

WebCruiser Web Vulnerability Scanner for Mac OS X User Guide

V1.0 by Janusec, Oct 25, 2013

1 Introduction

WebCruiser Web Vulnerability Scanner for Mac OS X 10.7+, an effective and convenient web penetration testing tool that will aid you in auditing your website!

WebCruiser can find the following web vulnerabilities currently:

- GET SQL Injection(Int, String, Search)
- POST SQL Injection(Int, String, Search)
- Cross Site Scripting(XSS)

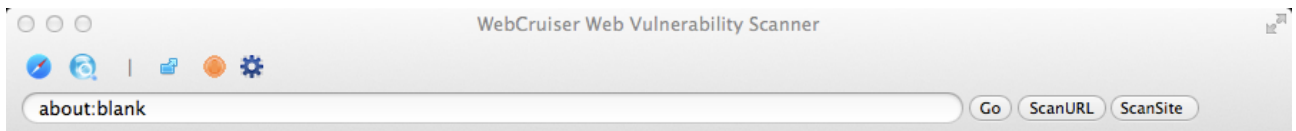
WebCruiser provide a HTTP Request resend tool (or call it HTTP repeater) and Cookie tool also.

2 Usage

Launch WebCruiser from /Application

The toolbar items include:

- Web Browser: switch to web browser view.
- Scanner: switch to scanner view, show vulnerabilities list, scanning progress.
- Resend tool: HTTP request resend tool or repeater.
- Cookie tool: View cookies, clear cookies, modify cookies.



WebCruiser Web Vulnerability Scanner

Web Vulnerability Scanner

- SQL Injection
- Cross Site Scripting

Web Security Tools

- GET/POST Resend Tool
- Cookie Tool

Vulnerabilities Demo Site: <http://vulnweb.janusec.com/>

Product Site: <http://sec4app.com>

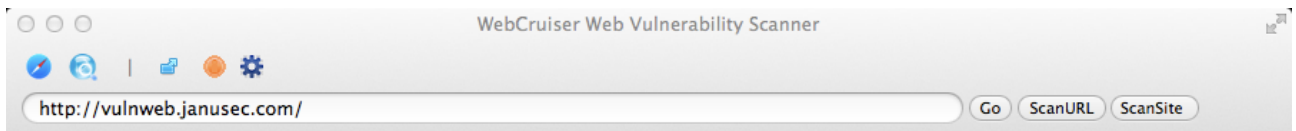
Copyright reserved by Janusec (<http://www.janusec.com/>).

- Go: navigating with designated URL.
- ScanURL: Scan vulnerabilities of designated URL.
- ScanSite: Scan vulnerabilities of whole website and begin with designated URL.

Open target site or URL

Open the target web site by entering an address and press Enter or click button Go.

Objective: To acquire cookies for subsequent scanning if authentication is required.



This is a demo site for Web Vulnerability Scanner

The index page intentionally lacks links and forms.
Please access the following pages to perform specific tests:

[index-sql.php](#)

[index-xss.php](#)

