Application Penetration Testing

No application is impervious to malicious threats. Casaba can help identify vulnerabilities and prevent attacks.

Why Application Penetration Testing?

The accessibility of web and mobile applications inevitably comes with a certain level of risk. This risk can be costly, leading to unexpected losses and a lack of compliance. Your level of risk depends on the measures you take to ensure your applications are as secure as they can be.

Casaba's application penetration testing reduces risk and preempts malicious attacks by exposing vulnerabilities before they are exploited. We perform a comprehensive analysis that exposes configuration problems, hardware and software issues, and operational weaknesses that hackers use against you. Then we provide the results of our evaluation, as well as recommended methods of remediation. You'll rest assured knowing your applications are as secure—and your risk as low—as they can be.

Black Box, White Box, or Gray Box?

Some security companies advise the use of "black box" testing—or "blind" testing—where penetration testers work from the outside in, with little or no knowledge of the application to be tested. Others insist that a "white box" approach is more effective, where testers understand the application's design and work directly with the source code.

Casaba believes that both of these methods have their merits, but that neither alone is right for every job. We take a "gray box" approach to penetration testing, weighing the specific needs of a particular client and the application to be tested against the benefits of the different testing methods. Ultimately, our test programs include the best elements of both.

Get Started

Contact us today for a free consultation and security review.

- Phone: 888.869.6708
- Email: info@casaba.com
- Web: www.casaba.com

Get Our Tools

Grab our free tools for your own testing program.

- Watcher

http://websecuritytool.codeplex.com/

- X5S

http://xss.codeplex.com/

What We Test

- User Interface
- Authentication
- Authorization
- Session Management
- Input Validation and Sanitation
- Information Disclosure
- Integrity
- Transport and Protocol
- Business Logic
- Internationalization
- Stability and Availability

Tools or Manual Testing?

Because penetration testing requires simulating repeated attack attempts on different parts of an application's surface, many security specialists rely on automated tools to do the job. Some of these tools are very effective, but no single tool is a standalone solution.

At Casaba, we use tools to augment our manual testing process, allowing us to cover more of an application's surface while we focus our attention on the areas that need it most. In fact, we have developed two of our own tools: *Watcher*—an industry-leading passive scanner, and *X5s*—an active testing tool for identifying cross-site scripting. We also often create custom tools to meet specific project needs and deliver these to our clients for their ongoing use.

Reverse Engineering

An application's security, to a great extent, depends upon how difficult it is for hackers to figure out. Casaba can review and test the measures you use to prevent reverse engineering, such as cryptographic protections, control-flow obfuscation, and anti-debugging. We can help ensure any hardening efforts you employ do indeed protect your intellectual property and functionality.

Results and Deliverables

Upon completion, Casaba delivers a report that catalogs your application's strengths and weaknesses, documents bugs and vulnerabilities, and recommends improvement measures. We also deliver any custom tools and test cases that were developed for testing. Finally, we debrief your management and development teams in person if desired.

About Casaba

Casaba is a strongly integrated team of security pioneers with a reputation for relentlessly researching, developing, and implementing innovative solutions to the most difficult security problems. We are prepared to assist in every phase of security consulting and auditing, and we are fully bonded and insured by Lloyds of London.

Flexibility

Applications come in all shapes and sizes, and business requirements differ. Casaba can tailor an application penetration testing program to meet your specific needs—from one day to several months, working on site or remotely from our offices.

Compliance

Casaba's application penetration testing meets the requirements of the Payment Card Industry Data Security Standard (PCI DSS), the Federal Information Security Management Act of 2002 (FISMA), and other important industry standards.

casaba