



# Getting Started with WebCruiser Web Vulnerability Scanner 3

©JANUSEC

[HTTP://WWW.JANUSEC.COM/](http://www.janusec.com/)

# Introduction

The screenshot displays the WebCruiser interface with the following components:

- Menu Bar:** File, Tools, View, Configuration, Help
- Toolbar:** Browser, Scanner, SQL, POC, Resend, Bruter, Cookie, Setting, ScanURL, ScanPage, ScanSite
- URL Bar:** http://vulnweb.janusec.com/ GET
- Navigation:** Crawler, Scan Current URL, Scan Current Page, Scan Current Site, Reset Scanner
- Left Panel (Tools):** Browser, Scanner, POC (SQL Injection, XSS/LFI/RFI/Redirect, AdminEntrance), Tools (ResendTool, BruterTool, CookieTool, CodeTool, StringTool, Settings, Report, About)
- Main Content Area:**
  - Items Table:**

Items	Detailed Information
Vuln Type	SQLInjection
Refer Address	http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1
Request Type	GET
Action URL	http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1
Parameter	id
Description	GET SQL INJECTION ErrorBased Integer
POC	http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1 or (select 1 from (select count(*), concat((0x
  - Directory:** Vulnerability Information
  - Vulnerabilities Table:**

Address (Refer URL)	Vulnerability	Action URL
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.ph...	GET SQL INJECTION LogicBased Integer	http://vulnweb.janus
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.ph...	GET XSS Reflected	http://vulnweb.janus
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.ph...	GET SQL INJECTION ErrorBased Integer	http://vulnweb.janus
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.ph...	GET SQL INJECTION LogicBased Integer	http://vulnweb.janus
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php...	GET SQL INJECTION TimeBased Integer	http://vulnweb.janus
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php...	GET XSS Reflected	http://vulnweb.janus
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php...	GET SQL INJECTION LogicBased Integer	http://vulnweb.janus
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php...	GET SQL INJECTION ErrorBased Integer	http://vulnweb.janus
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php...	GET SQL INJECTION LogicBased Integer	http://vulnweb.janus
http://vulnweb.janusec.com/Case03-SQLI-GET-STRING-AND...	GET SQL INJECTION LogicBased String	http://vulnweb.janus
  - Scan Log:**

```
16:27:21 Depth: 2 Scanning: http://vulnweb.janusec.com/Case16-SQLI-POST-SEARCH-FORM-AND.php
16:27:21 Depth: 2 Scanning: http://vulnweb.janusec.com/Case17-SQLI-POST-SEARCH-FORM-OR.php
16:27:21 Depth: 2 Scanning: http://vulnweb.janusec.com/Case51-XSS-GET.php?username=aaa
16:27:21 Depth: 2 Scanning: http://vulnweb.janusec.com/Case51-XSS-GET.php
16:27:21 Depth: 2 Scanning: http://vulnweb.janusec.com/Case52-XSS-FORM-GET.php
16:27:22 Depth: 2 Scanning: http://vulnweb.janusec.com/Case53-XSS-FORM-POST.php
```
- Status Bar:** Done | HTTP Thread: 0

Launch Scan

Vulnerabilities

Scan Log

# Test Report with WAVSEP v1.5

WAVSEP, Web Application Vulnerability Scanner Evaluation Project

<http://sourceforge.net/projects/wavsep/>

WebCruiser Web Vulnerability Scanner Test Report

[http://www.janusec.com/download/WebCruiser\\_Web\\_Vulnerability\\_Scanner\\_Test\\_Report.pdf](http://www.janusec.com/download/WebCruiser_Web_Vulnerability_Scanner_Test_Report.pdf)

WebCruiser 3.4	SQL Injection	XSS	LFI	RFI	Redirect	Backup
Benchmark Results	100%	100%	100%	100%	100%	100%
False Positive	0%	0%	0%	0%	0%	0%

# Introduction

- ▶ WebCruiser Web Vulnerability Scanner, an effective and powerful web penetration testing tool that will aid you in auditing your website!
- ▶ It can support scanning website as well as POC (Proof of concept) for web vulnerabilities: SQL Injection, Cross Site Scripting, Local File Inclusion, Remote File Inclusion, Redirect etc.
- ▶ The most typical feature of WebCruiser comparing with other Web Vulnerability Scanners is that WebCruiser Web Vulnerability Scanner focuses on high risk vulnerabilities, and WebCruiser can scan a designated vulnerability type, or a designated URL, or a designated page separately, while the others usually will not.

# Key Features

- ▶ Scanner:
  - ▶ SQL Injection
  - ▶ XSS
  - ▶ Local File Inclusion
  - ▶ Remote File Inclusion
  - ▶ Redirect
  - ▶ Obsolete Backup
- ▶ SQL injection and database takeover tool.
- ▶ XSS, LFI, RFI, Redirect POC tool.
- ▶ Resend & Bruter tool.
- ▶ Cookie tool.