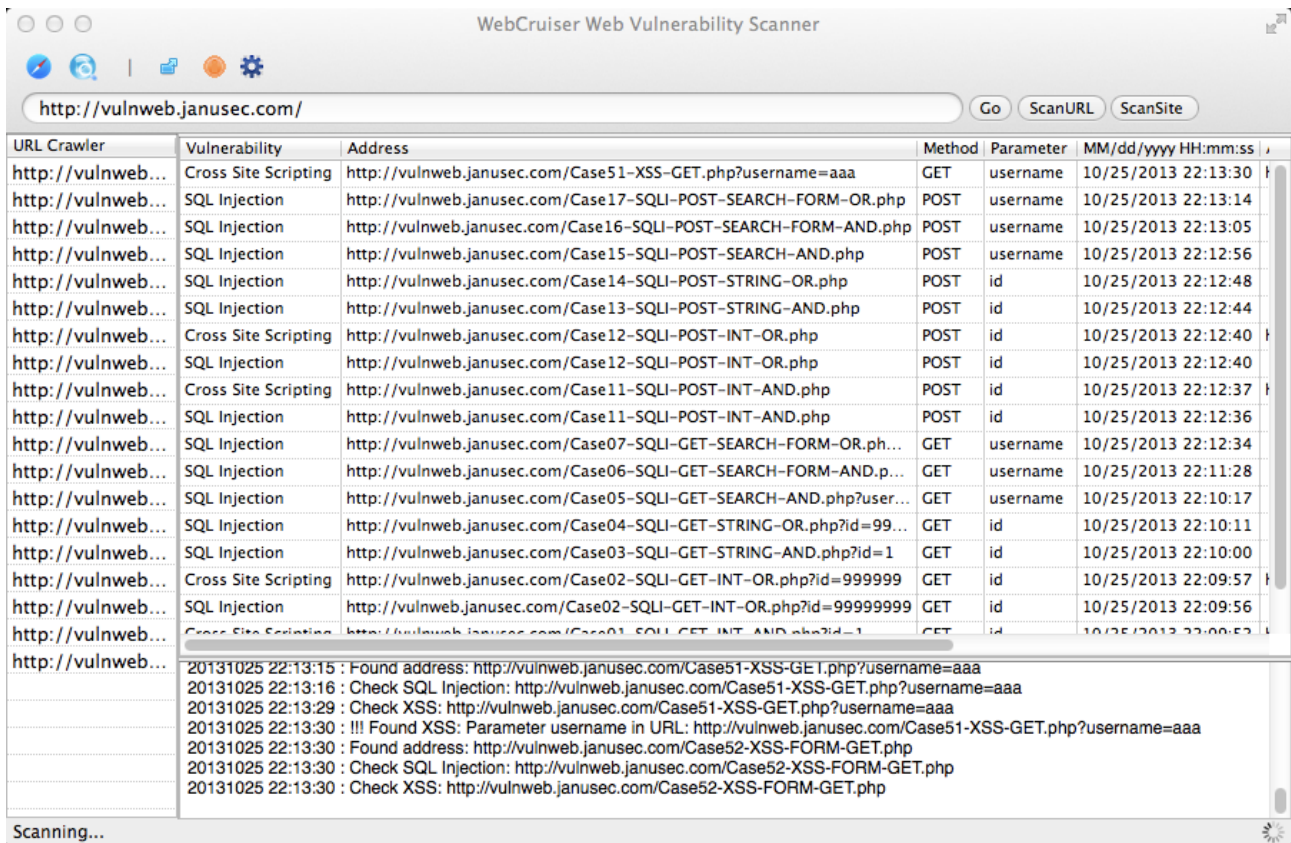
Test Objective: to get text links and continue to check vulnerabilities of them.

Scan for vulnerabilities

Click button “ScanSite” to scan whole website, or “ScanURL” to scan designated URL only.

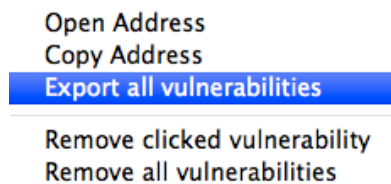
The left table lists URLs found by crawler, and the right table lists vulnerabilities found by scanner.

The right bottom textview displays the scanning progress.

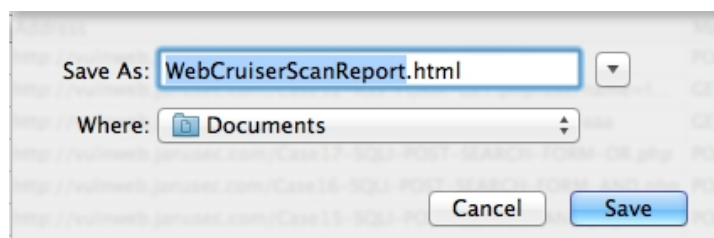


Export scan report

Right click vulnerabilities list, and select “Export all vulnerabilities”,



then, save to your selected directory.



