Vulnerability Assessment Report: www.nasa.gov

SECURITY SCORE: 80/100

OVERALL RISK LEVEL: MEDIUM

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	http		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 192.0.66.108
+ Target Hostname: www.nasa.gov
+ Target Port: 80
+ Start Time: 2026-02-22 12:33:15 (GMT0)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://www.nasa.gov/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'access-control-allow-methods' found, with contents: GET, HEAD
+ Uncommon header 'access-control-allow-origin' found, with contents: *
+ /cfappman/index.cfm - Redirects (301) to https://www.nasa.gov/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://www.nasa.gov/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://www.nasa.gov/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://www.nasa.gov/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://www.nasa.gov/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://www.nasa.gov/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://www.nasa.gov/ssdefs/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /sshome/ - Redirects (301) to https://www.nasa.gov/sshome/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /tiki/ - Redirects (301) to https://www.nasa.gov/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://www.nasa.gov/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://www.nasa.gov/scripts/samples/details.idc , See RFP 9901; www.wiretrip.net
```

```
+ /includes/conexion.inc - Redirects (301) to
https://www.nasa.gov/includes/conexion.inc , Database connection file found.
+ /.svn/entries - Redirects (301) to https://www.nasa.gov/.svn/entries , Subversion
Entries file may contain directory listing information.
+ /.svn/wc.db - Redirects (301) to https://www.nasa.gov/.svn/wc.db , Subversion SQLite
DB file may contain directory listing information.
+ /.git/index - Redirects (301) to https://www.nasa.gov/.git/index , Git Index file may
contain directory listing information.
+ /.hg/dirstate - Redirects (301) to https://www.nasa.gov/.hg/dirstate , Mercurial
DirState file may contain directory listing information.
+ 26 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2026-02-22 12:33:18 (GMT0) (3 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)

Legacy Vulnerability Intelligence
- ■■ NOTICE: Engine identified 5 additional legacy vulnerabilities (pre-2016).

5. Attack Possibilities & Mitigation

Attack: Cross-Site Scripting (XSS) / Data Injection
Mitigation: Implement a strict Content-Security-Policy (CSP) to restrict untrusted script execution.

Attack: Clickjacking Vulnerability
Mitigation: Implement X-Frame-Options: SAMEORIGIN or DENY in your web server configuration.