

GamaSec Explore your Web Vulnerabilities

Differential Report

Target Scanned: www.GamaSec-Test.com

Previous Scan: Wed Jul 2 15:29:12 2008

Recent Scan: Wed Jul 9 00:50:01 2008

Report Generated: Thu Jul 10 12:00:51 2008



GamaSec **Explore your** Web Vulnerabilities

Differential Report

Target Scanned :	www.GamaSec-Test.com:80
Report Generated :	Thu Jul 10 12:00:51 2008

Table Of Contents








Introduction	2
Executive Summary	3
Technical Details	7

Introduction

"Explore Your Web Vulnerabilities"

This report displays the differential comparison between the previous scan results to the current scan results.

GamaScan Automated Web-Application Vulnerability Assessment Service Key features:

-  **Zero time setup.**
-  **No software installation.**
-  **No special hardware.**
-  **No special training.**
-  **Pre defined or customizable scans.**
-  **Detailed, Crystal clear, reports.**
-  **Constant updates.**

GamaSec Explore your Web Vulnerabilities

Executive Summary

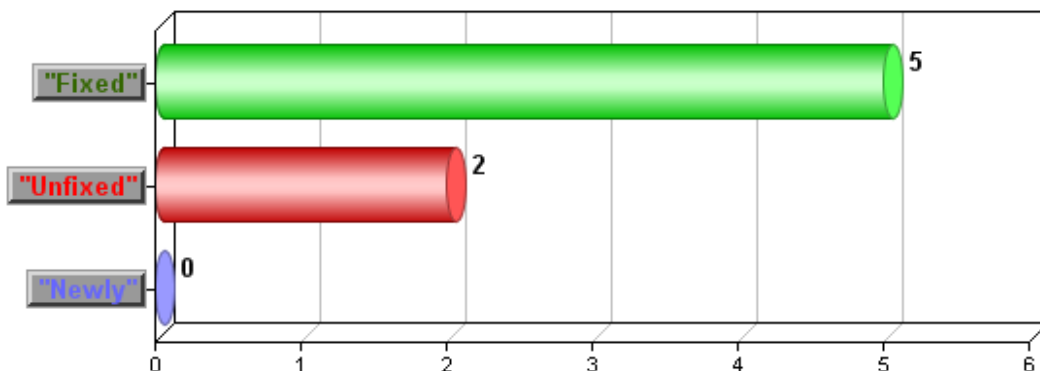
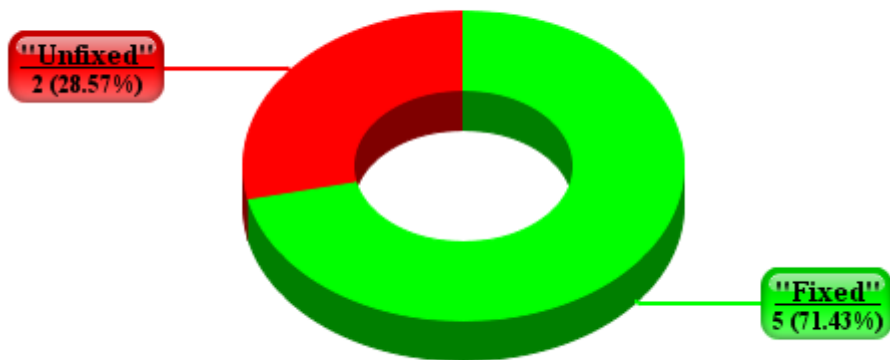
This section provides an overview on the difference in security postures of the scanned web-interfaced system.

Comparison statistics

Scans conducted on	Wed Jul 2 15:29:12 2008	Wed Jul 9 00:50:01 2008
Identified Vulnerabilities	Previous Scan	Recent Scan
High	1	0
Medium	4	2
Low	2	0
Info	8	8
Total Vulnerabilities (Without the "Info" findings)	7	2
Security Threat Level	High	Medium
Open Ports	2	2

Distribution of Vulnerabilities

Number of vulnerabilities fixed in the recent scan ("Fixed")	5
Number of Vulnerabilities identified in both scans ("Unfixed")	2
Number of newly vulnerabilities identified in the recent scan ("Newly")	0



GamaSec Explore your Web Vulnerabilities

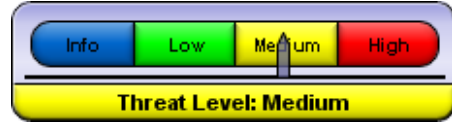
Security Threat Level

The charts below presents the security threat levels based on the vulnerabilities identified by GamaScan in both scans. The "Threat Level" is classified as being of Informational, Low, Medium or High severity.

