Privia SECURITY

Web Application Security Service

Professional Offensive Security Services

"Take Your Application Security One Step Ahead!"

The information contained in this document is related to the Professional Offensive Services provided by Privia Security Information and Consulting Services and is of a general nature. All information presented in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“We offer a secure experience in the digital world by detecting potential vulnerabilities in web applications. Make your applications more secure against cyber threats with Privia Security's expert team.”

Our social engineering service aims to reveal the weak points of your organization by simulating threats targeting your employees. Social Engineering service is critical to emphasize the role of the human factor in cyber security. It increases the information security awareness of your employees through realistic scenarios.

Simulations are designed to include phishing emails, phone scams and other social engineering techniques. By experiencing how to react to such attacks, employees become better prepared for these threats. The data obtained is used to identify vulnerabilities and improve security training.

Our social engineering service not only identifies vulnerabilities, but also aims to raise security awareness within the organization. Through simulations, employees learn the methods of attackers and become better equipped to ensure their personal security. This significantly strengthens your organization's cybersecurity posture.

Service Components

Application Analysis

The architecture, components and functionality of web applications are analyzed in detail. In this process, potential risks that may lead to security vulnerabilities are identified and areas where improvements can be made are identified and reported.

Authentication and Authorization

User authentication and authorization processes are evaluated and security weaknesses are revealed. User information is protected and security mechanisms are strengthened to prevent unauthorized access.

Data Security

Data processing and storage methods in the application are examined to ensure the security of sensitive data. Data encryption and protection methods are tested to ensure the confidentiality of user and system data.

Communication Security

All channels through which applications communicate with the outside world are tested to ensure the security of data traffic. Encryption protocols are tested to protect data integrity in network communication and prevent unauthorized access.

Vulnerability Detection and Reporting

Security vulnerabilities detected in web applications are classified according to their severity and presented in a detailed report. The report includes the effects of each vulnerability, methods of elimination and solution suggestions. The report also provides guidance for increasing the level of cyber security.

Security Standards Compliance Assessment

Applications are supported to comply with regulatory and sectoral security standards such as PCI DSS, GDPR, ISO 27001, BRSA, EMRA, CMB and SGT. In order to comply with the regulations, the necessary security measures are determined and recommendations are provided to create a structure that is fully compliant with the regulations.

FAQ

What is Web Application Security Testing?

Web application security testing is a set of tests performed to evaluate the resilience of an application against cyber attacks. With the tests performed, vulnerabilities such as SQL injection, XSS and authentication vulnerabilities are detected. Tests are performed with manual and automated tools. The aim is to identify application vulnerabilities, minimize risks and ensure that the application becomes secure.

What is OWASP Top 10 and Why is it Important?

The OWASP Top 10 lists the most critical security risks common to web applications. Threats such as SQL injection, lack of authentication and XSS are included in this list. OWASP provides guidance to developers and security teams to prevent common mistakes. The OWASP list is considered the essential reference point for application security.

What is SQL Injection and How to Avoid It?

SQL injection is the name given to the method of gaining unauthorized access to the database using offensive SQL commands. SQL Injection can be prevented with parameterized queries and data validation methods. Avoiding dynamic SQL commands increases security. The risk of attack is reduced by implementing strong input validation policies.

What is XSS (Cross-Site Scripting) and How to Prevent It?

XSS is an attack technique that allows malicious code to be executed in users' browsers. Input validation, content security policy (CSP) and output encoding are used to prevent these attacks. There are three types of XSS attacks: Reflected, Stored and DOM Based XSS. Each requires different protection methods and should be checked with regular tests. In addition, Web Application Firewalls (WAFs) are actively used to detect and prevent these attacks.

What is the Difference Between Penetration Testing and Vulnerability Scanning?

Vulnerability scanning is a method of scanning for known vulnerabilities using automated tools. Penetration testing evaluates the impact of vulnerabilities by simulating real attack scenarios. Penetration tests include vulnerability tests. Vulnerability scans are fast but have limited detection and the vulnerability has a higher false/positive probability. Penetration tests are more detailed but require more time and expertise and have a lower probability of false/positive findings.

How to Prevent CSRF (Cross-Site Request Forgery) Attacks?

CSRF is a type of attack that causes transactions to be performed without the user's knowledge. Anti-CSRF can be prevented with token usage and referer header validation. It requires strict measures, especially in critical areas such as banking applications. It is also recommended to use additional verification methods for user transactions.

Why Session Management is Critical

Session management provides protection against attacks such as Session Fixation and Session Hijacking. Short session durations and encrypted session IDs are used for secure sessions. Cookies are only transmitted on secure connections. Sessions should be automatically terminated after periods of time when the user has not taken any action.

What Actions Should Be Taken After Security Tests?

After testing, identified vulnerabilities need to be prioritized and closed quickly. The improvement process is accelerated by providing detailed reports to developers. Planned solutions are implemented to eliminate vulnerabilities. At the same time, periodic testing against new threats is recommended.

What Steps Should Be Taken to Ensure Web Application Security?

The first step to ensure web application security is to adopt secure coding standards and teach developers to write code in accordance with OWASP guidelines. Multi-factor authentication (MFA) and encrypted session management provide effective protection against threats such as phishing. Regular vulnerability scans and penetration tests are conducted to monitor the security status of the application. At the same time, keeping system components up-to-date and providing user awareness training ensures preparedness against new threats.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You," we bring a fresh, innovative perspective to security and privacy—

Privia
SECURITY