## WebCruiser Web漏洞扫描器使用手册 V3

#### 目 录

1.	软件简	简介3
2.	主要項	力能4
	2.1.	Web 漏洞扫描器4
	2.2.	SQL 注入工具6
	2.3.	跨站 XSS7
	2.4.	LFI/RFI/Redirect POC
	2.5.	重放测试工具
3.	DVW	A 演示11
	3.1.	环境12
	3.2.	暴力破解12
	3.3.	SQL 注入17
	3.4.	XSS
4.	WAV	SEP 测试报告
	4.1.	测试环境及测试用例
	4.2.	测试方法
	4.3.	SQL 注入测试报告
	4.4.	XSS 测试报告21
	4.5.	LFI 测试报告
	4.6.	RFI 测试报告
	4.7.	Redirect 测试报告24

	4.8. 误报测试报告	25
5.	购买/注册	25
6.	-AQ	26
	-	

### V3.2 by Janusec

http://www.janusec.com

# 1. 软件简介



WebCruiser - Web 漏洞扫描器, 是一款轻量级但非常实用的 Web 安全扫描工具, 能够扫描 SQL 注入(SQL 注入), Cross Site Scripting(跨站), Local File Inclusion(本地文件包含), Remote File Inclusion(远程文件包含), Redirect(重定向) 等等, 并且支持漏洞的 POC(Proof of Concept, 概念验证).

与其它 Web 漏洞扫描器相比,WebCruiser 最典型的特点是能够根据设置,只扫描指定的漏洞类型,指定的 URL,或者指定的页面,通常这是其它扫描器并不具备的。

关键特性:

\* 爬虫(站点目录及文件).

\* 漏洞扫描器: SQL注入(SQL注入), Cross Site Scripting(跨站), LFI(本地文件 包含), RFI(远程文件包含), Redirect(重定向) 等.

\* 漏洞评估应用 WAVSEP v1.5 SQL 注入& XSS 测试用例 100% 通过.

\* SQL 注入 POC 工具,支持 SQL Server, MySQL, Oracle, DB2, Access.

\* POC 工具(XSS, LFI, RFI, Redirect 等).

\* 重放测试工具.

- \* 暴力猜解工具.
- \* Cookie 工具.

系统需求: .NET 框架 2.0 以上, IE8 以上

免责声明:

- \* 执行渗透测试必须获得应用所有者的授权;
- \* 扫描过程可能会造成系统的完整性受到破坏,使用前请备份业务数据;

\* 风险自担

## 2. 主要功能

#### 2.1. Web 漏洞扫描器

WebCruiser - Web 漏洞扫描器提供了 3 种扫描模式:

- ◆ ScanURL(扫描 URL):只扫描指定的 URL(地址).
- ◇ ScanPage(扫描页面):只扫描指定的页面及该页面内的链接,如果页面内的链接位 于其它目录下则跳过.
- ◇ ScanSite (扫描网站):扫描同一域名下的整个网站,如果链接属于其它域名则跳过.



扫描结果如下图所示,上方树形目录为爬虫识别的目录和文件,下方列表为扫描出来的漏洞:

9	WebCruiser - Web Vulnerability Scanner Enterprise Edition – 🗖 💌
File Tools View Conf	iguration Help Scanner   🛃 SQL   📀 XSS   📽 Resend 🚊 Bruter 🧧 Cookie   🎯 Setting   🛛 ScanURL   💽 ScanPage   💽 ScanSite
WebBrowser	Crawler   Scan Current URL   Scan Current Page   Scan Current Site   Reset Scanner
Vulner abilitys canner SQL Injection SQL Injection Cross Site Scriptin AdministrationEntre SystemTool CodeTool CodeTool StringTool CodeTool StringTool CodeTool StringTool CodeTool StringTool	<pre>wavsep</pre>
About	Address Vulnerabil
	<ul> <li>http://192_168_100_1_8080/*wvsp/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case01 URL SQL II</li> <li>http://192_168_100_1:8080/*wvsp/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case01 URL SQL II</li> <li>http://192_168_100_1:8080/*wvsp/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case03 URL SQL II</li> <li>http://192_168_100_1:8080/*wvsp/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case04 URL SQL II</li> <li>http://192_168_100_1:8080/*wvsp/active/SQL-Injection/SInjection-Detection-Evaluation-GET-500Error/Case05 URL SQL II</li> </ul>
< >	Done HTTP Thread: 0
Done	HTTP Thread: 0

右键单击漏洞项,可以发起 POC (Proof of Concept,概念验证):

URL / Refer URL	Parameter Type	KeyWord/ActionURL	Vulnerability
🐻 http://192.168.254	Corry IRI To ClinBoord	table	POST SQL INJECTION
🖸 http://192.168.25	Copy OKE TO CITPBOARD	http://192.168	Cross Site Scripting(Form)
	SQL INJECTION POC	•	• • •
	Delete Vulnerability		

### 2.2. SQL 注入工具

SQL 注入工具可以单独使用,也可以从扫描器发起 POC 验证。

WebCruiser 支持:

- \* GET/Post/Cookie 注入;
- \* SQL Server: 明文/Union/盲注;
- \* MySQL/DB2/Access: Union/盲注;
- \* Oracle: Union/盲注/跨站式注入;

右键单击漏洞,选择 SQL Injection POC (SQL 注入验证).