Previous Scan



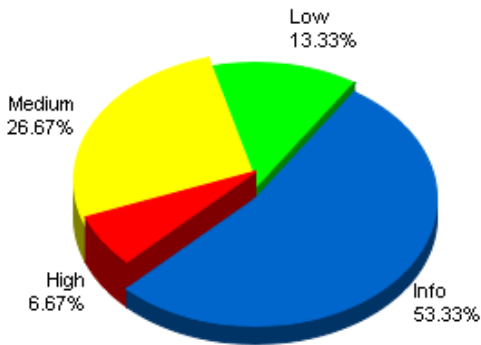
Recent Scan



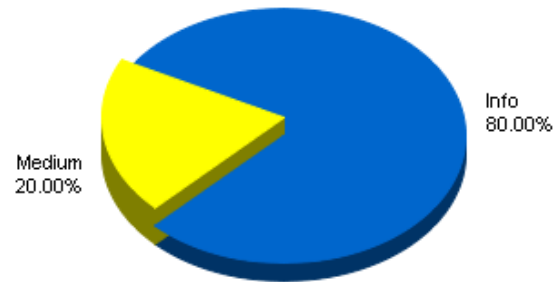
Vulnerabilities by Severity

The charts below shows the percentage of vulnerabilities identified by GamaScan in both scans, grouped according to their severity levels. vulnerabilities are classified as being of High, Medium, Low or Informational severity.

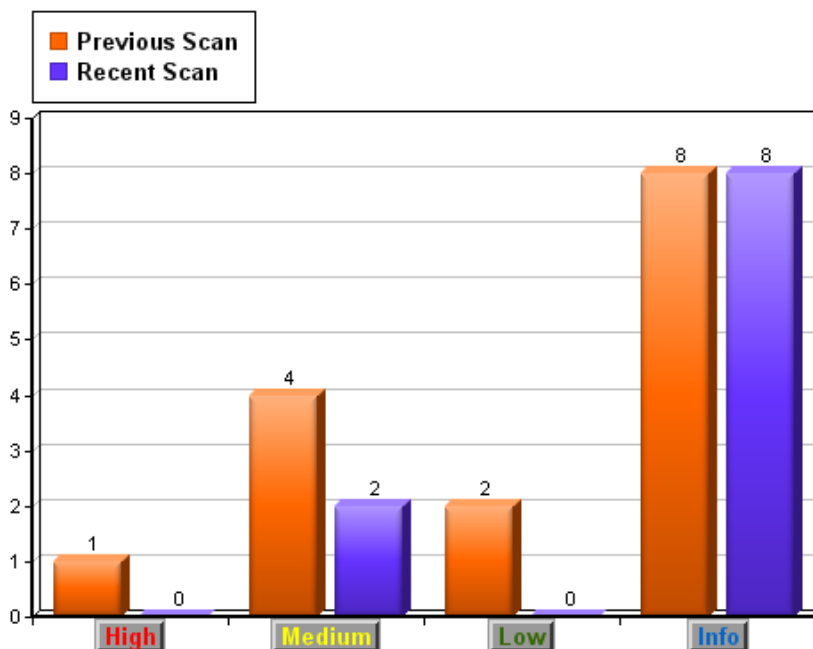
Previous Scan



Recent Scan



The graph below shows the difference in number of vulnerabilities identified by GamaScan in both scans.



GamaSec Explore your Web Vulnerabilities

Vulnerabilities by Category

This section shows the number of vulnerabilities identified by GamaScan in both scans, grouped according to their categories.

Previous Scan	
Category	Number Of Vulnerabilities
Web Servers	2 28.57%
Directory Indexing	2 28.57%
SQL Injection	1 14.28%
.NET Exception	2 28.57%
Recent Scan	
Category	Number Of Vulnerabilities
Directory Indexing	2 100%

GamaSec Explore your Web Vulnerabilities

Open Ports

This table shows the open ports identified by GamaScan on the system in both scans.

Previous Scan

Port Number	Service	Description
21 (tcp)	ftp	File Transfer [Control]
80 (tcp)	http	World Wide Web HTTP

Recent Scan

Port Number	Service	Description
21 (tcp)	ftp	File Transfer [Control]
80 (tcp)	http	World Wide Web HTTP




GamaSec Explore your Web Vulnerabilities

Technical Details

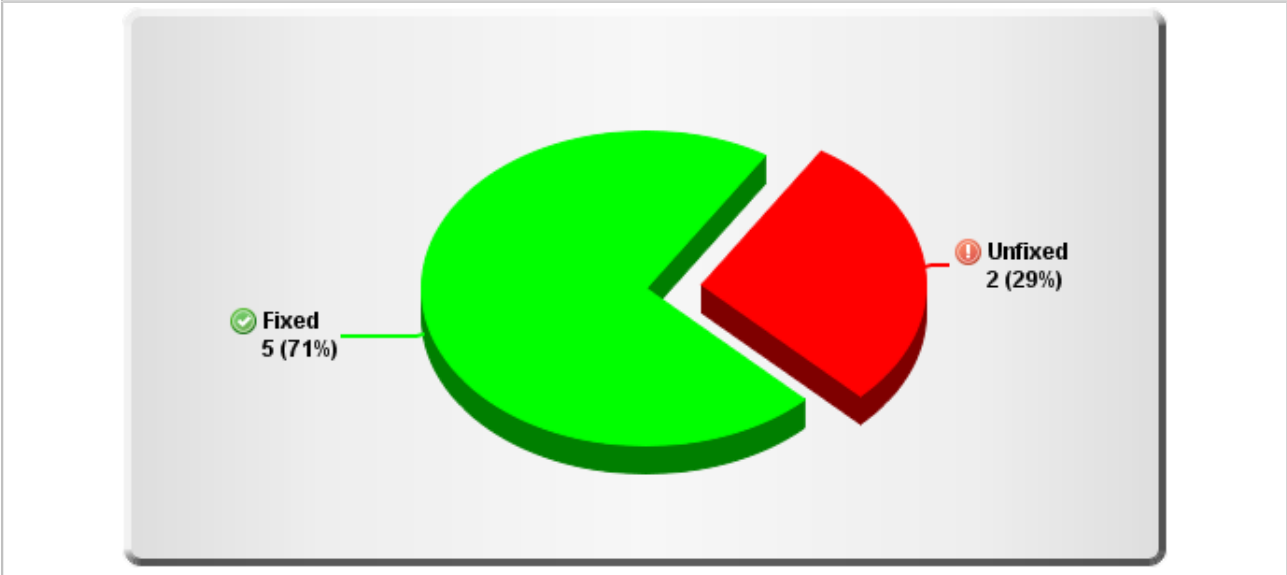
This section provides technical details on the differential comparison between the previous scan results to the current scan results.

Status Icons

The icons below present the status for each vulnerability in this section. A relevant icon is displayed on the "Scan Request" section on each vulnerability details.

	"Fixed" , The vulnerability has been fixed in the recent scan.
	"Unfixed" , The vulnerability has been identified in both scans.
	"Newly" , The vulnerability has been identified only in the recent scan.

The graph below shows the distribution of vulnerabilities by status.






GamaSec Explore your Web Vulnerabilities

Vulnerabilities fixed in the recent scan ("Fixed")

This section provides technical details on the vulnerabilities fixed in the recent scan.



Possibility of SQL Injection

Script:default.aspx **Variable:**Login1:txtUserName
Value: '



Description	GamaScan has identified a flaw that may allow an attacker to carry out an SQL injection attack. This flaw exists because the application does not properly sanitizing user-supplied input to the variable. This may allow an attacker to inject or manipulate SQL queries in the backend database.	
	Form Method: POST	
	The Form Inputs	
	Type	Name
	hidden	__VIEWSTATE
	text	Login1:txtUserName
	password	Login1:txtPassword
	image	Login1:ImageButton1
Scan Request 	www.GamaSec-Test.com:80/default.aspx	
Recommendation	<p>It is possible to correct the flaw by manually editing the code to properly sanitize the user-supplied input.</p> <p>External References:</p> <ul style="list-style-type: none">  Wikipedia  sqlsecurity 	



An unhandled exception (Microsoft .NET)

Script:default.aspx **Variable:**Login1:txtUserName
Value: <GS>



Description	ASP.NET produces an error page when an application throws an unhandled exception the error page might contain sensitive information. This flaw exists because ASP.NET is configured to show verbose error messages.	
	Form Method: POST	
	The Form Inputs	
	Type	Name
	hidden	__VIEWSTATE
	text	Login1:txtUserName
	password	Login1:txtPassword
	image	Login1:ImageButton1
Scan Request 	www.GamaSec-Test.com:80/default.aspx	
Recommendation	<p>Create a custom error page to handle the exception.</p> <p>External References:</p> <ul style="list-style-type: none">  Microsoft Article ID: 308132 	

GamaSec Explore your Web Vulnerabilities

An unhandled exception (Microsoft .NET) Script: default.aspx Variable: Login1:txtPassword Value: <GS>											
Description	ASP.NET produces an error page when an application throws an unhandled exception the error page might contain sensitive information. This flaw exists because ASP.NET is configured to show verbose error messages.										
	Form Method: POST										
	The Form Inputs										
	<table border="1"> <thead> <tr> <th>Type</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>hidden</td> <td>__VIEWSTATE</td> </tr> <tr> <td>text</td> <td>Login1:txtUserName</td> </tr> <tr> <td>password</td> <td>Login1:txtPassword</td> </tr> <tr> <td>image</td> <td>Login1:ImageButton1</td> </tr> </tbody> </table>	Type	Name	hidden	__VIEWSTATE	text	Login1:txtUserName	password	Login1:txtPassword	image	Login1:ImageButton1
	Type	Name									
hidden	__VIEWSTATE										
text	Login1:txtUserName										
password	Login1:txtPassword										
image	Login1:ImageButton1										
Scan Request 	www.GamaSec-Test.com:80/default.aspx										
Recommendation	Create a custom error page to handle the exception. External References:  Microsoft Article ID: 308132										

