GamaSec
Innovative Website Security

We go Behind Generic Tools to Locate All Web Vulnerabilities and Threats

White paper GamaScan: Web Application Online Scanner

GamaSec provides the industry-leading cloud-based (SaaS) solution for identifying web site and web application vulnerabilities. Built from the ground up on a completely different technology backbone than its competitors, GamaSec goes beyond traditional signature-based scanners to find more "real-world" vulnerabilities based on deeper and more granular inspection.

Military-Grade Technology : GamaSec was developed for the detection of website vulnerabilities and data breaches of highly-sensitive military and government entities. Our technologies have passed extensive and rigorous testing in order to comply with levels of security that surpass the standards of most commercially-available scanning solutions.

Artificial Intelligence : GamaSec scanning solutions are built on next-generation artificial intelligence technologies that penetrate deeply with surgical precision within the application layers. Our vulnerability scanners use simulated scenarios for third-party attack and adapt and learn on a real time basis to identify undetected infections.

False-Positive Free: GamaSec solutions that generate false positives cause companies to spend resources on additional and unnecessary remediation costs. GamaSec uses a sophisticated and proprietary hashing system to minimize false positives. This is done via dynamic false-positive filter rules that are run automatically without any manual interference

First, the scanner explores the entire Web application environment and registers its structure and contents. Then it mimics actual hacking methods to identify and uncover the details of any point that is susceptible to attack including:

- SQL Injection Attack - Attempt to get the database server to execute arbitrary SQL.
- Cross Site Scripting Attack - Attempt to coerce the program to outputting third party Javascript.
- Parameter Manipulation Attack - Attempt to manipulate input to application validation and filtering.
- Code Injection Attack - Attempt to execute arbitrary code.
- Hidden Tag Issues - If forms are used sensitive information, such as price, should never be hard coded into the form using hidden tags.

The web scanner can be used to discover a wide variety of vulnerabilities and, following detection, actually recommends solutions designed to protect the vulnerable data.

GamaScan's online web application vulnerability scanner will focus on the general makeup of a web-site/web-application structure. Below is a description of the mechanisms used by the scanner to learn as much as possible about the targeted web-site.

The following list shows the type of vulnerabilities and data that will be discovered by GamaSec during a website scan:

- Web services and Web Applications - An unsecured web service and web applications can have many vulnerabilities caused by poor programming technique and insecure application design.
- Web Site management interfaces – Many large server solutions come with management interfaces that allow the administrator to have full control over their server remotely.
- Directory and file structure – If directory browsing is not turned off, a hacker can learn about the file structure of the web server, thus exposing files and folders that the web administrator may not have meant to expose to the user.
- Discovery of backend database connectivity – If backend database connectivity is discovered, a hacker might be able to bypass the front end to get directly to the database, or use the same username and password from the database to access other parts of the site if the username is reused.
- Backup files – If a hacker can access these files, he/she can read any information in the file, which might contain secured directory paths, usernames and/or passwords.
- User names and passwords – An improperly secured web server can grant access to anonymous web users by releasing user name and encrypted password lists. Once a hacker has a complete list of user names and passwords, he can start cracking the passwords using a number of password auditing techniques.
- Vulnerable scripts – The scanner will identify known vulnerable scripts that compromise the server by allowing a hacker to exploit the script to allow them to upload malicious files, gain access to files already on the server that should be protected or execute application code on the server that should be unavailable.
- Server misconfigurations – The scanner will locate web server misconfigurations that can lead to problems ranging from site defacement to complete server control.
- Enumeration of ports on the server – GamaScan will identify open or non-sheathed ports which hackers can use as entryways to the server. Each port can represent a new vulnerability.
- Discovery of authentication mechanisms – The scanner will locate vulnerabilities related to authentication mechanisms and potential attacks to crack specific authentication types.

GamaSec
Innovative Website Security

Application Vulnerability attacks cover by GamaScan

Sql Injection	Xpath Injection	LDAP Injection
Blind SQL Injection	CRLF Injection	Cookie Manipulation
Installation Path Disclosure	Directory Traversal Disclosure	Source Code
Net Exception	Scrip Language Error	Cross-Site Scripting
Command Execution	URL Redirection	Cross-Frame Scripting
PHP Code Injection	Remote File Inclusion	Internal IP Disclosure

General Tests cover by GamaScan

Web Servers	Directory Enumeration	Directory Permissions
Web Server Technologies	Directory Indexing	Sensitive/Commom Files
HTTP Methods	Directory Access	Third party Application
Backup Files		

The GamaSec vulnerability scanner consists of 5 main processes: First, a Port Scan is launched to determine which ports are open. Secondly, the GamaScan Crawler gathers a set of target web sites. Thirdly, the Scanner launches the configured attacks against these targets. Finally, the Analyzer examines the results returned by the web applications to determine whether an attack was successful.

Phase 1 - Port Scan

This phase consists of a port scan of the target to determine which ports are open. Not each open port is a security threat, but open ports on the system are often invitations to attackers.

Phase 2- Crawling Component

Because of the relatively slow response time of remote web servers (typically ranging from 100 to 10,000 milliseconds), GamaSec uses a queued workflow system which executes several concurrent worker threads to improve crawling efficiency. Depending on the performance of the machine that hosts GamaSec, the bandwidth of the uplink, and the targeted web servers, 10 to 30 concurrent worker threads are typically deployed during a vulnerability detection run to reduce the total scanning time.

To start a crawling session, the crawling component of GamaSec needs to be seeded with a root web address. Using this address as a starting point, the crawler steps down the link tree, collecting all pages and included web forms during the process. Just like a typical SEO web crawler, GamaSec has configurable options for the maximum link depth, maximum number of pages per domain to crawl, maximum crawling time, and the option of dropping external links.

Phase 3- Scan Component

After the crawling phase has completed, GamaSec starts processing the list of target pages. In particular, the scan component scans each page for the presence of web forms. The reason is that the fields of web forms constitute potential entry points to web applications.

For each web form, GamaSec extracts the action (or target) address and the method (i.e., GET or POST) used to submit the form content. Also, the form fields and its corresponding CGI parameters are collected. Then, depending on the actual attack that is launched, appropriate values for the form fields are chosen. Finally, the form content is uploaded to the server specified by the action address (using either a GET or POST request). As defined in the HTTP protocol, the attacked server responds to such a web request by sending back a response page via HTTP.

Phase 4- Analysis Modules

After an attack has been launched, the analysis module proceeds to parse and interpret the server response. An analysis module uses attack-specific response criteria.

Phase 5- Report and recommendations Modules

Reports clearly define vulnerabilities found during the internet security test conducted by the web application scanner. Recommendations offer solutions to fix or provide a viable workaround, designed efficiently in color-coded and graphical format to provide the flexibility necessary to satisfy all audiences ranging from upper management to system administrators.