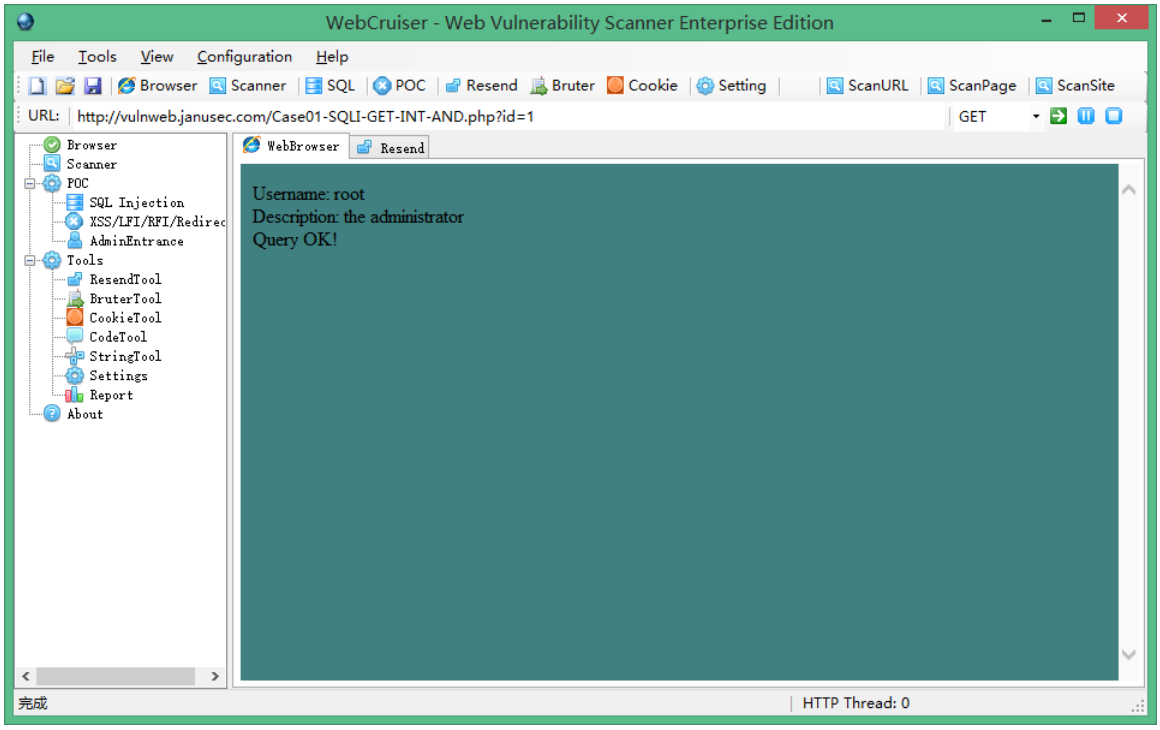
WebCruiser Web 漏洞扫描器使用手册 V3

目 录

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

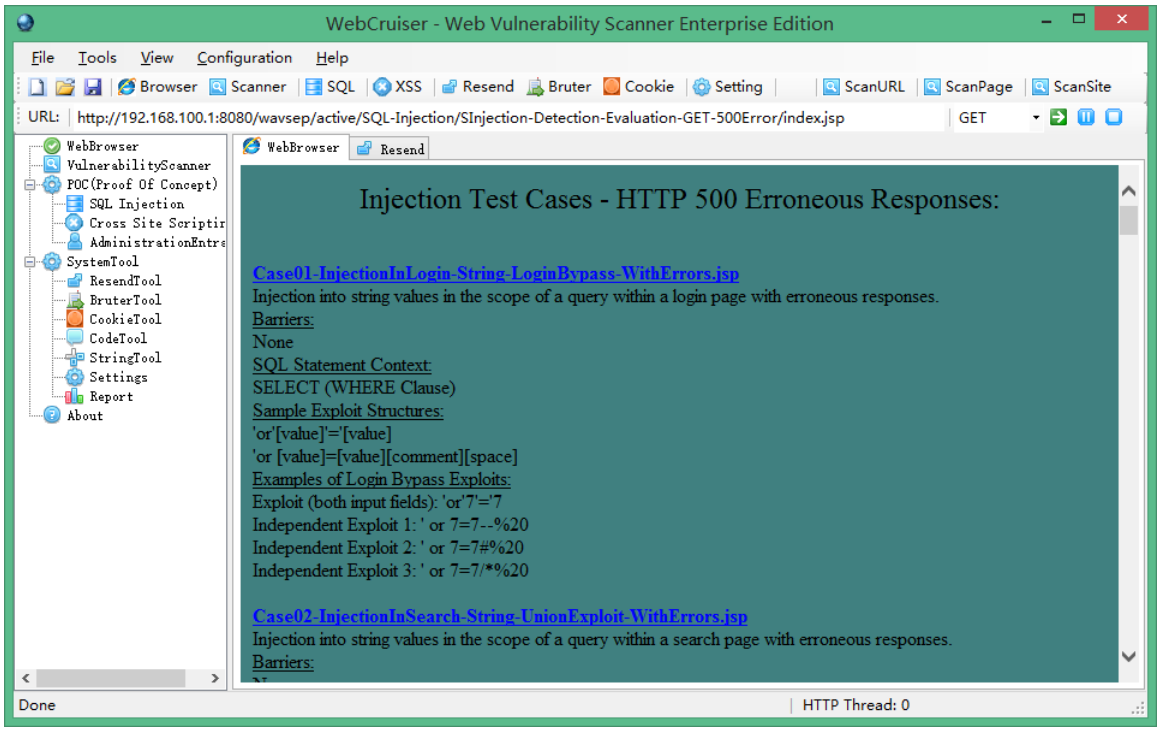
2.1. Web 漏洞扫描器

WebCruiser - Web 漏洞扫描器提供了 3 种扫描模式:

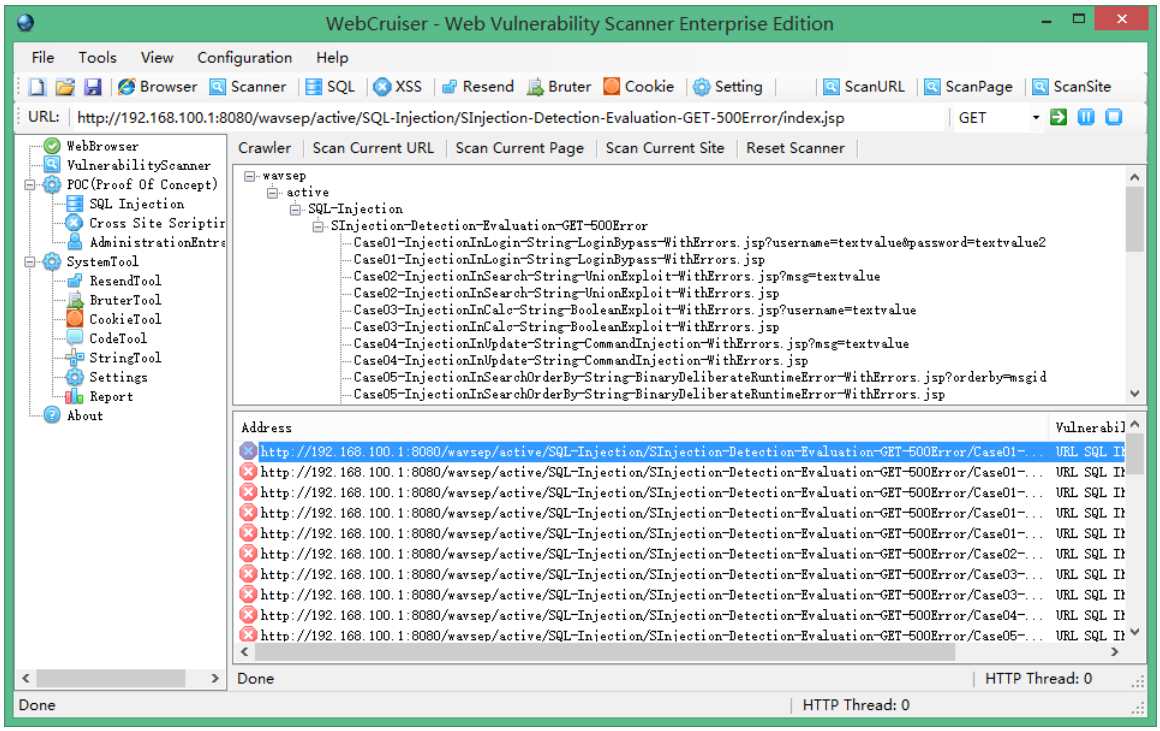
✧ ScanURL（扫描 URL）：只扫描指定的 URL（地址）.

✧ 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.

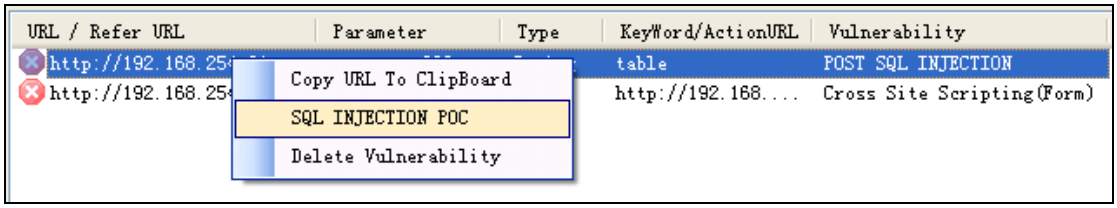
✧ ScanSite（扫描网站）：扫描同一域名下的整个网站，如果链接属于其它域名则跳过.



