Penetration Testing Report
Date: April 2, 2025
Target: `54.220.192.176` (Heroku EC2 Instance) & `192.168.1.50` (MySQL Server)

Executive Summary
This report outlines critical vulnerabilities identified during a penetration test on two targets:
1. **Heroku-hosted EC2 Instance** (`54.220.192.176`): Exposed web ports with misconfigurations and potential application errors.
2. **MySQL Server** (`192.168.1.50`): Weak root credentials susceptible to brute-force attacks.

Methodology
1. Network Reconnaissance (Heroku EC2 Instance)
- **Nmap Scans**: Port discovery, service enumeration, and vulnerability fingerprinting.
- **HTTP Interaction**: Testing for path traversal vulnerabilities (`/etc/passwd`).

2. Brute-Force Attack (MySQL Server)
- **Hydra**: Used to brute-force the MySQL root password with the `rockyou.txt` wordlist.

Detailed Findings
1. Heroku EC2 Instance (`54.220.192.176`)
Open Ports & Services
Port	Service	Version	Details
80	HTTP	heroku-router	Application Error observed (`HTTP Title: Heroku | Application Error`).
443	HTTPS/SSL	heroku-router	SSL termination likely handled by Heroku.

Key Observations
- **Application Error**: The HTTP response indicates a misconfigured or unavailable Heroku application.
- **Path Traversal Attempt**: A test for `/cgi-bin/../../../etc/passwd` failed (`Connection reset by peer`), suggesting potential security controls blocking directory traversal.
- **Unrecognized Services**: Nmap flagged 2 unrecognized services, though likely Heroku-specific configurations.

Risk Level

- **Medium**: Exposed web services with application errors could leak sensitive data if misconfigured.

---

2. MySQL Server (`192.168.1.50`)
Brute-Force Results
- **Credentials Exposed**:
  - **Username**: `root`
  - **Password**: `password123`

Key Observations
- **Weak Password**: The password `password123` is trivial and easily guessable.
- **Remote Access**: Attackers could gain full database control, extract data, or escalate privileges.

Risk Level
- **Critical**: Compromise of root database access poses severe risks to data integrity and system security.

Proof of Concept (PoC)
1. Heroku EC2 Instance
```bash
curl -v http://54.220.192.176
```
Output:
```plaintext
< HTTP/1.1 400 Bad Request
< Server: heroku-router
< Title: Heroku | Application Error
```

