



WEB APPLICATION SECURITY

OWASP (Open Web Application Security Project) is a community project about web security implicating several members from all business sectors. In other words, all methodology documents, articles and tools are created by the community and are free of any rights.

The **OWASP** foundation is a non-profit organization without ties to any IT companies. Its most popular documents are the "OWASP guide to building secure web applications v2" and the "OWASP top 10".

In order to carry out rigorous website evaluations, **Virtual Guardian** follows the **OWASP** methodology guide. This guide describes the industry's best practices relating to website creation. **Virtual Guardian** experts also use the guide to validate a website's security level. Finally, there will be a validation of all development procedures to pinpoint each and every weakness in order to correct them. Here is a short summary of the different test categories the guide refers to as well as the impact of those tests on your website's security.

Test category	Impacts
<i>Input parameters</i>	Each application parameter is a potentially dangerous opening to hackers. The received parameters as well as the process are considered « at risk » elements because hackers can use these openings to gain direct access to web applications or servers.
<i>Access control</i>	If access control is faulty or not well protected, a malevolent person can easily get into your system to gain access to sensitive information.
<i>Session management</i>	Can a hacker steal another user's identity and modify its parameters to gain unauthorized access to your information system? Session management reduces this risk.
<i>Cross Site Scripting (XSS)</i>	A successful XSS attack can enable hackers to submit false information to unsuspecting users and ultimately obtain confidential information about that user.
<i>Buffer Overflow</i>	This technique implies sending more information to the system than it can handle. This can render the application vulnerable especially if the hacker gains control of it.
<i>Command injection</i>	This is another external technique where the system can't validate all the information it receives. The risk here is that the hacker can modify the original parameters or even add false parameters to the original ones.
<i>Error management</i>	It is important that all information about a system error given to a user must not contain any information, technical or otherwise, about the application itself.
<i>Log management</i>	The main objective of log management consists of finding the origins of an event that happened in an application. Without an adequate log of errors, attacks can be performed unbeknownst to system administrators.
<i>Encryption</i>	Unfortunately, badly configured encryption modules are commonplace. This causes your's system's perimeter defense to be weak.

Source : http://www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents

**Do you need to evaluate the security of your web applications?
Contact Virtual Guardian today to get a free estimate!**



WEB APPLICATION ANALYSIS: THE VIRTUAL GUARDIAN WAY

Evaluating delays and costs is not always an easy task in the IT security field. This difficulty is even greater when dealing with web applications due to the intangible aspect of the task. To try to resolve this situation and at least give ballpark estimates of delays and costs, **Virtual Guardian** developed a three-leveled methodology. This system allows our clients to match the level of analysis depth they are seeking with their available budget.

This methodology still only gives estimates⁽¹⁾, but short of the customer supplying us with extremely detailed information regarding their application, these estimates are considered fair.

TYPES	« LIGHT »			« CLASSIC »		« DEEP »	
	2 to 5 days	4 to 8 days	9+ days	4 to 8 days	9+ days	4 to 8 days	9+ days
Delay (estimated)⁽²⁾	Very wide but not very deep (targets 60% of vulnerabilities)	Wide and deep (targets 85% of vulnerabilities)	Wide and very deep (targets 95% of vulnerabilities)				
Scope	✓	✓	✓	✓	✓	✓	✓
Automatic vulnerability scanning	✓	✓	✓	✓	✓	✓	✓
False positives validation	✓	✓	✓	✓	✓	✓	✓
OWASP test: Top 10 only	✓	✓	✓	✓	✓	✓	✓
SANS Top 20	✓	✓	✓	✓	✓	✓	✓
OWASP test: complete	✓	✓	✓	✓	✓	✓	✓
False negatives validation	✓	✓	✓	✓	✓	✓	✓
Server security evaluation	✓	✓	✓	✓	✓	✓	✓
Manual security test	✓	✓	✓	✓	✓	✓	✓
Source code analysis (checklist of potential vulnerabilities)	✓	✓	✓	✓	✓	✓	✓

1) Rates may change without notice.

2) Based on **Virtual Guardian**'s best estimates. Actual delay may vary based on task complexity.

For inquiries about **Virtual Guardian's** Web application analysis methodology, call **Virtual Guardian** and ask for a **free evaluation today!**