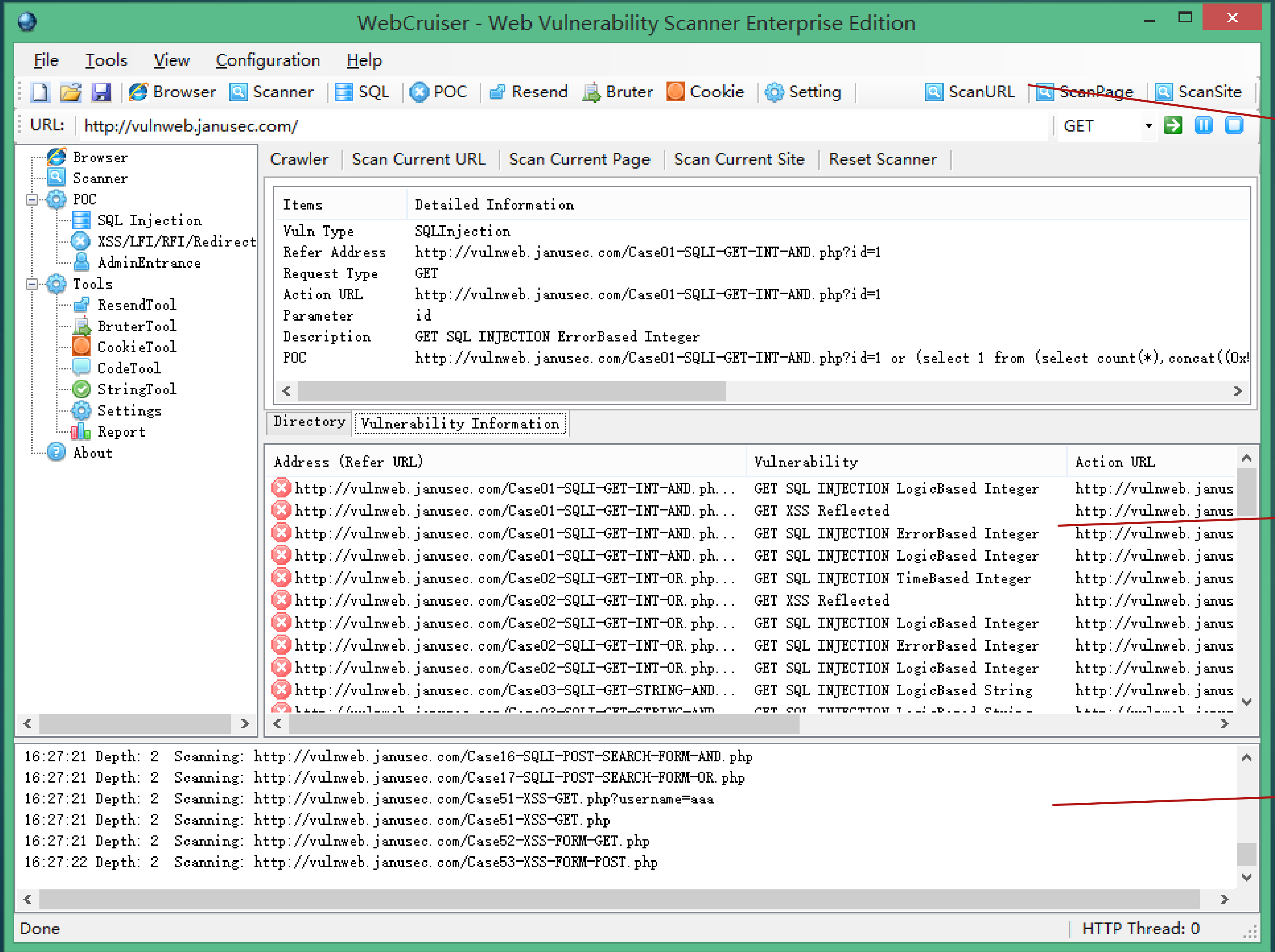
Getting Started with WebCruiser Web Vulnerability Scanner 3

@Janusec https://www.Janusec.com/

Introduction



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

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
http://vulnweb.janusec.com/Case03-SQLI-GET-STRING-AND...	GET SQL INJECTION LogicBased String	http://vulnweb.janus

```
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
```

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

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!