WebCruiser 会切换到 SQL 注入工具,并自动填充相关信息.

如下是一个 SQL 注入示例.

<b>9</b>	WebCruiser - W	eb Vulnerability Scanner	Enterprise Edition	- 🗆 🗙
File Iools View Confi URL: http://vulnwebjanusec URL: http://vulnwebjanusec Scanner POC SQL Injection XSS/LIJ/RIJ/Redirec AdminEntrance CookiFool CookiFool CookiFool StringTool StringTool StringTool StringTool About	iguration Help Scanner SQL POC POC com/Case01-SQLI-GET-INT-AND DataBase: MySQL • KeyW Environment DataBase Knvironment Version Server SS user V Database root_PasswordHash	Resend 🔊 Bruter 💽 Cookie uphp?id=1 ord: Username PileReader 🔊 StringEncod Value vulnweb		InPage ScanSite
< >> Done	Get Environment Infomation	Reset	HTTP Thread: 0	

小提示:详细的扫描日志默认是关闭的,如果您需要,可以在注册表中添加一个键值打开:

HKCU\Software\Sec4App\WebCruiser

在上述位置添加一个字符串键值 Edition: Debug ,然后重新启动 WebCruiser.

WebCruiser 将在程序同一目录下生成形如 WebCruiseryyyymmdd.log 的日志文件。

Edition REG\_SZ Debug

#### 2.3. 跨站 XSS

右键单击漏洞,选择 "XSS POC":

Address			Vulnerability
http://192.168.100.	Navigate URL Copy URL To ClipBoard XSS POC Sort by Address Delete Vulnerability	/RXSS-Detection-Evaluation-GE	ReflectedXSS-GET
<		]	>

检查待提交的数据,点击"Submit POC 测试"(提交).

😔 WebCruiser - Web Vulnerability Scanner Enterprise Edition – 🗖 🗖	
File       Iools       Yiew       Configuration       Help         Image: Second Sec	1
Submit XSS Test	
Vsage: * Launch, from Scanner, right click vulnerability item and select "XSS POC"; * Click "Submit XSS Test" to get the response code. Done HTTP Thread: 0	

提交之后,刚才输入的脚本会出现在响应代码中:

WebCruiser - Web Vulnerability Scanner Enterprise Edition         -	×
WebCruiser - Web Vulnerability Scanner Enterprise Edition       -         File       Lools       Yew Configuration       Help         WebCruiser Scanner       SQL       XSS       Resend       Bruter       Cookie       Setting       ScanURL       ScanPage       S ScanSite         URL:       05:8080/wavsep/active/Reflected-XSS/RXSS-Detection-Evaluation-GET/Case01-Tag2HtmlPageScopejsp?userinput=textvalue       GET       *       Image: ScanSite         WebBrowser       VulnerabilityScanner       (PCTVTE hal PUBLIC "-//WSC//UTD HTML 4.01 Transitional//EM" "http://www.w3.org/TR/html4/loose.dtd">         SQL Injection       (PCTVTE hal PUBLIC "-//WSC//UTD HTML 4.01 Transitional//EM" "http://www.w3.org/TR/html4/loose.dtd">         SQL Injection       (PCTVTE hal PUBLIC "-//WSC//UTD HTML 4.01 Transitional//EM" "http://www.w3.org/TR/html4/loose.dtd">         SQL Injection       (PCTVTE hal PUBLIC "-//WSC//UTD HTML 4.01 Transitional//EM" "http://www.w3.org/TR/html4/loose.dtd">         Mainistrational       (Ada)       (Ada)       (Ada)         CookisTool       SystemTool       (Ada)       (Ada)       (Ada)         BruterTool       (Ada)       (Ada)       (Ada)       (Ada)         StringTool       Settings       Report       (About       (Ada)       (Ada)         BruterTool       (Ada)       (Ada)       (Ada)	×
	~
Content     Code From Current URL     Get Code From Current Browser       Done     HTTP Thread: 0	

## 2.4. LFI/RFI/Redirect POC

LFI(本地文件包含), RFI(远程文件包含), Redirect(重定向) 等漏洞的概念验证,同 XSS POC.

#### 2.5. 重放测试工具

当您通过内置浏览器提交数据的时候, WebCruiser 会自动捕获, 演示如下:



切换到"Resend"(重放)界面,可以看到刚才提交的请求列表:

9	WebCruiser - Web Vulnerability Scanner Enterprise Edition -	×
File Iools View Configura File Iools View Configura WebBrowser	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -         rration       Help         anner       SQL       XSS       Resend       ScanPage       ScanPage <td>ScanSite</td>	ScanSite
SystemTool     ResenTool     Cookifool     Cookifool     Cookifool     StringTool     Settings     Report     About	GET       http://vulnweb.januseo         GET       http://vulnweb.januseo         Image: State St	
完成	HTTP Thread: 0	

现在,我们可以修改这些数据并重新送出.比如,我们执行一个 SQL 注入:

#### 首先,修改 id 参数值为 1 and 1=1 提交:



然后,修改为1 and 1=2

9	WebCruiser - Web Vulnerability Scanner Enterprise Edition – 🗖 🗖
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> onfig	uration <u>H</u> elp
: 🗋 📔 🛃 🧭 Browser 💽 S	canner 📑 SQL   🚳 XSS 🛛 🔐 Resend 🚊 Bruter 🦲 Cookie 🧠 Setting 📔 🛛 🖾 ScanURL 🔤 ScanPage 🔤 ScanSite
URL: http://vulnweb.janusec.o	xom/Case11-SQLI-POST-INT-AND.php GET 🔹 🔁 🕕 📮
WebBrowser	🏈 WebBrowser 🧧 Resend
POC(Proof Of Concept)	Request Response
	Method URL POST http://vulnweb.janusec.com/Case11-SQLI-POST-INT-AND.php Resend Bruter
AdministrationEntre	POST http://vulnweb.janusec Content-Type: application/x-www-form-urlencoded GET http://vulnweb.janusec
Bystemiool ResendTool	GET http://vulnweb.janusec
BruterTool	id=1 and 1=2
Stringsool	
About	
	< >> RawView TabularView
< >	
Done	THIF HIEAU. V
9	WebCruiser - Web Vulnerability Scanner Enterprise Edition – 🗖 🗖
	WebCruiser - Web Vulnerability Scanner Enterprise Edition – – – – – – – – – – – – – – – – – – –
€       File     Iools       ∑iew     Config       ∑     ☑       ☑     ☑       ☑     ☑	WebCruiser - Web Vulnerability Scanner Enterprise Edition       –
File Iools View Config	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -
File Iools View Config WebBrowser S WebBrowser	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -
File Iools View Config File Iools View Config Browser S URL: http://vulnwebjanusec.c WebBrowser VulnerabilityScanner O FOC (Proof Of Concept) SUL Thiestion	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -
File Iools View Config File Iools View Config Browser C S URL: http://vulnweb.janusec.c WebBrowser VulnersbilityScanner POC(Proof Of Concept) SQL Injection Cross Site Scriptir	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -
File Iools View Config File Iools View Config WebBrowser S Wull: http://vulnwebjanusec.c WebBrowser File VulnerabilitySoanner File VulnerabilitySoanner Sul Injection Cross Site Scriptir AdministrationEntre SystemIool	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -
File Iools View Config Browser S S URL: http://vulnwebjanusec.co WebBrowser VulnerabilitySoaner OC(Proof Of Concept) SQL Injection Cross Site Soriptir AdministrationEntre SystemTool ResendTool ResendTool	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration       Help         canner       SQL       XSS       @ Resend       Bruter       Cookie       Setting       ScanURL       ScanPage       ScanSite         com/Case11-SQLI-POST-INT-AND.php       GET       •
File Iools View Config Browser S URL: http://vulnwebjanusec.c WebBrowser VulnerabilitySoanner OC(Proof Of Concept) SQL Injection Cross Site Scriptir AdministrationEntre SystemTool BruterTool CookieTool	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       -       SQL       XSS       Resend       Bruter       Cookie       Setting       ScanURL       ScanPage       ScanSite         com/Case11-SQLI-POST-INT-AND.php       GET       •
File Iools View Config Bile Iools View Config WebBrowser WebBrowser POC(Proof Of Concept) SQL Injection Cross Site Soriptir AdministrationEntre SystemTool ResentTool BruterTool CookieTool CookieTool StringTool	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       -       SQL       SSCanURL       ScanPage       ScanSite         com/Case11-SQLI-POST-INT-AND.php       GET       •
File Iools View Config Browser S URL: http://vulnwebjanusec.co WebBrowser VulnerabilityScanner POC(Froof Of Concept) SQL Injection Cross Site Scriptir AdministrationEntre SystemTool Cookifool Cookifool StringTool Settings Benort	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       Canner SQL & XSS & Resend Bruter Cookie & Setting & ScanURL & ScanPage & ScanSite         com/Case11-SQLI-POST-INT-AND.php       GET *       Image: Cookie & Setting & GET *       Image: Cookie & Setting & GET *       Image: Cookie & Setting & Setting & Cookie & Setting & Setting & Cookie & Setting & Setting & Cookie & Setting & Setting & Setting & Seting & Setting & Setting & Setting & Settin
File Iools View Config Browser S S URL: http://vulnwebjanusec.co WebBrowser DOC(froof 0f Concept) SQL Injection Cross Site Scriptir AdministrationEntre SystemTool CookieTool CookieTool CookieTool StringTool Settings Report About	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -
File Iools View Config Browser S S URL: http://vulnwebjanusec.co WebBrowser VulnerabilitySoaner POC(Proof Of Concept) SQL Injection Cross Site Soriptir AdministrationEntre SystemTool CookieTool CookieTool CookieTool Settings Report About	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -
File Iools View Config Browser S URL: http://vulnwebjanusec.co WebBrowser VulnerabilitySoanner POC(Proof Of Concept) SQL Injection Cross Site Soriptir AdministrationEntre SystemTool ResendTool CodeTool CodeTool StringTool StringTool Administration CodeTool CodeTool StringTool StringTool Administration CodeTool Co	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       -       SQL > XSS Present       Resend Present       ScanURL < ScanPage ScanSite
File Iools View Config WebBrowser WebBrowser SURL: http://vulnwebjanuse.cc WebBrowser SUL Injection FOC(Froof Of Concept) SUL Injection Cross Site Scriptir AdministrationEntre ResentTool CookieTool CookieTool StringTool StringTool StringTool About	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       -       ScanURL ScanPage ScanSite         canner SQL & XSS Resend Bruter Cookie Scatting       ScanURL ScanPage ScanSite         com/Case11-SQLI-POST-INT-AND.php       GET •       Image: ScanSite         WebBrowser       Resend       -       Image: ScanURL ScanPage ScanSite         Image: Response       Image: Response       -       Image: ScanURL ScanPage ScanSite         Image: Response       Image: Response       -       Image: ScanURL ScanPage ScanSite         Image: Response       Image: Response       -       Image: ScanURL ScanPage ScanSite         Image: Response       Image: Response       -       Image: ScanURL ScanPage ScanSite         Image: Response       Image: Response       -       Image: ScanURL ScanPage ScanSite       Image: ScanURL ScanPage ScanSite         Image: Response       Image: ScanURL ScanPage ScanSite       Image: ScanURL ScanPage ScanSite       Image: ScanURL ScanPage ScanSite       Image: ScanURL ScanSite         Image: Response       Image: ScanSite ScanSite       Image: ScanSite ScanSite ScanSite       Image: ScanSite Scan
File Iools View Config WebBrowser WebBrowser POC(Proof Of Concept) SystemTool ResentTool BruterTool CookeTool StringTool StringTool AdministrationEntre Administration	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       -       ScanURL ScanPage ScanSite         canner SQL XSS Resend Bruter Cookie Scatting       ScanURL ScanPage ScanSite         com/Case11-SQLI-POST-INT-AND.php       GET *       Image: ScanSite         #webBrowser       Response         Image: Response       -       -         Image: Response       -       -         Sever: nginx/1.6.2       -       -         Y-Powered By: PHP/5.3.3       -       -         SQL=select * from userinfo where id=1 and 1=2(br)No Record!       -       -
File Iools View Config Browser S S URL: http://vulnwebjanusec.co WebBrowser OC(Froof Of Concept) SQL Injection Cross Site Soriptir AdministrationEntre SystemTool BruterTool CookieTool CodeTool StringTool StringTool About	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       -       SQL ScanURL ScanPage ScanSite       ScanSite         com/Case11-SQL1-POST-INT-AND.php       GET *       •       •       •         @ WebBrowser       Resend       -       •       •       •       •         [ransfer=Enoding: chunked       Connection: keep=live       •
File Iools View Config Browser S URL: http://vulnwebjanusec.co WebBrowser VulnerabilitySoanner POC(Froof Of Concept) SQL Injection Cross Site Soriptir AdministrationEntre SystemTool Cookifool Cookifool StringSol Settings Report About	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration       Help       -       -       ×         canner       SQL       XSS       Resend       Bruter       Cookie       Setting       ScanURL       ScanPage       ScanSite         com/Case11-SQL-POST-INT-AND.php       GET       •       Image: Constant ScanPage       <
File Iools View Config Browser S S URL: http://vulnwebjanusec.co WebBrowser VulnerabilitySoanner VulnerabilitySoanner SQL Injection SQL Injection Cross Site Soriptir AdministrationEntre SystemTool CookieTool CookieTool CookieTool Stettings Report About	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration Help       canner       SQL © XSS @ Resend @ Bruter © Cookie © Setting © ScanURL © ScanPage © ScanSite         com/Case11-SQLI-POST-INT-AND.php       GET •       Image: Consection: Response         Preafer=Encoding: chunked       Content-Type: text/hml         Content-Type: text/hml       Date: Pri, 16 Jan 2015 01:54:09 GMT         Server: nginx/1.6.2       X-Towered=Tpy: PMP/5.3.3         SQL=select * from userinfo where id=1 and 1=2(br>No Record!       Image: Consection PMP/5.3.3
File Iools View Config WebBrowser WebBro	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -       -       ×         uration       Help       -       -       ×         canner       SQL (• XSS (• Resend (• Bruter (• Cookie (• Setting (• ScanURL (• ScanPage (• ScanSite com/Case11-SQL1-POST-INT-AND.php)       GET (• (• ) (• ) (• ) (• ) (• ) (• ) (• )

