AMAZON KUBERNETES SERVICES

Amazon has a ECS (Elastic Container Service) under its container services which is used to run Docker applications on a scalable cluster. You can deploy the Docker application with Load Balancing [optional], as it automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones.

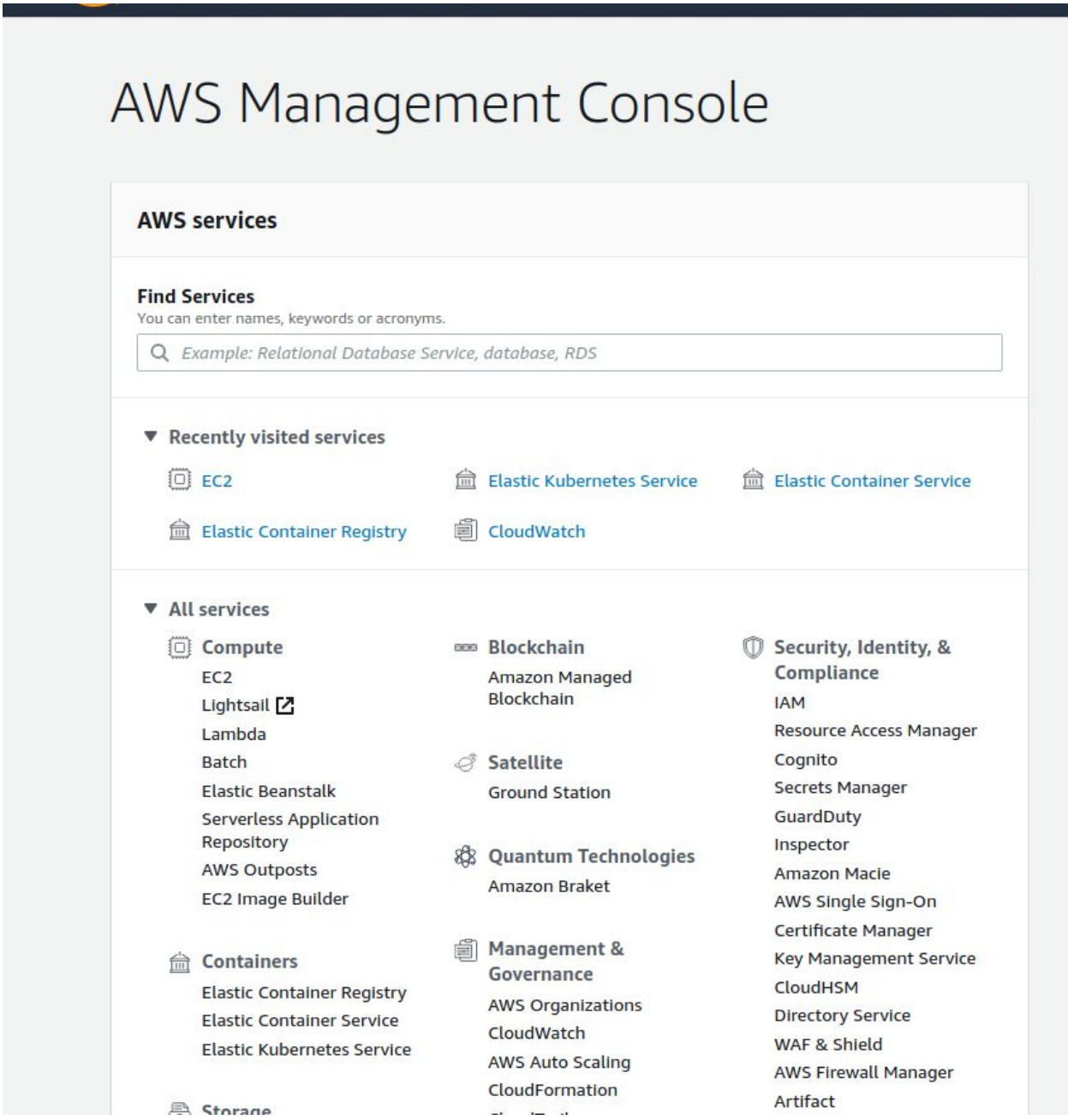
Elastic Load Balancing supports the following types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers. Amazon ECS services can use either type of load balancer. Application Load Balancers are used to route HTTP/HTTPS (or Layer 7) traffic.

Prerequisites

- Account on AWS with Free Tier or Paid.
- https://aws.amazon.com/

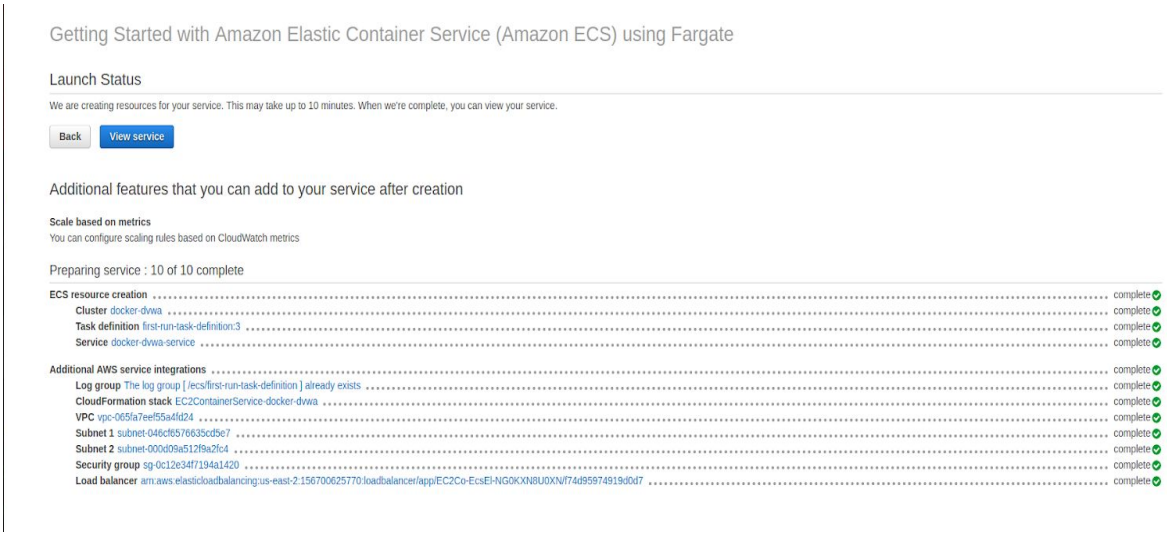
STEPS

1. DVWA Docker Image deployment
    a. Login to AWS Console.

b. 

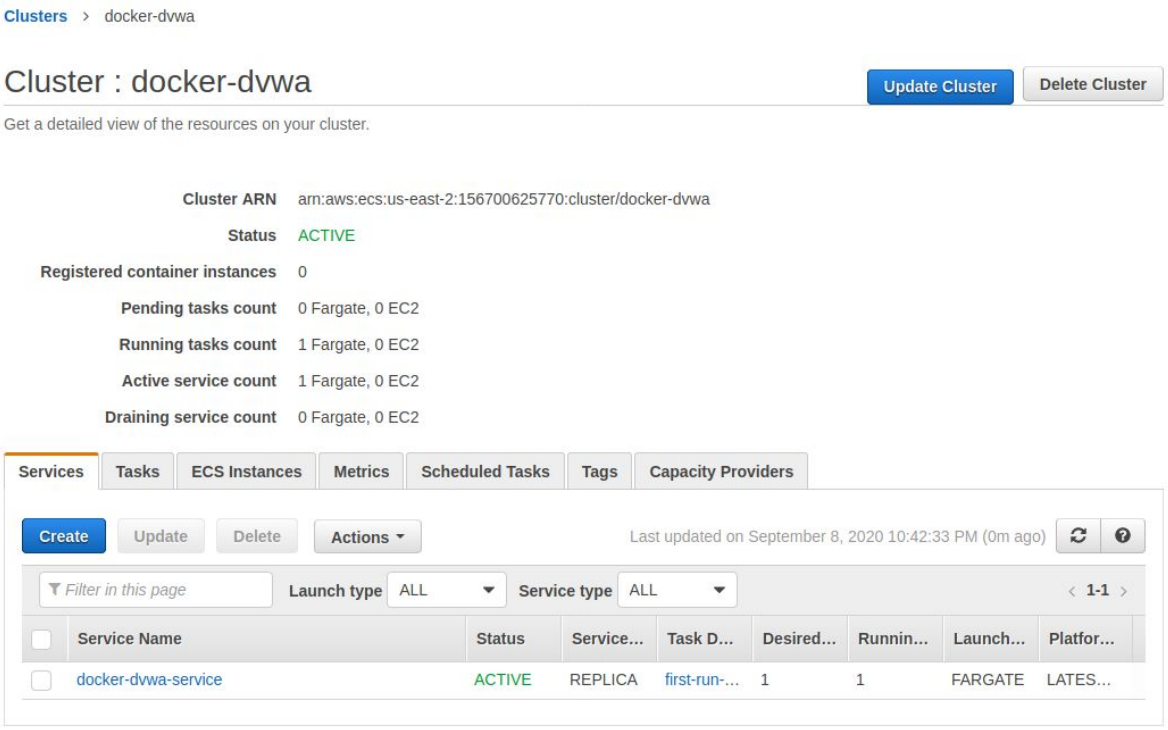
c. In AWS Management Console, choose **Elastic Container Service** (All Services > Containers > Elastic Container Service).
d. On the Left Pane, Choose **Clusters** under Amazon ECS.
e. Click on **Get Started.**
f. In Step 1, **Custom image configure** (Container and Task -> Container definition)
g. Give any container name.

h. Image: **vulnerables/web-dvwa**
i. Memory Limits: **300**
j. Port mappings: **80 tcp**.
k. In Step 2, **Load Balancer type: None (default)**. But if you want to add then create a Load Balancer in ELB, then add it under **Application Load Balancer.**
l. Give a **Cluster name**.
m. Click **Next** and then **Create.**
n.

