Vulnerability Assessment Report: amazon.com

SECURITY SCORE: 80/100

OVERALL RISK LEVEL: MEDIUM

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	https		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 98.87.170.71
+ Target Hostname: amazon.com
+ Target Port: 80
+ Start Time: 2026-02-13 13:10:34 (GMT0)
---------------------------------------------------------------------------
+ Server: Server
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://amazon.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /cfappman/index.cfm - Redirects (301) to https://amazon.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://amazon.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://amazon.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://amazon.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://amazon.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
+ /ssdefs/ - Redirects (301) to https://amazon.com/ssdefs/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /sshome/ - Redirects (301) to https://amazon.com/sshome/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /tiki/ - Redirects (301) to https://amazon.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://amazon.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://amazon.com/scripts/samples/details.idc , See RFP 9901; www.wiretrip.net
+ /includes/conexion.inc - Redirects (301) to https://amazon.com/includes/conexion.inc
, Database connection file found.
+ /.svn/entries - Redirects (301) to https://amazon.com/.svn/entries , Subversion
Entries file may contain directory listing information.
+ /.svn/wc.db - Redirects (301) to https://amazon.com/.svn/wc.db , Subversion SQLite DB
```

```
file may contain directory listing information.
+ /.git/index - Redirects (301) to https://amazon.com/.git/index , Git Index file may
contain directory listing information.
+ /.hg/dirstate - Redirects (301) to https://amazon.com/.hg/dirstate , Mercurial
DirState file may contain directory listing information.
+ 26 items checked: 0 error(s) and 1 item(s) reported on remote host
+ End Time: 2026-02-13 13:11:00 (GMT0) (26 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

- https://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId;=508088
- [FORM] https://www.amazon.com/errors/validateCaptcha
-
https://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId;=468496

4. Vulnerabilities Detected

- Missing Security Headers
- Information Disclosure

5. Vulnerability Intelligence (CVE Mapping)

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

6. Attack Possibilities & Mitigation

Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.

Attack: Data Leaks / Reconnaissance
Mitigation: Restrict access to sensitive directories (like .git or /admin) and disable directory listing.