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：



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



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：

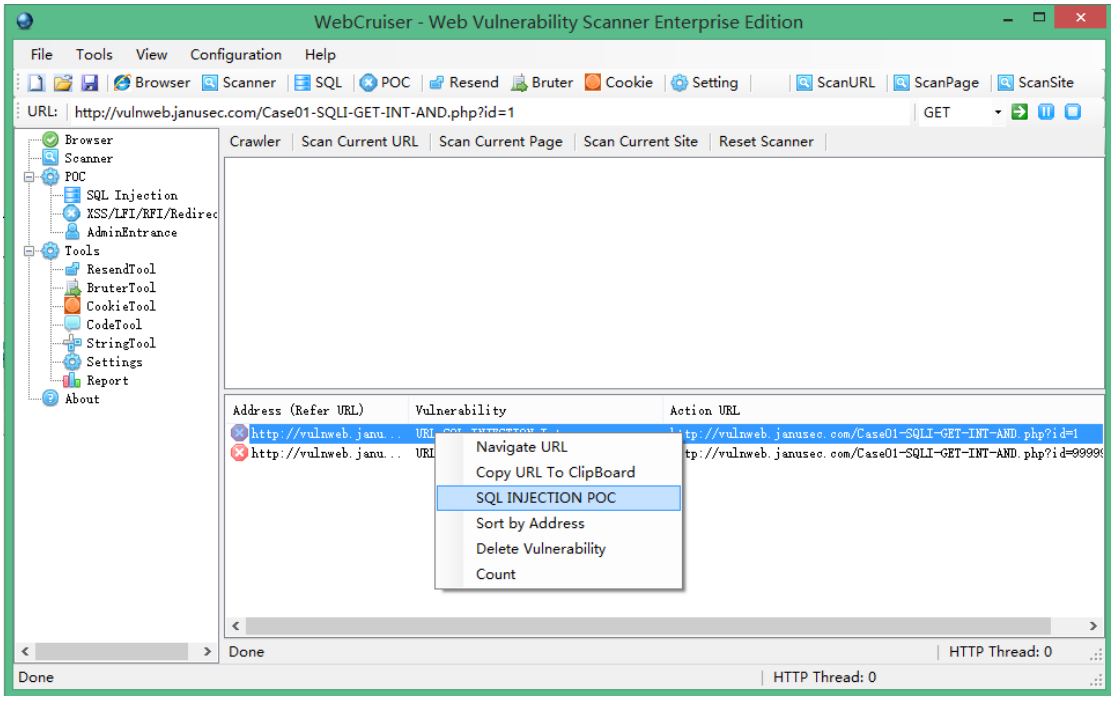
* GET/Post/Cookie 注入；

* SQL Server：明文/Union/盲注；

* MySQL/DB2/Access：Union/盲注；

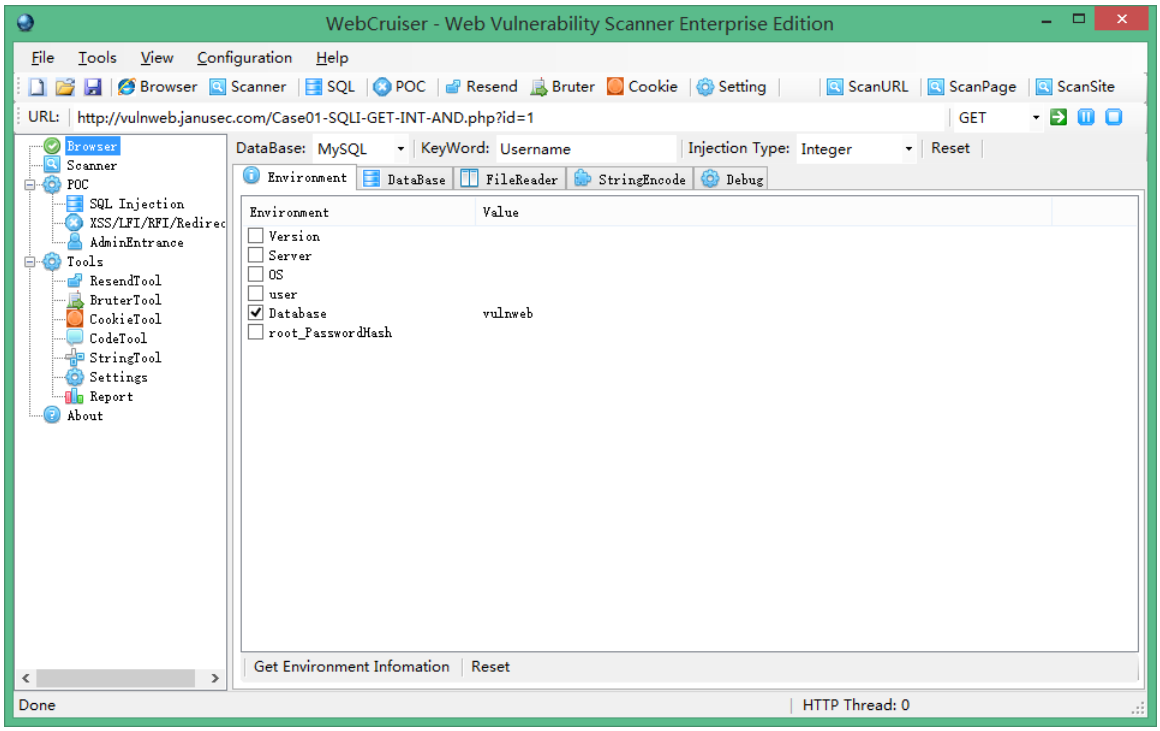
* Oracle：Union/盲注/跨站式注入；

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.

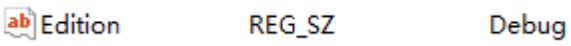


小提示：详细的扫描日志默认是关闭的，如果您需要，可以在注册表中添加一个键值打开：

HKCU\Software\Sec4App\WebCruiser

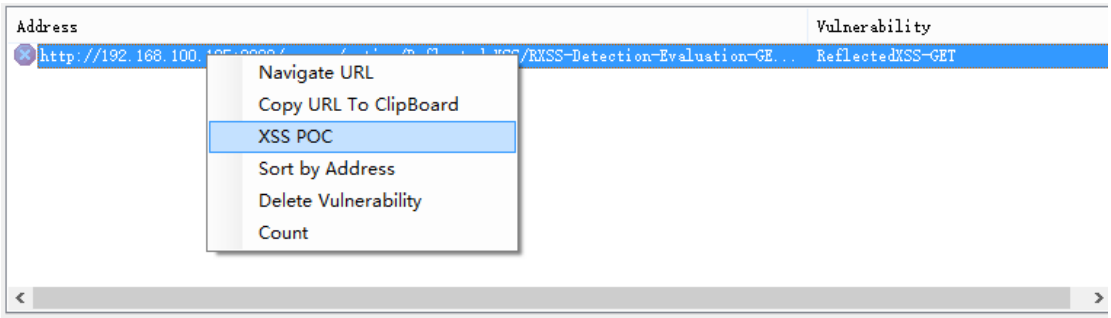
在上述位置添加一个字符串键值 Edition：Debug ,然后重新启动 WebCruiser.