# 3. DVWA 演示

DVWA (Damn Vulnerable Web Application, 这是一个故意制作的含有漏洞的应用) V1.8

可以看到,两次请求得到了不同的响应.意味着这里可能存在着 SQL 注入漏洞.

测试演示,使用 WebCruiser.

#### 3.1. 环境

操作系统: Windows 8.1 or Windows 7

运行框架: .Net Framework 3.5

PHP+MySQL: XAMPP V3.2.1

DVWA 设置文件 config.inc.php:

\$\_DVWA[ 'db\_server' ] = 'localhost';

\$\_DVWA[ 'db\_database' ] = 'dvwa';

\$\_DVWA[ 'db\_user' ] = 'root';

\$\_DVWA[ 'db\_password' ] = '123456';

\$\_DVWA['default\_security\_level'] = "low";

访问 http://127.0.0.1/DVWA/login.php

		- 🗆 🗙
🔶 🔿 🖾 http://127.0.0.1/DVWA/login.php	þ	幕 🛧 🕆 しゃの
🔀 Damn Vulnerable Web A 🗙		
	DVWA	^
Username		
Password		
	Login	~
		🔍 100% 👻 📑

#### 3.2. 暴力破解

首先,任意输入用户名和密码,比如 123 和 456:

0	WebCruiser - Web Vulnerability Scanner Enterprise Edition	- 🗆 🗙
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> onf	iguration <u>H</u> elp	
📘 🚰 🛃 🧭 Browser 💽	Scanner   📑 SQL   🔇 XSS   💣 Resend 🚊 Bruter 🧕 Cookie   💼 Report   🍪 Setting	🔍 Scan Site 🛛 🔍 Scan URL
URL: http://127.0.0.1/dvwa/	login.php	GET 🔹 🄁 🛄 🔲
WebBrowser VulnerabilitySeamer POC(Proof Of Concept) Cross Site Soriptin AdministrationEntre BruterTool CookieTool CookieTool StringFool Settings About	Vebbrowser Resend	
< >		
Done		HTTP Thread: 0

提交之后切换到重放"Resend"界面.

0	WebCruiser - Web Vulnerability Scanner Enterprise Edition	- 🗆 🗙
<u>File T</u> ools <u>V</u> iew <u>C</u> onfig	guration <u>H</u> elp	
🗄 🗋 对 🛃 🧭 Browser 🔍 S	canner 🛛 📑 SQL 🛛 🔇 XSS 🖙 Resend 🚊 Bruter 🥘 Cookie 🛯 🕕 Report 🖓 Setting	🔍 Scan Site 🛛 🔍 Scan URL
URL: http://127.0.0.1/dvwa/lc	ogin.php	GET 🔹 🄁 🛄 🔲
	🧭 WebBrowser 🧧 Resend	
VulnerabilityScanner	Request Response	
SQL Injection	IIII http://127.0.0.1/daga/logia.php	Recend Bruter
- 😳 Cross Site Scriptir		Resend Druter
AdministrationEntre	GET http://127.0.0.1/dvwa/ GET http://127.0.0.1/dvwa/ Cookie: security=low; PHPSESSID=mb8kos6lpj6nmvlm7h03kk0ge4	
ResendTool	GET http://192.168.106.46/	
	GET http://192.168.106.46/	
CookieTool	GET http://192.168.106.46/	
CodeTool	GET http://192.168.106.46/	
Settings	GET http://192.168.106.46/	
	GET http://192.168.106.46/	
	GET http://192.168.106.46/	
	GET http://192.166.106.46/	
	POST http://192.168.106.46/	
	GET http://192.168.106.46/	
	GET http://192.168.106.46/	
	GET http://192.168.106.46/	
	GET http://192.168.106.46/	
	GET http://192.168.106.46/	
	TUS1 http://192.100.100.40/	
	GE1 http://132.100.100.40/	
	KawView TabularView	
< >		
Done		HTTP Thread: 0

选择刚才提交的含有 123 和 456 的请求. 点击重放界面右上角的"Bruter".

0	WebCruiser - W	/eb Vulnerability Scanner Enterprise Edition		- 🗆 🗙
File Iools View Conf Conf URL: http://127.0.0.1/dwwa/ VulnerabilitySeamer POC(Froof Of Concept) SystemTool CodeTool StringTool StringTool About	WebCruiser - W iguration Help Scanner SQL XSS http://127.0.0.1/dwwa/login.p username=123&password=456&Log vsername Field username=ad Username Field username Option © Use username list and Username List File Fassword List File Combo List File Stop when found one u Username	/eb Vulnerability Scanner Enterprise Edition Resend Bruter Cockie Cockie Setting hp in=Login min&password=123456 v Password Field password v FOST v Reset sername.vst password list(if password include username, use %username% ) username.txt password list combo.txt sername/password. Password Password	GET           GET	<ul> <li>×</li> <li>Scan URL</li> <li>→</li> <li>→</li> <li>↓</li> <li>↓</li></ul>
< >> Done			HTTP :	Thread: 0 _;;

可以看到,已经自动识别出用户名和密码字段(如果用了其它不规则的字段名,手工选择它) 这里有两种方式进行暴力尝试,一种是使用单独的用户名列表和单独的密码列表,尝试每一 种组合,第二种是利用网络上已经泄露的(用户:密码)快速进行尝试。

字典文件位于 WebCruiser 的同级目录下,可以打开查看并进行自定义修改。

其中 username.txt 和 password.txt 一起使用, combo.txt 单独使用。

点击"Go"发起猜解.

WebCruiser - Web Vulnerability Scanner Enterprise Edition         -	
File Iools View Configuration Help	Scan URL
URL:       http://127.0.0.1/dwwa/login.php       GET •         WebBrowser       VulnerabilityScamer         POC(Froof Of Concept)       SQL Injection         SQL Injection       SQL Injection         SQL StatistationEntre       PassendTool         BruterTool       CookieTool         CookieTool       CodeTool         StringTool       Settings         About       Vusername List file         Username List File       username.txt         Password List File       combo(txt         Combo List File       combo(txt         Stop when found one username/password.       Username         Visername       Password	
Done HTTP Three	ad: 0 .::

#### 很快就找到了一种组合: admin/password .

切换到内置浏览器, 输入刚才猜出的用户名和密码登录.



登录之后,检查 "DVWA Security"页面,确保安全级别为低 low.

登录之后的第一个测试,是另外一个暴力猜解测试.