Microsoft ASP.NET Error Message (Version)	
Description	Web Services running on ASP.NET framework contains a flaw that may lead to an ASP.NET version disclosure. the error message disclose the version. Identified Version: Microsoft .NET Framework Version:1.1.4322.2407; ASP.NET Version:1.1.4322.2407
Scan Request 	www.GamaSec-Test.com:80/Version.aspx
Recommendation	create a custom error page for a 404 "File Not Found" error. External References:  Microsoft Article ID: 308132

GamaSec Explore your Web Vulnerabilities



Microsoft ASP.NET Error Message (Path)	
Description	Web Services running on ASP.NET framework contains a flaw that may lead to an to an internal system path disclosure. the error message disclose the path. Identified Path: d:\hosting\imertest\
Scan Request 	www.GamaSec-Test.com:80/Path.aspx
Recommendation	create a custom error page for a 404 "File Not Found" error. External References:  Microsoft Article ID: 308132

GamaSec Explore your Web Vulnerabilities



Vulnerabilities identified in both scans ("Unfixed")

This section provides technical details on the vulnerabilities identified by GamaScan in both scans.

Directory Indexing (Empty Directory)

Description	It is possible to lists the directory contents.
Scan Request 	www.GamaSec-Test.com:80/temp/
Recommendation	Disable directory indexing or create a default Index file for each directory. External References:  Securing Web Servers:

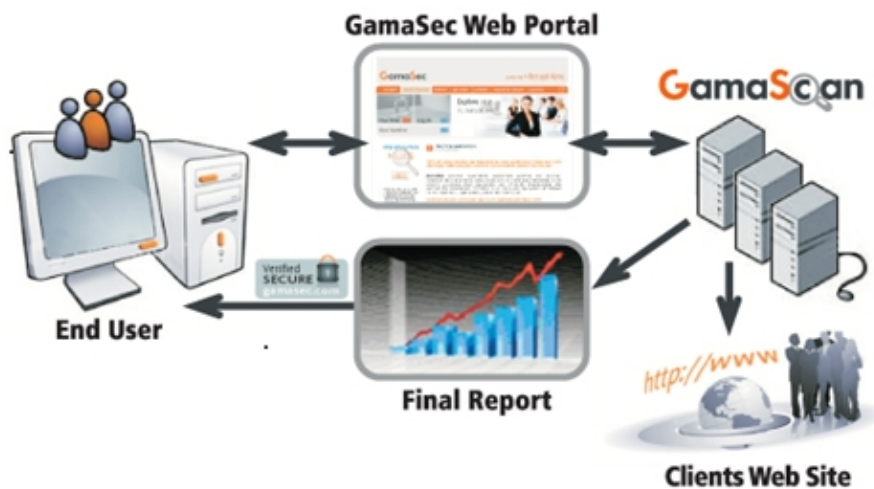
GamaSec Explore your Web Vulnerabilities

Directory Indexing	
Description	It is possible to lists the directory contents.
Scan Request 	www.GamaSec-Test.com:80/modules/
Recommendation	Disable directory indexing or create a default Index file for each directory. External References:  Securing Web Servers:

GamaSec Explore your Web Vulnerabilities

GamaScan The Web Application Security Solution

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. GamaScan provides a flexible, interactive security scan which requires no installation, no setup, no new hardware, no software development, no security expertise and no special training.



Scan your web site today with GamaScan and find vulnerabilities before hackers do!

GamaSec

Explore your
Web Vulnerabilities

Contact Us



Technical

support@gamasec.com

Sales

sales@gamasec.com

Information

info@gamasec.com

Partner Program

partnerprogram@gamasec.com

GamaSec Explore your Web Vulnerabilities

By displaying the GamaSec security seal your customers know your website is secure.

Verified Site **GamaSec**



GamaScan

Domain Name: www.gamasec.com

GamaScan the most complex web application security services executes continuous dynamic tests combined with simulation web-application attacks during the scanning process.

The GamaSec service identifies security vulnerabilities and produces Recommended solution that can fix, or provide workaround to the identified vulnerabilities

GamaSec has recently tested the website identified on this certificate.

Assure your customers that your website is secure, courtesy of the GamaSec Verified Secure seal displayed on your website.

 www.GamaSec.com