



ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

ຄວາມປອດໄພເວບໄຊ້ (Web Security)

ສອນໂດຍ: ອຈ ເພັດ ສອນວິໄລ

ມືຖື: 020 58390300

ອີເມວ: p.sonevilay@nuol.edu.la

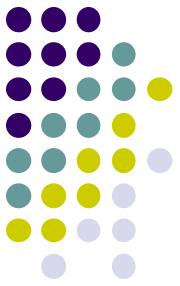


ບົດທີ10

ການນຳໃຊ້ເຄື່ອງມື WebCruiser



ເນື້ອໃນໂດຍລວມ



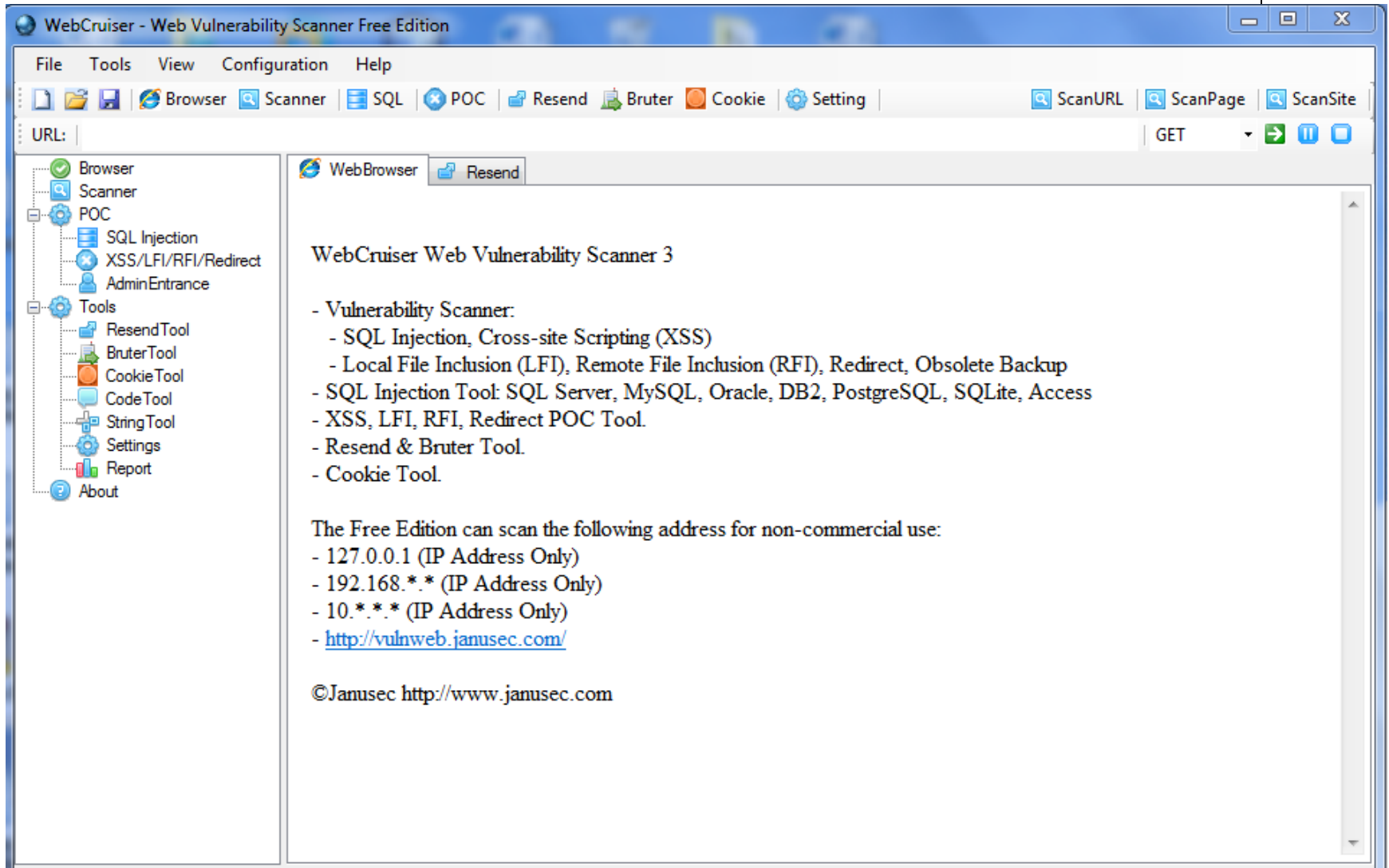
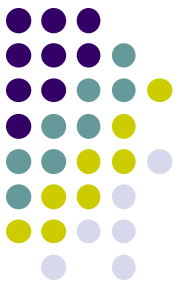
- ແນະນຳກ່ຽວກັບ WebCruiser
- ການນຳໃຊ້ WebCruiser
- ຕົວຢ່າງການທົດສອບດ້ວຍ WebCruiser



ແນະນຳກ່ຽວກັບ WebCruiser

- WebCruiser ເປັນເຄື່ອງມືທີ່ຊ່ວຍໃນການກວດສອບຫາຈຸດອ່ອນ ຫຼື ຊ່ອງໂວ່ຂອງ Web application.
- WebCruiser ສາມາດຕອບສະໜອງການກວດສອບຫາຈຸດອ່ອນຂອງເວບ POC (Proof of concept) ໄດ້ດັ່ງນີ້: SQL Injection, Cross Site Scripting, Local File Inclusion, Remote File Inclusion, Redirect ແລະອື່ນໆ.
- WebCruiser ເປັນເຄື່ອງມືທີ່ດສອບຂ້ອນຂ້າງນຳໃຊ້ງ່າຍຖ້າທຽບໃສ່ກັບເຄື່ອງມືອື່ນໆ

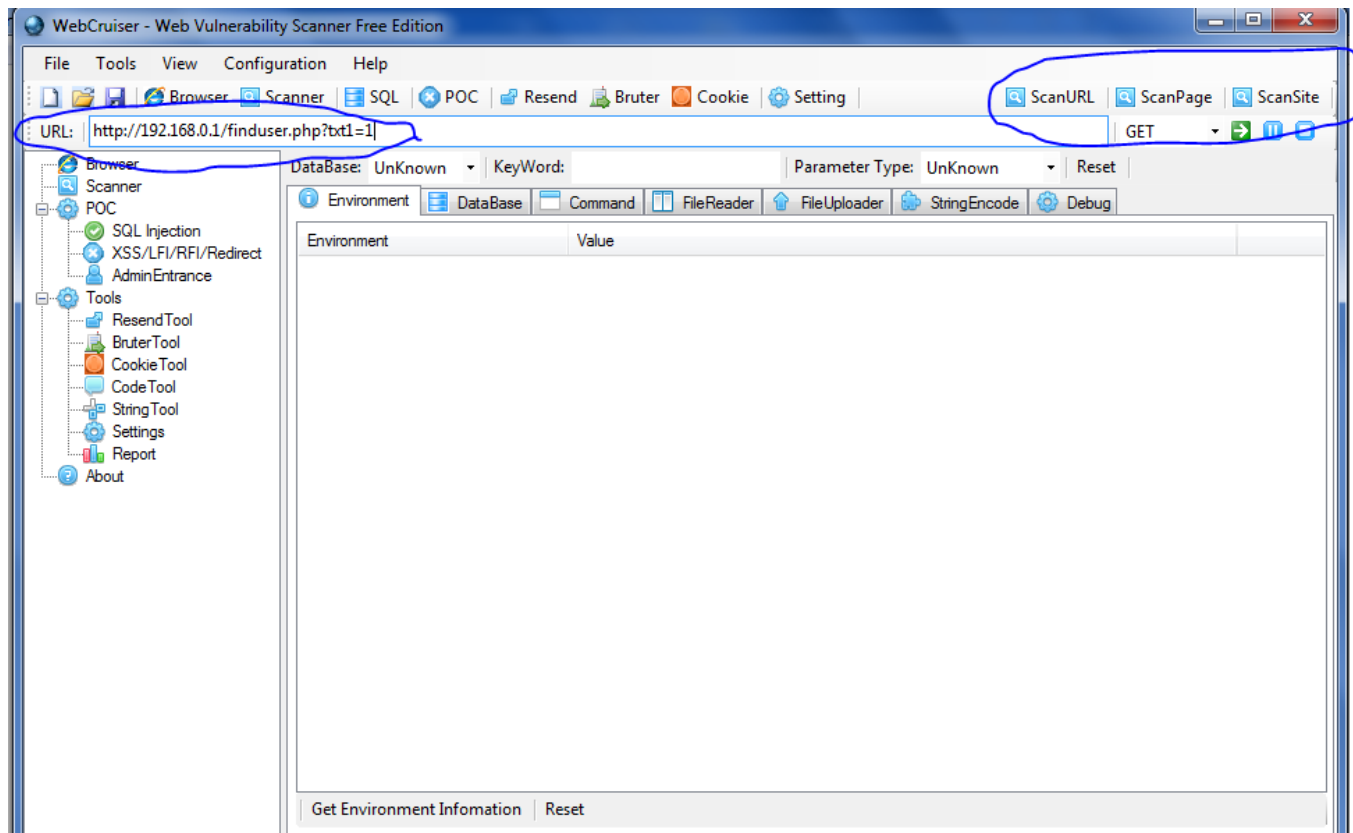
ການນຳໃຊ້ WebCruiser



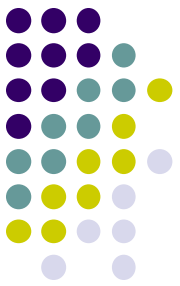
ຕົວຢ່າງການທົດສອບດ້ວຍ WebCruiser



- SQL-Injection



ຕົວຢ່າງການທົດສອບດ້ວຍ WebCruiser



The screenshot displays the WebCruiser application window. The top menu bar includes File, Tools, View, Configuration, and Help. Below the menu is a toolbar with icons for Browser, Scanner, SQL, POC, Resend, Bruter, Cookie, and Setting. The main window shows the URL `http://192.168.0.1/finduser.php?txt1=1` and the request type `GET`. The left sidebar contains a tree view with categories like Browser, Scanner, POC, SQL Injection, XSS/LFI/RFI/Redirect, AdminEntrance, Tools, ResendTool, BruterTool, CookieTool, CodeTool, StringTool, Settings, Report, and About.

The main content area is divided into two tabs: Directory and Vulnerability Information. The Vulnerability Information tab is active, showing a table of scan results. A context menu is open over the first row, with the option `SQL INJECTION POC` highlighted.

Items	Detailed Information
Vuln Type	SQLInjection
Refer Address	<code>http://192.168.0.1/finduser.php?txt1=1</code>
Request Type	GET

Address (Refer URL)	Vulnerability
<code>http://192.168.0.1/finduser.php?txt1=1</code>	GET SQL INJECTION ErrorBased
<code>http://192.168.0.1/finduser.php?txt1=1</code>	GET SQL INJECTION BooleanBased
<code>http://192.168.0.1/finduser.php?txt1=1</code>	GET SQL INJECTION TimeBased

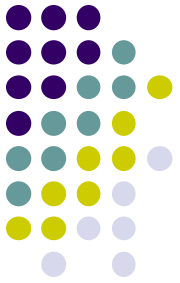
The bottom status bar shows the following log entries:

```
10:26:12 Depth: 0 Scanning: http://192.168.0.1/finduser.php?txt1=1
10:26:12 Checking SQL Injection: http://192.168.0.1/finduser.php?txt1=1
10:26:13 Checking SQL Injection, ErrorBased, Parameter: txt1
10:26:13 Found ErrorBased SQL Injection Vuln: http://192.168.0.1/finduser.php?txt1=1 or (select 1 from (select count(*),concat((0x574352575653),0x5E,floor(rand(0)*2))x from information_schem...
10:26:13 Checking SQL Injection, BooleanBased, Parameter: txt1
10:26:13 Found BooleanBased SQL Injection Vuln: http://192.168.0.1/finduser.php?txt1=1 aNd 4941801=4941801 aNd 7193=7193
10:26:13 Checking SQL Injection, BooleanBased Rlike Blind, Parameter: txt1
10:26:13 Checking SQL Injection, TimeBased, Parameter: txt1
10:26:22 Found TimeBased SQL Injection Vuln: http://192.168.0.1/finduser.php?txt1=1 oR if(length(0x574352575653)>1,sleep(3),0)
10:26:22 Checking URL XSS: http://192.168.0.1/finduser.php?txt1=1
10:26:23 Checking LFI: http://192.168.0.1/finduser.php?txt1=1
10:26:23 Checking RFI: http://192.168.0.1/finduser.php?txt1=1
10:26:23 Checking Form Vuln with Referer: http://192.168.0.1/finduser.php?txt1=1
```

ຂໍ້ມູນອ້າງອີງ



- [1] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan. Improving Web Application Security, Microsoft Corporation, 2013
- [2] ການປ້ອງກັນ ແລະ ຮັກສາຄວາມປອດໄພເຄືອຂ່າຍ, www.mict4u.net
- [3] WebCruiser Web Vulnerability Scanner for Windows User Guide
<http://www.janusec.com/download/WebCruiserUserGuide.pdf>



ព្យាបាល និង ព្យាបាល

ឧបករណ៍