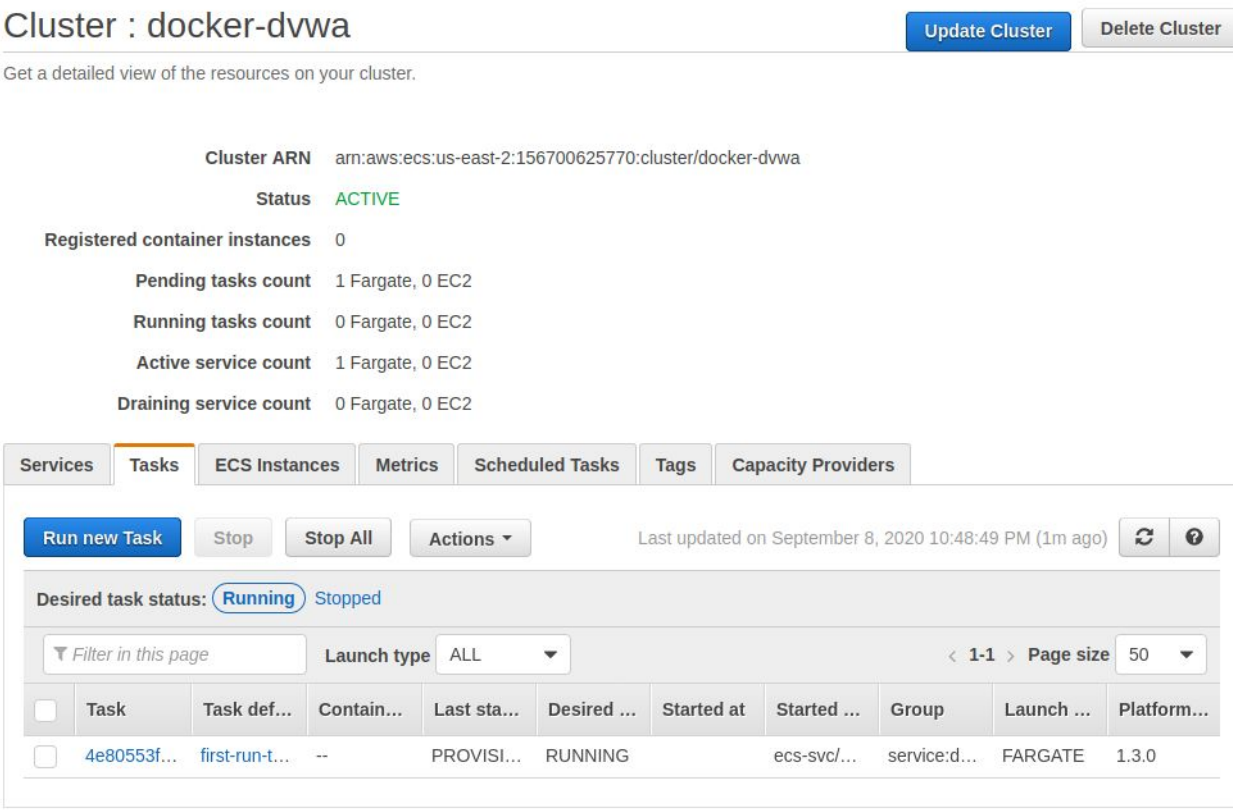


2. Opening the DVWA Application

a. **Click on your Cluster Name** that you just created. (Amazon ECS > Clusters > Cluster-Name)



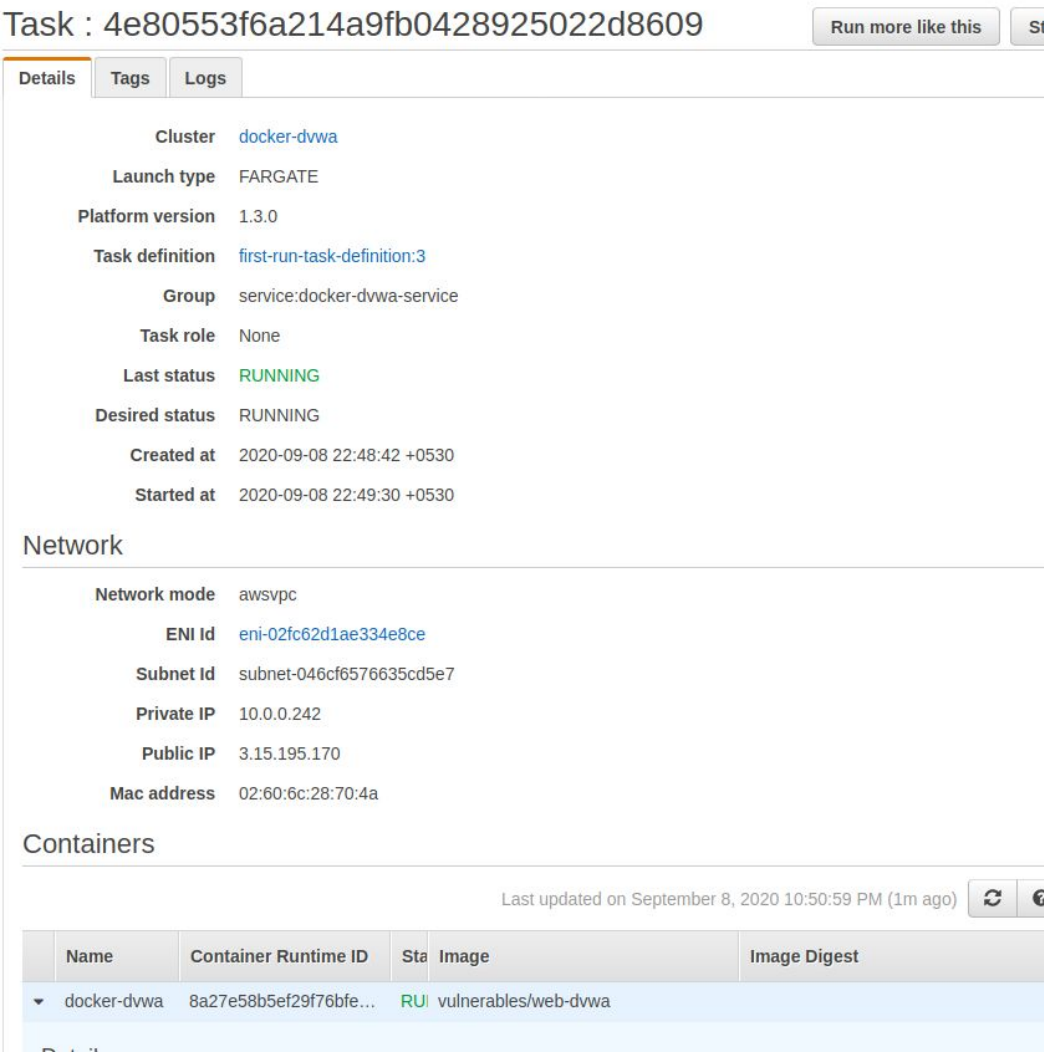
b. **Go to Tasks** tab, and click on the task which should be in RUNNING STATE.



c.

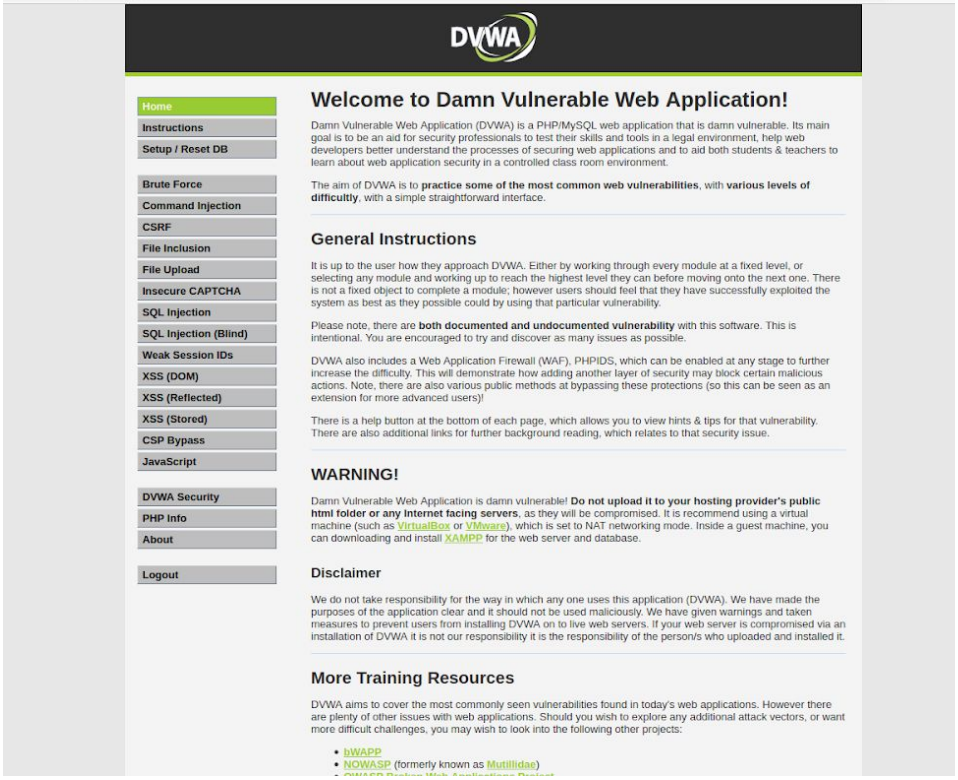
d. Find the **Public IP** mentioned for your application.

e.