The scan report is like the following:

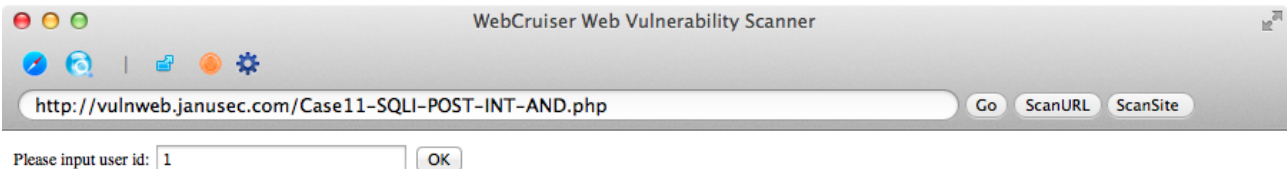
WebCruiser Scan Report

index	Name	Address	Parameter	Method	Time
1	SQL Injection	http://vulnweb.janusec.com/Case17-SQLI-POST-SEARCH-FORM-OR.php	username	POST	10/25/2013 22:13:14
2	SQL Injection	http://vulnweb.janusec.com/Case16-SQLI-POST-SEARCH-FORM-AND.php	username	POST	10/25/2013 22:13:05
3	SQL Injection	http://vulnweb.janusec.com/Case15-SQLI-POST-SEARCH-AND.php	username	POST	10/25/2013 22:12:56
4	SQL Injection	http://vulnweb.janusec.com/Case14-SQLI-POST-STRING-OR.php	id	POST	10/25/2013 22:12:48
5	SQL Injection	http://vulnweb.janusec.com/Case13-SQLI-POST-STRING-AND.php	id	POST	10/25/2013 22:12:44
6	SQL Injection	http://vulnweb.janusec.com/Case12-SQLI-POST-INT-OR.php	id	POST	10/25/2013 22:12:40
7	SQL Injection	http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php	id	POST	10/25/2013 22:12:36
8	SQL Injection	http://vulnweb.janusec.com/Case07-SQLI-GET-SEARCH-FORM-OR.php?username=	username	GET	10/25/2013 22:12:34
9	SQL Injection	http://vulnweb.janusec.com/Case06-SQLI-GET-SEARCH-FORM-AND.php?username=%25	username	GET	10/25/2013 22:11:28
10	SQL Injection	http://vulnweb.janusec.com/Case05-SQLI-GET-SEARCH-AND.php?username=%25	username	GET	10/25/2013 22:10:17
11	SQL Injection	http://vulnweb.janusec.com/Case04-SQLI-GET-STRING-OR.php?id=99999999	id	GET	10/25/2013 22:10:11
12	SQL Injection	http://vulnweb.janusec.com/Case03-SQLI-GET-STRING-AND.php?id=1	id	GET	10/25/2013 22:10:00

Display a menu

Resend tool usage

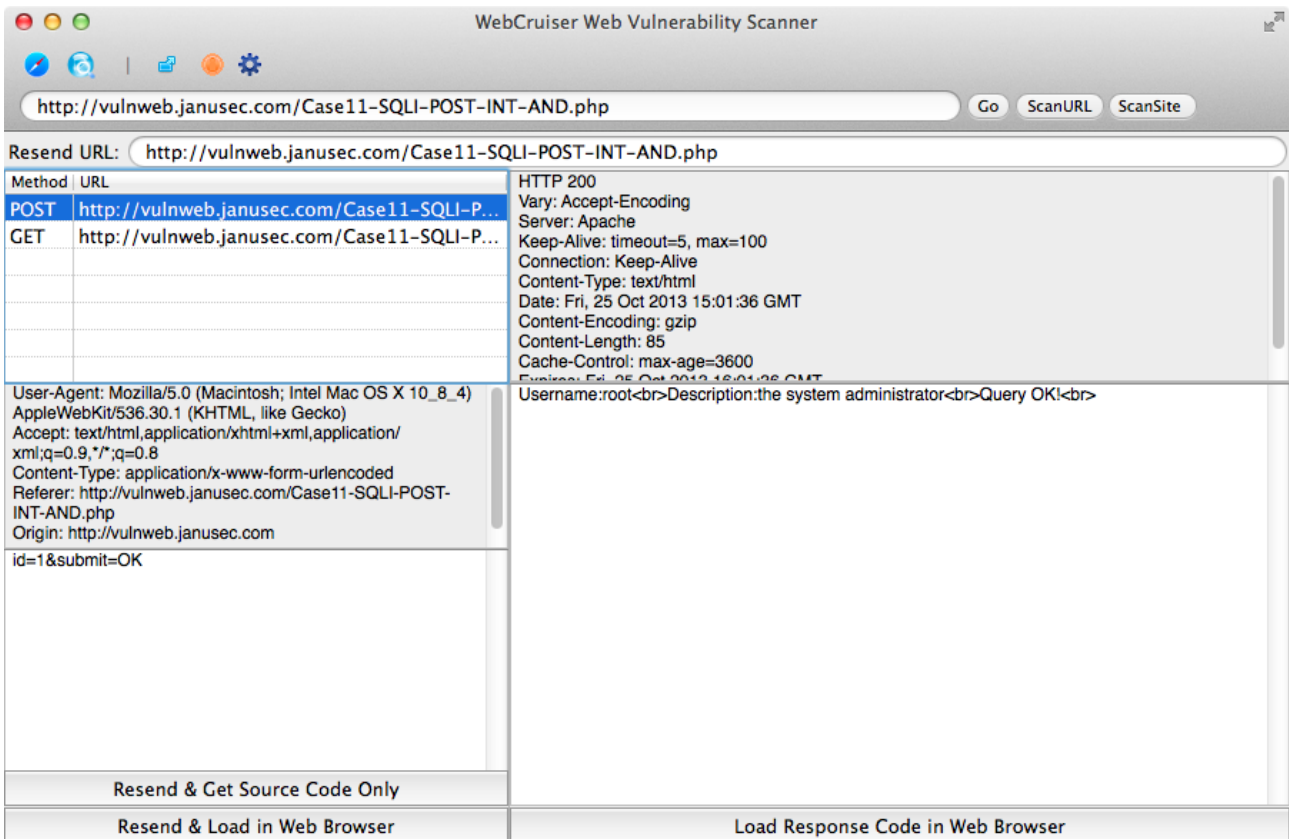
Resend tool will record each HTTP request launched by the web browser in WebCruiser, now double click a URL in URL table or vulnerabilities table to open it.



