



Website Security Tests Protect Against Application Vulnerabilities

Small and medium-sized enterprises can protect websites against application vulnerabilities with simple, easy-to-use, and affordable service. Firewall, Intrusion prevention and Detection System (IDS/IPS) are not enough to protect your Website against today's application vulnerabilities

Introduction

More than four out of every five (85 percent) U.S. businesses have experienced a data breach, according to a [recent study by Colchester, Conn.-based law firm Scott + Scott](#), putting millions of consumers' Social Security numbers and other sensitive information in the hands of criminals.

Website owners are vulnerable to unwanted intrusions by malicious hackers and other harmful codes. If a website's server and applications are not protected from security vulnerabilities, identities, credit card information, and billions of dollars are at risk.

Many companies rely on a firewall to protect their websites from security breaches. Unfortunately, firewalls do not provide enough protection.

Hackers are constantly looking for new ways to compromise systems through unguarded, and sometimes not so obvious, side doors.

Firewalls, IDS, IPS Are Not Enough

Attackers are well-aware of the valuable information accessible through Web applications, and their attempts to get at it are often unwittingly assisted by several important factors. Conscientious organizations carefully protect their perimeters with intrusion detection systems and firewalls, but these firewalls must keep ports 80 and 443 (SSL) open to conduct online business. These ports represent open doors to attackers, who have figured out thousands of ways to penetrate Web applications.

The standard security measures for protecting network traffic, network firewalls and Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS), do not offer a solution to application level threats. Network firewalls are designed to secure the internal network perimeter, leaving organizations vulnerable to various application attacks.

Intrusion Prevention and Detection Systems (IDS/IPS) do not provide thorough analysis of packet contents. Applications without an added layer of protection increase the risk of harmful attacks and extreme vulnerabilities.

Extreme Vulnerabilities

Web Application Level Attacks is the Achilles heel. In the past, security breaches occurred at the network level of the corporate systems. Today, hackers are manipulating web applications inside the corporate firewall. This entry enables them to access sensitive corporate and customer data. An experienced hacker can break into most commercial websites with even the smallest hole in a company's website application code. These sophisticated attacks have become increasingly threatening to organizations.

The standard security measures for protecting network traffic do not protect against web application level attacks.

OWASP's Top 10 Web Application Security Vulnerabilities 2007

Open Web Application Security Project (OWASP), an organization that focuses on improving the security of application software, has put together a [list of the top 10 web application security vulnerabilities](#).

1. Cross Site Scripting (XSS)
2. Injection Flaws
3. Malicious File Execution
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to Restrict URL Access

Web Application Security Consortium Most Common Vulnerabilities Report

The Web Application Security Consortium (WASC)—an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best practice security standards for the World Wide Web—reported the [top five web application vulnerabilities](#) by testing 31,373 sites. (See Figure 1)

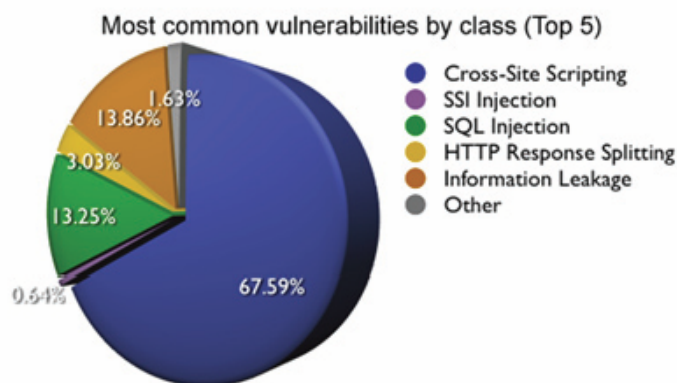


Figure 1

According to the **Gartner Group**, "97% of the over 300 web sites audited were found vulnerable to web application attack," and "75% of the cyber attacks today are at the application level."

Web application vulnerability assessment

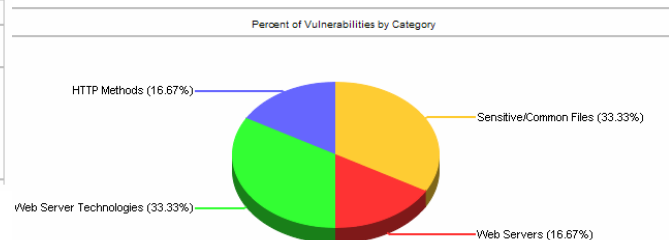
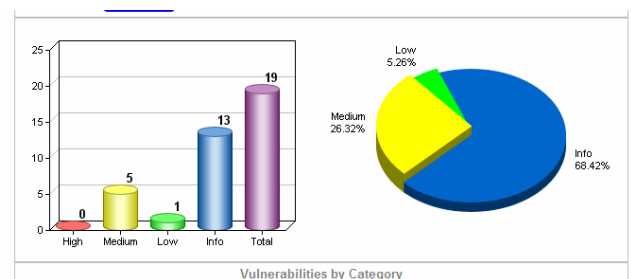
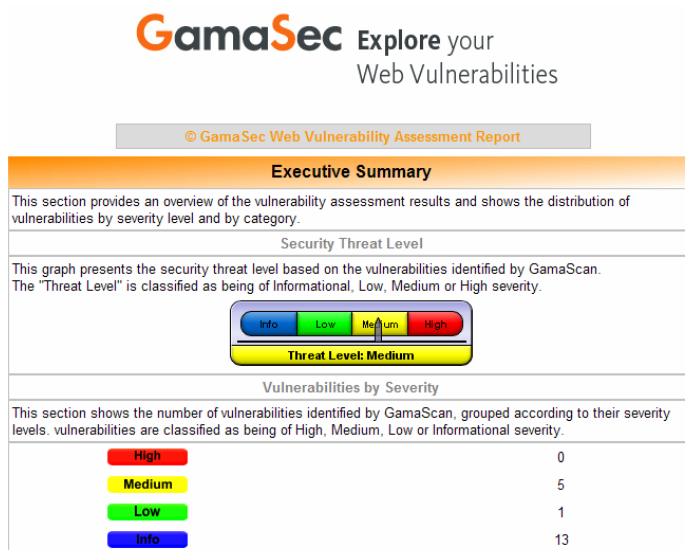
From the information above it's clear that most e-commerce websites are wide open to attack and easy victims when targeted. While the security posture of some industries is stronger than others, the difference is insignificant when it comes to actually preventing a website compromise because intruders need only to exploit a single vulnerability.