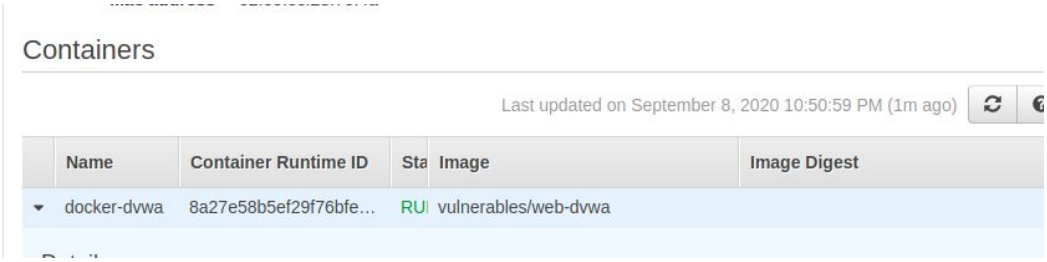


f. Just paste the Public IP, in your Browser url bar.

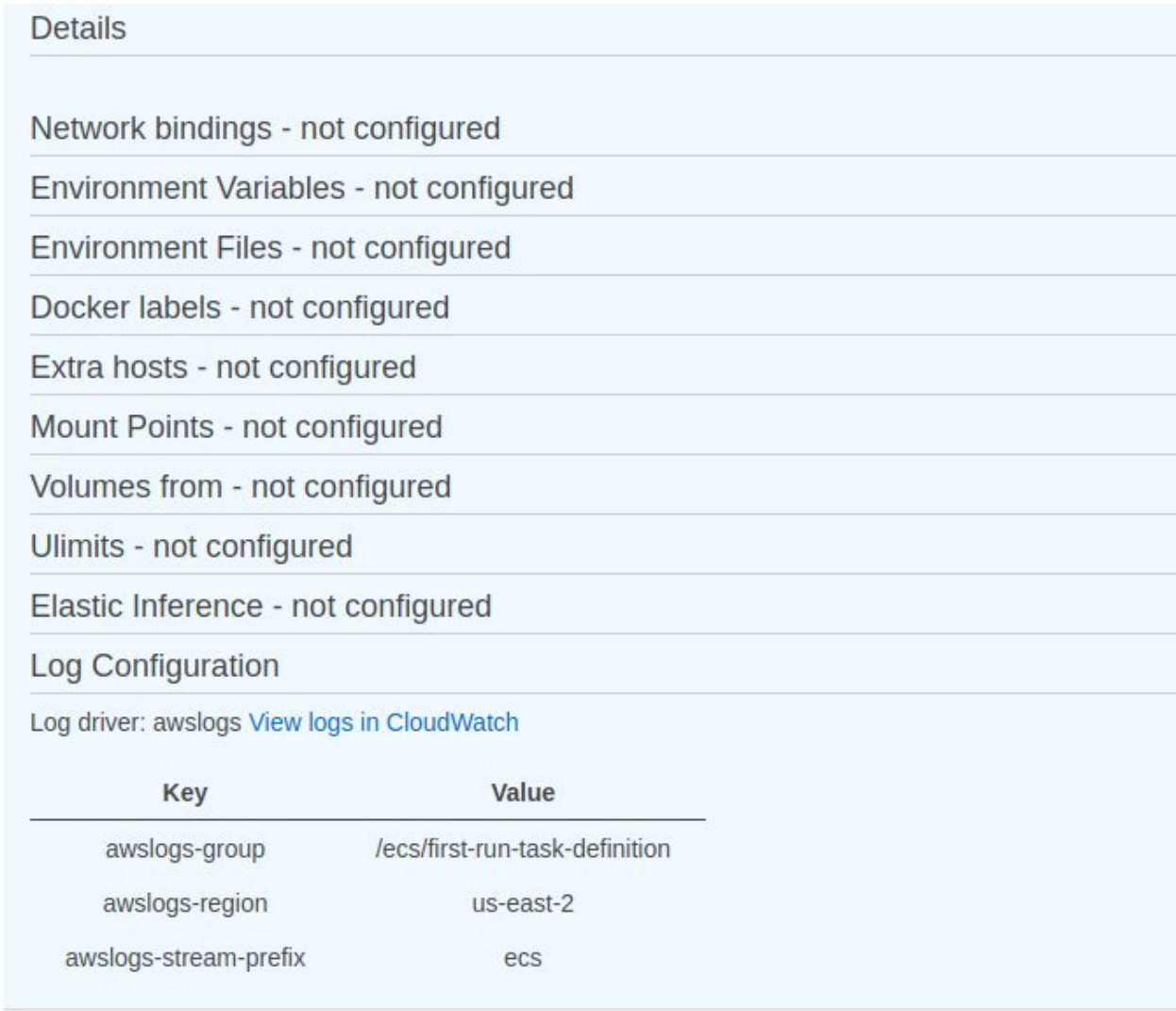
g. You will see a DVWA application.

