CONFIRMATION OF PENETRATION & VULNERABILITY TESTING

Date of Test: December 10, 2019

Performed By: Bob Shantz
Director of Infrastructure & Cloud Services

Penetration & vulnerability testing is performed annually on CGC's Cloud Hosted Environment utilizing third party tools in order to identify and exploit vulnerabilities. The types of tests and results are also provided to our SOC auditor. Below are the test types and findings resulting from tests conducted on the date specified above:

Tests Performed	Results
✓ Fingerprint web server software	✓ No fingerprinting software or technology found
✓ Analyze HTTP headers for security misconfiguration	✓ No security misconfiguration found
✓ Check the security of HTTP cookies	✓ No security issue found regarding HTTP cookies
✓ Check the SSL certificate of the server	✓ Communication is secure
✓ Check if the server software is affected by known vulnerabilities	✓ No vulnerabilities found for server-side software
✓ Analyze robots.txt for interesting URLs	✓ Robots.txt file not found
✓ Check whether a client access file exists, and if it contains a wildcard entry (clientaccesspolicy.xml, crossdomain.xml)	✓ No security issue found regarding client access policies
✓ Discover server configuration problems such as Directory Listing	✓ Directory listing not found
✓ Check for password auto-complete	✓ No password input found (auto-complete test)
✓ Check for clear-text submission of password	✓ No password input found (clear-test submission test)

Result: 10/10

Note: CGC hosted customers are welcome to carry out security assessments and penetration tests against their specific cloud hosted eCMS environment. We ask that customers first notify CGC of the date, time and types of testing that will be performed.