0	WebCruiser - Web Vul	nerability Scanner Enterprise Edition 🛛 🚽 🗖 💌
File <u>T</u> ools <u>V</u> iew <u>C</u> onfiguratic <b>D</b> 20 <b>F</b> Browser <b>S</b> Scanne URL: http://127.0.0.1/dvwa/vulnera	n <u>H</u> elp r   <mark>]≣</mark> SQL   <b>(⊗</b> XSS   <b>⊴</b> Resend bilities/brute/	📓 Bruter 🧧 Cookie 👔 Report   🍪 Setting   🔍 Scan Site   🔍 Scan URL
VuherabilitySonner VuherabilitySonner O POC(Froof Of Concept) SQL Injection Cross Site Scriptir AdministrationEntre	bBrowser 💣 Resend	DYWA
ResendTool BruterTool CookieTool StringTool Settings Report About	Home Instructions Setup Brute Force Command Execution CSRF Insecure CAPTCHA File Inclusion SQL Injection SQL Injection (Blind) Upload	Vulnerability: Brute Force         Login         Username:         Password:         Login         Login         More info         http://www.security/ocus.com/infocus/1192         http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-withplanet
< > <		>
		HTTP Thread: 0

重复刚才的过程,任意输入,然后切换到重放 "Resend":

File Tools Yiew Configuration Help   Help Stans Scanner SQL XSS Resend Bruter Cookie Report Setting Scan Site Scan VLL   URL: http://127.0.0.1/dvwa/vulnerabilities/brute/?username=5558/password=6668/Login=Login GET - Image: Cookie Setting Scan Site Scan VLL   WulnerabilityConner Superson Sesting Sesting Sesting Setting Image: Cookie Sesting Setting Image: Cookie Image: Scan VLL   System Tool Setting Setting Setting Image: Cookie Image: Cookie Setting Image: Cookie Setting Image: Cookie Setting Image: Cookie Image: Cookie Setting Image: Cookie<	😔 WebCruiser - Web Vulnerability Scanner Enterprise Edition – 🗖	×
061     attp://192.168.106.       GET     http://192.168.106.	WebCruiser - Web Vulnerability Scanner Enterprise Edition       -         File Iools View Configuration Help         Image: Second String Str	x URL
÷dt UTTP Thread: 0	GET             http://192.168.106. GET             http:/192.168.106. GET             http:/192.168.106. GET             http:/192.168.106. GET             http:/192.168.106. GET             http:/192.168.106. GET             http:/192.168.106. GET	

#### 点击"Bruter":

0	WebCruiser - W	eb Vulne	erability Scanner Enterprise Edition		- 🗆 🗙
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> onfig	uration <u>H</u> elp				
📄 📴 🛃 🧭 Browser 💽 Sc	anner 📑 SQL 🙆 XSS 📑	Resend 📗	🜡 Bruter [ Cookie 🛛 🕕 Report 🛛 🍪 Setting 🗎	🔍 Scan Site	Scan URL
URL: http://127.0.0.1/dvwa/vu	Inerabilities/brute/?username=	555&passv	vord=666&Login=Login	GET	- 🖸 🔲 🔲
Veller map://27.00.1/90Wa/VU VellersbilityScanner Of POC (Froof Of Concept) Syl Injection AdministrationEntre O SystemTool CookeTool CodeTool CodeTool SettingS Report O About	http://127.0.0.1/dvwa/vulnere http://127.0.0.1/dvwa/vulnere PostData Example: username=ad Username Field username Option © Use username list and Username List File Password List File Combo List File Vsername admin	bilities/b min@password password : password : password : combo.txt sername/pass	rute/?username=5558password=666&Login=Login# -d=123456 -d Field password v GET v Reset list(if password include username, use %username% ) txt txt txt ssword. Password password	Go Go	
Done				HTTP	Thread: 0 .::

继续点击 "Go":

0	WebCruiser - W	eb Vulnerability Scanner Enterprise Edition		- 🗆 🗙
File Iools Yiew Confi WebBrowser VIRL: http://127.0.0.1/dvwa/v WebBrowser VulnerabilitySommer SQL Injection SQL Injection SystemTool SystemTool CookieTool CodeTool Settings Resport About	WebCruiser - W guration Help Scanner SQL XSS vulnerabilities/brute/?username= http://127.0.0.1/dvwa/vulnera PostData Example: username=adu Username Field username Option Outer username List File Password List File Use Combo(username:p Combo List File Stop when found one u Username admin admin	/eb Vulnerability Scanner Enterprise Edition         Resend Bruter Cookie Beport String         5558upassword=6668ulogin=Login         bilities/brute/?username=5558password=6668ulogin=Login#         min&password=123456         v Password Field password v GET v Reset         password Field password include username, use %username% )         username.txt         password list         combo.txt         sername/password         Password         password	© Scan Site GET Go Go	Scan URL
< >> Done			HTTP T	hread: 0 .::

发现 username/password: admin/password.

