



VC HackScan Website Audit

20 August, 2008

Scan Comparison

Scan comparison

Scan details

Start URL

First scan	http://compare.testwebsite.com
Second scan	http:// compare.testwebsite.com

Threat levels

First scan



Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Second scan



Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alert counts

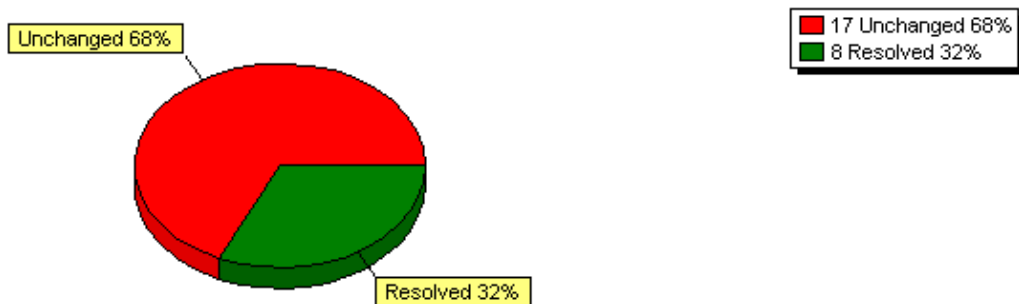
First scan

Total alerts found	25
🔴 High	6
🟡 Medium	0
🟢 Low	14
🟦 Informational	5

Second scan

Total alerts found	17
🔴 High	0
🟡 Medium	0
🟢 Low	12
🟦 Informational	5

Comparison chart



Unchanged issues

Application error message

Severity	Low
Type	Validation
Reported by module	Parameter manipulation

Description

This page contains an error/warning message that may disclose the sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Affected items

/codepage.asp

Details

The GET variable **id** has been set to **0x3ffffff** .

/codepage.asp

Details

The GET variable **id** has been set to **NULL** .

/codepage.asp

Details

The GET variable **id** has been set to **\"");][*%0d%0a<%00** .

/codepage.asp

Details

The GET variable **id** has been set to **0xffffffff** .

/codepage.asp

Details

The GET variable **id** has been set to **0x7ffffff** .

/codepage.asp

Details

The GET variable **id** has been set to **0x80000000** .

/codepage.asp

Details

The GET variable **id** has been set to .

/default.asp

Details

The GET variable **ContentID** has been set to **268435455** .

Email address found

Severity	Informational
Type	Informational
Reported by module	Text search

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Affected items

/default.asp

Details

We found

privacy@testwebsite.com

GHDB: robots.txt file

Severity	Informational
Type	Informational
Reported by module	GHDB - Google hacking database

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.

Category : [Files containing juicy info](#)

Webmasters wanting to exclude search engine robots from certain parts of their site often choose the use of a robot.txt file on the root of the server. This file basically tells the bot which directories are supposed to be off-limits. An attacker can easily obtain that information by very simply opening that plain text file in his browser. Webmasters should **never** rely on this for real security issues. Google helps the attacker by allowing a search for the "disallow" keyword.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Affected items

/robots.txt

Details

We found

[\(inurl:"robot.txt" | inurl:"robots.txt" \) intext:disallow filetype:txt](#)

GHDB: robots.txt with Disallow tag

Severity	Informational
Type	Informational
Reported by module	GHDB - Google hacking database

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.

Category : [Files containing juicy info](#)

The robots.txt file serves as a set of instructions for web crawlers. The "disallow" tag tells a web crawler where NOT to look, for whatever reason. Hackers will always go to those places first!

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Affected items

/robots.txt

Details

We found

["robots.txt" "Disallow:" filetype:txt](#)

GHDB: Typical login page

Severity	Informational
Type	Informational
Reported by module	GHDB - Google hacking database

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.

Category : [Pages containing login portals](#)

This is a typical login page. It has recently become a target for SQL injection. Comsec's article at <http://www.governmentsecurity.org/articles/SQLInjectionBasicTutorial.php> brought this to my attention.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Affected items

/inc/doLogin.asp

Details

We found

[inurl:login.asp](#)

/inc/doLogin.asp

Details

We found

[inurl:login.asp](#)

Possible sensitive directories

Severity	Low
Type	Validation
Reported by module	Directory checks

Description

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for

known sensitive directories like: backup directories, database dumps, administration pages, temporary directories. Each of those directories may help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Affected items

/downloads
Details
No details are available.
/inc/tree
Details
No details are available.
/mail
Details
No details are available.
/pages
Details
No details are available.

Resolved issues

Application error message

Severity	Low
Type	Validation
Reported by module	Parameter manipulation

Description

This page contains an error/warning message that may disclose the sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Affected items

/inc/doNewPassword.asp

Details

The POST variable **username** has been set to `\");[]*{%0d%0a<%00 .`

/inc/doUserName.asp

Details

The POST variable **email** has been set to `\");[]*{%0d%0a<%00 .`

SQL injection

Severity	High
Type	Validation
Reported by module	Parameter manipulation

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Affected items

/inc/doNewPassword.asp

Details

The POST variable **username** has been set to **vulnocity"** .

/inc/doNewPassword.asp

Details

The POST variable **username** has been set to **'** .

/inc/doNewPassword.asp

Details

The POST variable **username** has been set to **'** .

/inc/doUserName.asp

Details

The POST variable **email** has been set to **'** .

/inc/doUserName.asp

Details

The POST variable **email** has been set to **vulnocity"** .

/inc/doUserName.asp

Details

The POST variable **email** has been set to **'** .