



SQLi Detection Accuracy (General)



Scanner	SQLi-Total	SQLi-FalsePositive	SQLi-FalsePositive-Info
arachni	100.00% (136 of 136)	20.00% (2 of 10)	7,8
Wapiti	100.00% (136 of 136)	50.00% (5 of 10)	1,2,6,7,8
Netsparker (Commercial Edition)	98.53% (134 of 136)	30.00% (3 of 10)	2,4,6
sqlmap	97.06% (132 of 136)	10.00% (1 of 10)	zero false positives from the sql cases, but case 4 from the false positive xss cases is sometimes detected, and unrelated HTTP headers are sometimes classified as vulnerable as well (in time based tests).
ParosPro	93.38% (127 of 136)	0.00% (0 of 10)	None
IBM Rational AppScan	93.38% (127 of 136)	30.00% (3 of 10)	2,4,6
Acunetix WVS (Commercial Edition)	89.71% (122 of 136)	0.00% (0 of 10)	None
NTOSpider	85.29% (116 of 136)	0.00% (0 of 10)	None
Nessus	82.35% (112 of 136)	20.00% (2 of 10)	7,8
ZAP	77.94% (106 of 136)	40.00% (4 of 10)	2,4,6,8
Andiparos	77.21% (105 of 136)	40.00% (4 of 10)	2,4,6,8
Paros Proxy	77.21% (105 of 136)	40.00% (4 of 10)	2,4,6,8
WebInspect	75.74% (103 of 136)	30.00% (3 of 10)	2,4,6
Vega	75.74% (103 of 136)	0.00% (0 of 10)	None
Burp Suite Professional	72.06% (98 of 136)	0.00% (0 of 10)	The tool had false positives for header & cookie parameters (for cases 7 & 8), but none for GET or POST parameters.
Netsparker Community Edition	70.59% (96 of 136)	30.00% (3 of 10)	2,4,6 (Reported as High Possibility)
Watobo	65.44% (89 of 136)	30.00% (3 of 10)	6,7,8
Cenzic Hailstorm Professional	63.24% (86 of 136)	10.00% (1 of 10)	Case 1 was reported as a 500 error - blind sql injection (cases 2,4,6 were reported as SQL errors, but the scan log explains why they were not included in the FP states).

Scanner	SQLi-Total	SQLi-FalsePositive	SQLi-FalsePositive-Info
JSky (Commercial Edition)	61.03% (83 of 136)	0.00% (0 of 10)	None
Sandcat Free Edition	58.82% (80 of 136)	20.00% (2 of 10)	7,8
WebSecurify	58.82% (80 of 136)	50.00% (5 of 10)	2,4,6,7,8
Sandcat Pro	58.82% (80 of 136)	50.00% (5 of 10)	2,4,6,7,8
Oedipus	58.82% (80 of 136)	40.00% (4 of 10)	1,2,6 (identified as errors); the false positive RXSS case 5 and the RXSS cases 27,30,32 are all identified as vulnerable to SQL injection. RXSS FP case 5 was included in the SQL false positive count.
W3AF	56.62% (77 of 136)	30.00% (3 of 10)	2,4,6
SandcatCS	55.88% (76 of 136)	20.00% (2 of 10)	7,8
ProxyStrike	52.21% (71 of 136)	0.00% (0 of 10)	None
PowerFuzzer	51.47% (70 of 136)	40.00% (4 of 10)	1,2,6,8
WebCruiser Enterprise Edition	51.47% (70 of 136)	0.00% (0 of 10)	None (But Confuses SQLi with XPATHi)
SkipFish	50.74% (69 of 136)	10.00% (1 of 10)	None of the regular cases, but the scanner identifies *many* 404 HTTP messages as query injection vectors (after sending injection payloads in HTTP headers).
WebCruiser Free Edition	50.74% (69 of 136)	0.00% (0 of 10)	None
Gamja	50.00% (68 of 136)	80.00% (8 of 10)	False SQLi Cases: 1-4,6-8, and in addition various XSS instances (represented as an addition of 1)
WSTool	45.59% (62 of 136)	40.00% (4 of 10)	1,2,6,7
Grendel Scan	42.65% (58 of 136)	50.00% (5 of 10)	2,4,6,7,8
Damn Small SQLi Scanner (DSSS)	39.71% (54 of 136)	20.00% (2 of 10)	7,8
JSKY Free Edition	38.24% (52 of 136)	20.00% (2 of 10)	7,8
SQLiX	37.50% (51 of 136)	20.00% (2 of 10)	Case 8 (warning), RXSS false positive cases 1,3,6,7 (represented as an addition of 1)
safe3wvs	36.03% (49 of 136)	0.00% (0 of 10)	None, Or None Scanned
Mini MySqlatOr	26.47% (36 of 136)	0.00% (0 of 10)	None

Scanner	SQLi-Total	SQLi-FalsePositive	SQLi-FalsePositive-Info
Uber Web Security Scanner	21.32% (29 of 136)	40.00% (4 of 10)	Case 8 (identified as vulnerable); the false positive RXSS cases 1,2,3,4,6,7 and many other RXSS were all identified as vulnerable to SQL injection (false). All the RXSS FP cases were represented in the SQL false positive count as an addition of 3.
Secubat	18.38% (25 of 136)	70.00% (7 of 10)	1-4,6-8
Grabber	15.44% (21 of 136)	20.00% (2 of 10)	4,8
Scrawler	13.24% (18 of 136)	0.00% (0 of 10)	None
aidSQL	11.76% (16 of 136)	0.00% (0 of 10)	None
LoverBoy	0.00% (0 of 136)	0.00% (0 of 10)	Execution Failed.
openAcunetix	0.00% (0 of 136)	0.00% (0 of 10)	Execution Failed.
Web Injection Scanner (WIS)	0.00% (0 of 136)	0.00% (0 of 10)	Execution Failed.
iScan	0.00% (0 of 136)	0.00% (0 of 10)	The tool did not manage to scan URLs with upper case characters.
SQID (SQL Injection Digger)	0.00% (0 of 136)	0.00% (0 of 10)	None
Xcobra	0.00% (0 of 136)	0.00% (0 of 10)	Execution Failed.
Priamos	0.00% (0 of 136)	0.00% (0 of 10)	None
VulnDetector	0.00% (0 of 136)	0.00% (0 of 10)	Execution Failed.