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

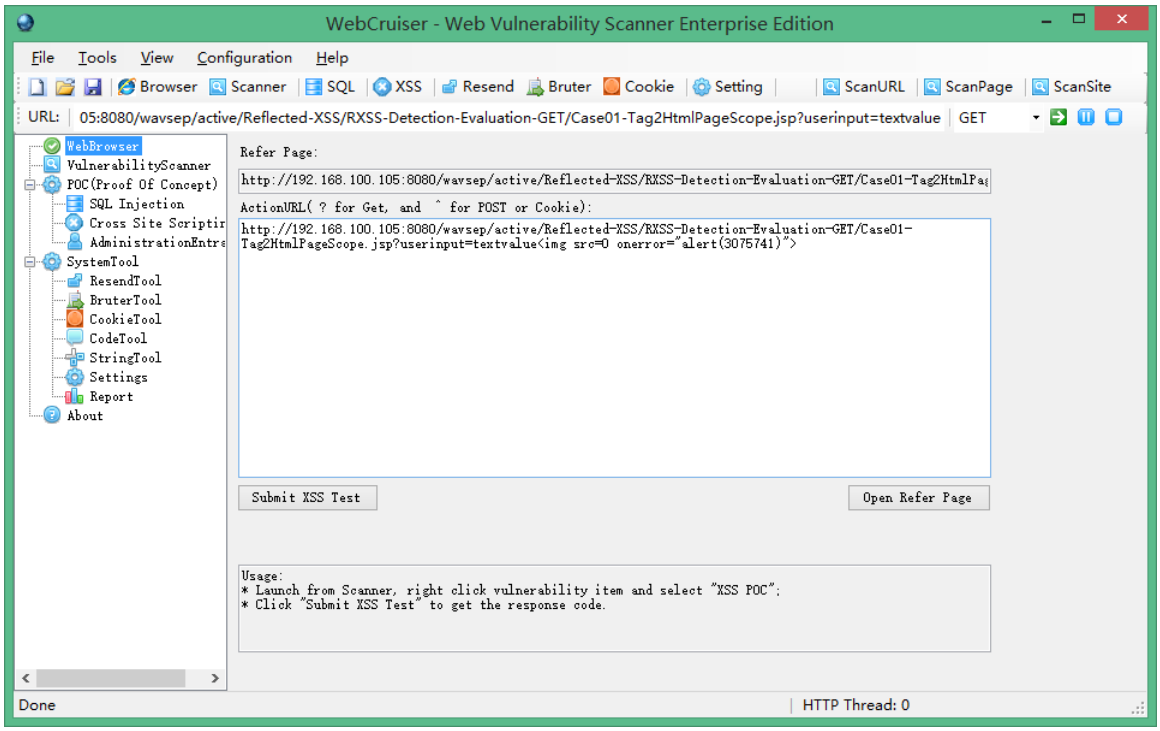


2.3. 跨站 XSS

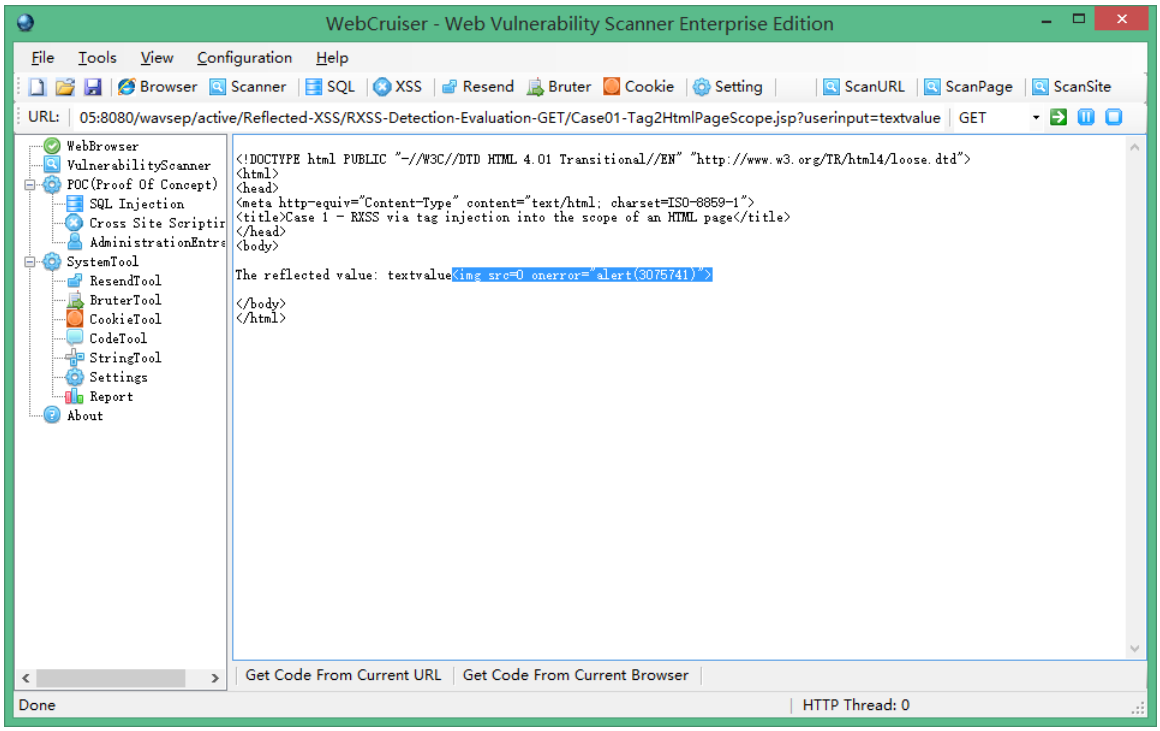
右键单击漏洞，选择“XSS POC”：



检查待提交的数据，点击"Submit POC 测试" (提交).



提交之后，刚才输入的脚本会出现在响应代码中：



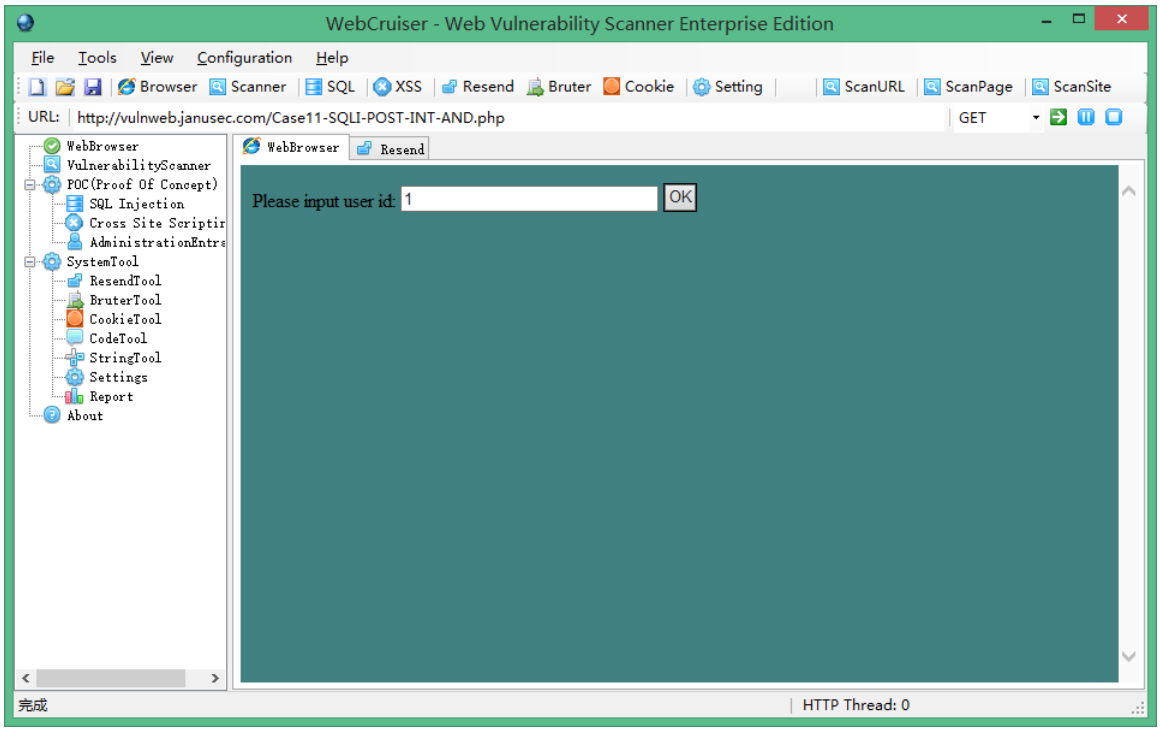
2.4. LFI/RFI/Redirect POC

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

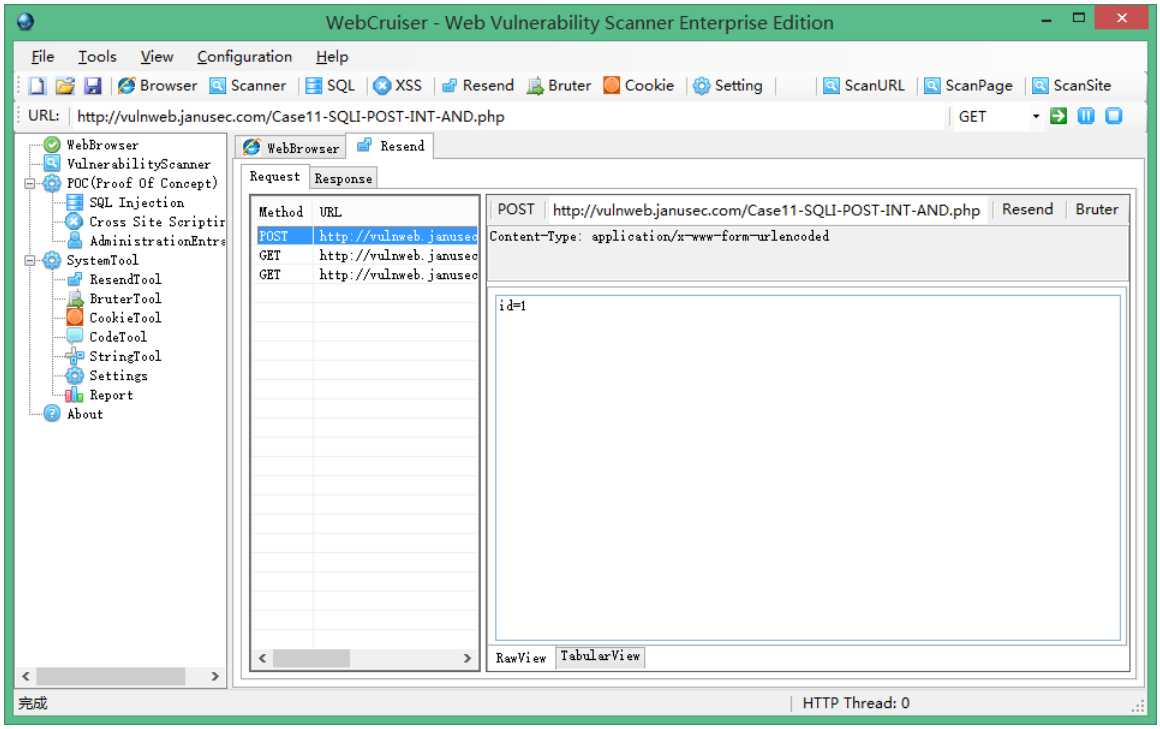
XSS POC.

