RESPONSIBLE DISCLOSURE POLICY

Qualys, Inc has great concern for the security of its cloud platform, application and services which we are offering to our customers. If you are a security researcher and have discovered a security vulnerability in one of our services, we appreciate your help in disclosing it to us in a responsible manner. We will validate and fix vulnerabilities in accordance with our policies. Qualys reserves all its legal rights in the event of any noncompliance to the applicable laws and regulations.

REPORTING:

If you believe you've found a security issue in one of our products or services, please send it to us on bugreport@qualys.com along with your contact details and include the following in your report:

- A description of the issue and where it is located along with screenshots.
- A description of the steps required to reproduce the issue.

Examples of vulnerabilities include, inter alia:

- Authentication flaws
- Circumventing of platform and/or privacy permissions
- Privilege escalations
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Server-Side request forgery (XSRF)
- Injection Attacks (SQL, XML, Json, etc)
- Business logic Bypass
- Arbitrary redirect
- Server-side code execution (RCE)

RULES FOR FINDING SECURITY VULNERABILITIES

- Take responsibility and act with extreme care and caution.
- When investigating the matter, only use methods or techniques that are compliant with law and necessary in order to find or demonstrate the weaknesses. Without limiting the

generality of the foregoing.

In any event, please refrain from the following:

- Do not use weaknesses you discover for purposes other than your own investigation.
- Do not use social engineering to gain access to a system.
- Do not install any back doors – not even to demonstrate the vulnerability of a system. Back doors will weaken the system's security.
- Do not alter or delete any information in the system. If you need to copy information for your investigation never copy more than you need. If one record is sufficient, do not go any further.
- Do not alter the system in any way.
- Do not share access or details of any vulnerable system with others.
- Do not use brute force techniques, such as repeatedly entering passwords, to gain access to systems.

Also refrain from

- Accessing, Downloading, or Modifying data residing in an account that does not belong to you or attempt to do any of the foregoing
- Executing or Attempting to execute any "Denial of Service" attack
- Posting, transmitting, uploading, linking to, sending, or storing any malicious software;
- Testing in a manner that would result in the sending unsolicited or unauthorized junk mail, spam, pyramid schemes, or other forms of duplicative or unsolicited messages;
- Testing in a manner that would degrade the operation of any Qualys properties; or testing third-party applications, websites, or services that integrate with or link to Qualys properties.
- Issues with out-dated or unpatched browsers
- Lack of the Secure flag on non-sensitive cookies
- Lack of the HTTP Only flag on non-sensitive cookies
- Security vulnerabilities in third-party websites and applications that integrate with issues
- Vulnerabilities requiring a potential victim to install nonstandard software or otherwise take steps to become susceptible to attack
- Social engineering of vulnerabilities requiring very unlikely user interactions
- Findings primarily from social engineering (e.g., phishing, vishing)
- Findings from physical testing such as office access (e.g., open doors, tailgating)
- UI/UX bugs and spelling mistakes
- Spamming
- Disclosure of known public files or directories, (e.g. robots.txt)
- Click-jacking and issues only exploitable through click-jacking
- CSRF on forms that are available to anonymous users (e.g. the contact form)
- Logout Cross-Site Request Forgery (logout CSRF)

- Presence of application or web browser ‘autocomplete’ or ‘save password’ functionality
- SSL Attacks such as BEAST, BREACH, Renegotiation attack
- SSL Forward secrecy not enabled
- SSL Insecure cipher suites
- The Anti-MIME-Sniffing header X-Content-Type-Options
- Missing HTTP security headers

POINTS TO KEEP IN MIND:

- Do not put any customer or Qualys data at risk, degrade any of our system’s performance.
- If your actions are intrusive or an attack on our system, we may act against the same including reporting them to law enforcement agencies.
- Qualys reserves its right to initiate legal action against any person and/or report to relevant authorities of such person who conduct any Tests or investigations which are prohibitive or not in compliance with law or not as per this Policy.

Do not publicly announce the vulnerability but get in touch with us and give us the time to examine the issue. The safety of our customers’ information and assets is our top priority. Therefore, we encourage anyone, who have discovered a vulnerability in our systems to act instantly and help us improve and strengthen the safety of our sites and systems.

OUR RECOGNITION

If you identify a valid security vulnerability in compliance with this Responsible Disclosure Policy, Qualys shall –

- Acknowledge receipt of your vulnerability report
- Work with you to understand and validate the issue
- Address the risk as deemed appropriate by Qualys team
- Work together to prevent cyber-crime.

Qualys will review the submission to determine if the finding is valid and has not been previously reported. Publicly disclosing the submission details of any identified or alleged vulnerability without express written consent from Qualys will deem the submission as noncompliant with this Responsible Disclosure Policy

++++++ END OF DOCUMENT +++++++