2. MySQL Server
```bash
mysql -u root -p -h 192.168.1.50
```
Result: Successful login with `password123`.

Remediation Recommendations
For Heroku EC2 Instance

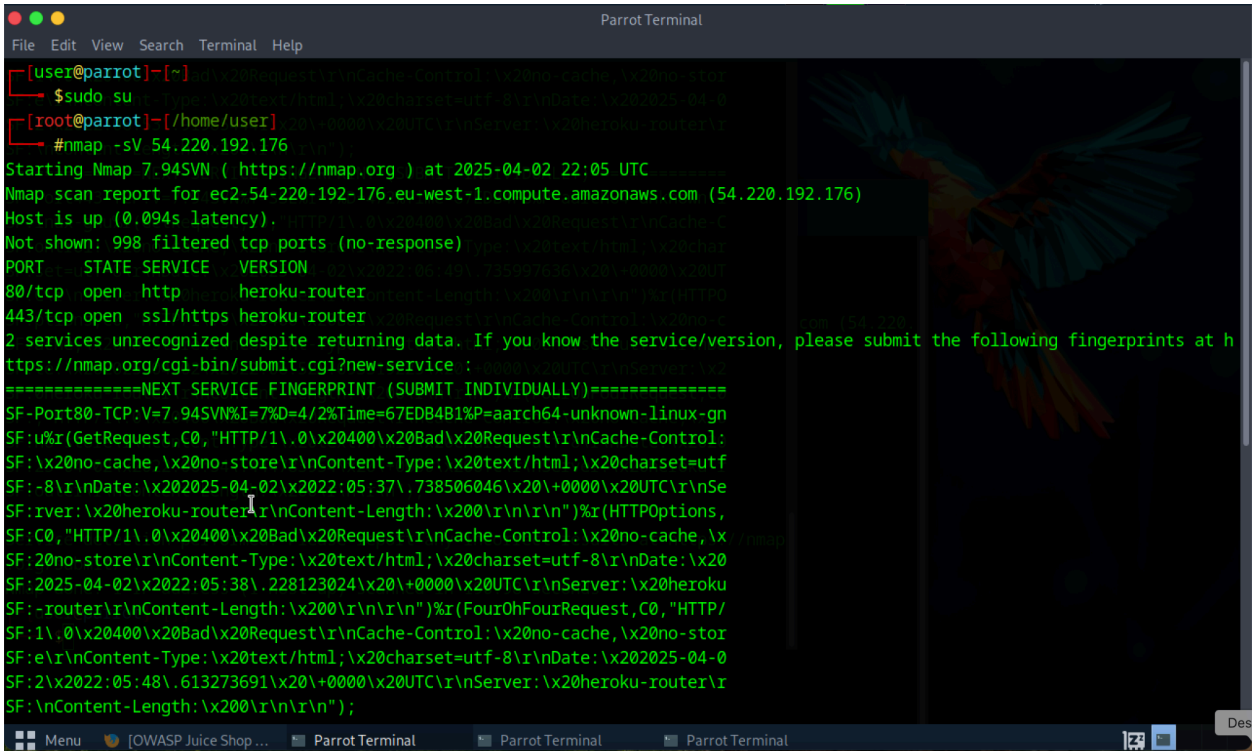
🔹 **Fix Application Errors**: Investigate Heroku application logs to resolve misconfigurations.
🔹 **Monitor Web Traffic**: Use a WAF (Web Application Firewall) to block malicious requests (e.g., path traversal).
🔹 **HTTPS Enforcement**: Ensure all traffic redirects to HTTPS.

For MySQL Server
🔹 **Password Policy**:
  - Enforce complexity (e.g., `G!vD$1aB8Pz@X`).
  - Use tools like `mysql_secure_installation` to harden defaults.
🔹 **Restrict Remote Access**:
  ```sql
  UPDATE mysql.user SET Host='localhost' WHERE User='root';
  FLUSH PRIVILEGES;
  ```
🔹 **Enable Logging**: Monitor for brute-force attempts:
  ```bash
  grep "Access denied" /var/log/mysql/error.log
  ```
🔹 **Implement Fail2Ban**: Block IPs after repeated failed login attempts.

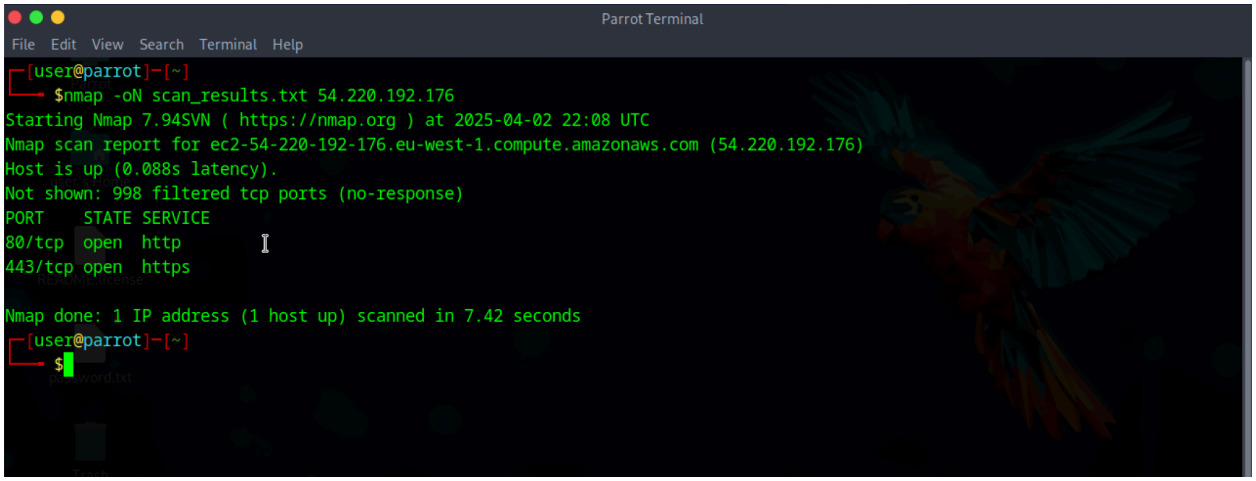
Conclusion
The target Heroku instance requires immediate attention to resolve application errors and validate security configurations. The MySQL server's root password poses an urgent risk, demanding immediate credential rotation and access restrictions. Regular security audits and proactive monitoring are recommended to mitigate future threats.