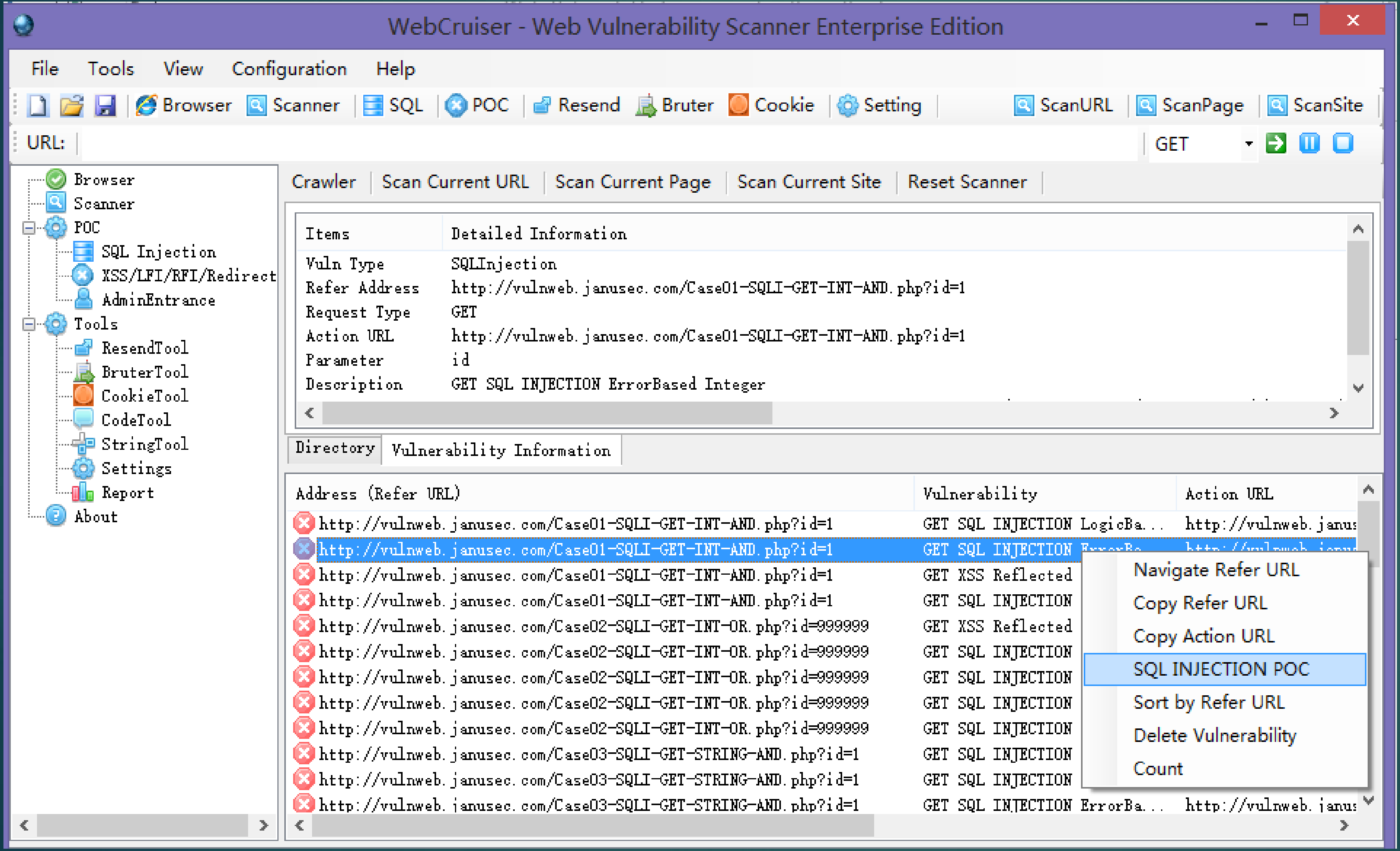
- It can support scanning website as well as POC (Proof of concept) for web vulnerabilities: SQL Injection, Cross Site Scripting, Local File Inclusion, Remote File Inclusion, Redirect etc.

- 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

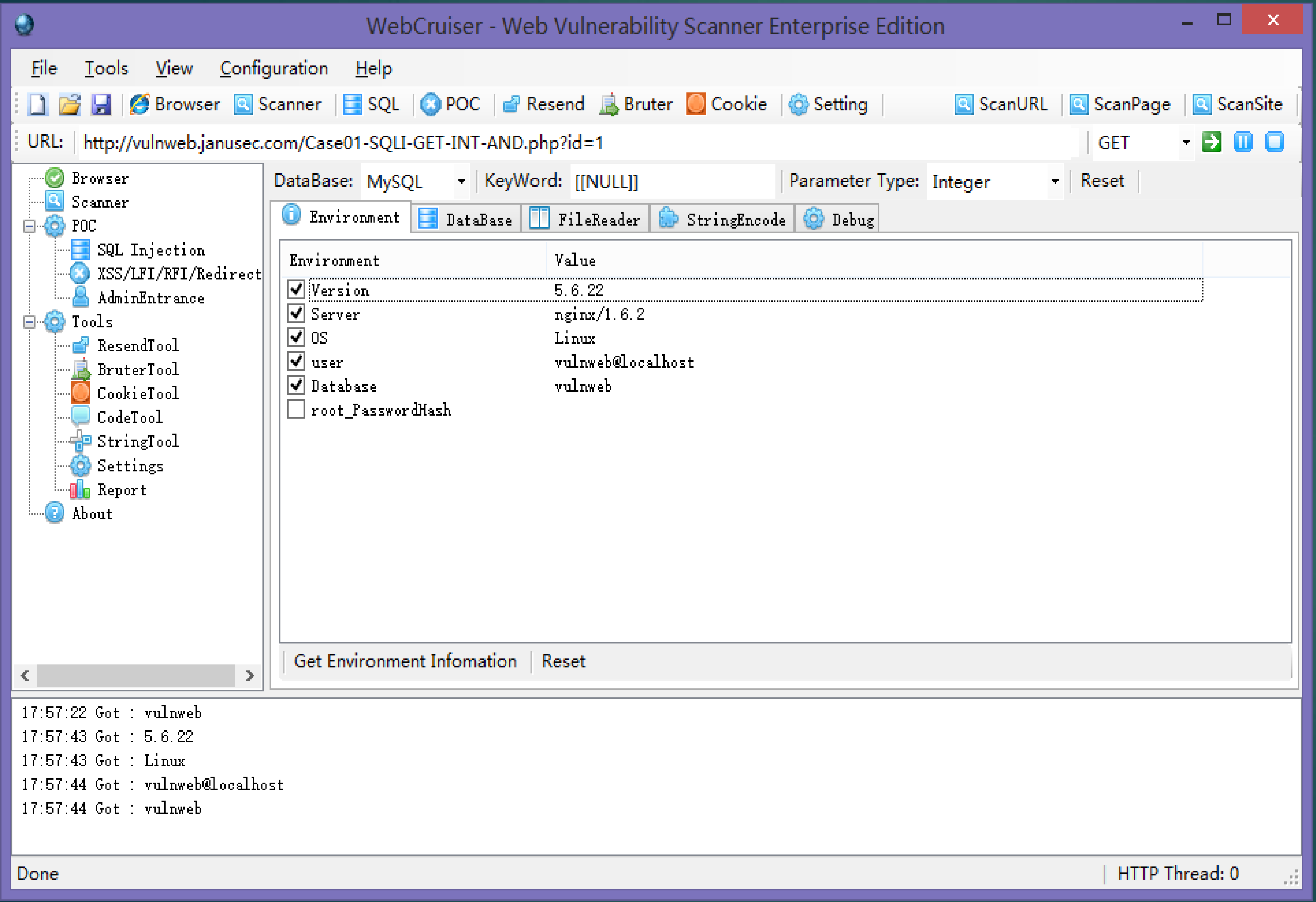


Items	Detailed Information
Vuln Type	SQLInjection
Refer Address	http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1
Request Type	GET
Action URL	http://vulnweb.janusec.com/Case01-SQLI-GET-INT-AND.php?id=1
Parameter	id
Description	GET SQL INJECTION ErrorBased Integer

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/Case02-SQLI-GET-INT-OR.php?id=999999	GET SQL INJECTION	
http://vulnweb.janusec.com/Case02-SQLI-GET-INT-OR.php?id=999999	GET SQL INJECTION	
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