h. 

i. Go to SQL Injection and do SQLi attacks.

3. Logs Generation
    a. **Click on your Cluster Name** that you just created. (Amazon ECS > Clusters > Cluster-Name)
    b. **Go to Tasks** tab.
    c. 

    d. **Click the arrow** (before the Container Name) to get the details of the container.



e.

f. Click on the **View logs in CloudWatch.**

g. There you will find all the logs of your application.

h.

2020-09-08T20:22:40.225+05:3...	203.81.241.206 - - [08/Sep/2020:14:52:39 +0000] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 200 626 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Li...
2020-09-08T20:22:40.225+05:3...	203.81.241.206 - - [08/Sep/2020:14:52:39 +0000] "GET /dvwa/css/main.css HTTP/1.1" 200 1446 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; ...
2020-09-08T20:22:40.225+05:3...	203.81.241.206 - - [08/Sep/2020:14:52:40 +0000] "GET /dvwa/images/logo.png HTTP/1.1" 200 5330 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_6...
2020-09-08T20:22:40.225+05:3...	203.81.241.206 - - [08/Sep/2020:14:52:40 +0000] "GET /dvwa/images/spanner.png HTTP/1.1" 200 748 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86...
2020-09-08T20:22:43.225+05:3...	203.81.241.206 - - [08/Sep/2020:14:52:43 +0000] "POST /setup.php HTTP/1.1" 302 337 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)...
2020-09-08T20:22:43.225+05:3...	==> /var/log/apache2/error.log <==
2020-09-08T20:22:43.225+05:3...	[Tue Sep 08 14:52:43.075031 2020] [:error] [pid 319] [client 203.81.241.206:65210] PHP Notice: Constant DVWA_WEB_PAGE_TO_ROOT already defined in /var/www/html/dvwa/i...
2020-09-08T20:22:44.225+05:3...	==> /var/log/apache2/access.log <==
2020-09-08T20:22:44.225+05:3...	203.81.241.206 - - [08/Sep/2020:14:52:43 +0000] "GET /setup.php HTTP/1.1" 200 2184 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)...
2020-09-08T20:22:50.226+05:3...	203.81.241.206 - - [08/Sep/2020:14:52:49 +0000] "GET /login.php HTTP/1.1" 200 1048 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)...
2020-09-08T20:23:01.228+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:00 +0000] "POST /login.php HTTP/1.1" 302 337 "http://3.137.140.87/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)...
2020-09-08T20:23:01.228+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:01 +0000] "GET /index.php HTTP/1.1" 200 3037 "http://3.137.140.87/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)...
2020-09-08T20:23:05.228+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:04 +0000] "GET /vulnerabilities/sqli/ HTTP/1.1" 200 1771 "http://3.137.140.87/index.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_...
2020-09-08T20:23:05.228+05:3...	10.0.1.65 - - [08/Sep/2020:14:53:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:05.228+05:3...	10.0.0.53 - - [08/Sep/2020:14:53:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:16.230+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:16 +0000] "GET /vulnerabilities/sqli/?id=%27+or+1%3D1&Submit=Submit HTTP/1.1" 200 503 "http://3.137.140.87/vulnerabilities/sql...
2020-09-08T20:23:23.231+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:22 +0000] "GET /vulnerabilities/sqli/ HTTP/1.1" 200 1772 "http://3.137.140.87/vulnerabilities/sqli/" "Mozilla/5.0 (X11; Ubuntu...
2020-09-08T20:23:26.231+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:26 +0000] "GET /vulnerabilities/view_help.php?id=sqli&security=low HTTP/1.1" 200 1951 "http://3.137.140.87/vulnerabilities/sql...
2020-09-08T20:23:27.232+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:26 +0000] "GET /dvwa/css/help.css HTTP/1.1" 200 522 "http://3.137.140.87/vulnerabilities/view_help.php?id=sqli&security=low" "...
2020-09-08T20:23:35.233+05:3...	10.0.1.65 - - [08/Sep/2020:14:53:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:35.233+05:3...	10.0.0.53 - - [08/Sep/2020:14:53:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:45.234+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:44 +0000] "GET /vulnerabilities/sqli/?id=%3Fid%3Da%27+UNION+SELECT+%22text1%22%2C%22text2%22%3B--+-%26Submit%3DSubmit&Submit=S...
2020-09-08T20:23:57.236+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:57 +0000] "GET /security.php HTTP/1.1" 200 2456 "http://3.137.140.87/vulnerabilities/sqli/?id=%3Fid%3Da%27+UNION+SELECT+%22tex...
2020-09-08T20:23:58.236+05:3...	203.81.241.206 - - [08/Sep/2020:14:53:57 +0000] "GET /dvwa/images/lock.png HTTP/1.1" 200 1045 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x8...
2020-09-08T20:24:01.237+05:3...	203.81.241.206 - - [08/Sep/2020:14:54:00 +0000] "POST /security.php HTTP/1.1" 302 427 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv...
2020-09-08T20:24:01.237+05:3...	203.81.241.206 - - [08/Sep/2020:14:54:01 +0000] "GET /security.php HTTP/1.1" 200 2475 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv...
2020-09-08T20:24:05.237+05:3...	203.81.241.206 - - [08/Sep/2020:14:54:04 +0000] "GET /vulnerabilities/sqli/ HTTP/1.1" 200 1812 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x...
2020-09-08T20:24:05.237+05:3...	10.0.1.65 - - [08/Sep/2020:14:54:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:24:05.237+05:3...	10.0.0.53 - - [08/Sep/2020:14:54:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:24:10.238+05:3...	203.81.241.206 - - [08/Sep/2020:14:54:09 +0000] "POST /vulnerabilities/sqli/ HTTP/1.1" 200 1845 "http://3.137.140.87/vulnerabilities/sqli/" "Mozilla/5.0 (X11; Ubunt...
2020-09-08T20:24:14.239+05:3...	203.81.241.206 - - [08/Sep/2020:14:54:13 +0000] "GET /vulnerabilities/view_help.php?id=sqli&security=medium HTTP/1.1" 200 1951 "http://3.137.140.87/vulnerabilities/...
2020-09-08T20:24:33.242+05:3...	203.81.241.206 - - [08/Sep/2020:14:54:32 +0000] "POST /vulnerabilities/sqli/ HTTP/1.1" 200 1845 "http://3.137.140.87/vulnerabilities/sqli/" "Mozilla/5.0 (X11; Ubunt...
2020-09-08T20:24:35.242+05:3...	10.0.1.65 - - [08/Sep/2020:14:54:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:24:35.242+05:3...	10.0.0.53 - - [08/Sep/2020:14:54:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
	No newer events at this moment. *Auto retry paused.* *Resume*