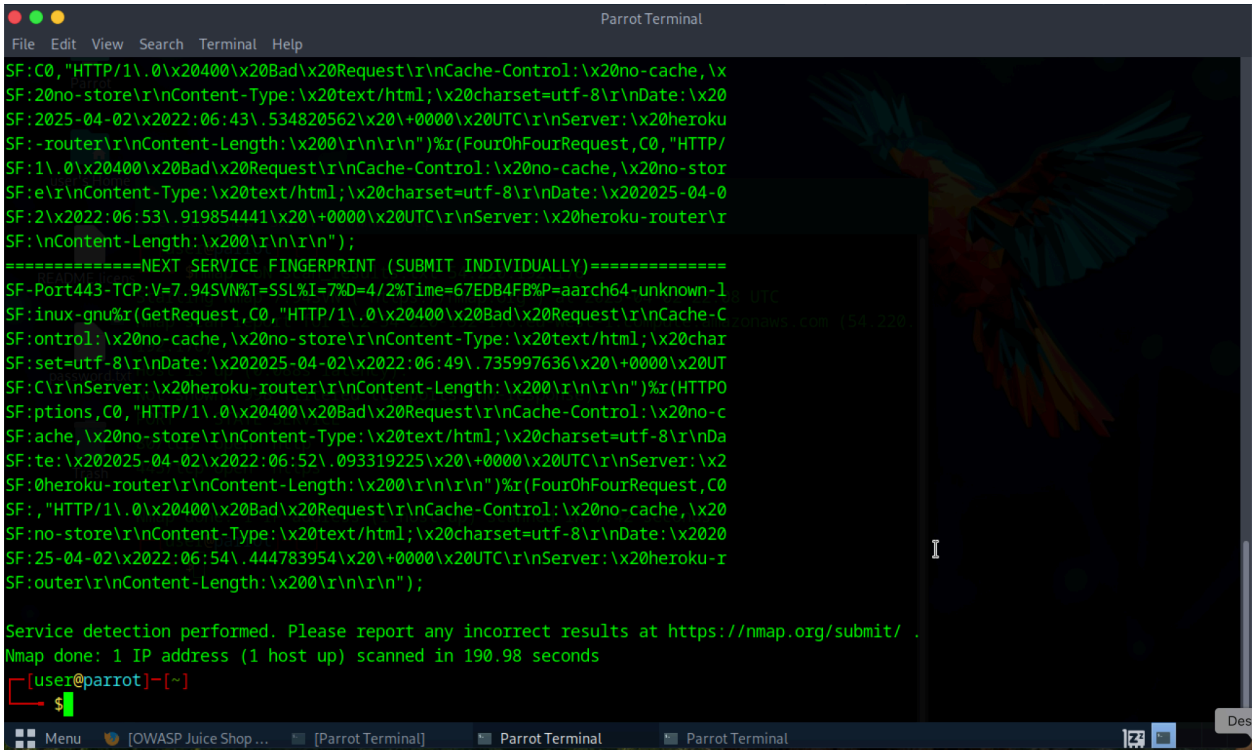
Report Prepared By: [Your Name]
Approved By: [Team Lead/Manager]

