Potential Security Risks in Blockchain RPC and Bridge Endpoints

Node Detection: Scan IP ranges to identify open blockchain node ports.

Identifying RPC Endpoints:

- https://testnet.ethernitychain.io/
- https://mainnet.ethernitychain.io/

Identifying Bridge Endpoints:

- https://bridge.ethernity.io/

Node Identification: Determine the type of blockchain node based on the open port.

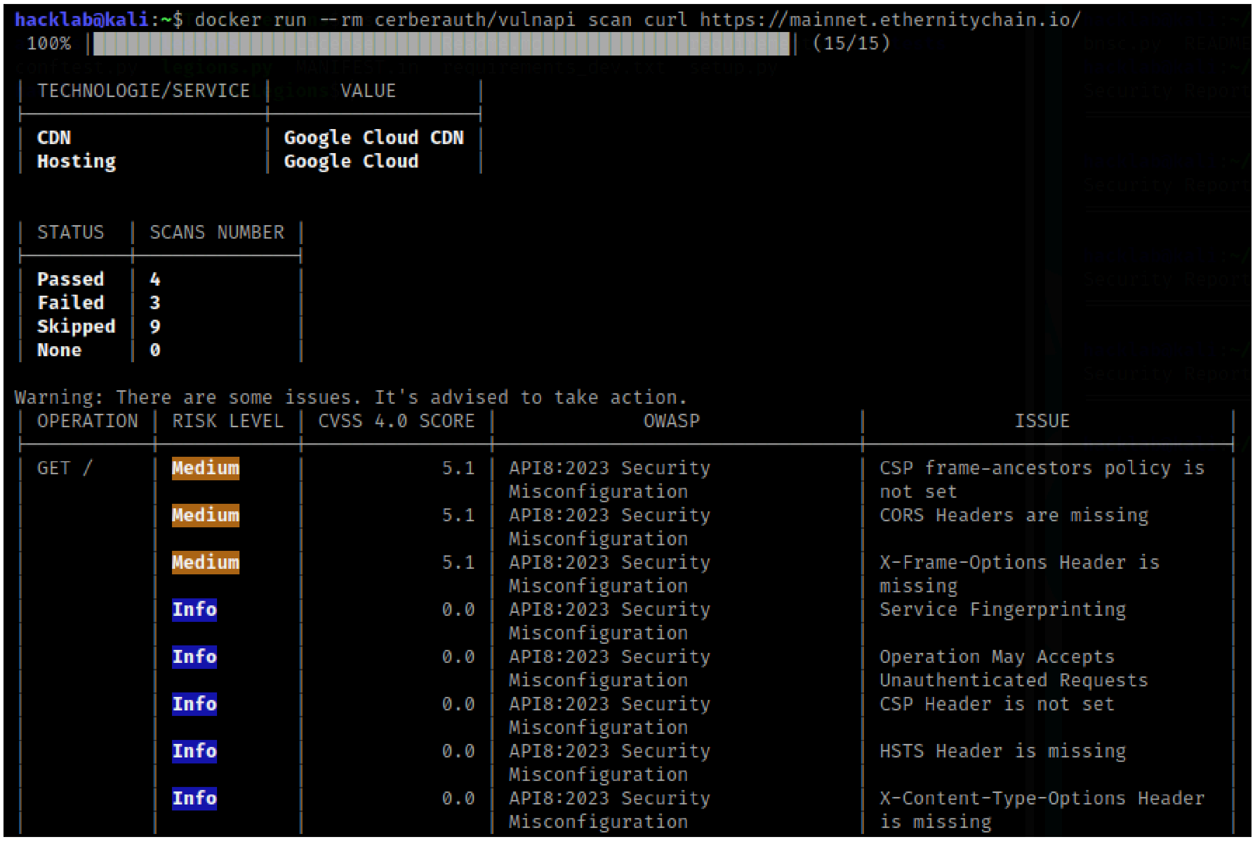
RPC Interface Check: Identify exposed RPC interfaces that shouldn't be public.