## 3.3. SQL 注入

DVWA 菜单选择"SQL Injection":



点击"ScanURL":

0	WebCruiser - Web Vulnerability Scanner Enterprise Edition -	□ ×
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> ont	nfiguration <u>H</u> elp	
🗄 🗋 🚰 🛃 🧭 Browser 💽	🛿 Scanner 🛛 📑 SQL 🛛 🔇 XSS 🛛 💣 Resend 🚊 Bruter 🧧 Cookie 🛛 🕼 Report 🖓 Setting 🛛 🔤 Scan Site 📲	Scan URL
URL: http://127.0.0.1/dvwa/	/vulnerabilities/sqli/ GET •	D
WebBrowser     WulnerabilityScanner     YoulnerabilityScanner     FOC(Proof Of Concept)     SQL Injection     Cross Site Scripting     AdministrationEntrance     SystemTool     ResendTool     BruterTool     CodeTool     CodeTool	Scan Current Site   Scan Current URL   Reset/Clear Scanner   Import   Export	
- O SettingS - Report		
G ADOUT	URL / Refer URL Parameter Type KeyWord/ActionURL Vu	ılnerability
	♥ http://127.0.0.1/dwwa/vulnerabilities/sqli/?Submit=Submit&i id=99999999 String First UF	1 SQL INJECTI
	<	>
< >	Checking Form Vul: http://127.0.0.1/dvwa/vulnerabilities/sqli/	ead: 0 🔡
Done	HTTP Three	ead: 0 🤢

右键单击漏洞,选择 "SQL Injection POC":

0	WebCruiser - Web Vulnerability Scanner Enterprise Edition	- 🗆 🗙
Ele Iools View Confi Big Configuration Configuration Wells http://127.0.0.1/dvwa/v Wells of the configuration FOC(Proof Of Concept) SQL Injection FOC(Proof Of Concept) SQL Injection FOC(Proof Of Concept) SQL Injection Conso Site Scripting AdministrationEntrance SystemTool FurtherTool CodeTool CodeTool StringTool StringTool StringTool StringTool StringS	WebCruiser - Web Vulnerability Scanner Enterprise Edition         guration       Help         Scanner       SQL         SQL       XSS         @ SQL       XSS         @ SQL       XSS         @ SQL       XSS         @ Environment       DataBase         Wersion       StringEncode         @ User       OS         @ Isserver       OS         @ Version       *E962EDBD283F2E1F0371C9AF86530A2EF2C545FFEE	an Site Scan URL
StringTool Settings Report About		
< >>	Get Environment Infomation	
Done		HTTP Thread: 0

开始获取数据.

#### 3.4. XSS

先测试反射型跨站,菜单选择 XSS Reflected,点击"ScanURL":



#### 发现一个 XSS:

0	WebCruiser - Web Vulnerability Scanner Ente	erprise Edition		- 🗆 🗙
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> onf	iguration <u>H</u> elp			
🗄 🗋 对 🛃	Scanner 🛛 🧮 SQL 🛛 🔕 XSS 🛛 💣 Resend 🛛 🚊 Bruter 🧕 Cookie 🛛 🚺	Report 🛛 🚳 Setting	🔍 Scan Site	🔍 Scan URL
URL: http://127.0.0.1/dvwa/	vulnerabilities/xss_r/		GET	- 🗈 🔲 🖸 🕯
<ul> <li>WebBrowser</li> <li>VulnerabilityScanner</li> <li>POC(Proof Of Concept)</li> <li>SQL Injection</li> <li>Cross Site Scripting AdministrationEntrance</li> <li>SystemTool</li> <li>BruterTool</li> <li>CodeTool</li> <li>StringTool</li> <li>Settings</li> </ul>	Scan Current Site   Scan Current URL   Reset/Clear Scanner   Im	port Export		
About	URL / Refer URL	Parameter Type	KevWord/ActionURL	Vulnerability
	3 http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&i	id=999999999 String	First	URL SQL INJECTI
	Shttp://127.0.0.1/dvwa/vulnerabilities/sqli_blind/?Submit=Su	id=999999999 String	First	URL SQL INJECTI
	Whttp://127.0.0.1/dwwa/vulnerabilities/xss_r/	name GET	http://127.0.0.1	Cross Site Scri
	Checking Form Vult http://127.0.0.1/daga/uulparabilities/yes.r/			broad: 0
	checking rorm vol. http://127.0.0.1/dvwa/vulnerabilities/xss_1/		HTTP 1	hread: 0

继续存储型跨站测试,选择 stored XSS, 点击"ScanURL":

同样,漏洞列表中会增加扫出的漏洞.

# 4. WAVSEP 测试报告

WAVSEP v1.5 全部 SQL 注入 & XSS 测试用例 100%通过,测试报告参见: http://www.janusec.com/download/WebCruiser\_Web\_Vulnerability\_Scanner\_Te st\_Report.pdf

#### 4.1. 测试环境及测试用例

WAVSEP (Web Application Vulnerability Scanner Evaluation Project) v1.5

WAVSEP Environment: Windows8.1 + XAMPP (Tomcat + MySQL)

WebCruiser Web Vulnerability Scanner Enterprise Edition V3.1.0

#### 4.2. 测试方法

为尽快得到测试结果,我们将使用 WebCruiser 的一个新特性"ScanPage".

