owasp vulnerable web application testing

As Web applications continue to grow in both on-premise and cloud deployments, several security implications along with security vulnerabilities continue to plague these deployments. Although there are several vulnerability scanners in the marketplace, developers need to test them prior to production level validation. Most of the shareware tools do not perform effectively. A typical security researcher may use a series of testing tools developing in the complexity of the application or platform. The DEVOPS team creating Docker container deployment may develop a new series of tools looking for specific security breaches in this new environment. Most of the free software applications are available as Docker images these days, which makes it easy to use them. WebGoat as an example is available as a Docker image and we can quickly spin up a container.

The security team at a large organization may find themselves overwhelmed by the number of new threats and attacks every day. But there are ways to help them focus on the ones that matter most. One of the simplest things an IT department can do is to regularly scan sites and apps for known vulnerabilities. By doing so, they can quickly identify potential problems and take steps to protect against them. Another thing that helps is having access to a list of common vulnerabilities.

VulnerableApp is built as a project with OWASP, and helped develop this tool for the developer community. This testing tool incorporated a scalable, extensible, easier to integrate with the developed DEVOPS agile framework. Once the developer incorporated VulernableApp into their testing sprints, the DEVOPS and SECOPS teams began to align their strategy around the OWASP application security verification standard or (ASVS).

The OWASP ASVS framework is known across the cybersecurity landscape as a detailed list of security requirements and guidelines which can be used by developers, architects, security experts, tests and even consumers to design, build and test highly secure applications.

The level of engagement with the OWASP ASVS project kept on increasing with time and the culmination of community efforts and feedback led to the introduction of the latest version of ASVS.

Value of the pen testing web applications

Many companies rely on third-party vendors to perform penetration testing. This involves scanning the network and applications to see if hackers could break in and steal data. Organizations can save money by outsourcing this work to experts who know how to spot the most common types of vulnerabilities. All of these methods can help IT teams stay focused on the most important threats.

Pen testing is a great way to find areas of your application with insufficient logging too. Establishing effective monitoring practices is also essential. Pen testing helps ensure the various OPSWAT top 10 security controls against the web applications have been deployed correctly.

Frequent pen testing exposed several known and unknown vulnerabilities within the entire platform including network, application, systems control and monitoring.

- Identifying and addressing vulnerabilities before cybercriminals have the opportunity to take advantage of them.
- A retest is highly recommended after all remediation recommendations have been completed to ensure they are fixed.

After reviewing the results of the pen test, software architects will be able to make decisions about application security along with providing detailed security architecture guidance for ongoing development efforts.

Ultimately, leveraging the continuous pen testing to support the ASVS framework against web applications will help agile development efforts to deliver a level of security assurance, new degree of security application security, and greater protection for executable code. Hybrid code reviews during the agile sprint process will provide greater integration with code scanning by embedding code scanning tools for continuous application source code testing and validation.

Conclusion

Using it as a well-defined metric for application owners and developers who could verify the level of security their applications possessed. Suitable guidance for developers so that they could build effective security controls into their application. *Leveraging pen testing* as an agile sprint work stream is far more effective than a stop gap once a year test cycle.

What makes CYBRI one of the Premier penetration testing companies?

Our outstanding penetration testing company services have attracted several clients that range from small startups to huge multinational companies. We are dedicated to improving cybersecurity across the board, so our services to your organization continue even after the pen test report has been delivered.

No matter the size of your organization, we will assess all of your cybersecurity needs from scratch to provide security measures tailored to your business needs. Our experts are always available to all of our clients in an advisory capacity should you wish to contact us.

Discuss your project with Us!

Click here to go to our site, fill out the form and the engagement team will contact you shortly!

https://cybri.com/red-team/