Safeguarding Enterprise Web Applications

Abstract

As digital technologies and connected devices become an integral part of the enterprise IT infrastructure, they open up new avenues of attack for threat actors. If successful, these can not only cause expensive data breaches but also attract regulatory penalties. The high tech industry is possibly the most vulnerable sector since they are the leading technology adopters – launching new applications every second. Since web applications today serve as the backbone for supporting mission-critical business processes, there needs to be a more cohesive strategy built-in across the software development life cycle (SDLC).

Most industry experts note a clear disconnect between the way developers and security professionals approach vulnerability testing protocols. Herein, DevSecOp or web application security testing can bridge this gap.

This paper recommends building a dedicated security operations center (SOC) specifically for strengthening the SDLC. This will help developers embed novel, effective defense mechanisms across application layers and continuously improve them through knowledge gained by extensive pen testing.

Ensuring Application Security

While most high tech companies have a well-defined, established SDLC process, security has become a major concern, given the numerous breaches being reported in recent times.

Figure 1 highlights a complete test cycle that should be followed while rolling out new applications.

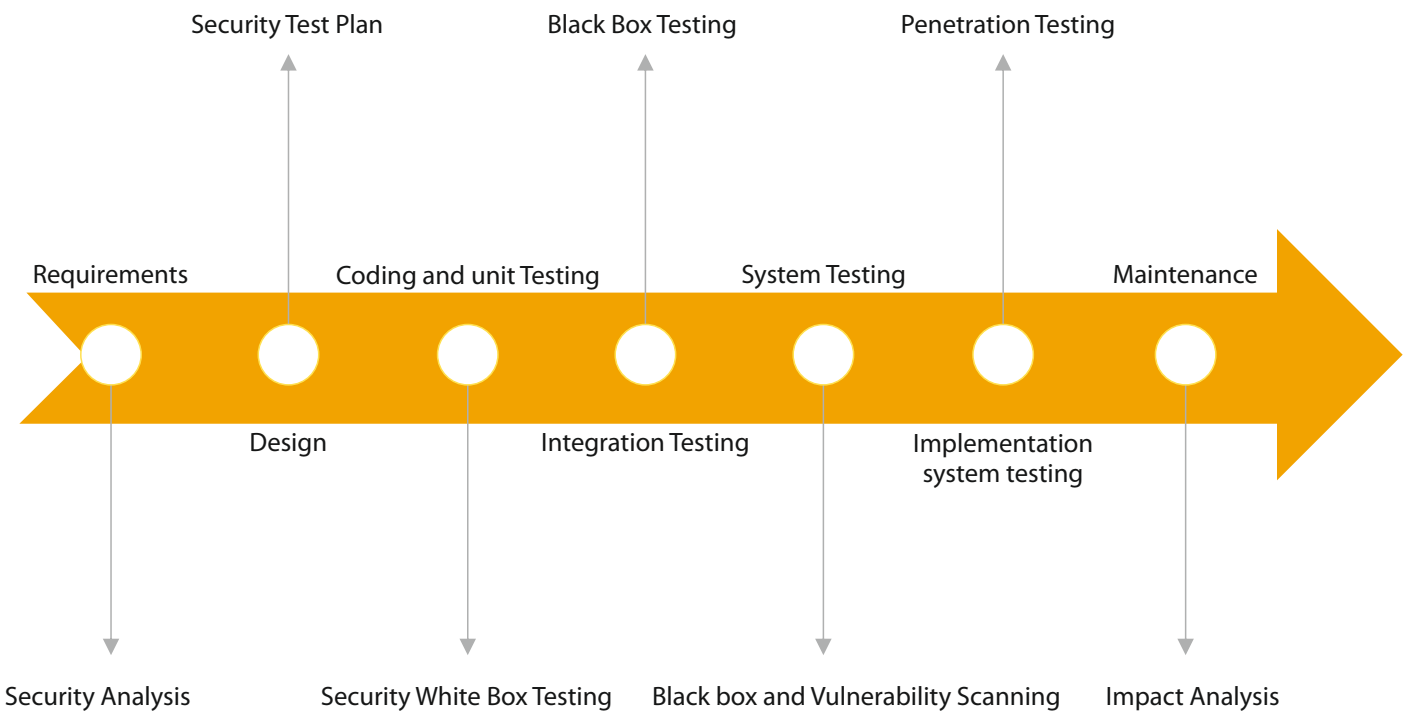

Figure 1: Security Implementation in SDLC Process

Most enterprises often fail to adopt continuous threat monitoring protocols across the lifecycle. Usually, when it comes to the development phase, the delivery deadlines are so short that developers tend to ignore secure code practices. The reasons for this vary, but is mostly attributed to the lack of knowledge. As for the testing phase, this comprises unit, integration, regression, and sanitation tests, which makes it all the more cumbersome to include security related functional and manual test cases against the applications. Some organizations are vigilant about cyber threats across these two phases, but again, fail to do a thorough security check during the planning phase. This is largely because there's hardly any time left when an application finally reaches the security team for sanitization.

To make matters worse, most security teams are either overburdened with numerous tasks including application delivery, or comprise inexperienced testers. To stay on schedule, most change requests (CRs) are ignored, which may need sufficient time and effort to complete from a security perspective.

If anything the recent Equifax data breach has taught us, it's that ensuring enterprise application security during the SDLC process should be a priority across industry. The consumer credit reporting agency reported an impact on 143 million U.S. consumers PII (Personally identifiable information) data due to a CVE-2017-5638 vulnerability in Apache Struts. [1,2]

The need of the hour is a continuous security process as a plug in within the planning, development, and testing phases. This needs to be supported by a dedicated security team comprising experienced and trained specialists working independently of the application development team. To ensure timelines are not stretched, the application security assessment and delivery schedules will need to be synced. The security team will also need to educate the application development team on the latest threats in the industry and guide them on the specific processes for avoiding these across the SDLC phases.

Securing Cloud Native Applications

Let's start by looking at 'cloud native' applications such as containerized applications or applications developed in the form of microservices. These applications, though natively secure, are considered more vulnerable due to their inherent placement techniques in a somewhat multitenant environment. While the cloud environment is generally more secure, most service providers will operate in a shared services-like model when it comes to security. Given the different service providers we have today – AWS, Azure, or Google – it will be effective to plug in services (AWS inspector, Azure Security Center) to the application architecture right from the start.

For microservices, additional checks will be required to monitor and keep track of how different services communicate with each other. The usual standard here is to ensure API interfaces between services, and encryption of any data in transit and data at rest.

These applications will also require fine-grained firewall controls such as API gateways between services. For containerized applications, it becomes important to secure

container configurations and scan static images at the time these are uploaded to the repository during the build process.

Further, even with these measures for cloud native applications in place, one has to actively pen test these application for ensuring complete security. This also means, when these applications are hosted on a public cloud platform, the enterprise's security teams will need to take permission from the provider for penetration testing.

