

Maven Security's Favorite Web App Security Tools (Sept 2007)



SQL Exploiter

<http://axf.watchfire.com/extensions/exploiter.aspx>
Finally, a free SQL exploitation tool that works. It runs as extension to Watchfire's AppScan, or as a stand-alone program (i.e. free). Impressive.

Burp Suite (\$)

<http://portswigger.net/suite/>
Burp Suite is a low cost web app security testing tool kit (includes Burp Spider & Intruder). It is very powerful in knowledgeable hands. It lets you dig deep. Cost is an unbeatable \$200 US.

Burp Spider

<http://portswigger.net/spider/>
The best free web crawling tool. Three choices for forms encountered: skip, fill in customizable data, or prompt for manual input. That rocks.

Paros

<http://www.parosproxy.org/>
The best free all-purpose point-n-click web application security scanner. Includes Achilles-style manual editing of live transactions too.

Wikto

<http://www.sensepost.com/research/wikto/>
Web server security auditing tool. Scans for default directories and files. Dynamically builds a list of things to look for based on directories seen while spidering, default file names, and various file extensions. Uses the Nikto and Google hacks databases. Includes a web mirroring (spider) tool.

WebScarab

<http://www.owasp.org/>
General-purpose web app security suite. Includes a handy session ID analyzer and graphing tool (if the session ID is cookie based).

Crowbar (brute force auth easier than Burp Suite)

<http://www.sensepost.com/research/crowbar/>
Web request brute-force tool. It can extract any portion of the responses. For example, use it to collect URL-based session IDs.

cURL

<http://curl.haxx.se/>
A command line tool for generating requests in HTTP, FTP, LDAP, and more.

Regex

http://en.wikipedia.org/wiki/Regular_expression
Learn regular expression to enhance your overall quality of life (as a security tester).

Browser Enhancements for IE

IECookiesView <http://www.nirsoft.net/>

Tamper IE <http://www.bayden.com/Other/>

Its like having Achilles built right into the browser. No proxies needed.

Cooxie <http://www.diodia.com/cooxietoolbar.htm>

Rapidly switch proxies (useful for running more than one on your system, like Paros and WebScarab). Also can view cache files, view and edit cookies.

Browser Extensions for Firefox

NoScript <http://noscript.net/> (Defensive tool)

iMacros <http://www.iopus.com/imacros/firefox/>

Record and replay a sequence of web transactions.

Check4Change <http://check4change.mozdev.org/>

Monitor a site for changes; Keeps your session alive or verifies a change somewhere in the application.

Foxy Proxy <http://editcookies.mozdev.org/>

Capture traffic only for sites of interest.

View Cookies

<http://www.bitstorm.org/extensions/view-cookies/>

Edit Cookies <http://editcookies.mozdev.org/>

ASCII Chart: Hex # is column then row. Eg. Space (SP) is %20

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL