Global Association ISACA Leads the Way on Web Application Security with Netsparker

ISACA is an independent and non-profit global association that is focused on the development and adoption of industry-leading best practices for information systems, IT governance and IT security. It serves more than 140,000 members and professionals who hold ISACA certifications in more than 180 countries; most of which are security consultants, professionals, and educators.

The Risks and Repercussions of Getting Hacked

As an international association which advocates IT governance and security best practices to all its members, ISACA is considered a leader in a community of IT security experts. Therefore, as part of their security practice, a top priority is placed on all of their websites & portals to ensure they are constantly monitored for security threats & vulnerabilities that could happen at any time.

If any of ISACA’s website’s succumbed to a security breach, it could potentially lead to the loss of private user information and data or the potential loss of control over the affected website. Any access to important user data from an unauthorized user or having an unusable website would result in a negative impact to the association’s reputation as the arbiter of IT governance & security practices and a significant public relation crisis.
As part of their due diligence process, ISACA’s security team tested several tools before choosing Netsparker Web Application Security Scanner. The main reasons for choosing Netsparker over the rest were:

- It clearly defines and explains imminent vulnerabilities;
- It assists in vulnerability assessments during different development stages;
- It has a facility to customize, scan, and automate tasks;
- It is easy to use.

As the leaders in advocating security, compliance and IT governance best practices by delivering courses and training about these subjects, suffering any security breach is simply not acceptable.

The Web Application Security Challenge

As an international organisation, ISACA not only hosts their main website but also host and maintain several other related websites, which contains multiple login forms, user registration areas, online payment capabilities, different user portals and tens of thousands of pages. The auditing of, and ensuring the security of such a large portfolio of international websites is not a simple task.

In adherence to their own best practices for security, ISACA has a staging environment where all code is thoroughly tested before being transferred to live environments. However, despite these security protocols, ISACA’s own security department still faced a large operational task. That task was to maintain the integrity of all their sites, despite frequently being changed and updated to address the business needs and services provided by individual websites within their portfolio. This, of course, presents a major challenge for all international businesses and ISACA was no different.

The previous solution they used to deal with this issue was to use open source tools and rely on third party consultants. Unfortunately, most of the tools they used only provided high level details around the issues and were relatively unreliable. Highly trained consultants are, by their nature, very expensive, and it is virtually impossible for consultants to audit all possible attack surfaces on all of their websites, 24/7. Therefore, they were in urgent need of an alternative solution. Ideally, this alternative solution should be one that automated the process of identifying vulnerabilities and security issues and could be used across multiple websites, simultaneously.

The Solution: Automating Web Application Security

As part of their due diligence process, ISACA’s security team tested several tools before choosing Netsparker Web Application Security Scanner. The main reasons for choosing Netsparker over the rest were:

- It clearly defines and explains imminent vulnerabilities;
- It assists in vulnerability assessments during different development stages;
- It has a facility to customize, scan and automate tasks;
- It is easy to use.
Feedback from the senior management of the ISACA security team demonstrated that: "Netsparker was able to further define and explain the specific issues at hand. It was also able to assist in the proof of concept for vulnerability assessments during development."

"It is very easy to use, thus allowed everyone in our team to cooperate. Of course, the ability to customize, scan, and automate the tasks was a big plus. Netsparker helped us identify the areas to remediate before we migrated new code into the production environment."

For over 3 years, Netsparker has been an integral part of ISACA's development life cycle and has been used to scan website changes and new web applications, both on their staging server and development environment.

**Staying on Top of the Web Application Security Game**

Identifying vulnerabilities is one thing; continuously developing secure code and staying on top of the game throughout the years is another.

A company or organization may have access to the best tools in the world, but these are useless unless such tools are backed by professional and trustworthy support that can be relied on unconditionally. Top-notch support is precisely what ISACA was looking for in the first place: not just a product, but a partner to help them when they end up with their backs against the wall.

Like everyone else in this industry, ISACA's security experts have had their share of challenges when securing web applications, but they have found the help they needed every single time. "Netsparker support has been engaged, they are very detailed and thorough. I am completely satisfied when speaking to Support on any issue or question that we have had," Evans concluded.

**About ISACA**

As an independent, non-profit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.