Let's simulate a POST request by click button “OK” and then switch to resend tool view manually.

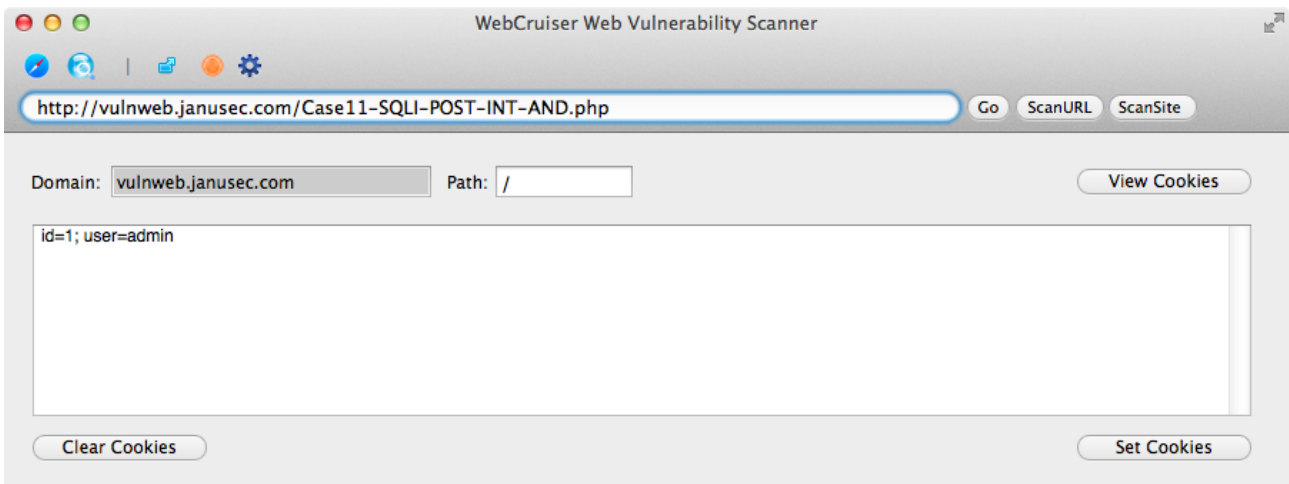
The left top table lists all HTTP requests by web browser, click one of the requests and then the detailed request information will be showed in others text fields, include request headers, post data.

There are two buttons at the left bottom, “Resend & Get Response Code Only” and “Resend & Load in Web Browser”.



Cookie tool usage

Cookie tool provide view, clear and set cookies function.



<http://sec4app.com/>

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

Copyright reserved by Janusec.