- Right Click Vulnerability
- Select SQL INJECTION POC

SQL Injection POC



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

DataBase: MySQL KeyWord: [[NULL]] Parameter Type: Integer

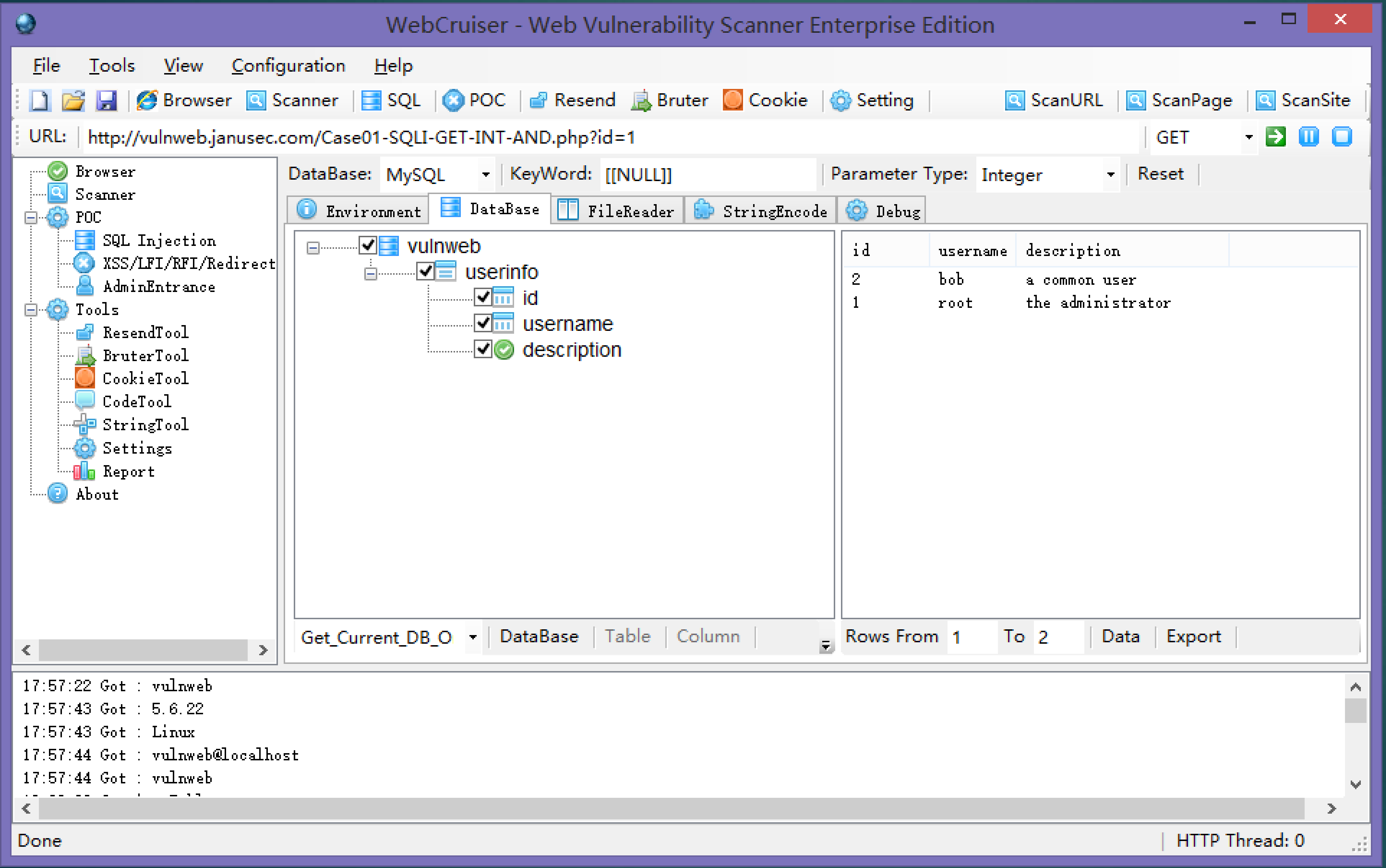
Environment	Value
☑ Version	5.6.22
☑ Server	nginx/1.6.2
☑ OS	Linux
☑ user	vulnweb@localhost
☑ Database	vulnweb
☐ root_PasswordHash	

```
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