# SQL Injection POC

WebCruiser - Web Vulnerability Scanner Enterprise Edition

File Tools View Configuration Help

Browser Scanner SQL POC Resend Bruter Cookie Setting ScanURL ScanPage ScanSite

URL: GET

Crawler Scan Current URL Scan Current Page Scan Current Site Reset Scanner

Items	Detailed Information
Vuln Type	SQLInjection
Refer Address	http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1
Request Type	GET
Action URL	http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1
Parameter	id
Description	GET SQL INJECTION ErrorBased Integer

Directory Vulnerability Information

Address (Refer URL)	Vulnerability	Action URL
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1	GET SQL INJECTION LogicBa...	http://vulnweb.janus...
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1	GET SQL INJECTION ErrorBa...	http://vulnweb.janus...
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1	GET XSS Reflected	
http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1	GET SQL INJECTION	
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php?id=999999	GET XSS Reflected	
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php?id=999999	GET SQL INJECTION	
http://vulnweb.janusec.com/Case03-SQLI-GET-STRING-AND.php?id=1	GET SQL INJECTION	
http://vulnweb.janusec.com/Case03-SQLI-GET-STRING-AND.php?id=1	GET SQL INJECTION	
http://vulnweb.janusec.com/Case03-SQLI-GET-STRING-AND.php?id=1	GET SQL INJECTION ErrorBa...	http://vulnweb.janus...

Context Menu:

- Navigate Refer URL
- Copy Refer URL
- Copy Action URL
- SQL INJECTION POC**
- Sort by Refer URL
- Delete Vulnerability
- Count

▶ Right Click Vulnerability

▶ Select SQL INJECTION POC

# SQL Injection POC

WebCruiser - Web Vulnerability Scanner Enterprise Edition

File Tools View Configuration Help

Browser Scanner SQL POC Resend Bruter Cookie Setting ScanURL ScanPage ScanSite

URL: http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1 GET

DataBase: MySQL Keyword: [[NULL]] Parameter Type: Integer Reset

Environment

Environment	Value
<input checked="" type="checkbox"/> Version	5.6.22
<input checked="" type="checkbox"/> Server	nginx/1.6.2
<input checked="" type="checkbox"/> OS	Linux
<input checked="" type="checkbox"/> user	vulnweb@localhost
<input checked="" type="checkbox"/> Database	vulnweb
<input type="checkbox"/> root_PasswordHash	

Get Environment Information Reset

17:57:22 Got : vulnweb  
17:57:43 Got : 5.6.22  
17:57:43 Got : Linux  
17:57:44 Got : vulnweb@localhost  
17:57:44 Got : vulnweb

Done HTTP Thread: 0

► Get Environment Information

# SQL Injection POC

WebCruiser - Web Vulnerability Scanner Enterprise Edition

File Tools View Configuration Help

Browser Scanner SQL POC Resend Bruter Cookie Setting ScanURL ScanPage ScanSite

URL: <http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1> GET

DataBase: MySQL Keyword: [[NULL]] Parameter Type: Integer Reset

Environment DataBase FileReader StringEncode Debug

vulnweb

- userinfo
  - id
  - username
  - description

id	username	description
2	bob	a common user
1	root	the administrator

Get\_Current\_DB\_O DataBase Table Column Rows From 1 To 2 Data Export

```
17:57:22 Got : vulnweb
17:57:43 Got : 5.6.22
17:57:43 Got : Linux
17:57:44 Got : vulnweb@localhost
17:57:44 Got : vulnweb
```

Done | HTTP Thread: 0

# XSS POC

The screenshot displays the WebCruiser - Web Vulnerability Scanner Enterprise Edition interface. The main window shows the URL `http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1` and the HTTP method `GET`. The left sidebar contains a tree view with categories: Browser, Scanner, POC, SQL Injection, XSS/LFI/RFI/Redirect, AdminEntrance, Tools, ResendTool, BruterTool, CookieTool, CodeTool, StringTool, Settings, Report, and About. The POC category is expanded, showing the configuration for the XSS/LFI/RFI/Redirect tool. The configuration fields are:

- Refer Page: `http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php`
- ActionURL( ? for Get, and ^ for POST or Cookie): `http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php?id=1<img src=0 onerror="alert(8328378)">`

Buttons for `Submit POC Test` and `Open Refer Page` are visible below the configuration fields. The bottom status bar shows the output of the scan:

```
17:57:22 Got : vulnweb
17:57:43 Got : 5.6.22
17:57:43 Got : Linux
17:57:44 Got : vulnweb@localhost
17:57:44 Got : vulnweb
```

The status bar also indicates `Done` and `HTTP Thread: 0`.

# HTTP Resend Tool

The screenshot displays the WebCruiser - Web Vulnerability Scanner Enterprise Edition interface. The main window shows the URL `http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php` and the HTTP method `GET`. The left sidebar contains a tree view with categories: Browser, Scanner, POC, Tools, and About. Under Tools, the ResendTool is selected. The main area is divided into Request and Response tabs. The Request tab shows a table with the following data:

Method	URL
POST	http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php
GET	http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php
GET	http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php

The Response tab shows the following content:

```
Content-Type: application/x-www-form-urlencoded  
  
id=1
```

The status bar at the bottom indicates "Done" and "HTTP Thread: 0".

The most simple way to launch Resend Test

- No Proxy Configuration required
- Direct modify & resend

# More

WebCruiser Web Vulnerability Scanner for Windows User Guide

<http://www.janusec.com/download/WebCruiserUserGuide.pdf>

Documentation

<http://www.janusec.com/documentation/>

Thank you!