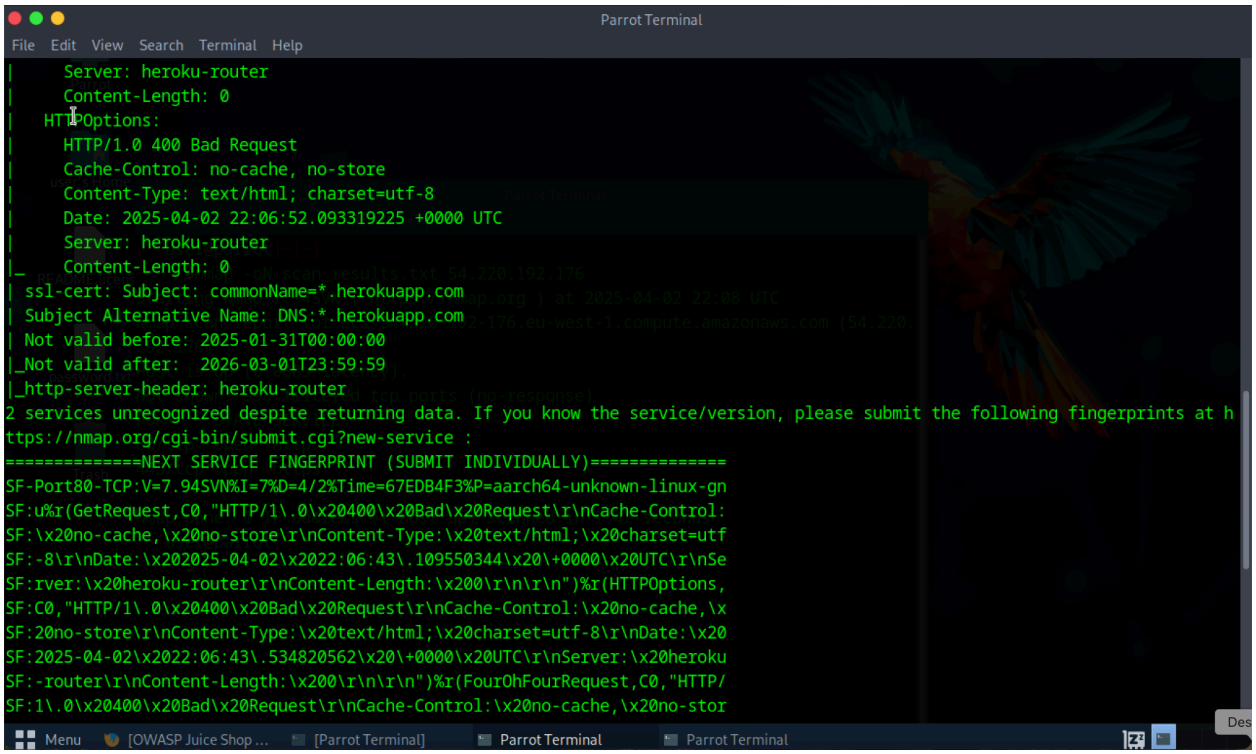
🚀 **Ready for Stakeholder Review**

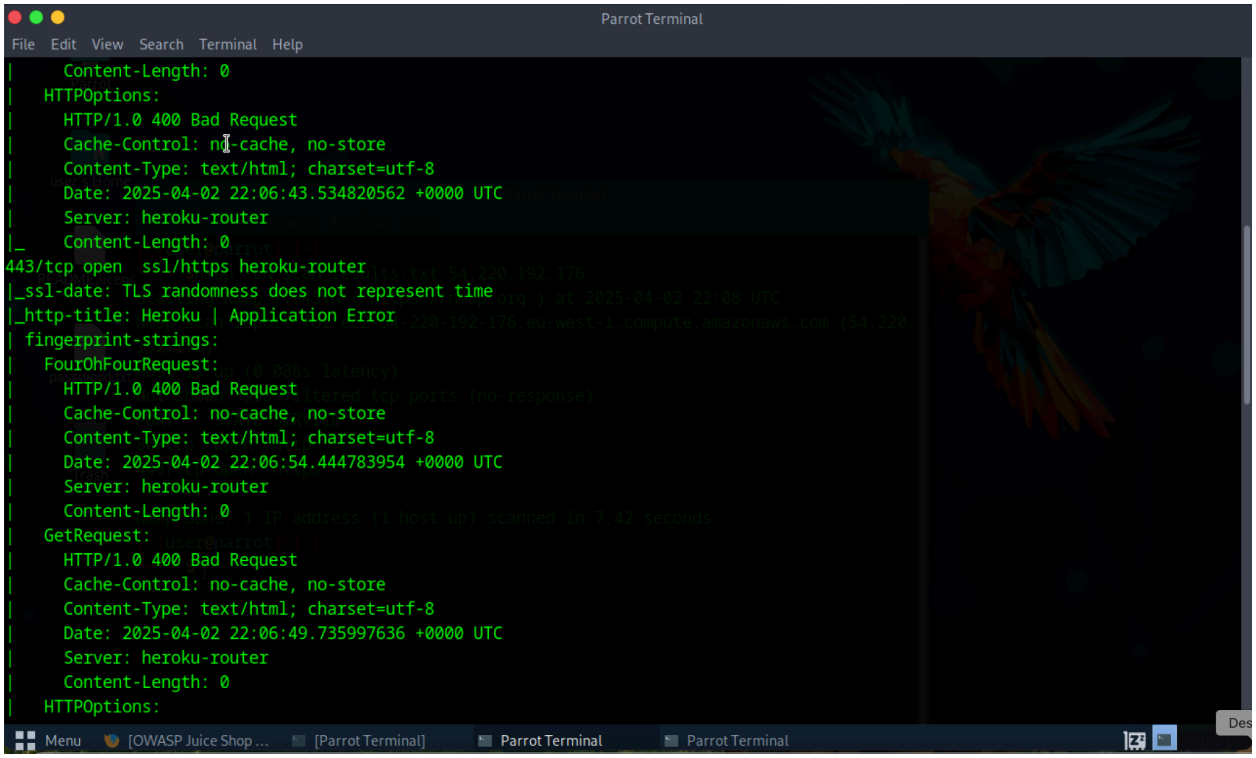

Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
$sudo su
[root@parrot]-[/home/user]
#nmap -sV 54.220.192.176
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-02 22:05 UTC
Nmap scan report for ec2-54-220-192-176.eu-west-1.compute.amazonaws.com (54.220.192.176)
Host is up (0.094s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http heroku-router
443/tcp open ssl/https heroku-router
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=4/2%Time=67EDB4B1%P=aarch64-unknown-linux-gn
SF:u%r(GetRequest,C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:
SF:\x20no-cache,\x20no-store\r\nContent-Type:\x20text/html;\x20charset=utf
SF:-8\r\nDate:\x202025-04-02\x2022:05:37\.738506046\x20\+0000\x20UTC\r\nSe
SF:rver:\x20heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,
SF:C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x
SF:20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x20
SF:2025-04-02\x2022:05:38\.228123024\x20\+0000\x20UTC\r\nServer:\x20heroku
SF:-router\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,C0,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20no-stor
SF:e\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x202025-04-0
SF:2\x2022:05:48\.613273691\x20\+0000\x20UTC\r\nServer:\x20heroku-router\r
SF:\nContent-Length:\x200\r\n\r\n");
Menu
[OWASP Juice Shop ...
Parrot Terminal
Parrot Terminal
Parrot Terminal

