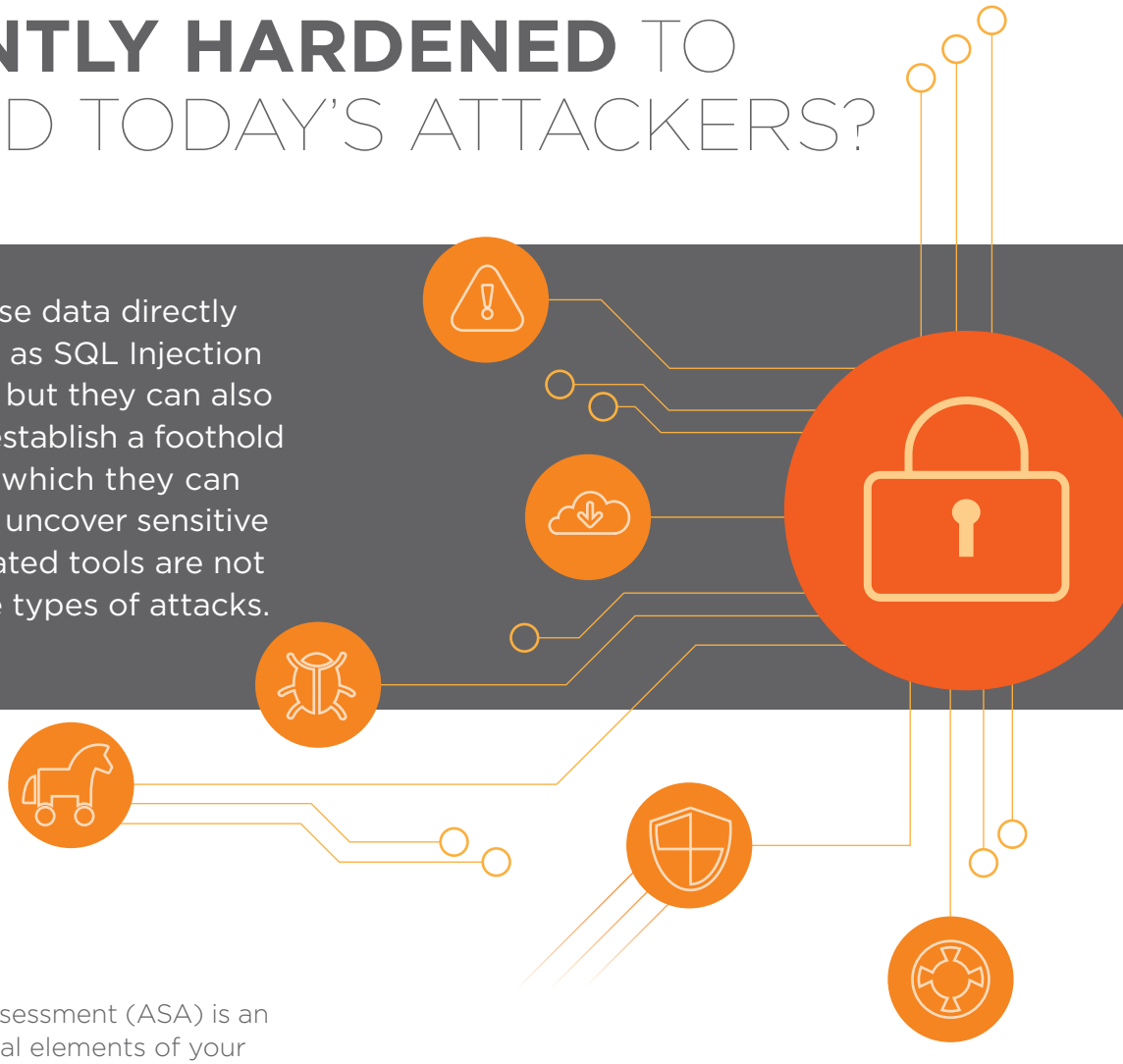
ARE YOUR WEB APPLICATIONS **SUFFICIENTLY HARDENED** TO WITHSTAND TODAY'S ATTACKERS?

Attackers can compromise data directly through techniques such as SQL Injection and Cross Site Scripting, but they can also use web applications to establish a foothold into your network, from which they can pivot to other assets and uncover sensitive or valuable data. Automated tools are not enough to uncover these types of attacks.



A PTP Application Security Assessment (ASA) is an assessment of the transactional elements of your web based application. Applications such as on-line banking, on-line trading, eCommerce, Business to Consumer (B2C), Government to Citizen (G2C), or any other critical application should have a comprehensive assessment of its security posture. A PTP ASA will provide you with confidence that your development team or third party developer has built a secure application and that your organization has demonstrated due diligence in its efforts to protect confidential or sensitive information.

PTP's approach to security assessments begins with established methodologies from organizations like the Open Web Application Security Project (OWASP) and the Institute for Security and Open Methodologies (ISECOM). We apply these methodologies using a balanced combination of automated tools and manual techniques with an emphasis in discovery of vulnerable application logic that cannot be found using an automated approach. Our certified professionals then add their own experience and creativity to provide a real world scenario that would be common in attacks by experienced cyber criminals and state sponsored actors.

SECURITY@PTPINC.COM • 1.800.787.4143

ptp experience transformation

This assessment will uncover vulnerabilities in the areas of:

- Web Server Configuration (IIS, Apache, IBM, Oracle, etc.)
- Authentication and Authorization
- Session Management
- Business Logic
- Transport Security (how data is moved)
- Cache Control (to prevent exposure of sensitive data)
- Data Integrity, Error Handling, and Validation (such as Buffer Overflows, and SQL Injection)
- Web Services (SOAP, WSDL, XML, WCF, RIA)
- AJAX and end-user accessible source-code/script (such as HTML, JavaScript, Flash, and Silverlight)

OWASP maintains a current list of the ten most critical web application security risks. This "Top 10" list will be covered by PTP when we perform an ASA. Examples of some common vulnerabilities in the OWASP Top 10 that an ASA will seek to identify include:

- The compromise of User ID's, passwords, or session credentials through Cross Site Scripting (XSS) attacks
- Full database access through SQL injection attacks resulting in exposure of Personal Privacy or HIPAA data
- User A being able to access User B's account and perform actions such as a transfer of funds from user B's account or placing an online trade (Broken Authentication and Session Management)
- The ability to duplicate legitimate user sessions (Session Cloning) through weak Session Management
- Manipulation of parameter and form variables to view other member or customer data (Insecure Direct Object Reference)
- Third party web sites that can trick a user's browser into performing an action using the user's current session in your web application (Cross Site Request Forgery)
- Post-login forwarding attacks that redirect users to a malicious site (Unvalidated Redirects and Forwards)
- Access to administrative pages by unauthorized users (Missing Function Level Access Control)

Business benefits Include:

- Regulatory compliance where applicable
- Decrease business risk by enhancing overall security posture
- Provide demonstrated due diligence
- Protection of the organization's reputation
- Reduced litigation expenses
- Decrease the expense and publicity of a breach notification
- Often allows for reduced insurance premiums where applicable
- Peace of mind that your application is well hardened
- Increased awareness by developers that will carry over to future development projects

Technical benefits Include:

- A hardened transactional web application that can better resist a concerted application level attack
- Reports that can also serve as guidelines and help educate your developers
- Reduced code refactoring time and expense through early detection and mitigation