

Web App Penetration Testing

www.clone-systems.com

The Ultimate Web App Safety Litmus Test

Think of a Web App Penetration Test as an audit by a group of the world's most accomplished hackers. Our network engineers connect to your site and proceed to needle, probe, poke, and assault your online apps in every way they can image. We know all the tricks the bad guys use, and our getting their first is the best preventative strategy for their ever appearing where they don't belong.

Whereas our CG-WebScan® vulnerability test will provide you with a structural understanding of weak points in your web infrastructure, CG-WebPenT® goes microscopic on all layers of your data, the data interactions, the network entry points, the exploitable areas of the HTTP protocol stack, memory management, and shared components used by multiple applications. Penetration testing is a wholesale attempt to modify your system in as many ways as it permits. How it can be modified suggests to us all of the ways it can also be compromised by a hacker.

Clone Guard® CG-WebPenT® Solution

CG-WebPenT®, not surprisingly, takes as long as seven days to perform. When all tests are concluded we will provide you complete documentation of the flaws detected and the remediation results for those flaws. After 30 days, we will run another scan on the areas flagged during testing to assure that the issues have been effectively resolved. Of course we can also help you determine the best solutions to use for securing the network. After the second scan reveals no security anomalies, we provide your organization a Web Penetration Test report and a certification that all web applications are optimized against external-facing security breaches.

Multi-Vendor Support



CG-WebPenT® Features

The most intensive examination of your web applications and all interrelated entities currently in existence.

Exhaustive audit of Environmental, Input, and Data/Logic application components. Detects the following security issues:

- Shared memory resources;
- Registry dependencies and changes;
- Application/web service relationships;
- Shared software resources (DLLs, etc.);
- All types of exposed communications functionality;
- XSS script routines;
- SQL injection;
- Embedded test accounts and APIs in an application;
- Logic flaws in authorization;
- Denial of service; and much more.

Detailed reports are generated for each functional area of the application describing its weaknesses and how they can be exploited.

Clone Systems assures all web applications tested are secure by performing a second scan after 30 days.