Endpoint Vulnerabilities:

docker run --rm cerberauth/vulnapi scan curl endpoint

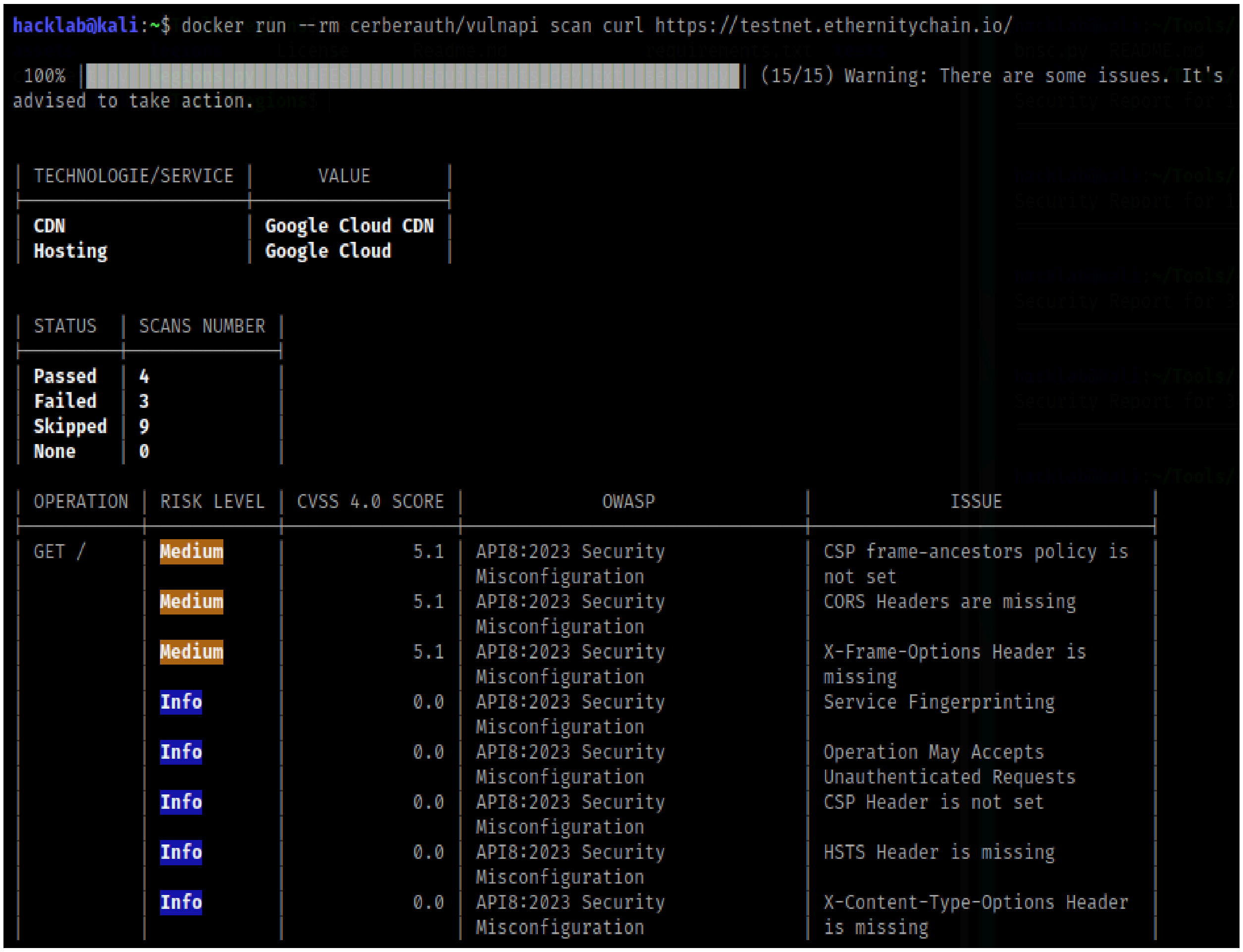
---

1. **Common Security Vulnerabilities https://mainnet.ethernitychain.io/**



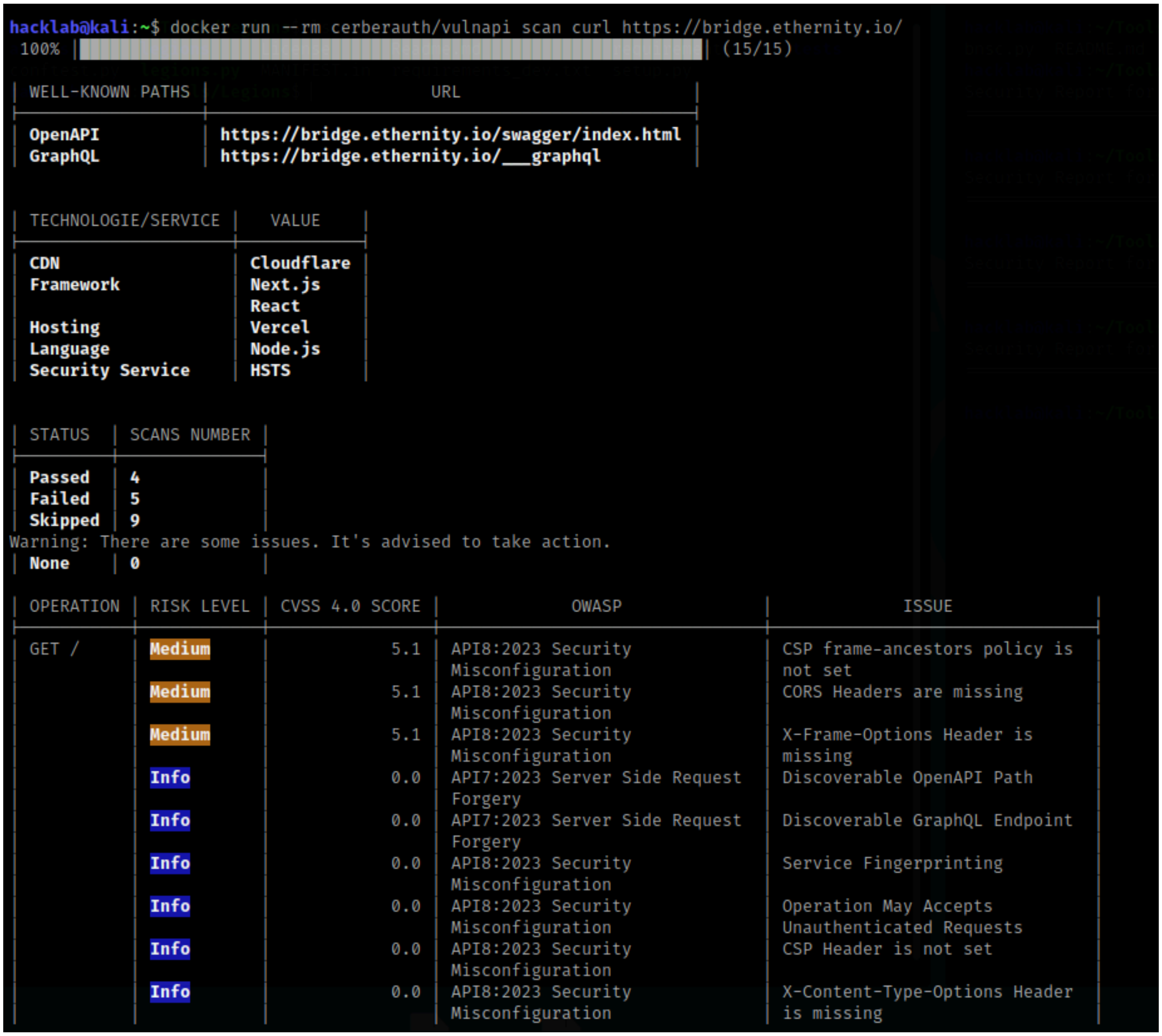
```
hacklab@kali:~$ docker run --rm cerberauth/vulnapi scan curl https://mainnet.ethernitychain.io/
 100% |████████████████████████████████████████████████████████████| (15/15)

| TECHNOLOGIE/SERVICE |       VALUE      |
|---------------------|------------------|
| CDN                 | Google Cloud CDN |
| Hosting             | Google Cloud     |

| STATUS  | SCANS NUMBER |
|---------|--------------|
| Passed  | 4            |
| Failed  | 3            |
| Skipped | 9            |
| None    | 0            |

Warning: There are some issues. It's advised to take action.
| OPERATION | RISK LEVEL | CVSS 4.0 SCORE |           OWASP            |            ISSUE            |
|-----------|------------|----------------|----------------------------|-----------------------------|
| GET /     | Medium     |            5.1 | API8:2023 Security         | CSP frame-ancestors policy is |
|           |            |                | Misconfiguration           | not set                     |
|           | Medium     |            5.1 | API8:2023 Security         | CORS Headers are missing    |
|           |            |                | Misconfiguration           |                             |
|           | Medium     |            5.1 | API8:2023 Security         | X-Frame-Options Header is   |
|           |            |                | Misconfiguration           | missing                     |
|           | Info       |            0.0 | API8:2023 Security         | Service Fingerprinting      |
|           |            |                | Misconfiguration           |                             |
|           | Info       |            0.0 | API8:2023 Security         | Operation May Accepts       |
|           |            |                | Misconfiguration           | Unauthenticated Requests    |
|           | Info       |            0.0 | API8:2023 Security         | CSP Header is not set       |
|           |            |                | Misconfiguration           |                             |
|           | Info       |            0.0 | API8:2023 Security         | HSTS Header is missing      |
|           |            |                | Misconfiguration           |                             |
|           | Info       |            0.0 | API8:2023 Security         | X-Content-Type-Options Header |
|           |            |                | Misconfiguration           | is missing                  |
```

2. Common Security Vulnerabilities https://testnet.ethernitychain.io/



```
hacklab@kali:~$ docker run --rm cerberauth/vulnapi scan curl https://testnet.ethernitychain.io/

 100% |████████████████████████████████████████████████████████████| (15/15) Warning: There are some issues. It's
advised to take action.


│ TECHNOLOGIE/SERVICE │      VALUE       │
├─────────────────────┼──────────────────┤
│ CDN                 │ Google Cloud CDN │
│ Hosting             │ Google Cloud     │


│ STATUS  │ SCANS NUMBER │
├─────────┼──────────────┤
│ Passed  │ 4            │
│ Failed  │ 3            │
│ Skipped │ 9            │
│ None    │ 0            │

│ OPERATION │ RISK LEVEL │ CVSS 4.0 SCORE │              OWASP               │              ISSUE              │
├───────────┼────────────┼────────────────┼──────────────────────────────────┼─────────────────────────────────┤
│ GET /     │ Medium     │            5.1 │ API8:2023 Security               │ CSP frame-ancestors policy is   │
│           │            │                │ Misconfiguration                 │ not set                         │
│           │ Medium     │            5.1 │ API8:2023 Security               │ CORS Headers are missing        │
│           │            │                │ Misconfiguration                 │                                 │
│           │ Medium     │            5.1 │ API8:2023 Security               │ X-Frame-Options Header is       │
│           │            │                │ Misconfiguration                 │ missing                         │
│           │ Info       │            0.0 │ API8:2023 Security               │ Service Fingerprinting          │
│           │            │                │ Misconfiguration                 │                                 │
│           │ Info       │            0.0 │ API8:2023 Security               │ Operation May Accepts           │
│           │            │                │ Misconfiguration                 │ Unauthenticated Requests        │
│           │ Info       │            0.0 │ API8:2023 Security               │ CSP Header is not set           │
│           │            │                │ Misconfiguration                 │                                 │
│           │ Info       │            0.0 │ API8:2023 Security               │ HSTS Header is missing          │
│           │            │                │ Misconfiguration                 │                                 │
│           │ Info       │            0.0 │ API8:2023 Security               │ X-Content-Type-Options Header   │
│           │            │                │ Misconfiguration                 │ is missing                      │
```

3. Common Security Vulnerabilities https://bridge.ethernity.io/



```
hacklab@kali:~$ docker run --rm cerberauth/vulnapi scan curl https://bridge.ethernity.io/
 100% |████████████████████████████████████████████████████████████████| (15/15)
| WELL-KNOWN PATHS |                    URL                     |
|------------------|--------------------------------------------|
| OpenAPI          | https://bridge.ethernity.io/swagger/index.html |
| GraphQL          | https://bridge.ethernity.io/___graphql     |

| TECHNOLOGIE/SERVICE |   VALUE    |
|---------------------|------------|
| CDN                 | Cloudflare |
| Framework           | Next.js    |
|                     | React      |
| Hosting             | Vercel     |
| Language            | Node.js    |
| Security Service    | HSTS       |

| STATUS  | SCANS NUMBER |
|---------|--------------|
| Passed  | 4            |
| Failed  | 5            |
| Skipped | 9            |
Warning: There are some issues. It's advised to take action.
| None    | 0            |

| OPERATION | RISK LEVEL | CVSS 4.0 SCORE |              OWASP               |              ISSUE               |
|-----------|------------|----------------|----------------------------------|----------------------------------|
| GET /     | Medium     |            5.1 | API8:2023 Security               | CSP frame-ancestors policy is    |
|           |            |                | Misconfiguration                 | not set                          |
|           | Medium     |            5.1 | API8:2023 Security               | CORS Headers are missing         |
|           |            |                | Misconfiguration                 |                                  |
|           | Medium     |            5.1 | API8:2023 Security               | X-Frame-Options Header is        |
|           |            |                | Misconfiguration                 | missing                          |
|           | Info       |            0.0 | API7:2023 Server Side Request    | Discoverable OpenAPI Path        |
|           |            |                | Forgery                          |                                  |
|           | Info       |            0.0 | API7:2023 Server Side Request    | Discoverable GraphQL Endpoint    |
|           |            |                | Forgery                          |                                  |
|           | Info       |            0.0 | API8:2023 Security               | Service Fingerprinting           |
|           |            |                | Misconfiguration                 |                                  |
|           | Info       |            0.0 | API8:2023 Security               | Operation May Accepts            |
|           |            |                | Misconfiguration                 | Unauthenticated Requests         |
|           | Info       |            0.0 | API8:2023 Security               | CSP Header is not set            |
|           |            |                | Misconfiguration                 |                                  |
|           | Info       |            0.0 | API8:2023 Security               | X-Content-Type-Options Header    |
|           |            |                | Misconfiguration                 | is missing                       |
```