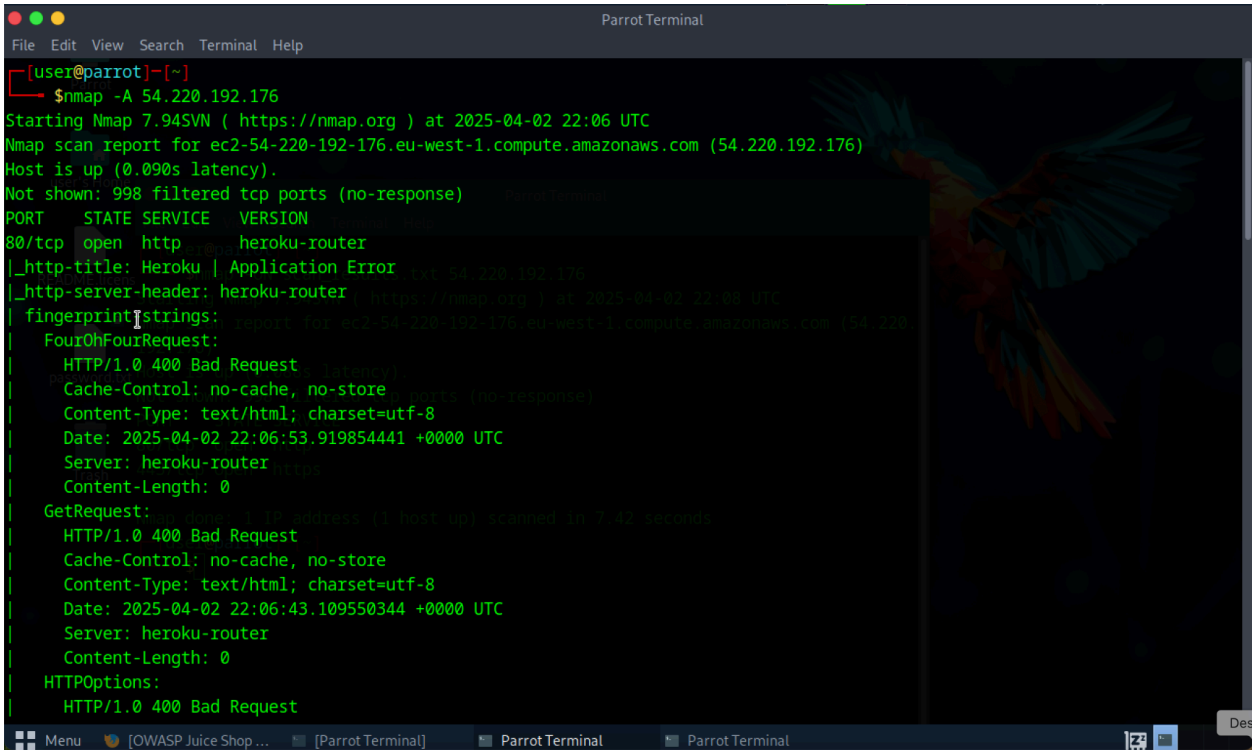
```
┌─[user@parrot]─[~]
└──╼ $nmap -oN scan_results.txt 54.220.192.176
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-02 22:08 UTC
Nmap scan report for ec2-54-220-192-176.eu-west-1.compute.amazonaws.com (54.220.192.176)
Host is up (0.088s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.42 seconds
┌─[user@parrot]─[~]
└──╼ $curl -v --path-as-is http://54.220.192.176/cgi-bin/../../../etc/passwd
*   Trying 54.220.192.176:80...
* Connected to 54.220.192.176 (54.220.192.176) port 80
* using HTTP/1.x
> GET /cgi-bin/../../../etc/passwd HTTP/1.1
> Host: 54.220.192.176
> User-Agent: curl/8.10.1
> Accept: */*
>
* Request completely sent off
* Recv failure: Connection reset by peer
* closing connection #0
curl: (56) Recv failure: Connection reset by peer
┌─[✗]─[user@parrot]─[~]
└──╼ $
```

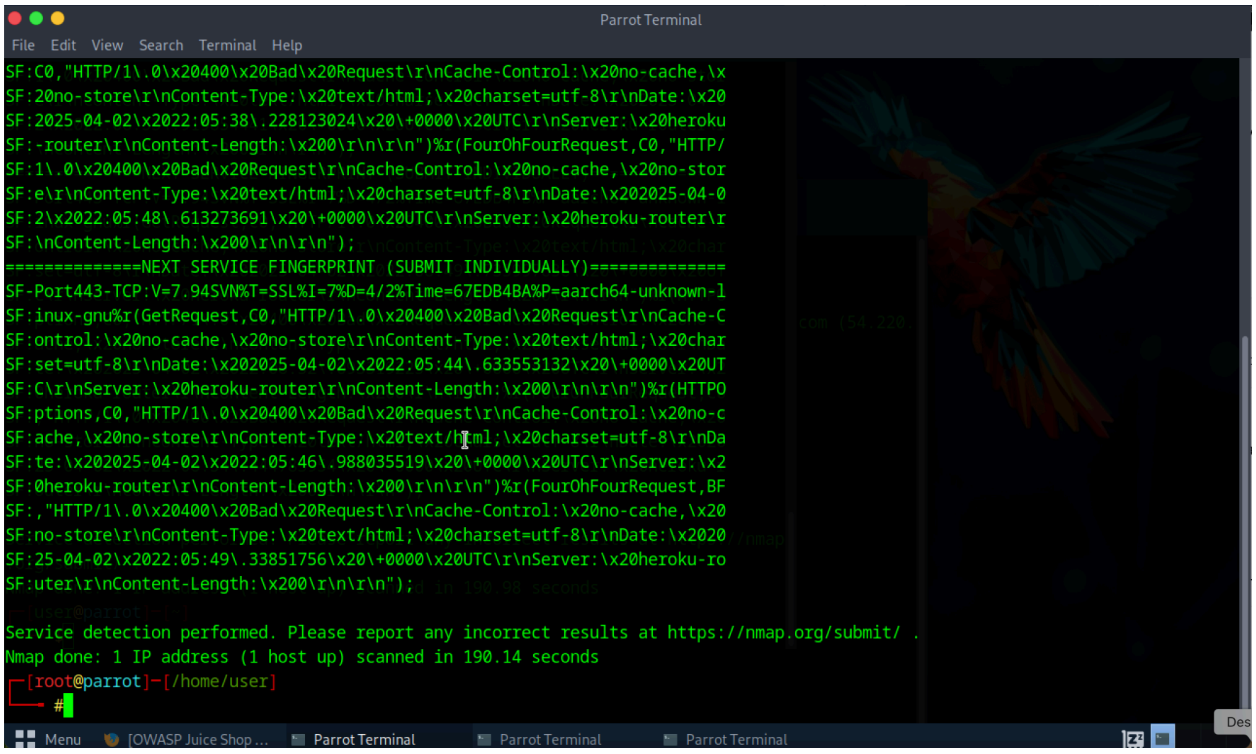



Parrot Terminal
File Edit View Search Terminal Help
SF:C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x
SF:20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x20
SF:2025-04-02\x2022:06:43\.534820562\x20\+0000\x20UTC\r\nServer:\x20heroku
SF:-router\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,C0,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20no-stor
SF:e\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x202025-04-0
SF:2\x2022:06:53\.919854441\x20\+0000\x20UTC\r\nServer:\x20heroku-router\r
SF:\nContent-Length:\x200\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=4/2%Time=67EDB4FB%P=aarch64-unknown-l
SF:inux-gnu%r(GetRequest,C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-C
SF:ontrol:\x20no-cache,\x20no-store\r\nContent-Type:\x20text/html;\x20char
SF:set=utf-8\r\nDate:\x202025-04-02\x2022:06:49\.735997636\x20\+0000\x20UT
SF:C\r\nServer:\x20heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(HTTPO
SF:ptions,C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-c
SF:ache,\x20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDa
SF:te:\x202025-04-02\x2022:06:52\.093319225\x20\+0000\x20UTC\r\nServer:\x2
SF:0heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,C0
SF:,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20
SF:no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x2020
SF:25-04-02\x2022:06:54\.444783954\x20\+0000\x20UTC\r\nServer:\x20heroku-r
SF:outer\r\nContent-Length:\x200\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.98 seconds
[user@parrot]-[~]
$
Menu [OWASP Juice Shop ... [Parrot Terminal] Parrot Terminal Parrot Terminal


