Cyber Security Website Vulnerability Testing Datasheet

About Cyber Security Website Vulnerability Testing:

Customer's websites are one of the primary threat surfaces that cyber-attackers seek to exploit in order to penetrate a customer's information system infrastructure.

Website vulnerability testing is a service focussed on testing a customer's website for security vulnerabilities that could be exploited by these cyber attackers. The test scope covers a broad range of tests including an assessment of the top 13 OWASP listed security vulnerabilities found on web-sites today. The testing is not limited to specific website development languages or web-server technology.

The tests are also an important part of any organisation's regulatory compliance programme and most cyber security standards require that a customer's website should be assessed on at least on an annual basis.

The tests are not automated tests and involve the use of expert cyber penetration team members to ensure full test coverage regardless of the test environment. The test includes a full test report that will be produced for the customer and the test expert/s will be made available via a WebEx conference call to discuss the results and provide guidance on ways that the customer can mitigate any identified vulnerabilities.

Target Audience:

Chief Information / Chief Risk / Chief Security Officers, IT management.

Key Benefits:

The website cyber vulnerability assessment will provide customers with:

- ✓ A thorough assessment of the security vulnerabilities of their website;
- ✓ A vulnerability risk register and supporting evidence of the exploit used;
- ✓ A set of priority steps to take in order to mitigate the identified risks and
- ✓ Guidance on how to address the identified issues.

Tests Covered Include:

- ✓ Review of site architecture, design considerations and security configurations;
- ✓ Authentication and session security management, user management and auditing;
- ✓ Cross Site Scripting (XSS) and Cross Site Request Forgery (XSRF);
- ✓ Insecure Direct Object references, URL access restrictions, redirects and forwarding validations;
- ✓ System and code vulnerabilities;
- ✓ Cryptographic usage and storage and
- ✓ Denial of Service and transport level security issues

Customer Benefits:

- ✓ Comprehhensive test report including a management summary, a detailed risk register, prioritised remediation process and technical details and evidence for the outcomes of each test; and

- ✓ A technical and managerial results review with the team conducting the test to provide clarity on the identified vulnerabilities and advice on the best practice remediation steps that can be implemented.

Contact information:

For further information about this course please contact Dr Graham Wright at-

Mobile: +27 83 252 5727

Email: Grahamw@gnlcyber.com