Adopting Vulnerability Scanning and Penetration Testing Practices

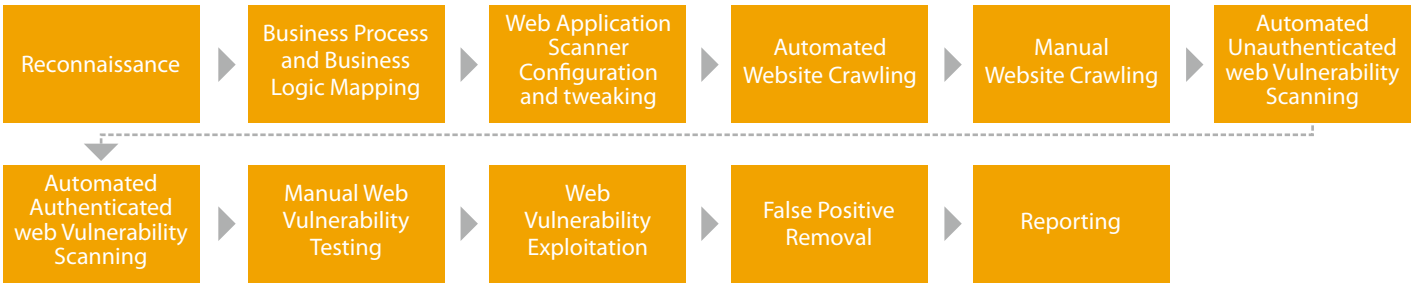

Figure 2: Web Application Security Testing Methodology

When it comes to penetration testing (see Figure 2), methodologies differ across organizations. However, enterprises must follow these processes in a fixed chronological order. The team performing these tasks will need to adopt the mindset of a hacker to gain a wider perspective – particularly keeping in mind the compliance requirements that threat actors effectively navigate to steal data.

An approach would be to explore and exploit the application with deliberate and intuitive thinking. The security team must not only possess the necessary skill set but must also closely examine the application to pinpoint its weakest link. Once identified, these 'weak spots' or vulnerabilities must be exploited to pivot the actual attack across other areas of the application.

Moreover, most applications come with their own set of vulnerabilities. Security specialists will need to extract insights from pen testing and other application evaluation reports that are published on yearly basis to gain a thorough understanding. This information will help teams correctly identify false negatives, which can be tested and patched despite not appearing in the pen test findings.

Table 1 highlights what enterprises need to keep in mind when building a holistic security strategy for their applications.

Building a Cohesive Strategy for Application Security – A Checklist	
1.	Plug-in security in SDLC phases
2.	Dedicated application security team: ▪ With a hacker mindset ▪ Comprising strategists, analysts, and ethical hackers
3.	Security education for developers ▪ Emphasizing on practicing a secure code culture
4.	Extensive use of cloud security services
5.	Fine-grained firewall control for cloud native applications
6.	Security best practices for traditional, containerized, and cloud native applications
7.	Keeping tab on industry hacks, exploits, and top vulnerabilities, such as: ▪ OWASP application security framework ▪ Latest reports on top vulnerabilities and industry or domain specific compliance
8.	Organization and domain specific application security policies

Table 1: A Check List for Ensuring Application Security

Toward an Invulnerable IT Infrastructure

Since the high tech industry is a gatekeeper for cutting-edge platforms and software solutions, enterprises operating in this domain will need to guarantee robust data security for every application they develop. In particular, these companies must protect against:

Zero Day vulnerabilities: This will require constantly exploiting and testing the application's code for vulnerabilities, so that these can be identified early on and patched before hackers can exploit them. This will prevent security events like Spectre and Meltdown.

Session hijacking: A common threat across web application, this must be addressed by undergoing a thorough (established) application security testing mechanism and secure source code review.

But the question that still remains is whether implementing these methodologies can ensure complete protection against breaches. Although they might be capable of providing a good measure of security right now, but as the pace of technological change accelerates, these solutions may be rendered obsolete in the near future.

The focus should be on security systems updated at all times, while defining a time period for retiring them well in advance.

References

[1] Equifax, Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes, September 15, 2017, accessed on March 19, 2018, https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832

[2] Equifax, Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation Of Cybersecurity Incident, October 2, 2017, accessed on March 19, 2018, https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821

About The Authors

Mohd. Anees

Mohd. Anees is a Security Solution Architect with TCS' HiTech business unit. He has an experience of three years in the security domain, and is part of the Cyber Security team within the Digital and Enterprise Transformation group. A passionate ethical hacker, Anees has a B.Tech. degree from KNIT Sultanpur, UP, India, and holds the industry-recognized CompTIA Security+ certification.

Shariq Aijaz Syed

Shariq Aijaz Syed is an Enterprise Architect - Cloud (Hybrid, Public, and Private) with TCS' HiTech business unit. He spearheads cloud transformation initiatives and specializes in AWS Cloud architectures, software defined networking, storage and virtualization. He has extensive experience in hybrid cloud migrations, and designing solution architectures across technology stack spanning Public Cloud – AWS, Storage – NetApp, Servers and Networks.

Syed is an AWS certified solution architect, with additional certifications from VMware, NetApp, Microsoft, and Cisco.

Contact

Visit the Hitech page on www.tcs.com

Email: hitech.marketing@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services I M I 04I 18