Technical Testing - Web Application Testing

eSentire will scan IP addresses or web applications identified by Client for such period of time as set out on the applicable Order Form to identify web application assessment, identify services running on each host, and identify service versions running on each host, as well as:

- Penetration attempts on hosts and/or services identified to have known vulnerabilities;
- Account privilege escalation and subversion;
- Attempt technical security violations of applications (including cross site scripting attacks, cross site referencing, and SQL injection attacks);
- Attempt external infrastructure attacks (excluding denial of service attacks);
- Attempt external data access attacks (including brute force attacks and escalation attacks), cross account data access attacks, cross client site data access attacks, user privilege escalation, and gray box' testing using accounts provided to eSentire by Client; and
- Attempt deep dive exploitation of identified weaknesses in external systems into internal systems.

Web Application Vulnerability Rescan.

eSentire will perform a Web Application Vulnerability Rescan if Client received a one-time or annual recurring Web Application Vulnerability Scan. After remediation activities undertaken by Client have been completed following a Web Application Vulnerability Assessment, eSentire will, no later than three months following eSentire delivering to Client its draft report, rescan only those servers identified by eSentire to have high or critical security issues to validate such remediation.