Nmap

Unveiling Nmap: Network Scanning Essentials

website:daraz.com

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Tengine httpd
|_http-passwd: ERROR: Script execution failed (use -d to debug)
| http-security-headers:
|   Strict_Transport_Security:
|     Header: Strict-Transport-Security: max-age=31536000
|   Cache_Control:
|     Header: Cache-Control: no-cache, no-store
|   Pragma:
|_    Header: Pragma: no-cache
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-headers:
|   Server: Tengine
|   Date: Sun, 05 Nov 2023 09:16:29 GMT
|   Content-Type: text/html
|   Content-Length: 239
|   Connection: close
|   Location: https://daraz.com/
|
|_  (Request type: GET)
|_http-comments-displayer: Couldn't find any comments.
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-errors: Couldn't find any error pages.
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
|_http-title: Did not follow redirect to https://daraz.com/
|_http-date: Sun, 05 Nov 2023 09:16:27 GMT; +15s from local time.
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-xssed: No previously reported XSS vuln.
| http-useragent-tester:
|   Status for browser useragent: 405
|   Redirected To: https://daraz.com/
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
```

```
|_http-chrono: Request times for /; avg: 352.73ms; min: 239.96ms; max: 634.90ms
443/tcp open  ssl/http Tengine httpd
|_http-date: Sun, 05 Nov 2023 09:16:02 GMT; +15s from local time.
|_ssl-date: TLS randomness does not represent time
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=daraz.com
|   Found the following error pages:
|
|   Error Code: 405
|_      https://daraz.com:443/
|_http-xssed: No previously reported XSS vuln.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spid
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-server-header:
|   Flywheel/5.1.0
|_  Tengine
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| No findings
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| No findings
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| No findings
|
| Exploit-DB - https://www.exploit-db.com:
| No findings
|
| OpenVAS (Nessus) - http://www.openvas.org:
| No findings
|
| SecurityTracker - https://www.securitytracker.com:
| No findings
|
| OSVDB - http://www.osvdb.org:
| No findings
|_
| tls-nextprotoneg:
|_  http/1.1
| tls-alpn:
|_  http/1.1
```

```
|
| Domain name record found at whois.verisign-grs.com
|    Domain Name: DARAZ.COM\x0D
|    Registry Domain ID: 421312005_DOMAIN_COM-VRSN\x0D
|    Registrar WHOIS Server: whois.psi-usa.info\x0D
|    Registrar URL: http://www.psi-usa.info\x0D
|    Updated Date: 2023-04-23T07:04:05Z\x0D
|    Creation Date: 2006-04-22T05:53:45Z\x0D
|    Registry Expiry Date: 2024-04-22T05:53:45Z\x0D
|    Registrar: PSI-USA, Inc. dba Domain Robot\x0D
|    Registrar IANA ID: 151\x0D
|    Registrar Abuse Contact Email: domain-abuse@psi-usa.info\x0D
|    Registrar Abuse Contact Phone: +49.94159559482\x0D
|    Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited\x0D
|    Name Server: A1-112.AKAM.NET\x0D
|    Name Server: A13-65.AKAM.NET\x0D
|    Name Server: A22-66.AKAM.NET\x0D
|    Name Server: A4-67.AKAM.NET\x0D
|    Name Server: A6-64.AKAM.NET\x0D
|    Name Server: A7-65.AKAM.NET\x0D
|    DNSSEC: unsigned\x0D
|    URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/\x0D
| >>> Last update of whois database: 2023-11-05T09:15:58Z <<<\x0D
| \x0D
```

```
|_asn-query: No Answers
| hostmap-crtsh:
|   subdomains:
|     daraz.com.np
|     sellercenter-staging.daraz.com.bd
|     pre-pull-alt2-drzlive.daraz.com
|     www.university.daraz.com.np
|     www.email.daraz.com
|     www.daraz.com
|     net.daraz.com
|     barcodes.daraz.com
|     hashi-ui.staging.daraz.com
|     bob.jm.daraz.com
|     gsearch.daraz.com
|     staging-dopsacademy.daraz.com
|     jm.daraz.com
|     email.daraz.com
|     blog-mm.daraz.com
|     sellercenter.daraz.com.bd
|     alimebot.daraz.com.np
|     http-echo.staging.daraz.com
|     staging-opsacademy.daraz.com
|     vms.live.daraz.com
|     staging.daraz.com
|     live.daraz.com
|     test.daraz.com
|     payment.daraz.com
|     lk.daraz.com
|     www.jm.daraz.com
|     gsearch.daraz.com.np
|     api.daraz.com
|     partner.daraz.com
|     bitools.daraz.com
|     careers.daraz.com
|     live-vms.daraz.com
|     www.university.daraz.com.bd
|     education.daraz.com.np
|     np.daraz.com
|     topup.daraz.com
|     gsearch.daraz.com.bd
|     spyder-api.daraz.com
|     ut.daraz.com
|     x-space.daraz.com
|     alimebot.daraz.com
|     sellercenter-staging.daraz.com.np
|     education.daraz.com.bd
|     alimebot.daraz.com.bd
```

```
| \x0D
| The Registry database contains ONLY .COM, .NET, .EDU domains and\x0D
|_Registrars.\x0D
| dns-brute:
|   DNS Brute-force hostnames:
|     shop.daraz.com - 199.7.200.45
|     vpn.daraz.com - 35.157.98.159
|     www.daraz.com - 170.33.96.99
|_    dev.daraz.com - 47.241.69.77
|_clock-skew: mean: 14s, deviation: 0s, median: 14s
| dns-blacklist:
|   SPAM
|     all.spamrats.com - FAIL
|_    l2.apews.org - FAIL
|_asn-query: No Answers
| hostmap-crtsh:
|   subdomains:
|     daraz.com.np
|     sellercenter-staging.daraz.com.bd
|     pre-pull-alt2-drzlive.daraz.com
|     www.university.daraz.com.np
|     www.email.daraz.com
|     www.daraz.com
|     net.daraz.com
|     barcodes.daraz.com
|     hashi-ui.staging.daraz.com
|     bob.jm.daraz.com
|     gsearch.daraz.com
|     staging-dopsacademy.daraz.com
|     jm.daraz.com
|     email.daraz.com
|     blog-mm.daraz.com
|     sellercenter.daraz.com.bd
|     alimebot.daraz.com.np
|     http-echo.staging.daraz.com
|     staging-opsacademy.daraz.com
|     vms.live.daraz.com
|     staging.daraz.com
|     live.daraz.com
```

```
|_http-referer-checker: Couldn't find any cross-domain scripts.
| ssl-enum-ciphers:
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_  least strength: C
```