SALUS

CYBER

APPLICATION SECURITY SERVICES

WWW.SALUSCYBER.COM

PROTECT YOUR WEBSITES AND ONLINE SERVICES

Web applications are used everywhere in today's digital world. And businesses' are no exception. From CRM systems to customer-facing portals, they are key components of working life.

They also make a very desirable target for cyber criminals, due to their connectivity across numerous internal resources and databases.

Understanding the threats

There are a number of well-known web application security threats such as:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures

Source code is often manipulated and weaknesses in APIs are exploited. Usually this is to gain valuable rewards such as private and sensitive data or intellectual property assets. Web application attacks are also easy to execute, often targeting a large volume of assets at any one time.

A failure to implement a secure development lifecycle around your web applications could leave you open to an attack. It's crucial that you build the appropriate security processes to reduce your vulnerabilities.

APPLICATION SECURITY SERVICES

Web Application Penetration Test

Web Application tests are used to identify vulnerabilities within web applications, and the potential risk presented to the organisation as a result of utilising them. This will consist of a holistic web application test, designed to evaluate all aspects of the web application including authentication best-practice, through to issues affecting specific versions of supporting libraries.

In addition to issues affecting the application itself, our consultants have extensive experience in identifying data protection issues concerning legal requirements, and organisation-specific security best-practices.

We use the best-practice Web Security Testing Guide as defined by OWASP. For more details on web-based vulnerabilities, refer to the following: **http://www.owasp.org**

API Testing

API tests are used to identify vulnerabilities within web-based APIs, and the potential risk presented to the organisation because of implementing them.

This will consist of a holistic test, designed to evaluate all aspects of the API, including authentication mechanisms, input validation issues, and logical flaws.

Our methodology is based on OWASP best-practices, and is designed to logically explore and enumerate all vulnerabilities present within the API.

APPLICATION SECURITY SERVICES

Container and Orchestration Review

Orchestration and Containerisation is fast becoming the preferred way to deploy and maintain complex application and computation environments whilst retaining consistency across differing infrastructure. Salus Cyber has experience in both utilizing orchestration tools in internal development projects, as well as auditing clients' systems.

This testing searches for configuration errors in both the container engine configuration, in addition to the containers under review, affecting a broad subset of security considerations including appropriate configuration of file permissions, built-in security features of the specific container engine, and the adherence to overall cyber security best-practice within the environment, including the principle-of-least-privilege and the use of defence-in-depth.

Our review process is based on accepted best-practice, and is considered a 'review', meaning no interaction with the environment is conducted except for that required to confirm the issues specified in the methodology. Consultants use a combination of configuration file reviews, in addition to 'live' reviews of the functioning environment where necessary to ensure your deployed environment, and deployment process, is secure.

Mobile Application Testing

Mobile application tests aim to identify any security vulnerabilities present as a result of insecure coding of mobile interfaces. Our mobile testing methodology is based on the OWASP Mobile Testing Guide, and covers both on-host security considerations, in addition to network-based attack vectors.

Our testing includes identifying unintentionally exposed sensitive data through methods such as logging or unprotected screens. This may also include attempts to manipulate the application behaviour through broadcast receivers, input validation issues and other potentially vulnerable locations. This also identifies any network endpoints within scope that may then be subject to API or web application testing.

We will also take time to understand any best-practice issues affecting the configuration of the application through files such as AndroidManifest.xml.

Each application is reviewed according to the platform on which it runs, with platform specific security considerations tested for as a matter of course.

APPLICATION SECURITY SERVICES

Thick Client Application Test

Thick client application testing is used to assess the security of an installable application. Such an application typically installs locally to a laptop or desktop system but may also interact with application servers and/or databases, which can also fall within the scope of an assessment. Testing considers elements such as user rights & password policies, applied software updates along with any running services necessary to the application's execution. The outcome is to identify the potential risk presented to the organisation as a result of utilising them.

This will consist of a holistic evaluation of the software, including static and dynamic testing, including looking at data held in memory, held on storage, and transferred across the network. Remote network services may also be tested as part of this to identify any vulnerabilities therein, in addition to issues affecting the application itself.

The application will be evaluated from the perspective of an ordinary application user. Any available documentation will be examined, and a detailed understanding of the application functionality will be established. Potential threats and attack vectors will be identified to position the later stages of the test effectively. Any functionality will be thoroughly checked for weaknesses including, but not limited to, SQL injection, cross-site scripting and logic errors which might facilitate unauthorised access to the application or data.

APPLICATION SECURITY SERVICES

Manual Secure Code Review

Salus Cyber will determine the area of review, depth of audit and timeline depending on requirements specified by the code reviewer and client. The area of review will depend on type of code (technology, platform) and application logic being implemented. At this stage, the security requirements of the application and its intended behaviour will be discussed.

The first stage of code review is intended to familiarise the consultant with the codebase, as such any documentation such as interface definitions, UML diagrams will be used by the consultant to explore the codebase and gain a thorough understanding of the application.

Once performed the consultant can then identify architectural and design choices made by the client during development, ensuring they match client requirements and don't present a security risk.

Further to this, the consultant will then use automated tooling to identify known 'dangerous' functions or libraries that may present a security risk when used incorrectly, and then manually trace back the original inputs and any data validation for those. This ensures the inputs for any potentially dangerous functions are used securely.

Automated Secure Code Review

Salus Cyber will determine the area of review, depth of audit and timeline depending on requirements specified and realised by the code reviewer and client. The area of review will depend on type of code (technology, platform) and application logic being implemented. At this stage, the security requirements of the application and its intended behaviour will be discussed.

Interesting areas within the code will be identified using automated source code scanning utilities. Potential areas of vulnerability flagged by the code scanning utilities will be further drilled down in subsequent stages.

Code for each component of the application will be evaluated by deriving various input zones and trust boundaries. Coverage will be ensured by examining vulnerabilities corresponding to application logic and the development platform. Issues flagged by the code scanning utility will also be reviewed.

SALUS

CYBER

APPLICATION SECURITY SERVICES

WWW.SALUSCYBER.COM
01242 374087

CYBER ESSENTIALS CERTIFIED PLUS

THE CYBER SCHEME

Assured Service Provider
in association with National Cyber Security Centre

CHECK
IT Health Check Service

Crown Commercial Service Supplier

ISOQAR REGISTERED
UKAS MANAGEMENT SYSTEMS 0026
Certificate Number 18737
ISO 9001