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：

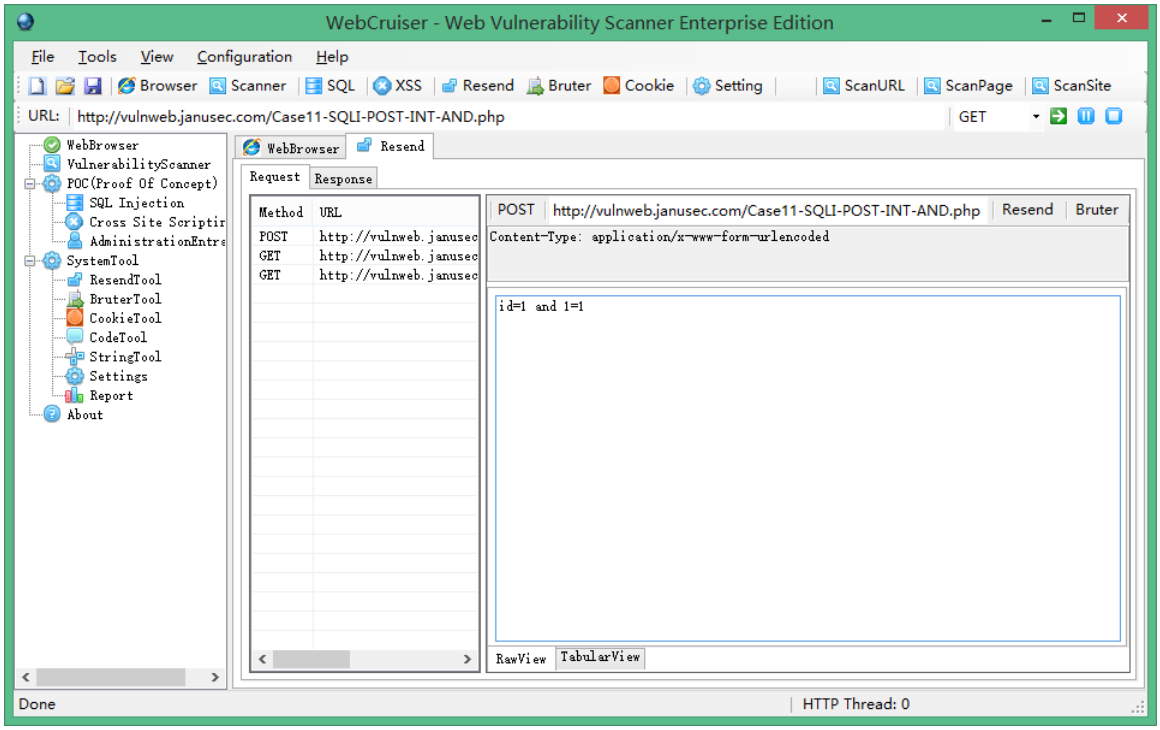


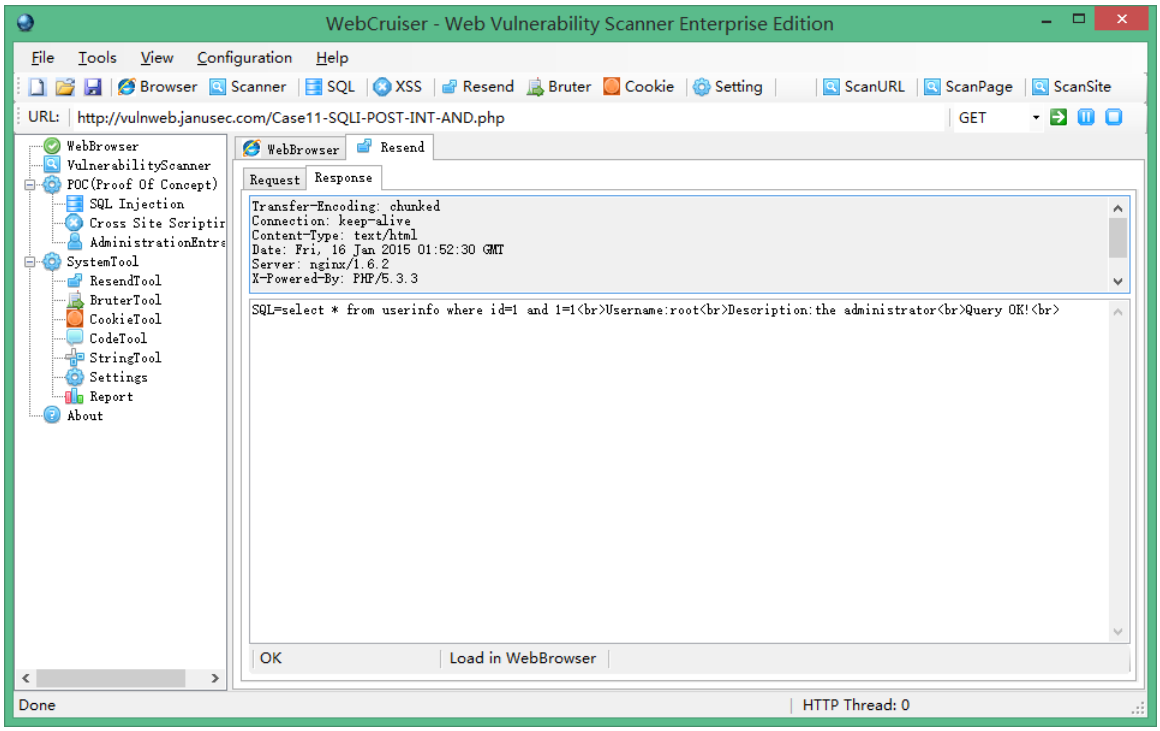
切换到"Resend"（重放）界面，可以看到刚才提交的请求列表：



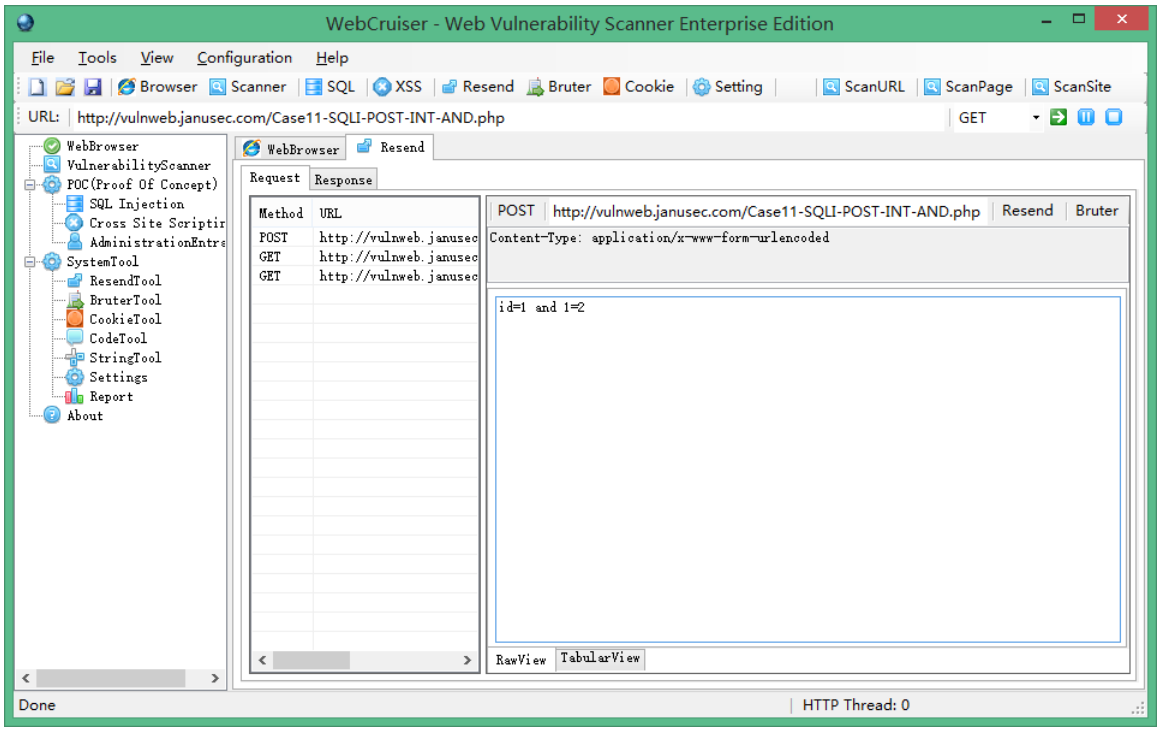
现在，我们可以修改这些数据并重新送出. 比如，我们执行一个 SQL 注入：

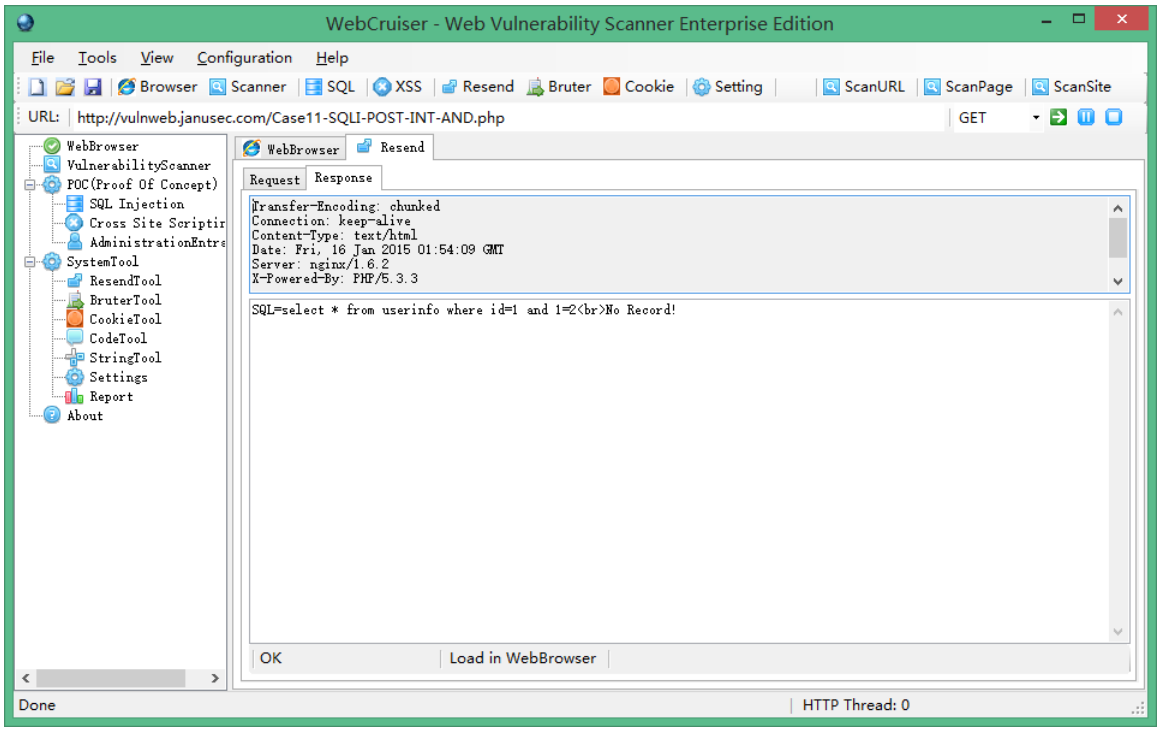
首先，修改 id 参数值为 *1 and 1=1* 提交：





然后，修改为 *1 and 1=2*





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．

