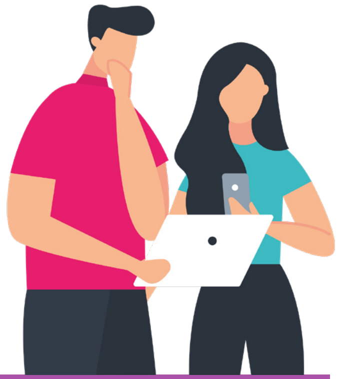
Web Application Health Check

Most organisations have an online presence, with a website or web application. Sites can vary in complexity from those holding read-only public information to highly bespoke applications with a large number of functions and forms that process all types of sensitive information.

The more complex an application, the greater the risk the software can be subverted or forced to behave in a manner it was not intended to. Web applications are often highly visible online and vulnerable to cyber criminals and hackers seeking to gain access to sensitive data or internal systems. Web applications are the most likely openly accessible service to hold personally identifiable information, making them a significant target for hackers.



The Service

Web applications are often the first port of call for a malicious individual targeting a company or organisation for attack. Due to the large volumes of traffic directed towards most web applications, malicious attacks often go unnoticed until they are successful and adverse effects are experienced. To reduce the risk of compromise, it is imperative to design and secure web applications to a very high standard and monitor all audit logs.

With over 30 years' experience conducting application penetration tests, we can assess your web applications and supporting environment to discover vulnerabilities or exploitable conditions. To determine risks posed by external and insider threats, we conduct testing from authenticated and unauthenticated standpoints.

Stage 1:
Our Methodology

Our application testing methodology is based on OWASP principles and tests for the OWASP Top Ten threats as a minimum.

Our Web Application Security Review is designed to identify notable security issues within a web application before malicious users find and exploit them. We have one of the industry's longest-standing penetration testing teams and are continuously evolving testing methodologies backed by industry recognised vulnerability awareness (OWASP Top 10 and SANS CWE/25). We use a combination of manual testing and automated testing to ensure all areas of the application are thoroughly tested. Typical areas tested include injection attacks (SWL injection, HTML injection etc), cross site scripting, error handling, malicious file uploads and authentication bypasses and weaknesses.

Our consultants will thoroughly test web sites, web applications and associated Application Programming Interfaces (APIs) inside and outside of expected user journeys.

Stage 2:
What we test

- Blended web application security testing
- Business logic testing
- Recent findings
- Federated access/SAML authentication testing
- User access testing
- Role access testing
- Inter-organisation access testing
- File upload validation
- Web services/API testing

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation

Stage 3:
Reporting

As a result of the application test, MTI will provide detailed issue descriptions and recommendations for remediation within a formal report upon completion of the test. The report will be led by Executive and Technical summaries to ensure results are accessible to all stakeholders, regardless of technical background.

A Remediation Action Plan is also supplied to enable the tracking and remediation progress of issues identified within the application, and the issue owners.

Service Deliverables include:

The web application health check provides:

- A formal report with detailed issue descriptions and recommendations for remediation.
- An action plan that details the stages to help you track your remediation progress.
- Executive and technical summaries that can be used to make results accessible to all stakeholders and justify expenditure to improve security.
- An outline of your path to make web applications more secure.

If there is a requirement to retest the application following the assessment to determine if applied remediation steps have been successful, we can perform either point retests or complete retests, depending on the volume of vulnerabilities identified within the original report.

A Remediation Action Plan is also supplied to enable the tracking and remediation progress of issues identified within the application, and the issue owners.

Outcomes & Benefits

Our web application health check delivers the following outcomes:

- Identifies notable security issues within a web application before malicious users find and exploit them.
- Provides a thorough test of web sites, web applications and associated APIs inside and outside of expected user journeys.
- Provides peace of mind by discovering vulnerabilities and outlining how they can be addressed.

> "Engaging and working with MTI performing our recurring penetration testing was a very smooth experience. The team quickly understood our specific needs, the technical environment, and any specific test scenarios we requested. Good feedback from the consultants during the actual penetration test and a very professional report with vulnerabilities in order of priority and suggested corrective measures. All in all a job well done."
>
> Michael Zetterlund
> Chief Product Officer
> Ariane Systems

Why MTI?

MTI has been conducting penetration testing for more than 30 years. As one of the first companies to provide this service, we have developed a wealth of knowledge and skills in the tactics used by malicious users to gain access to corporate networks. This enables us to identify risks to the business and outline remediation measures to counter them. If required, you can take advantage of our expertise to implement the necessary remediation measures via our professional services operation.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation