VAJRA
Offensive Security Platform

Comprehensive Security Assessment Report

TARGET	SCAN DATE	RISK LEVEL
192.168.11.128	2026-01-27 15:02	Critical

Executive Summary

- Discovered 6 subdomains, 1 are live
- Found 23 open ports across scanned hosts
- Nuclei identified 21 vulnerabilities (3 critical, 15 high)
- Nikto found 35 potential web server issues

Domain Registration Analysis

Domain Name	N/A
Registrar	N/A
Creation Date	N/A
Expiration Date	N/A
Last Updated	N/A
Name Servers	• N/A
DNSSEC Status	N/A
Registrant Org	N/A
Registrant Country	N/A

Subdomain Infrastructure Mapping

6	1
Total Discovered	Live Subdomains

Live Subdomains
http://192.168.11.128

Service Discovery & Availability

URL	Host	Port	Web Server
http://192.168.11.128	192.168.11.128	80	N/A

Network Infrastructure Analysis

SYN	1	23
Scan Type	Hosts Scanned	Total Open Ports

Host Details

192.168.11.128 (192.168.11.128) 23 Ports

Port	Service	Version	Note
21/tcp	FTP	vsftpd 2.3.4	Review service configuration for security best practices.
22/tcp	SSH	OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0	Ensure strong password policies and disable root login.
23/tcp	TELNET	Linux telnetd	Telnet is insecure. Disable and use SSH instead.
25/tcp	SMTP	Postfix smtpd	Review service configuration for security best practices.
53/tcp	DOMAIN	ISC BIND 9.4.2	Review service configuration for security best practices.
80/tcp	HTTP	Apache httpd 2.2.8 (Ubuntu) DAV/2	Unencrypted traffic. Redirect all HTTP traffic to HTTPS.
111/tcp	RPCBIND	2 RPC #100000	Review service configuration for security best practices.
139/tcp	NETBIOS-SSN	Samba smbd 3.X - 4.X workgroup: WORKGROUP	SMB exposed. Ensure latest patches and restrict access.
445/tcp	NETBIOS-SSN	Samba smbd 3.X - 4.X workgroup: WORKGROUP	SMB exposed. Ensure latest patches and restrict access.
512/tcp	EXEC	netkit-rsh rexecd	Review service configuration for security best practices.
513/tcp	LOGIN	N/A	Review service configuration for security best practices.
514/tcp	TCPWRAPPED	N/A	Review service configuration for security best practices.
1099/tcp	JAVA-RMI	GNU Classpath grmiregistry	Review service configuration for security best practices.
1524/tcp	BINDSHELL	Metasploitable root shell	Review service configuration for security best practices.
2049/tcp	NFS	2-4 RPC #100003	Review service configuration for security best practices.
2121/tcp	FTP	ProFTPD 1.3.1	Review service configuration for security best practices.
3306/tcp	MYSQL	MySQL 5.0.51a-3ubuntu5	Review service configuration for security best practices.
5432/tcp	POSTGRESQL	PostgreSQL DB 8.3.0 - 8.3.7	Review service configuration for security best practices.
5900/tcp	VNC	VNC protocol 3.3	Review service configuration for security best practices.

Port	Service	Version	Note
6000/tcp	X11	access denied	Review service configuration for security best practices.
6667/tcp	IRC	UnrealIRCd	Review service configuration for security best practices.
8009/tcp	AJP13	Apache Jserv Protocol v1.3	Review service configuration for security best practices.
8180/tcp	HTTP	Apache Tomcat/Coyote JSP engine 1.1	Review service configuration for security best practices.

Nuclei Vulnerability Scan

⚠ Total Vulnerabilities Found: 21

3	15	3	0	0
Critical	High	Medium	Low	Info
CVSS 9.0-10.0	CVSS 7.0-8.9	CVSS 4.0-6.9	CVSS 0.1-3.9	CVSS 0.0

Vulnerability Details:

HIGH [http]

http://192.168.11.128/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input

[CVE-2012-1823] [http] [high] http://192.168.11.128/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input

HIGH [javascript]

[passwords="password"]

[vnc-default-login] [javascript] [high] 192.168.11.128:5900 [passwords="password"]

HIGH [javascript]

[passwords="password123"]

[vnc-default-login] [javascript] [high] 192.168.11.128:5900 [passwords="password123"]

HIGH [javascript]

[passwords="postgres",usernames="postgres"]

[postgres-default-logins] [javascript] [high] 192.168.11.128:5432 [passwords="postgres",usernames="postgres"]

HIGH [javascript]

[database="postgres",password="postgres",usernames="postgres"]

[pgsql-list-database] [javascript] [high] 192.168.11.128:5432 ["postgres","template1","template0"] [database="postgres",password="postgres",usernames="postgres"]

HIGH [javascript]

[database="postgres",password="postgres",usernames="postgres"]

[pgsql-list-password-hashes] [javascript] [high] 192.168.11.128:5432 ["postgres : md53175bce1d3201d16594cebf9d7eb3f9d"] [database="postgres",password="postgres",usernames="postgres"]

HIGH [javascript]

[database="postgres",password="",usernames="postgres"]

[pgsql-default-db] [javascript] [high] 192.168.11.128:5432 [database="postgres",password="",usernames="postgres"]

HIGH [javascript]

[database="postgres",password="postgres",usernames="postgres"]

[pgsql-list-users] [javascript] [high] 192.168.11.128:5432 ["postgres"] [database="postgres",password="postgres",usernames="postgres"]

HIGH [javascript]

[database="template1",password="postgres",usernames="postgres"]

[pgsql-default-db] [javascript] [high] 192.168.11.128:5432 [database="template1",password="postgres",usernames="postgres"]

HIGH [javascript]

[database="postgres",password="postgres",usernames="postgres"]

[pgsql-default-db] [javascript] [high] 192.168.11.128:5432 [database="postgres",password="postgres",usernames="postgres"]

HIGH [javascript]

[database="postgres",password="postgres",usernames="postgres"]

[pgsql-file-read] [javascript] [high] 192.168.11.128:5432 ["pg_twophase","server.crt","postmaster.pid","pg_multixact","root.crt","pg_tblspc","postmaster.opts","pg_xlog","global","pg_clog","pg_subtrans","base","PG_VERSION","server.key"] [database="postgres",password="postgres",usernames="postgres"]

CRITICAL [javascript]

192.168.11.128:5432

[pgsql-empty-password] [javascript] [critical] 192.168.11.128:5432

HIGH [javascript]

[database="postgres",password="postgres",usernames="postgres"]

[pgsql-version-detect] [javascript] [high] 192.168.11.128:5432 ["PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)"] [database="postgres",password="postgres",usernames="postgres"]

HIGH [javascript]

[database="template1",password="",usernames="postgres"]

[pgsql-default-db] [javascript] [high] 192.168.11.128:5432 [database="template1",password="",usernames="postgres"]

HIGH [tcp]

192.168.11.128:3632

[CVE-2004-2687] [tcp] [high] 192.168.11.128:3632

CRITICAL [tcp]

192.168.11.128:6200

[CVE-2011-2523] [tcp] [critical] 192.168.11.128:6200

MEDIUM [tcp]

["2.3.4"]

[CVE-2015-1419:version] [tcp] [medium] 192.168.11.128:21 ["2.3.4"]

HIGH [tcp]

["2.3.4"]

[CVE-2021-30047:version] [tcp] [high] 192.168.11.128:21 ["2.3.4"]

CRITICAL [tcp]

192.168.11.128:8009

[CVE-2020-1938] [tcp] [critical] 192.168.11.128:8009

MEDIUM [javascript]

192.168.11.128:22

[ssh-weak-algo-supported] [javascript] [medium] 192.168.11.128:22

MEDIUM [tcp]

192.168.11.128:21

[ftp-anonymous-login] [tcp] [medium] 192.168.11.128:21

Nikto Web Server Scan

Targets Scanned: N/A | **Total Findings: 35**

7	6	22
High	Medium	Info
CVSS 7.0-8.9	CVSS 4.0-6.9	CVSS 0.0

Findings Details:

INFO — N/A

Target IP: 192.168.11.128

INFO — N/A

Target Hostname: 192.168.11.128

INFO — N/A

Target Port: 80

INFO — N/A

Start Time: 2026-01-27 15:02:34 (GMT5.5)

INFO — N/A

Server: Apache/2.2.8 (Ubuntu) DAV/2

INFO — N/A

/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.

INFO — N/A

/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

HIGH — N/A

/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

INFO — N/A

/index: Uncommon header 'tcn' found, with contents: list.

HIGH — N/A

/index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275

HIGH — N/A

Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

INFO N/A

/: Web Server returns a valid response with junk HTTP methods which may cause false positives.

INFO N/A

/: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing

INFO N/A

/phpinfo.php: Output from the phpinfo() function was found.

INFO N/A

/doc/: Directory indexing found.

INFO N/A

/doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678

MEDIUM N/A

/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

MEDIUM N/A

/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

MEDIUM N/A

/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

MEDIUM N/A

/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

HIGH N/A

/phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

INFO N/A

/phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 22:54:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418

HIGH N/A

/phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

INFO N/A

/test/: Directory indexing found.

INFO N/A

/test/: This might be interesting.

INFO N/A

/phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552

INFO N/A

/icons/: Directory indexing found.

MEDIUM N/A

/icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/

INFO N/A

/phpMyAdmin/: phpMyAdmin directory found.

HIGH N/A

/phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

HIGH N/A

/phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/

INFO N/A

/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.

MEDIUM N/A

8910 requests: 0 error(s) and 27 item(s) reported on remote host

INFO N/A

End Time: 2026-01-27 15:02:48 (GMT5.5) (14 seconds)

INFO N/A

1 host(s) tested

EyeWitness Screenshots

1

Screenshots Captured

Screenshot Directory: /tmp/Vajra-results/192.168.11.128_27012026_150037/Screenshots

Open EyeWitness Report

Security Recommendations

Priority Actions: Review all findings and prioritize remediation based on risk and business impact.

Priority	Recommendation	Timeline
Critical	Address 3 critical vulnerabilities from Nuclei scan immediately.	Immediate (24-48 hours)
High	Remediate 15 high-severity vulnerabilities within one week.	1 Week
High	Review and close unnecessary ports. 23 open ports detected - minimize attack surface.	1-2 Weeks