Securing Your Critical Infrastructure

Web Application Penetration Test

- ASSESS PERIMETER SECURITY
  Determine whether the security perimeter is well defined and if it affords adequate protection.

- ASSESS SYSTEM SECURITY
  Determine whether systems are adequately configured to prevent unauthorized access.

- ASSESS APPLICATION SECURITY
  Determine whether application-level vulnerabilities exist that might enable a user to obtain a level of unauthorized access or to process unauthorized tasks or transactions.

- ASSESS APPLICATION DESIGN/SECURITY PROCESSES
  Analyze whether existing practices are adequate to prevent a reoccurrence of vulnerabilities.

- ANALYZE AND DOCUMENT FINDINGS
  Final analysis and documentation, including findings and recommendations at both a technical and procedural level.

relay
SECURITY GROUP

Service Offering

Details

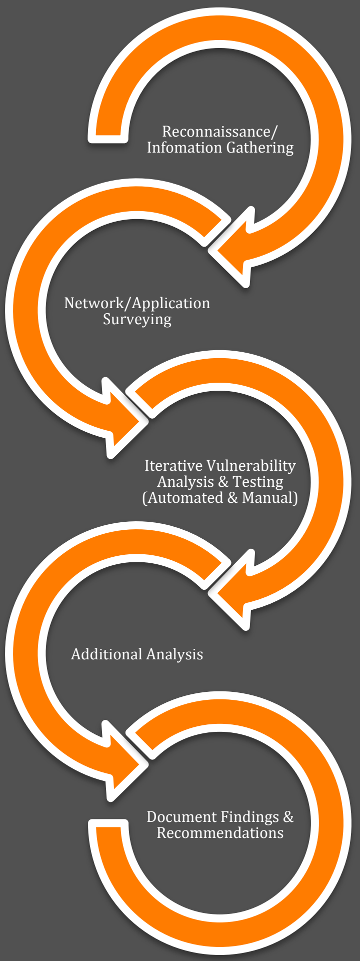
Relay Security Group, LLC (Relay) was founded in 2007 by information security professionals with over twenty years of cumulative IT security experience in a wide range of markets. Our mission is to provide our clients—through actual validation of vulnerabilities and with minimal impact on their often-sensitive operations—with the most accurate information about security threats to their environments and their readiness to meet current industry standards and regulations. Relay's validation methodology, processes, and recommendations take into account the complexities of these environments, which translate to recommendations that are both reasonable and actionable.

Relay's Web Application Penetration Testing services, which uses both the Open Source Security Testing Methodology Manual (OSSTMM) v3.0 in combination with the Open Web Application Security Project (OWASP) guidance will assist a client in identifying whether or not their web applications are poorly configured and if so, what probable attack vectors may be used to either gather information or gain access to the application or system. In addition, the testing helps ensure that future configuration changes or newly discovered vulnerabilities do not further weaken the defense of the web application/system.

The penetration test, which can be conducted as a blind or cooperative effort demonstrates the actual exposures linked with identified vulnerabilities. Relay positioned as an outside attacker (e.g. unauthorized) or as an authorized user (e.g. users with different privilege levels) will attempt manual and automated attempts to exploit weaknesses in the client's web application. No attempts are made to harm or cause degradation to any service, only to demonstrate capabilities of compromise for validation purposes.

Typically, the web application penetration testing process includes:

- Web application scan of relevant web pages;
- Review authentication/authorization;
- Assess component configurations;
- Test data validation;
- Review session management;
- Assess existing encryption;
- If possible, test transport security;
- Test, logging/error handling;
- Review application administration; and
- Conducting an analysis of the data and providing a report outlining the findings and recommendations of the engagement.



3750 Brodie Way Dublin California 94568 ☎ 800.613.0431 ✉ sales@relaysecurity.com WWW.RELAYSECURITY.COM