Brick

▨ Created by	Kaio
▨ Created time	@July 2, 2025 8:28 PM
▨ Last edited by	Kaio
▨ Last updated time	@July 3, 2025 10:16 PM

Enumeration

TCP scan

```
PORT     STATE    SERVICE  REASON         VERSION
22/tcp   open     ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ub
untu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 a0:70:a7:69:96:ad:b4:48:22:b5:f6:32:63:85:65:0d (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC9zpiKimmwqvPwMUEZc
cbMd9zarJfF18RtsteoI2nBRniUZYuX6t7DK+jLZ90UU8tmlXARXDxU43IibsH1i+
B4vYR99vQdBY8Zc6GK7JhiOLDpmhSJqMkrJmu8MygPrkWrFtIaBB7zOVI8Rsf
xSOs/ssnnj1lQeQBhom86I1SK1i726y+if4LcuKmi39XrnpI/XODcZzy9x95MUIeP
8PUuOyFGKI0XMQwILX6ZHGvexpOSuKGU7/UF3oEZ5rb+kAcr8b5cU0gwLwb
bRYgEfQH3ITnHuOH5FT0jxgd1qDz3s7954RIBDQWRMO7btXaHEGIGYzTSqYM
+pAZPm8cK/PLPI///b2FnQtf4Wf/w1aF3YxukNNhBWQNu4d/iqGIYHKv9dq+hh
nSFo3gTJeFOd0u4h5QY1sSPkOyNYh4azVZS9jRuWUEHORfB26J4EGttlcyZd
mUAtVWIj/SsFBkR/T3m5S4yhPeJvt6rFc5/BH/t60J3dJaD3iCUfNiyyEwYxyE=
|   256 21:da:e6:63:3c:fc:7e:58:7d:93:1d:44:7f:b5:bc:00 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBMFmyGIEIuimTvliZuE35Sh/1RqgOItOmrnRCy0cp7iAO6w65yWr
```

```
rOeg7pBjKrNordT4LNN8gsSb8Sr623QiaQk=
|   256 5e:2e:9d:a2:92:bf:17:0c:cf:09:15:ec:bf:ea:47:fa (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFX4H7Z+0W+dP6gDfNlXkj5eb
gWS/FkuYZVcOZvaAarj
80/tcp   open     http     syn-ack ttl 63 Python http.server 3.5 - 3.10
|_http-server-header: WebSockify Python/3.8.10
|_http-title: Error response
443/tcp  open     ssl/http syn-ack ttl 63 Apache httpd
|_http-server-header: Apache
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinc
eName=Some-State/countryName=US
| Issuer: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=S
ome-State/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-04-02T11:59:14
| Not valid after:  2025-04-02T11:59:14
| MD5:   f1df:99bc:d5ab:5a5a:5709:5099:4add:a385
| SHA-1: 1f26:54bb:e2c5:b4a1:1f62:5ea0:af00:0261:35da:23c3
| -----BEGIN CERTIFICATE-----
| MIIDazCCAlOgAwIBAgIUPbOGG+Xi6dsd8rNRzG/wI3DvA8MwDQYJKoZIhvc
NAQEL
| BQAwRTELMAkGA1UEBhMCVVMxEzARBgNVBAgMClNvbWUtU3RhdGUxITAf
BgNVBAoM
| GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yNDA0MDIxMTU5MTRa
Fw0yNTA0
| MDIxMTU5MTRaMEUxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApTb21lLVN0
YXRlMSEw
| HwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqG
SIb3DQEB
| AQUAA4IBDwAwggEKAoIBAQCtzw+eboW61zIzd/tI7LdrZCO86nc/MN0DkZfT
```

```
ngO7
| IJq/VQgR617FfExm26yI+wZSEkUWO5dg+1BYJbkYIayzr0Dyor3E2l73dIsM2U
r4
| s6hET6gYFD8pCu9z6YvMqxcq/1YWN+pOGsicAFeT6t8uQBYyA9NZZXSAISn
orUbV
| aRW/Z8cwijQquIfwIiBaVhOnqBAqoudHQ5yLb461PGgVpioNeS9DDe3I7+J5L
Pe7
| va5wcnTJ2xfKrCHIPipuAgj5lCJ7lihIvT0KDB1elFxy5yIPABR5MthRs36eiO4+
| 1AKfPDVrvC5IpBvycgT95qhR0AnS+N9CwmO4HUWq5AJtAgMBAAGjUzBRM
B0GA1Ud
| DgQWBBQHb6dwgvFLizbay0+nIgxlfzZYtjAfBgNVHSMEGDAWgBQHb6dwgv
FLizba
| y0+nIgxlfzZYtjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4
IBAQBJ
| gjQinsS5AIb/LJT4KVhHgDAVezICOx3kg6foyMV3z6CcU9e6QLuMpyMCR/U
GqUqs
| m0iJH8sR1jJdS3tDPTEmJXW8gBux3Y4xI9/A1sMhm97O5O7KHiBiwiW47Pwf
o4/a
| wchcSEcU/4jfivY7ifGcIBSN4GInUHjwfD63J0/LHh1GPEo/Wsoekk0586psicaV
| dv3UqrFcLFztwKGDgs+51Oc9a70xT96bko0huCZ1NFOh4zchZ3kno9mueUR
i/SJO
| ibgwFMBWO7mQHKnInQxxQwxER+QyftgnO+gXvkPGQU+o4rMnjHX5EAjyfo
utRjjN
| tQWUR7AJRMC+3VGdRcVV
|_-----END CERTIFICATE-----
|_http-generator: WordPress 6.5
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: Brick by Brick
3306/tcp open     mysql    syn-ack ttl 63 MySQL (unauthorized)
4900/tcp filtered hfcs     no-response
5357/tcp filtered wsdapi   no-response
Device type: general purpose
```

```
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
```

vulnerable scan ⇒ nothing

Cannot do gobuster

hydra ⇒ useless creds

Port 443:

Page-Source mention wp-admin, wp-theme

wpscan

```
[+] robots.txt found: https://bricks.thm/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://bricks.thm/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pin
```

```
gback_access/

[+] WordPress readme found: https://bricks.thm/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://bricks.thm/wp-cron.p
hp
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.5 identified (Insecure, released on 2024-04-02).
 | Found By: Rss Generator (Passive Detection)
 |  - https://bricks.thm/feed/, <generator>https://wordpress.org/?v=6.5</gene
rator>
 |  - https://bricks.thm/comments/feed/, <generator>https://wordpress.org/?v
=6.5</generator>

[+] WordPress theme in use: bricks
 | Location: https://bricks.thm/wp-content/themes/bricks/
 | Readme: https://bricks.thm/wp-content/themes/bricks/readme.txt
 | Style URL: https://bricks.thm/wp-content/themes/bricks/style.css
 | Style Name: Bricks
 | Style URI: https://bricksbuilder.io/
 | Description: Visual website builder for WordPress....
 | Author: Bricks
 | Author URI: https://bricksbuilder.io/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.9.5 (80% confidence)
 | Found By: Style (Passive Detection)
 | - https://bricks.thm/wp-content/themes/bricks/style.css, Match: 'Version: 1.9.5'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:15 <============> (137 / 137) 100.00% Time: 00:00:15

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Jul  2 21:14:46 2025
[+] Requests Done: 170
[+] Cached Requests: 7
[+] Data Sent: 41.615 KB
[+] Data Received: 110.502 KB
[+] Memory used: 262.25 MB
[+] Elapsed time: 00:00:31
```

CVE-2024-25600

look for sussy process

```
systemctl | grep running
```