protiviti®
Global Business Consulting

Application and Software Security

Security Assurance for Software and Applications

With the ever-growing risk landscape, companies face numerous challenges, including:

- **Limited availability** of qualified resources in the market to discover, remediate and report on vulnerabilities
- **Continually evolving landscape** of software and application-based vulnerabilities and exploits
- **Introduction of risk** through deployment of third-party SaaS and commercial off-the-shelf products
- **Compliance-based requirements** may drive testing but may not provide the right level of assurance

How Protiviti Can Help

- Web Application Penetration Test
- Mobile Application Penetration Test
- Source Code Review
- Thick Client Penetration Test
- Web Services/API Penetration Testing

> Application security vulnerabilities are increasingly the first step in successful attack chains and have been behind some of the biggest incidents in recent times.
>
> **— Krissy Safi**
> **Managing Director, Attack & Penetration**

Business Outcomes

- Full understanding of the risks associated with both applications and software that is consumed and created
- Peace of mind that software and application development processes are following secure coding practices
- Confidence that in-house developed applications have been tested and vulnerabilities are correctly understood
- Clear and concise remediation advice to allow for short- and long-term improvements to the security strategy

Application and Software Security

Our Approach and Methodology

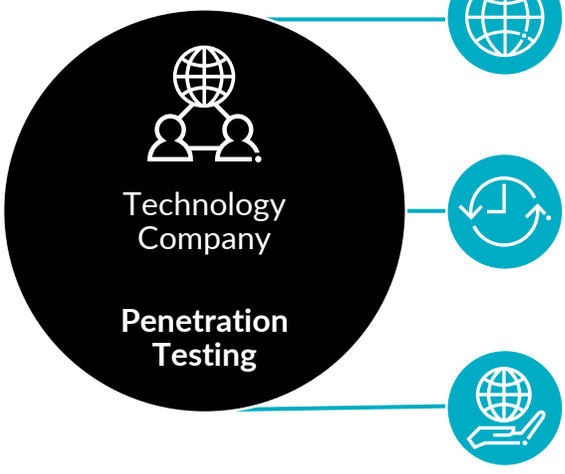
Web Application Penetration Testing: Protiviti will perform testing to identify web application vulnerabilities. With the support of automated tools, we crawl and map the application to understand the threat profile and application structure. A dynamic application assessment will then be conducted, attempting to bypass valid business logic and security controls. Testing against traditional web vulnerabilities, including the OWASP top ten, will be included.

Mobile Application Penetration Testing: Protiviti's mobile application assessment incorporates device level controls and APIs or web services used by the application. This assessment will include verification of the mobile device permissions and file protection analysis to understand if interactions with devices are secure during both runtime and while at rest. We will analyze how the application interacts with the underlying device and operating system and highlight any security concerns and potential business impacts.

Source Code Review: Protiviti will perform manual analysis to understand how data flows throughout the application. This includes an assessment of security controls such as authentication, access control, input validations, sanitization and interfaces to external components. Where appropriate, we will evaluate external dependencies such as APIs and libraries used by the application to ensure those dependencies do not expose the application to additional security risks.

Thick Client Penetration Test: Protiviti will perform static analysis through source code review and, where appropriate, reverse engineering of standalone executables typically installed locally. A thick client assessment will include dynamic analysis by interacting with the installed application. Debugging, monitoring and traffic interception are common activities that support the dynamic assessment phase. Due to the nature of thick client testing, customized tooling may need to be developed to carry out fuzzing and other attacks against the target.

Web Services / API Penetration Testing: Protiviti will perform web services penetration testing supported by automated scanning and tools. This type of test is designed to uncover vulnerabilities in API endpoints. Web services penetration testing is often included as part of a web or mobile application penetration test as those applications may consume data from APIs.



Business Requirement

A global security product company extended their portfolio of SaaS offerings, leading to an increase in exposure for both the product company and their clients. Protiviti carried out a series of penetration tests against the new and legacy offerings, along with a holistic assessment to identify areas that could be targeted by an attacker wishing to compromise the product, company or their clients.

Solution Delivered

Protiviti developed a testing program that allowed our client to gain confidence in the portfolio of services and organizational security posture. We were able to utilize internal subject matter experts in the client's services to remove the need for set up and deployment assistance, removing overheads for our client. Our resources developed holistic security assessments that covered different areas of their organization, including the newly deployed services and cloud solutions.

Business Results

Protiviti identified vulnerabilities in the new products, addressing them prior to release, allowing the new offerings to be launched with the issues remediated. Our client also gained further insight into the risk associated with their legacy products and at an organizational level and how perceived minor vulnerabilities could be chained together in line with real world threats.

Protiviti.com/TechnologyConsulting **TechnologyConsulting@Protiviti.com** **TCblog.Protiviti.com**