- Scanned the website with the help of tools such as OWASP ZAP, OWASP Xenotix, Nikto, and suggested a list of vulnerabilities such as CrossSite Scripting Attack, Anti CSRF tokens, X-Frame Options, SQL Injection, and so on along with their preventive actions.
- Successfully identified cross-site scripting attack on the client application, furnished details where vulnerability existed, and provided preventive action to resolve them.
- Regularly submitted reports to the client's development team so that they could implement the suggestions during the development cycle.

Business Results

Using Synoptek's Vulnerability Testing Services and through the implementation of the preventive actions against the identified vulnerabilities, the client has been able to overcome all vulnerabilities, including the one which the Open Bug Bounty researcher had disclosed, successfully

- With vulnerabilities identified and resolved in time, the client can safeguard itself from cyber-attacks.
- The client can offer secure access to its website for its users while protecting their data at all times.

Since known vulnerabilities have been identified, the client is also able to strengthen its security posture and prevent future attacks.

> "Thank you for your great job for identifying vulnerabilities from our web application. We are going to research and implement it."
>
> **– Head of tech & creative teams**

About Synoptek

Synoptek delivers accelerated business results through advisory-led, transformative full-life-cycle systems integration and managed services. We partner with organizations worldwide to help them navigate the ever-changing business and technology landscape, build solid foundations for their business, and achieve their business goals.