A web application scanner, which protects applications and servers from hackers, must provide an automated security service that searches for software vulnerabilities within web applications.

A web application scanner should crawl the entire website, analyze in-depth each & every file, and display the entire website structure. The scanner has to perform an automatic audit for common security vulnerabilities while launching a series of simulated web attacks. Web Security Seal and free trial should be available.

Most systems are vulnerable to thousands of known risk factors. A web application vulnerability Assessment should execute continuous dynamic tests combined with simulation web-application attacks during the scanning process.

The web application scanner must have the ability to validate security breaches and risks against a continually updated service database provides real-time vital business solutions. A website security test should identify the security vulnerabilities and recommend the optimally matched solution. The fix or workaround solution should be identified and implemented when you need it - not after it's too late.



Web Scanning Vulnerability Executive Report

Once the vulnerability scan is completed, the vulnerability check has to deliver an executive summary report to management and a detailed report to the technical teams. Both reports should list the vulnerabilities found along with the severity levels of each vulnerability.

It is recommended that the detailed report include an in-depth technical explanation of each vulnerability as well as appropriated recommendations and the website security test will conduct subsequent vulnerability scans and generate trend analysis reports that allow the customer to compare tests and track progress.

Web Scanning Vulnerability Technical Report

| Technical Details | | |
|---|---------|-------------------------|
| This section provides details on the open ports, web server, vulnerabilities and threats identified on the system. | | |
| Open Ports [5] | | |
| This table shows the open ports on the system. not each open port is a security threat, but open ports on the system are invitations to attackers. In general, the number of open ports should be kept to a minimum and only the mission-critical ports should be open. | | |
| Port Number | Service | Description |
| 21 (tcp) | ftp | File Transfer [Control] |
| 22 (tcp) | ssh | Secure Shell Login |
| 25 (tcp) | smtp | Simple Mail Transfer |
| 80 (tcp) | http | World Wide Web HTTP |
| 443 (tcp) | https | secure http (SSL) |

| Web Server | |
|--|--|
| This table provides general details on the web server identified by GamaScan | |
| Target Banner | Apache/1.3.33 (Unix) mod_fastcgi/2.4.2 mod_ssl/2.8.22 Open |
| Http Methods | GET, HEAD, OPTIONS, TRACE |
| Cookie | |

| Apache Version <= 1.3.33 | |
|--|--|
| Description | The Apache web server version is 1.3.33 or older. A vulnerability has been reported in the htpasswd utility distributed with Apache. While the program may contain a local overflow, this would only be of benefit if an administrator gave it SUID permissions, placed it in a chroot style environment or made it accessible via a web page. In each scenario there is a chance the vulnerability could be used to leverage permissions. <i>The vulnerability has been identified using banner grabbing (Server Header). This might be a false positive.</i> |
| Scan Request | OPTIONS / HTTP/1.0 |
| Recommendation | ensure that the htpasswd binary is not SUID, is not placed in a chroot environment, and is not called from a web page. |
| External References: OSVDB ID: 10058 | |

GamaSec Overview

GamaSec delivers the required vulnerability assessment solutions and services as described in this white paper. Proprietary tools specifically solve major cost and efficiency limitations which prevent businesses from successfully and efficiently implementing web vulnerability assessment. This website security test is an early-warning system of defence for web operation, applications, and online information.

Vulnerability assessment technology has been developed through experience gained in large scale worldwide security projects; in Europe and in Israel, in both civilian and military use. Many competitive services are based on open source rules providing generic solutions. GamaSec is active in security research and a pioneer in the field of vulnerability identification and definition. This website security scan is among the first and fastest at locating new vulnerabilities and mitigating new threats.

GamaSec offering GamaScan is a **remote online web vulnerability-assessment service** that tests web servers, web-interfaced systems and web-based applications against thousands of known vulnerabilities with dynamic testing, and by simulating web-application attacks during online scanning. The service identifies security vulnerabilities and produces recommended solutions that can fix, or provide a viable workaround to the identified vulnerabilities

For more information please visit: www.gamasec.com
 Or Contact: info@gamasec.com

Author: Avi D. Bartov – Co-Founder and CEO of GamaSec, Avi is a graduate of law from Nanterre University in Paris, France with over 12 years of experience & management in IT security. He is a technology executive who has led several companies to success in Europe and Israel.

Abstract: Website Security Tests Protect Against Application Vulnerabilities

Author: Avi D. Bartov Small and medium-sized enterprises can protect websites against application vulnerabilities with simple, easy-to-use, and affordable service. Firewall, Intrusion prevention and Detection System (IDS/IPS) are not enough to protect your Website against today's application vulnerabilities.