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

DataBase: MySQL KeyWord: [[NULL]] Parameter Type: Integer

- ☑ vulnweb
  - ☑ userinfo
    - ☑ id
    - ☑ username
    - ☑ description

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

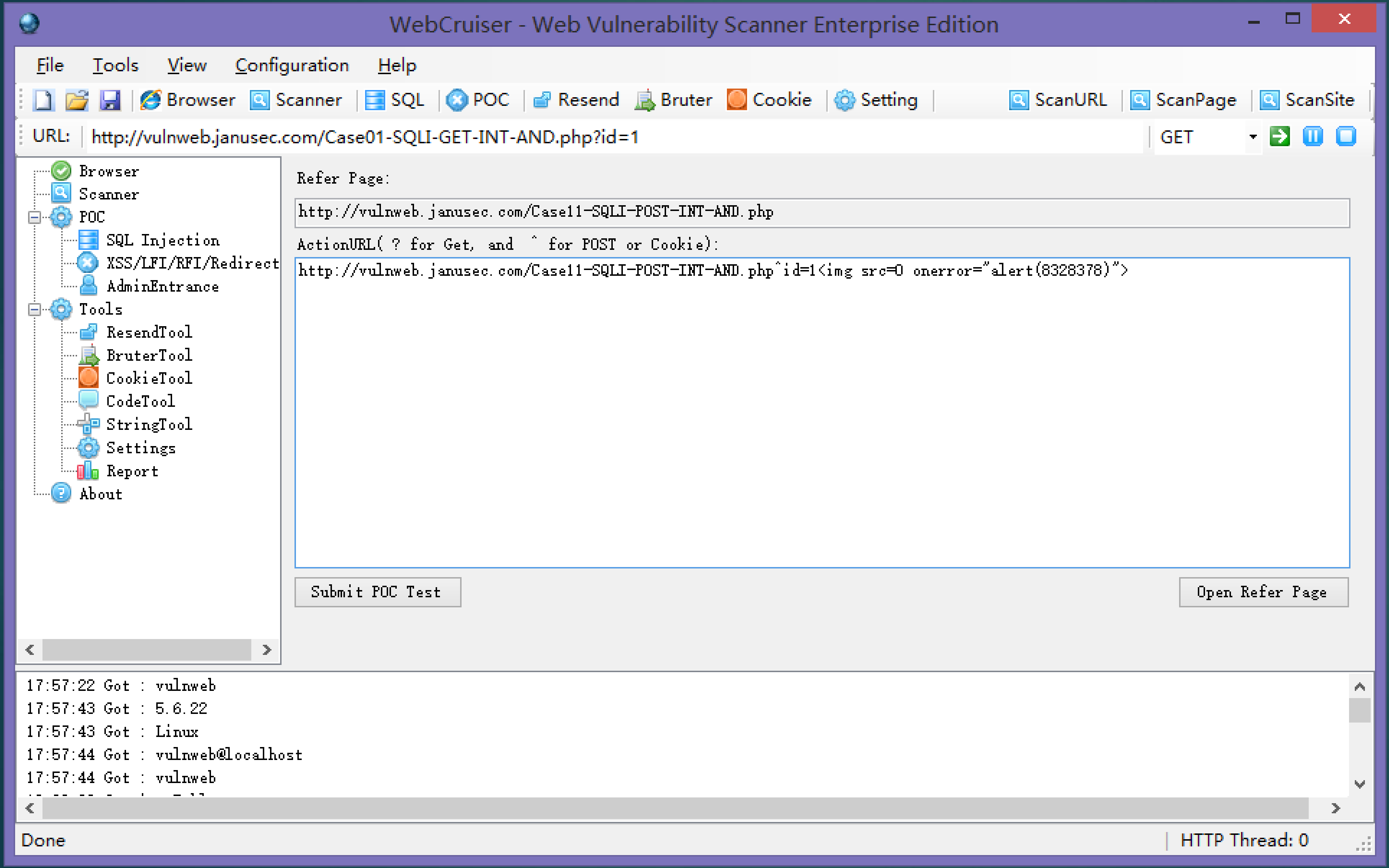
Get_Current_DB_O

Rows From 1 To 2

```
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



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

Refer Page:

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

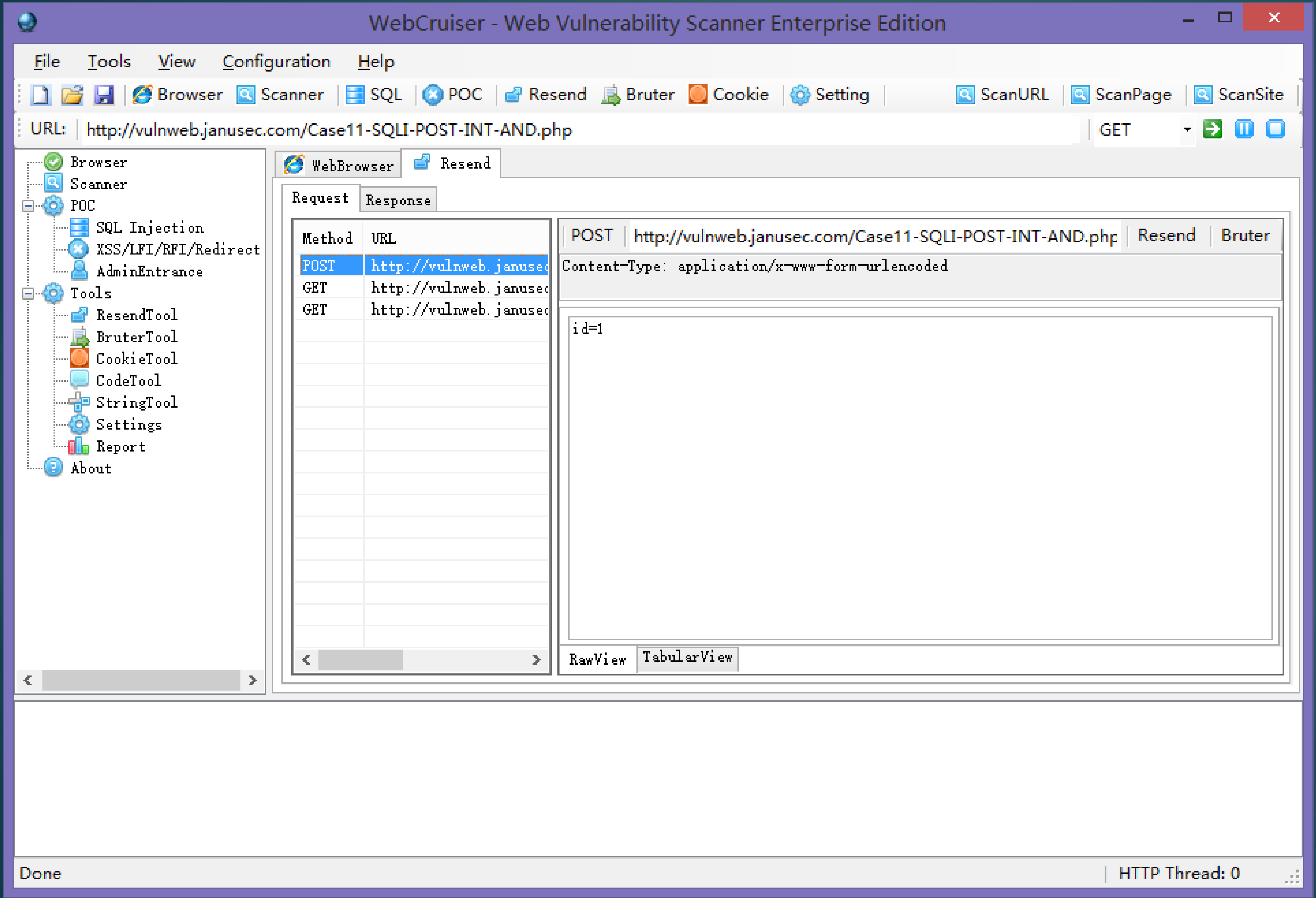
ActionURL(? for Get, and ^ for POST or Cookie):

```
http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php^id=1<img src=0 onerror="alert(8328378)">
```

```
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

HTTP Resend Tool



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

Method	URL
POST	http://vulnweb.janusec
GET	http://vulnweb.janusec
GET	http://vulnweb.janusec

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

Content-Type: application/x-www-form-urlencoded

id=1

Done

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
https://www.janusec.com/download/WebCruiserUserGuide.pdf