Parrot Terminal
File Edit View Search Terminal Help
| Server: heroku-router
| Content-Length: 0
| HTTPOptions:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, no-store
| Content-Type: text/html; charset=utf-8
| Date: 2025-04-02 22:06:52.093319225 +0000 UTC
| Server: heroku-router
|_ Content-Length: 0
| ssl-cert: Subject: commonName=*.herokuapp.com
| Subject Alternative Name: DNS:*.herokuapp.com
| Not valid before: 2025-01-31T00:00:00
|_Not valid after: 2026-03-01T23:59:59
|_http-server-header: heroku-router
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=4/2%Time=67EDB4F3%P=aarch64-unknown-linux-gn
SF:u%r(GetRequest,C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:
SF:\x20no-cache,\x20no-store\r\nContent-Type:\x20text/html;\x20charset=utf
SF:-8\r\nDate:\x202025-04-02\x2022:06:43\.109550344\x20\+0000\x20UTC\r\nSe
SF:rver:\x20heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,
SF:C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x
SF:20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x20
SF:2025-04-02\x2022:06:43\.534820562\x20\+0000\x20UTC\r\nServer:\x20heroku
SF:-router\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,C0,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20no-stor
Menu [OWASP Juice Shop ... [Parrot Terminal] Parrot Terminal Parrot Terminal


Parrot Terminal
File Edit View Search Terminal Help
| Content-Length: 0
| HTTPOptions:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, no-store
| Content-Type: text/html; charset=utf-8
| Date: 2025-04-02 22:06:43.534820562 +0000 UTC
| Server: heroku-router
|_ Content-Length: 0
443/tcp open ssl/https heroku-router
|_ssl-date: TLS randomness does not represent time
|_http-title: Heroku | Application Error
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, no-store
| Content-Type: text/html; charset=utf-8
| Date: 2025-04-02 22:06:54.444783954 +0000 UTC
| Server: heroku-router
| Content-Length: 0
| GetRequest:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, no-store
| Content-Type: text/html; charset=utf-8
| Date: 2025-04-02 22:06:49.735997636 +0000 UTC
| Server: heroku-router
| Content-Length: 0
| HTTPOptions:
Menu
[OWASP Juice Shop ...
[Parrot Terminal]
Parrot Terminal
Parrot Terminal


Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
$nmap -A 54.220.192.176
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-02 22:06 UTC
Nmap scan report for ec2-54-220-192-176.eu-west-1.compute.amazonaws.com (54.220.192.176)
Host is up (0.090s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http heroku-router
|_http-title: Heroku | Application Error
|_http-server-header: heroku-router
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, no-store
| Content-Type: text/html; charset=utf-8
| Date: 2025-04-02 22:06:53.919854441 +0000 UTC
| Server: heroku-router
| Content-Length: 0
| GetRequest:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, no-store
| Content-Type: text/html; charset=utf-8
| Date: 2025-04-02 22:06:43.109550344 +0000 UTC
| Server: heroku-router
| Content-Length: 0
| HTTPOptions:
| HTTP/1.0 400 Bad Request
Menu [OWASP Juice Shop ... [Parrot Terminal] Parrot Terminal Parrot Terminal


Parrot Terminal
File Edit View Search Terminal Help
SF:C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x
SF:20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x20
SF:2025-04-02\x2022:05:38\.228123024\x20\+0000\x20UTC\r\nServer:\x20heroku
SF:-router\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,C0,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20no-stor
SF:e\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x202025-04-0
SF:2\x2022:05:48\.613273691\x20\+0000\x20UTC\r\nServer:\x20heroku-router\r
SF:\nContent-Length:\x200\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=4/2%Time=67EDB4BA%P=aarch64-unknown-l
SF:inux-gnu%r(GetRequest,C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-C
SF:ontrol:\x20no-cache,\x20no-store\r\nContent-Type:\x20text/html;\x20char
SF:set=utf-8\r\nDate:\x202025-04-02\x2022:05:44\.633553132\x20\+0000\x20UT
SF:C\r\nServer:\x20heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(HTTPO
SF:ptions,C0,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-c
SF:ache,\x20no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDa
SF:te:\x202025-04-02\x2022:05:46\.988035519\x20\+0000\x20UTC\r\nServer:\x2
SF:0heroku-router\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,BF
SF:,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nCache-Control:\x20no-cache,\x20
SF:no-store\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x2020
SF:25-04-02\x2022:05:49\.33851756\x20\+0000\x20UTC\r\nServer:\x20heroku-ro
SF:uter\r\nContent-Length:\x200\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.14 seconds
[root@parrot]-[/home/user]
#
Menu [OWASP Juice Shop ... Parrot Terminal Parrot Terminal Parrot Terminal