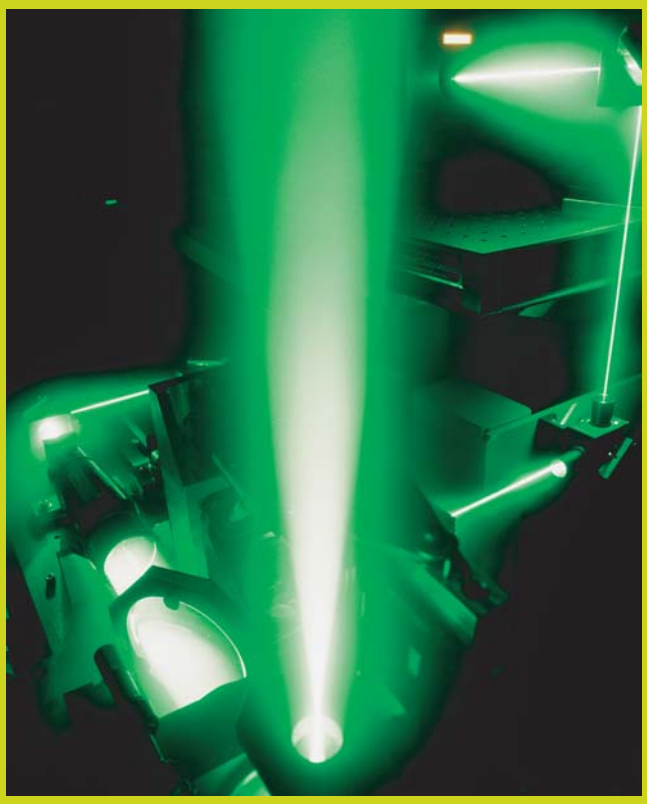
Web Application Penetration Testing



To ensure that your web application interacts with end users only in ways that was intended by the application's developers and that the underlying infrastructure is not vulnerable to attack, PricewaterhouseCoopers has developed the **Web Application Penetration Testing** (WAPT) methodolgy. WAPT is an approach to penetrate web application, which designed to assess each component of your critical web application and infrastructure. Security diagnostic reviews and the use of sophisticated tools probe your web application looking for vulnerabilities and advanced manual hands-on tests to attack your application.

Our Web Application Penetration Testing enables you to:

- Cover and eliminate areas of vulnerability within your web application (whether developed commercially or in-house) resulting from poor coding, misconfiguration of known bugs or weaknesses;
- Assess the possibility of exposure from various points of entry such as external connections via the Internet, external dial-up and other third-party connections;
- Test emerging and legacy systems and applications to ensure that security controls meet corporate policy and thwart hacking attempts;
- Improve you organisation's process of developing security controls and procedures;
- Learn how your security measures improve overtime through repeated penetration tests conducted throughout the year; and
- Gain confidence in your organisation's ability to protect its critical information assets, customer loyalty and brand name.

*connectedthinking

PRICEWATERHOUSECOOPERS

World Class Methodologies, Proven Performance, Trusted Professionals

By combining state-of-the-art web application vulnerability analysis software and the latest tools from the hacker underground, sophisticated techniques, industry knowledge and proven methodologies which help to ensure that your operations are not interrupted, PwC web application security specialists can assess the susceptibility of your web site to a variety of attacks including:

- **Hidden manipulation** — modifying hidden field values
- **Parameter tempering** — altering the parameters passed to an application through a URL
- **Cookie poisoning** — changing cookie files to access sensitive information or impersonate someone else
- **Stealth commanding** — inserting a code in text fields to take control of an application
- **Forceful browsing** — directly accession a web page that can normally only be reached with authentication
- **Backdoor and debug options** — attempting debug syntax on URLs
- **Known vulnerabilities** — widely reported holes in web applications
- **Third-party misconfiguration** — exploiting configuration errors in third party applications such as web or database servers
- **Cross-site scripting** — inserting script languages in a text field that other users can see
- **Buffer overflow** — passing excessive data in an application request

Now you can detect web application security problems quickly and get sound advice on correcting them — with Web Application Penetration Testing from PricewaterhouseCoopers.

To learn more about how we can reduce your company's security risks, please contact:

Pongsak Achakulwisut
Partner
PricewaterhouseCoopers
66 (0) 2344 1120
pongsak.achakulwisut@th.pwc.com
www.pwc.com/thailand