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

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';

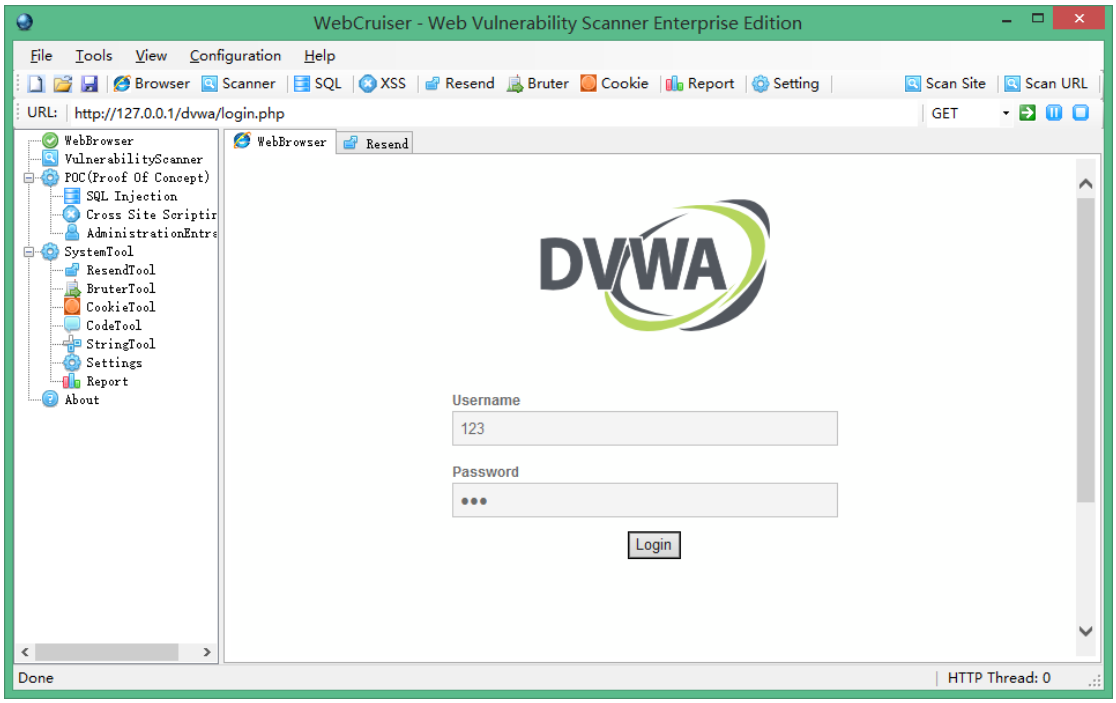
$_DVWA['db_password'] = '123456';

$_DVWA['default_security_level'] = "low";

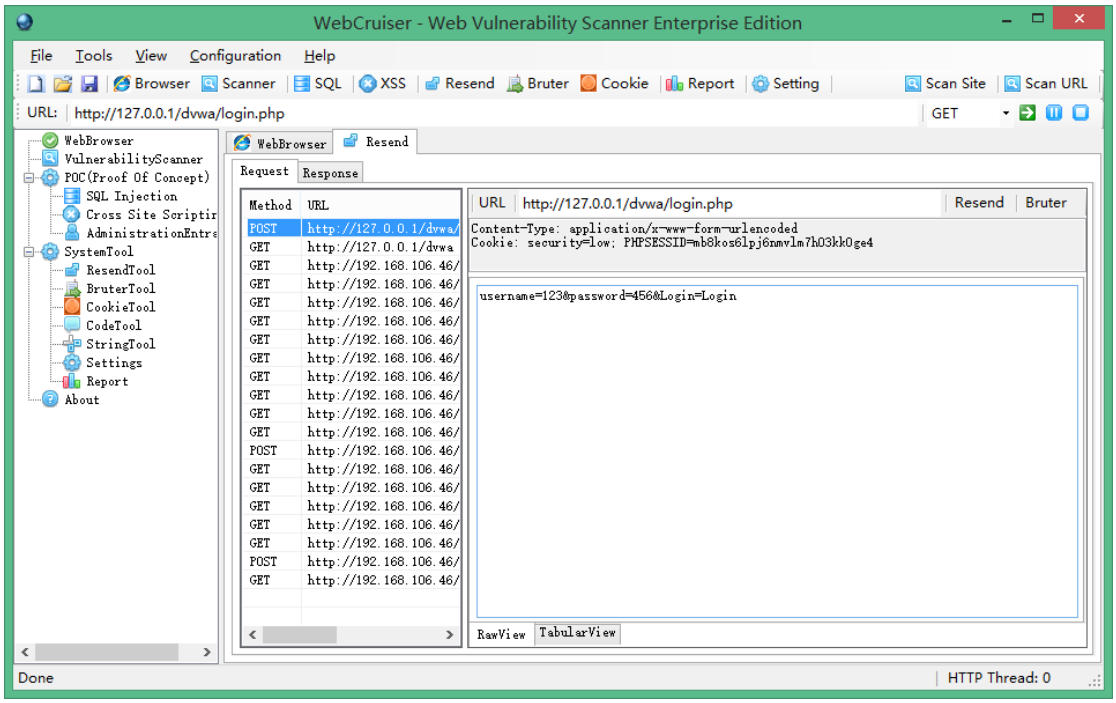
访问 http://127.0.0.1/DVWA/login.php

3.2. 暴力破解

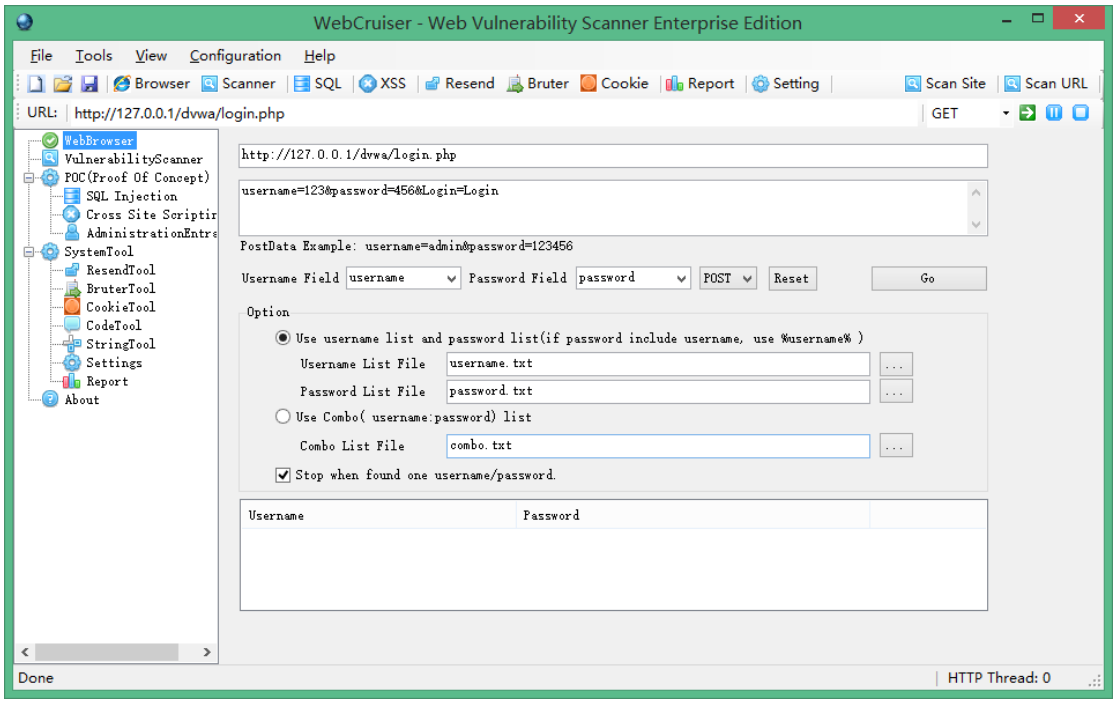
首先，任意输入用户名和密码，比如 123 和 456:



提交之后切换到重放“Resend”界面.



