Payatu

Web Application Security Assessment Datasheet

OVERVIEW OF THE SERVICE

In around 9 out of 10 web applications, users can be attacked by hackers. Businesses are not just utilizing web applications to smoothen their operations but are also putting their data at risk by overlooking the security aspects of their web apps. Day by day the number of vulnerabilities increases, making web app security assessment a requisite for a reputable, reliable, and revenue-protecting organization.

To identify any critical and high-severity vulnerabilities, a customized web app assessment is necessary as it ensures that these vulnerabilities can be identified and cyberattacks can be fend off beforehand. Payatu tailor-makes the roadmap and execution strategy as per its client's web app and business requirements.

KEY ATTRIBUTES

Payatu's objective is to perform controlled attack and penetration activities to assess the overall level of security of web applications and what sets Payatu apart is -

A combination of realistic and abstract approach

Having substantial experience in this arena paired with learning the application conceptually helps Payatu Bandits to define a process and roadmap specific to the client.

End-to-end defining of the scope

It is important for Payatu to address all types of potential attacks on the client's web apps, which is why its scope covers everything ranging from client-side vulnerabilities, server-side vulnerabilities, business logic vulnerabilities, and APIs endpoints, and all other application-specific configurations, etc.

Ultramodern tech integrations

Payatu strives to widen the attack surface to ensure identification of all vulnerabilities, and it does so by integrating different internal, external, and modern third-party tools and software.

Reports that go beyond reporting

Generalized reporting is a drawback that can make any web application security assessment futile. With Payatu, clients get a detailed report of the test cases that worked, a granular breakdown of the vulnerabilities, failed test cases, mitigation strategies, and recommendations.

The Payatu Extra Mile

Payatu goes an extra mile to retest and revalidate the apps, offer guidance to the in-house security team of the client on the mitigation plan, get the compliance of the application with the mandated standards, and a lot more.

Payatu

KEY BENEFITS

It is important for clients to identify issues and risks that threaten the confidentiality, integrity and availability of web applications, and it is equally important for Payatu to deliver on the same.

01 Protection against Potential Attacks

Identifying security gaps can help clients protect themselves against attacks and vulnerabilities such as DoS attacks, Cross-site scripting and forgery, Code Injection vulnerabilities, Brute force attacks, business logic flaws, etc.

02 Data Integrity is Ensured by Checking Encryption

To ensure that the clients have complete control over the integrity of their data, encryption checks are performed. The encryption check will look for weak/no encryption being used by applications to encrypt customer data/metadata and store or use the same for its own purpose.

03 Reduced Risk with Access Control Checks

In order to help the client with reducing several risks such as insider threat and sabotage, data loss/leakage, and compliance violations, applications are tested for poor access control to resources. In this test, Payatu looks for different levels of user privileges escalations which include both horizontal and vertical level privilege escalations.

04 Identification of Information Leakage to Protect Brand Reputation

Data breaches are the most common incidents that can damage corporate reputation. Payatu makes sure to check for any kind of information leakage happening in normal as well as abnormal communication with the application.

05 Granular Understanding via Extensive Documentation

In the documentation, the details of the test cases, Scan results, vulnerabilities found, and proof of vulnerabilities are captured along with an overview of the current security state of the target and how the customer can improve it.

06 Build Brand Confidence for Users

Clients can make security their value proposition in the competitive digital market by establishing trust within their users/clients by offering security as their brands' proposition.

07 High-Quality Testing

9 out of 10 industry leaders have made it a point to recommend Payatu's services to other pioneers because of the experiences they had while getting their applications tested. This has been made possible because of the best-in-class hires who have proved their mettle by going beyond their scope of work, even before they're hired.

Top Customers

amazon pay BCG NXP TATA DIGITAL

Payatu

ENGAGEMENT MODELS

You choose what works best for you!

Payatu offers different engagement models to let the client decide what floats their boat when they avail themselves of the web application security assessment service. They can choose from

01

Time-boxed Approach,

where the client shares the details of the scope of assessment with Payatu and the service provider evaluates the time and investment required to execute the project. This evaluation is done with the help of complexity models

Low Complexity	Medium Complexity	High Complexity
1-25 web pages/APIs 1-2 user roles	26-75 web pages/APIs 2-3 user roles	76-200 web pages/APIs 4-6 user roles
min. 5-mandays	**min. 10-mandays**	**min. 15-mandays**

For web pages/APIs > 200, a **custom complexity model** is generated by Payatu.

02

Staff Augmentation,

where the client leverages the skillset of Payatu's security consultants and has them work with their in-house security team for an agreed-upon period of time.

03

Master Services Agreement

Minimum duration & projects commitment,

where Payatu conducts a T-shirt sizing of the client-proposed minimum scope and classifies each project as per complexity.

Minimum T&M effort commitment,

where Payatu proposes investment mapped with resource skill, resource experience, duration of T&M engagement, based on the client-proposed minimum commitment.