Vulnerability Assessment Report: vulners.com

SECURITY SCORE: 95/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	http		open
8080	POTENTIAL-ADMIN-PANEL (http)		open
8443	POTENTIAL-ADMIN-PANEL (http)		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 172.66.165.7
+ Target Hostname: vulners.com
+ Target Port: 80
+ Start Time: 2026-02-16 16:29:24 (GMT0)
---------------------------------------------------------------------------
+ Server: cloudflare
+ IP address found in the 'report-to' header. The IP is "1.0.1.1".
+ IP address found in the 'content-security-policy-report-only' header. The IP is "1.0.1.1".
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'cf-ray' found, with contents: 9cee6c82e84e3c28-BOM
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'report-to' found, with contents: {"endpoints":[{"url":"https:\/\/csp-report
ing.cloudflare.com\/cdn-cgi\/script_monitor\/report?m=sjahq6gjRZmNgY3COmOiAa9WAKZJmm86yAw.4j.J
Nho-1771259366-1.0.1.1-nYEgkT6hcYM_8Z5M3kmiHS4zSTUHIKsxXRmA3sTi2PVw3hYwFxw_jdls3JNyDGOKMaJAVfp
zm8hArlZTzV_IbIjwagK3MTp87nH6yAbs4M83a6Ax6Tb2fg_tpgba_FwOP4brQvvxZ3sR6cKhkl5nAMMR.N5Rs.rIfsfyp
3He044"}],"group":"cf-csp-endpoint","max_age":86400}
+ Uncommon header 'speculation-rules' found, with contents: "/cdn-cgi/speculation"
+ Root page / redirects to: https://vulners.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'server-timing' found, with contents: cfEdge;dur=4,cfOrigin;dur=0
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'proxy-status' found, with contents:
Cloudflare-Proxy;error=http_request_error
+ /cfappman/index.cfm - Redirects (301) to https://vulners.com/cfappman/index.cfm , susceptible
to ODBC/pipe-style exploit; see RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/cvbeans/beaninfo.cfm - Redirects (301) to
https://vulners.com/cfdocs/examples/cvbeans/beaninfo.cfm , susceptible to our ODBC exploit; see
RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/parks/detail.cfm - Redirects (301) to
```

```
https://vulners.com/cfdocs/examples/parks/detail.cfm , susceptible to our ODBC exploit; see
RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /kboard/ - Redirects (301) to https://vulners.com/kboard/ , KBoard Forum 0.3.0 and prior have
a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/ - Redirects (301) to https://vulners.com/lists/admin/ , PHPList pre 2.6.4
contains a number of vulnerabilities including remote administrative access, harvesting user
info and more. Default login to admin interface is admin/phplist
+ /splashAdmin.php - Redirects (301) to https://vulners.com/splashAdmin.php , Cobalt Qube 3
admin is running. This may have multiple security problems as described by
www.scan-associates.net. These could not be tested remotely.
+ /ssdefs/ - Redirects (301) to https://vulners.com/ssdefs/ , Siteseed pre 1.4.2 has 'major'
security problems.
+ /sshome/ - Redirects (301) to https://vulners.com/sshome/ , Siteseed pre 1.4.2 has 'major'
security problems.
+ /tiki/ - Redirects (301) to https://vulners.com/tiki/ , Tiki 1.7.2 and previous allowed
restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php - Redirects (301) to https://vulners.com/tiki/tiki-install.php , Tiki
1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default
login/pass could be admin/admin
+ /scripts/samples/details.idc - Redirects (301) to
https://vulners.com/scripts/samples/details.idc , See RFP 9901; www.wiretrip.net
+ /includes/conexion.inc - Redirects (301) to https://vulners.com/includes/conexion.inc ,
Database connection file found.
+ /.svn/entries - Redirects (301) to https://vulners.com/.svn/entries , Subversion Entries file
may contain directory listing information.
+ /.svn/wc.db - Redirects (301) to https://vulners.com/.svn/wc.db , Subversion SQLite DB file
may contain directory listing information.
+ /.git/index - Redirects (301) to https://vulners.com/.git/index , Git Index file may contain
directory listing information.
+ /.hg/dirstate - Redirects (301) to https://vulners.com/.hg/dirstate , Mercurial DirState file
may contain directory listing information.
+ 26 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time: 2026-02-16 16:29:46 (GMT0) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[nikto stderr]
+ ERROR: Host maximum execution time of 180 seconds reached
```

3. Crawled Website Endpoints

- No endpoints found

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

Attack: Clickjacking Vulnerability
Mitigation: Implement X-Frame-Options: SAMEORIGIN or DENY.