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”.



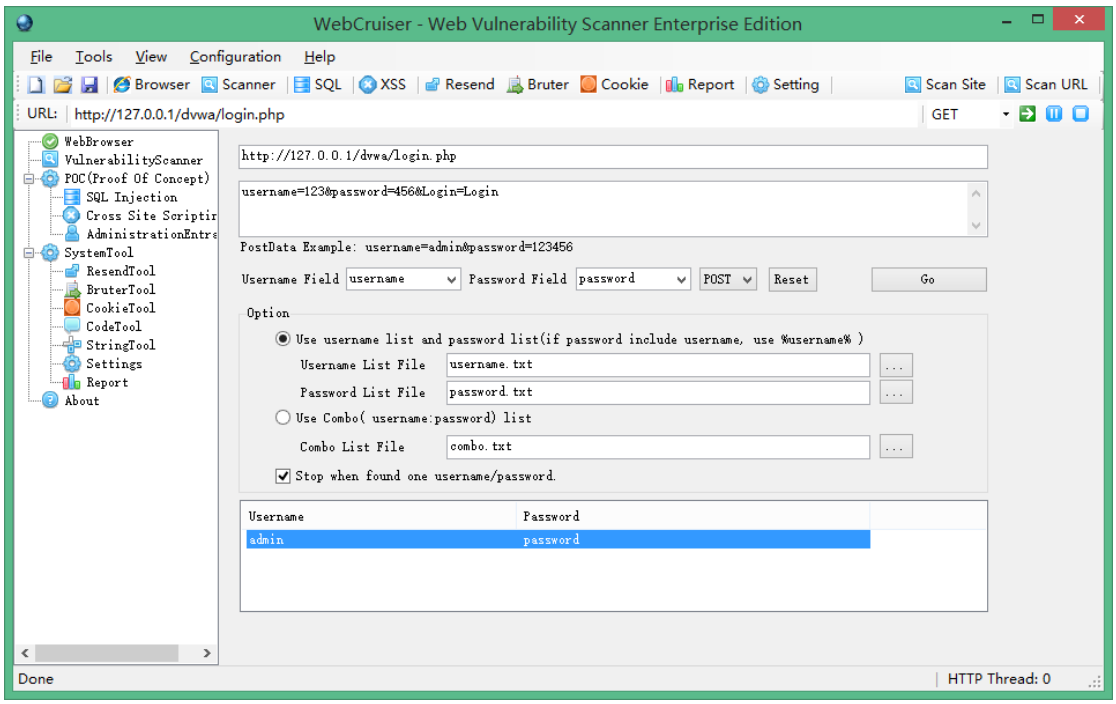
可以看到，已经自动识别出用户名和密码字段（如果用了其它不规则的字段名，手工选择它）

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。

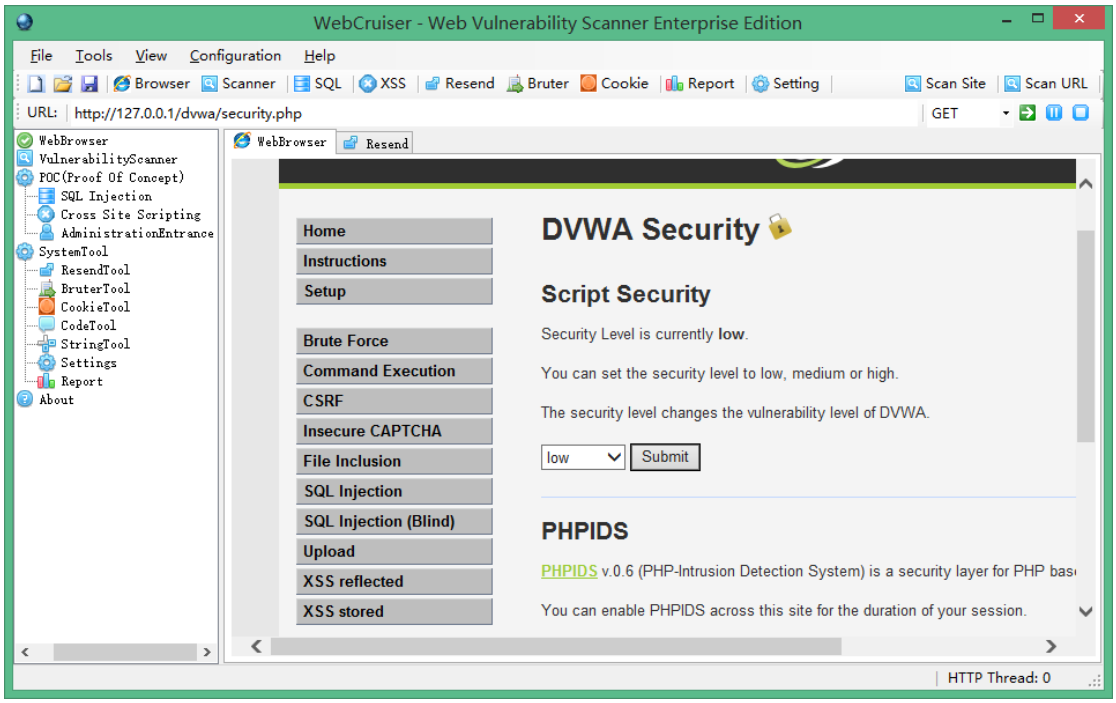
其中 username.txt 和 password.txt 一起使用，combo.txt 单独使用。

点击“Go”发起猜解.



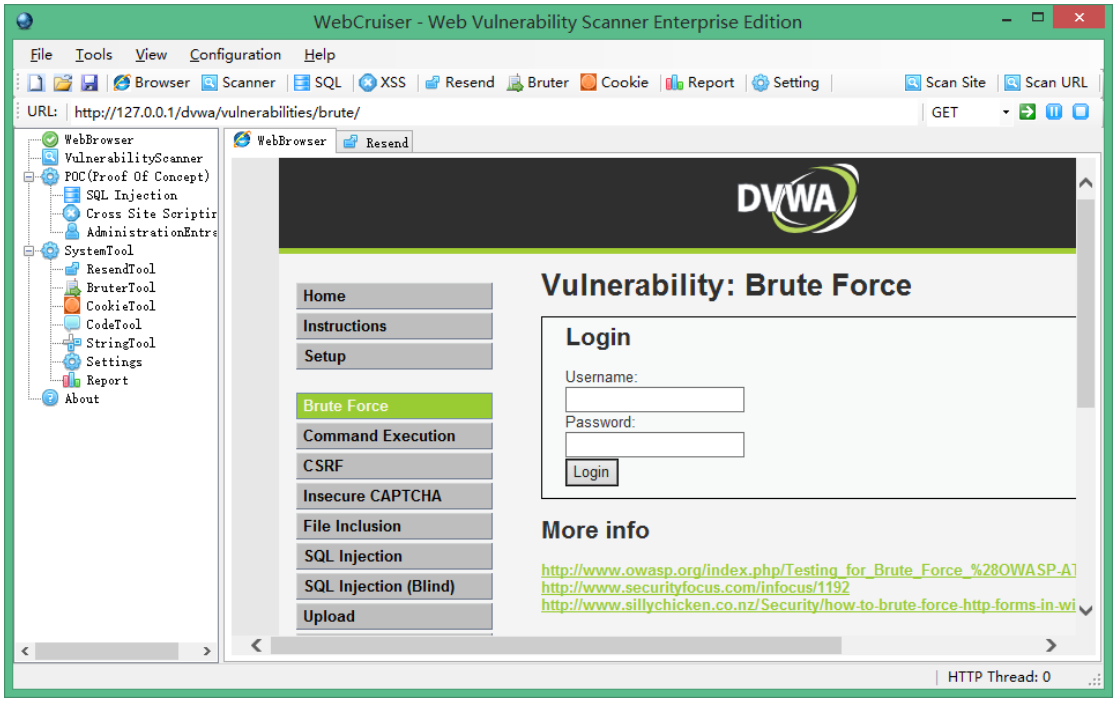
很快就找到了一种组合：admin/password .

切换到内置浏览器，输入刚才猜出的用户名和密码登录.

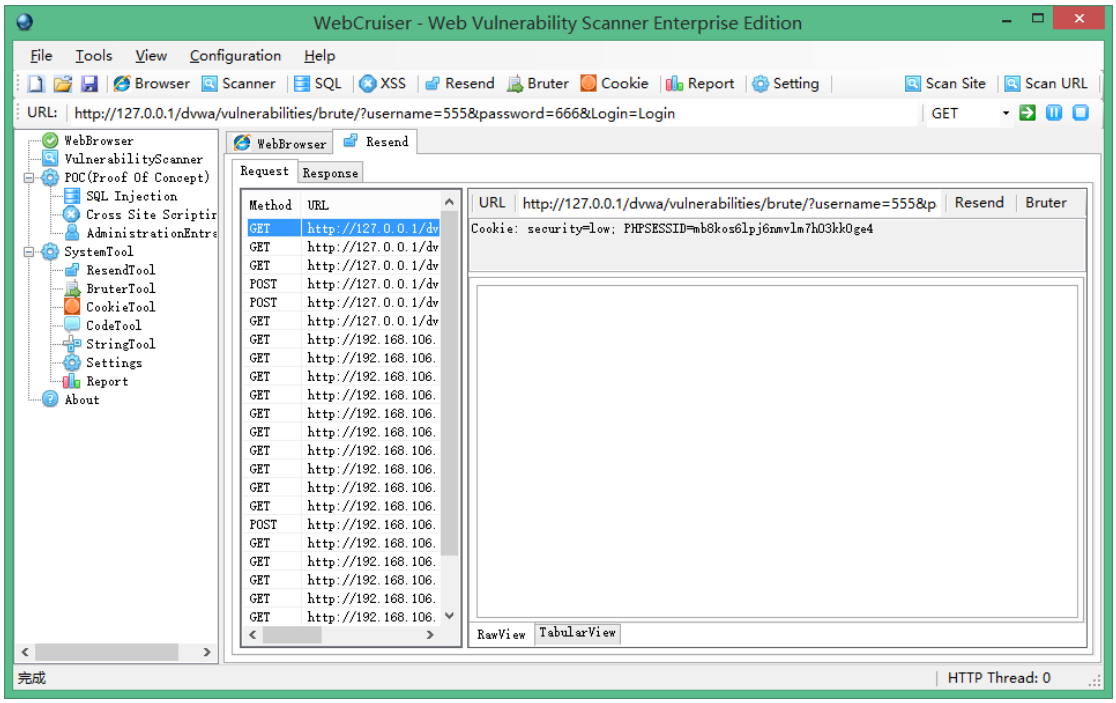


登录之后，检查“DVWA Security”页面，确保安全级别为低 low.

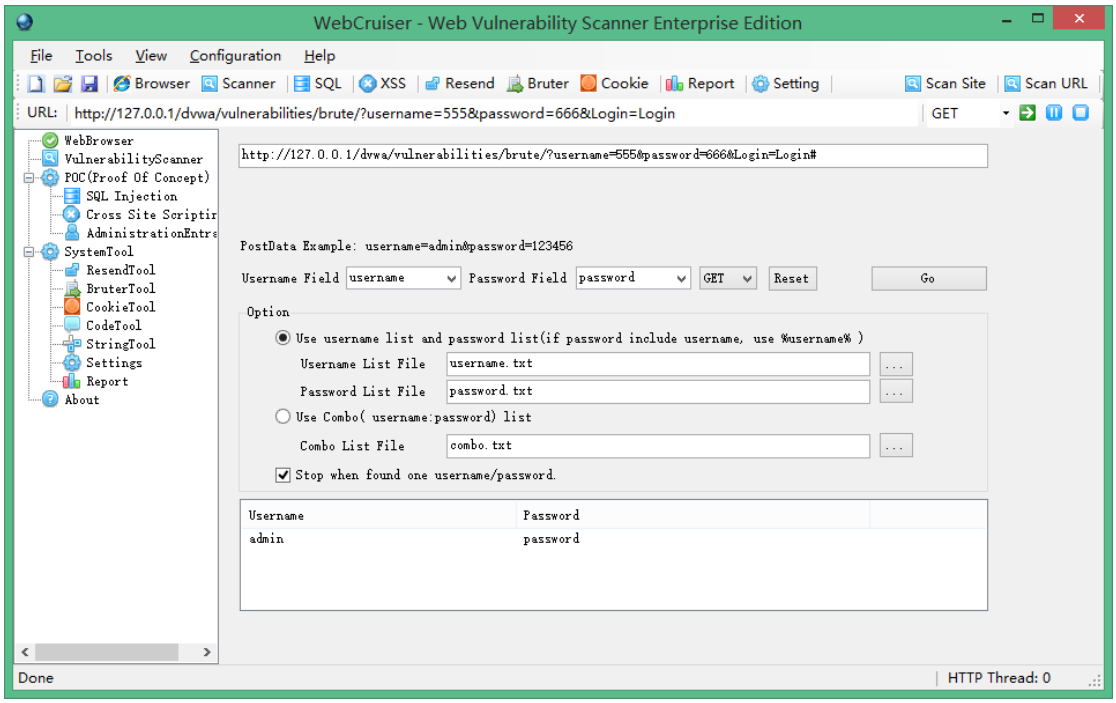
登录之后的第一个测试，是另外一个暴力猜解测试.



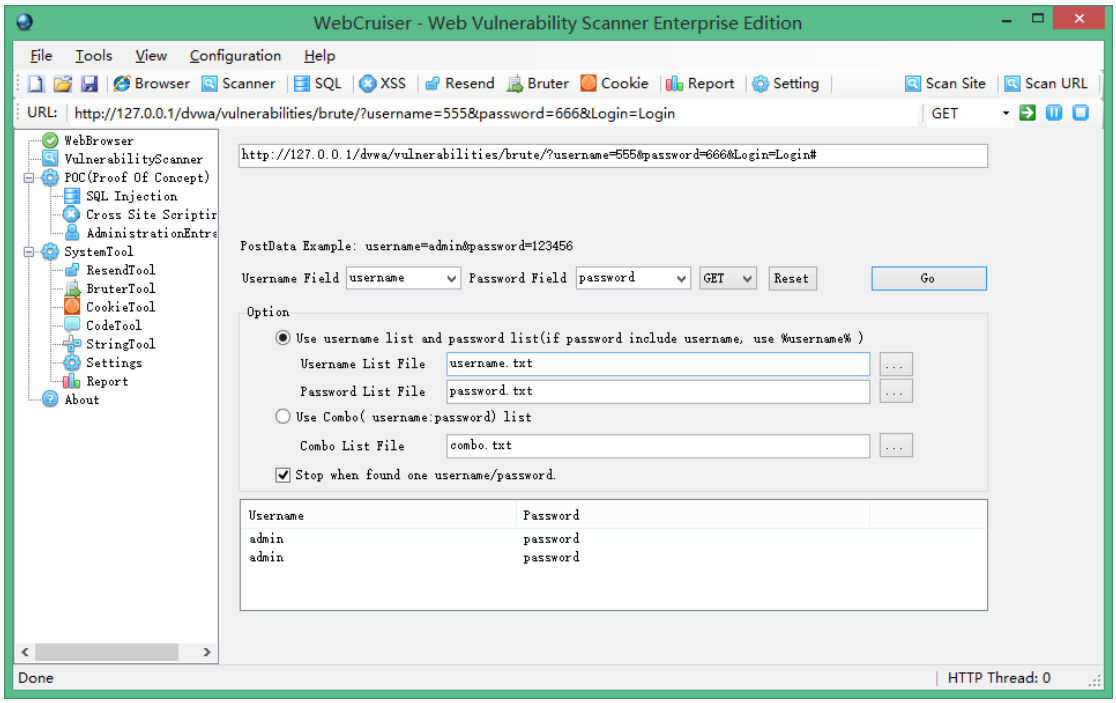
重复刚才的过程，任意输入，然后切换到重放“Resend”:



点击“Bruter”:



继续点击“Go”:

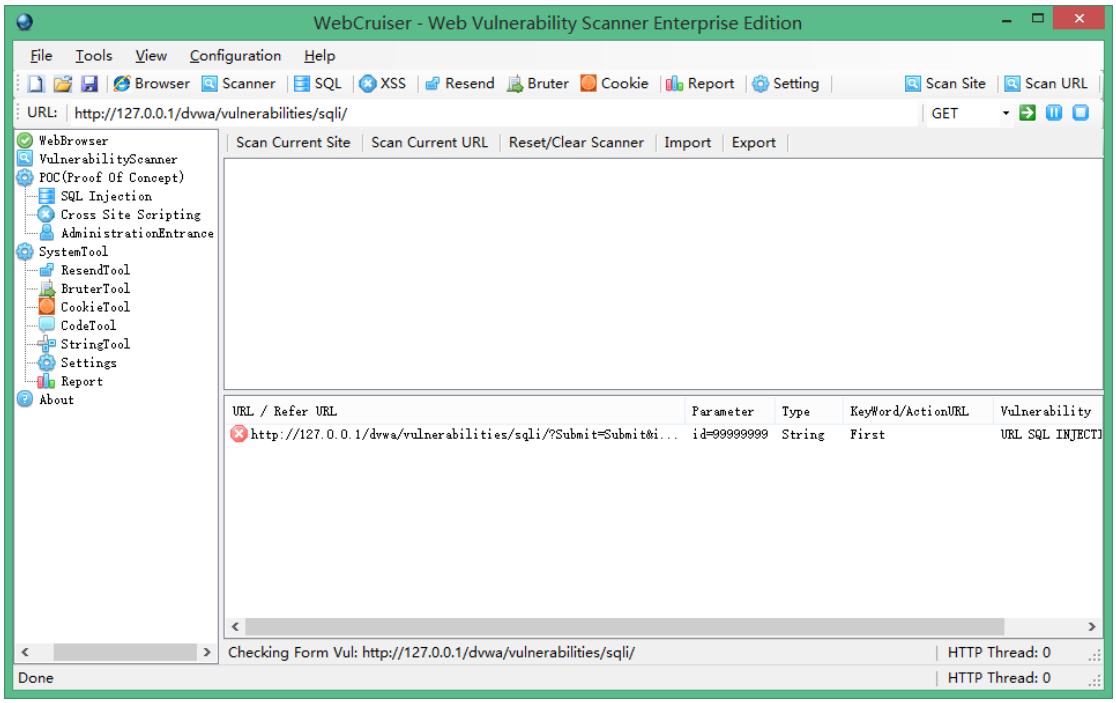


发现 username/password：admin/password.

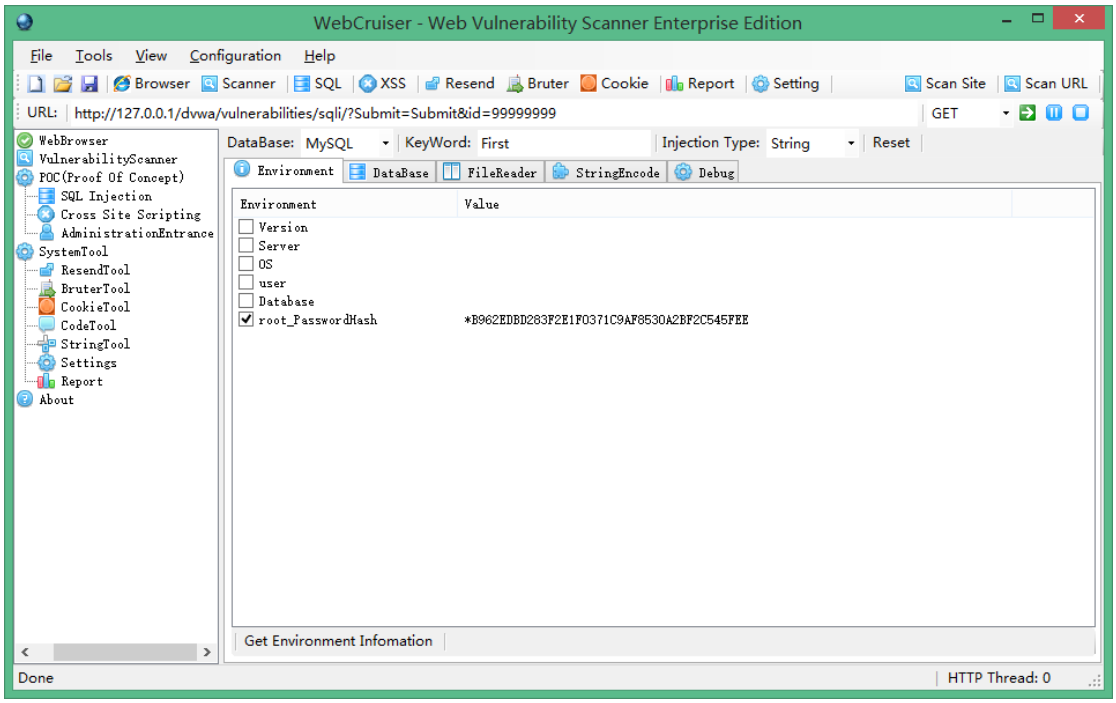
3.3. SQL 注入

DVWA 菜单选择”SQL Injection”：

点击“ScanURL”：



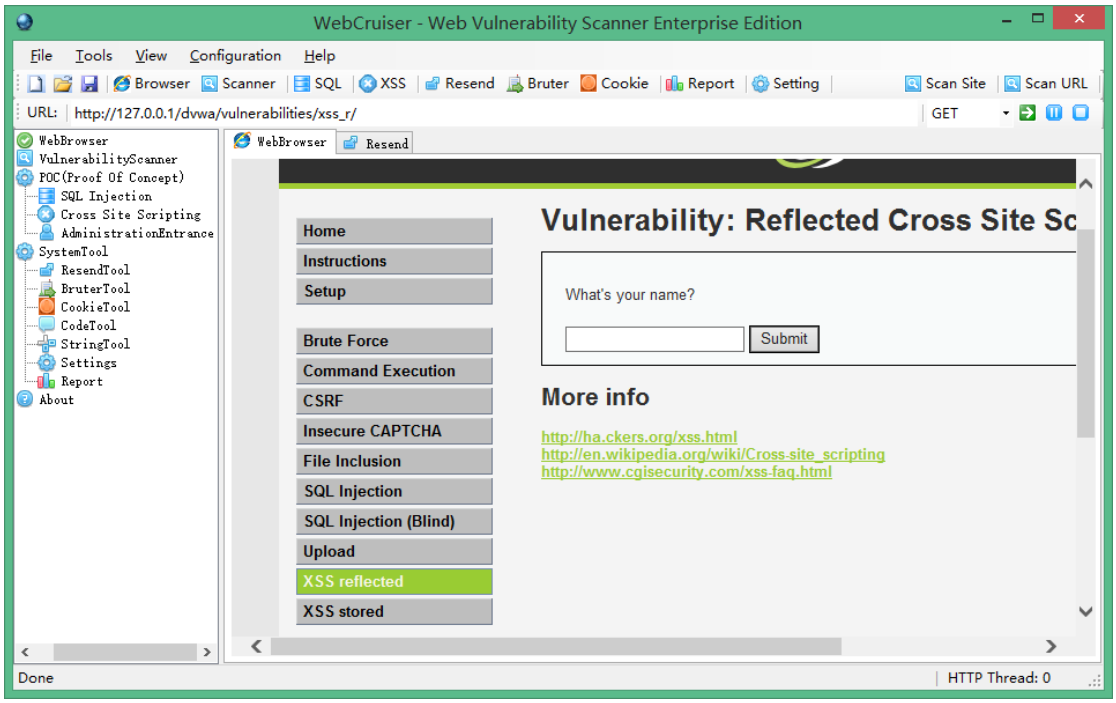
右键单击漏洞，选择“SQL Injection POC”:



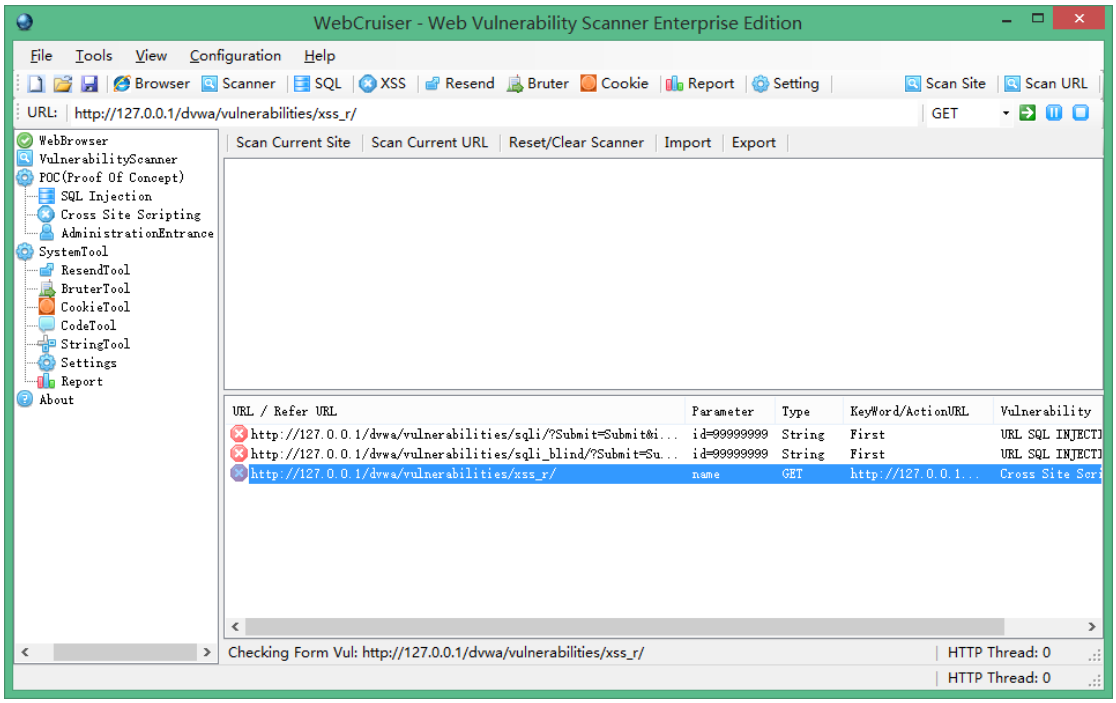
开始获取数据.

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:



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_Test_Report.pdf

4.1. 测试环境及测试用例

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

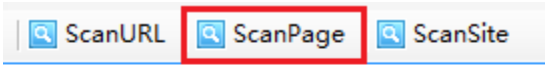
WAVSEP Environment: Windows8.1 + XAMPP (Tomcat + MySQL)

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。



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
Get 输入向量	Erroneous HTTP 500 Responses	68	68	100%
	Erroneous HTTP 404 Responses	68	68	100%
	Erroneous HTTP 200 Responses	68	68	100%
	HTTP 302 Redirect Responses	68	68	100%
	HTTP 200 Responses With Differentiation	68	68	100%
	HTTP 200 Responses	68	68	100%

	with Default File on Error			
POST 输入向量	Erroneous HTTP 500 Responses	68	68	100%
	Erroneous HTTP 404 Responses	68	68	100%
	Erroneous HTTP 200 Responses	68	68	100%
	HTTP 302 Redirect Responses	68	68	100%
	HTTP 200 Responses With Differentiation	68	68	100%
	HTTP 200 Responses with Default File on Error	68	68	100%

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 Responses	9	9	100%
	Erroneous HTTP 404 Responses	9	9	100%
	Erroneous HTTP 200 Responses	9	9	100%

	HTTP 302 Redirect Responses	9	9	100%
	HTTP 200 Responses With Differentiation	9	9	100%
	HTTP 200 Responses with Default File on Error	9	9	100%
POST 输入向量	Erroneous HTTP 500 Responses	9	9	100%
	Erroneous HTTP 404 Responses	9	9	100%
	Erroneous HTTP 200 Responses	9	9	100%
	HTTP 302 Redirect Responses	9	9	100%
	HTTP 200 Responses With Differentiation	9	9	100%
	HTTP 200 Responses 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 With Javascript Redirect	15	15	100%
POST 输入向量	HTTP 302 Redirect Responses	15	15	100%
	HTTP 200 Responses 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&CART=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&CART=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