Vulnerability Assessment Report: facebook.com

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 57.144.176.1
+ Target Hostname: facebook.com
+ Target Port: 80
+ Start Time: 2026-01-31 06:18:19 (GMT0)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'proxy-status' found, with contents: http_request_error; e_fb_vipaddr
="AcNZNNGD5TRwmyJUt1x91q6APF-b4odUCAqcF-cinqheHOiDE01ReeQuc6nJPUNBG-HwO7i_"; e_clientad
dr="AcP-0_ZgYtQjgmDin_UKSC4qbKVrad8v_RGjb0HFWp72AY0RrC2RSFHyJyg8RQo0md3mDD7xm0NR7SoO2A"
; e_fb_zone="AcMsKTmoETZPJ4Gra91E3xg-JwgJm1r7n0am5ss51sUHUzLomWzQ4k4pYXHtnw"; e_fb_twta
skhandle="AcPnjCa3L8Zm41QrN7q5DZBh2fkx2cqo8da3uDJbsh1_lK55wcRBXRFrAh3HErLXATBi1YwlMPDwK
SSAR9yP44KzSoN0OYGXrm8"; e_proxy="AcOoSimPKx8SliTOVM-zhJ1CaiERETf_gQarEnVhKyicPi9QJ823t
FtgyNKq1ca0AgGBm8z8XTFITSQ", http_request_error; e_fb_vipaddr="AcM7iXOhqpRuGWt2pJNPQPLo
sPPdXH_3R60QuWC_wGBdA6tDhjW_D-ffQVPXD1Kp1oCpokTi"; e_clientaddr="AcNTXI-ODSTugn1pmK8AjP
dBceG7Mos6W2ViC8wsXneN-7-_j2UhCmXtErZkm_-d-6Qz5NoT17SaxKsmtg";
e_fb_zone="AcN1NlrJZq5zd6AF6kmOqW80QC1iSb0e2o4QdalprkPRCufsZfkhJiHW0iM2MQ"; e_fb_twtask
handle="AcPmf7tUm5SHOdDgKgk_DJvY6TLMBpc3sKHPhlqH31YpPPK7khNkx9dJZ2fyXsvBFU4ixDQXAdUxBCC
BIXhLb59xo-T2pM6EtvI"; e_proxy="AcOn9qgUOzkyxHepwbdDNZt-HdV28haf1RRLZbgGZorqdaoPzHnIAfA
VVzaEAFzXNKFRUCAJGVLgl_w"
+ /cfappman/index.cfm - Redirects (301) to https://facebook.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://facebook.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://facebook.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://facebook.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://facebook.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://facebook.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://facebook.com/ssdefs/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /sshome/ - Redirects (301) to https://facebook.com/sshome/ , Siteseed pre 1.4.2 has
'major' security problems.
+ /tiki/ - Redirects (301) to https://facebook.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://facebook.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://facebook.com/scripts/samples/details.idc , See RFP 9901; www.wiretrip.net
+ /includes/conexion.inc - Redirects (301) to
https://facebook.com/includes/conexion.inc , Database connection file found.
+ /.svn/entries - Redirects (301) to https://facebook.com/.svn/entries , Subversion
Entries file may contain directory listing information.
+ /.svn/wc.db - Redirects (301) to https://facebook.com/.svn/wc.db , Subversion SQLite
DB file may contain directory listing information.
+ /.git/index - Redirects (301) to https://facebook.com/.git/index , Git Index file may
contain directory listing information.
+ /.hg/dirstate - Redirects (301) to https://facebook.com/.hg/dirstate , Mercurial
DirState file may contain directory listing information.
+ 26 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2026-01-31 06:18:22 (GMT0) (3 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

No crawlable endpoints found (site may block automated crawling or use dynamic content).

4. Vulnerabilities Detected

- Missing Security Headers
- Information Disclosure

5. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

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.