在每次 ScanPage 扫描完成后,点击扫描器界面的"Reset Scanner"(复位扫描器)清除 扫描结果,以免与下次扫描的结果混在一起。

ScanURL	🔍 S	canPage	🔍 So	anSite
Scan Current	Site	Reset Sc	anner	[

### 4.3. SQL 注入测试报告

输入向量	测试用例	用例数	报告	通过率
GET 输入向量	Erroneous 500	19	19	100%

	Responses			
	Erroneous 200 Responses	19	19	100%
	200 Responses With Differentiation	19	19	100%
	Identical 200 Responses	8	8	100%
POST 输入向量	Erroneous 500 Responses	19	19	100%
	Erroneous 200 Responses	19	19	100%
	200 Responses With Differentiation	19	19	100%
	Identical 200 Responses	8	8	100%
GET 输入向量 - Experimental	Insert / Delete / Other	1	1	100%
POST 输入向量 - Experimental	Insert / Delete / Other	1	1	100%

## 4.4. XSS 测试报告

输入向量	测试用例	用例数	报告	通过率
GET 输入向量	ReflectedXSS	32	32	100%
POST 输入向量	ReflectedXSS	32	32	100%

Cookie 输入向量 - Experimental	ReflectedXSS	1	1	100%
GET 输入向量 - Experimental	ReflectedXSS	11	11	100%
POST 输入向量 - Experimental	ReflectedXSS	11	11	100%
GET 输入向量 - Experimental	DomXSS	4	4	100%

## 4.5. LFI 测试报告

输入向量	测试用例	用例数	报告	通过率
	Erroneous HTTP 500	68	68	100%
	Responses			
	Erroneous HTTP 404	68	68	100%
	Responses			
	Erroneous HTTP 200	68	68	100%
Get 输入向量	Responses			
	HTTP 302 Redirect	68	68	100%
	Responses	0	0	10070
	HTTP 200 Responses	69	69	100%
	With Differentiation	00	00	100%
	HTTP 200 Responses	68	68	100%

	with Default File on Error			
	Erroneous HTTP 500	68	68	100%
	Responses	00	00	100 /0
	Erroneous HTTP 404	68	68	100%
	Responses	68	00	10070
	Erroneous HTTP 200	68	68	100%
	Responses	00		100 /0
	HTTP 302 Redirect	68	68	100%
	Responses	00	00	10070
	HTTP 200 Responses	69	69	1000/
	With Differentiation	00	00	100 /0
	HTTP 200 Responses	68	68	100%
	with Default File on Error	68		

## 4.6. RFI 测试报告

输入向量	测试用例	用例数	报告	通过率
Get 输入向量	Erroneous HTTP 500	9	0	100%
	Responses		,	
	Erroneous HTTP 404	٩	٩	100%
	Responses	2	, ,	100 /0
	Erroneous HTTP 200	0	0	100%
	Responses	3	9	10070

	HTTP 302 Redirect	9	9	100%
	Responses			
	HTTP 200 Responses	0	0	1000/
	With Differentiation	9	9	100%
	HTTP 200 Responses			
	with Default File on Error	9	9	100%
	Erroneous HTTP 500			1000/
	Responses	9	9	100%
	Erroneous HTTP 404	9	9	100%
	Responses			
	Erroneous HTTP 200			1000/
POST 输入向量	Responses	9	9	100%
	HTTP 302 Redirect	0	0	1000/
	Responses	9	9	100%
	HTTP 200 Responses	0		
	With Differentiation	۶	9	100%
	HTTP 200 Responses			1000/
	with Default File on Error	9	9	100%

### 4.7. Redirect 测试报告

输入向量	测试用例	用例数	报告	通过率
Get 输入向量	HTTP 302 Redirect	15	15	100%

	Responses			
	HTTP 200 Responses	15	15	1000/
	With Javascript Redirect	15	15	100%
POST 输入向量	HTTP 302 Redirect	4 5	15	1000/
	Responses	15	15	100%
	HTTP 200 Responses	15	15	1000/
	With Javascript Redirect	15	15	100%

### 4.8. 误报测试报告

False Vuln	测试用例	用例数	报告	通过率
SQL 注入	误报	10	0	100%
XSS	误报	7	0	100%

# 5. 购买/注册

WebCruiser - Web 漏洞扫描器下载/购买页面:

http://www.janusec.com/downloads/

Janusec 目前在两家软件分销商代理收款,分别为 MyCommerce 和 Avangate:

个人版 (非商业授权):

https://shopper.mycommerce.com/checkout/product/25854-1

https://secure.avangate.com/order/checkout.php?PRODS=4540814&QTY=1&C

ART=1

企业版 (商业授权):

https://shopper.mycommerce.com/checkout/product/25854-2

https://secure.avangate.com/order/checkout.php?PRODS=4540841&QTY=1&C

ART=1

软件注册码在您付款之后,由分销商订单系统自动发出。

感谢您选择 WebCruiser.

# 6. FAQ

Q: 使用 WebCruiser 对系统的需求?

A: 系统需求 IE8 以上, .Net Framework 2.0 或 3.5 (Win7 内置), 其它系统的.Net 框架可在如下地址下载::

http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en

Q: 个人版、企业版有什么区别?

- A: 商业授权上不同, 技术功能上一致.
- ◇ 个人版用于个人研究学习目的,非商业授权,提供12个月免费更新及技术支持服务;
- ◇ 企业版可用于商业目的或企业环境下使用,提供12个月免费更新及技术支持服务。

Q: 与其它 Web 漏洞扫描器相比, WebCruiser 的典型特点是什么?

A: 与其它 Web 漏洞扫描器相比, WebCruiser 最典型的特点是聚焦高危漏洞, 且能够根据设置, 只扫描指定的漏洞类型, 指定的 URL, 或者指定的页面, 通常这是其它扫描器并不具备的。

文档资料 http://www.janusec.com/documentation/

支持网站: http://www.janusec.com

支持 E-mail: janusecurity#gmail.com