# Honeypot Login Analyzer on AWS – Project Explanation

This project is a **honeypot web application hosted on AWS** designed to collect, process, and visualize unauthorized login attempts. The goal is to simulate a real login page, record attacker activity, and analyze brute-force attempts in a structured and meaningful way.

http://18.191.248.36/index.html
http://18.191.248.36/report.html
http://18.191.248.36/dataset.csv

## Project Overview

- **Hosting**: The project runs on an Amazon EC2 instance, which provides the web server environment.
- **Webpage**: Attackers interact with a **fake login page** served at the EC2 public IP (e.g., `http://18.191.248.36/index.html`).
- **Logging**: Any credentials entered are captured and logged without giving access to the system.
- **Analysis**: Logs are converted into structured CSV data, which is then used to generate visualizations.
- **Dashboard**: A web-based report (`report.html`) displays attack trends and statistics.

## File Breakdown

1. **`index.html`**
   - The decoy login page attackers see.
   - Collects a username and password when submitted.
2. **`login.py`**
   - A CGI script that handles login submissions.
   - Captures details such as:
     - Timestamp
     - IP address of the attacker
     - Entered username and password
     - User-Agent (browser/device info)
   - Logs each attempt into a text file (`sample_credentials.txt`) or directly into `dataset.csv`.
3. **`sample_credentials.txt`**
   - The raw log file storing all captured login attempts.

    - Each entry includes timestamp, IP, credentials, and user-agent.

4. **`parse_logs.py`**
    - Converts the raw log file into a structured CSV format.
    - The CSV is easier to analyze and contains columns such as:
        - `timestamp, ip, username, password, user_agent`.
5. **`visualize.py`**
    - Reads the CSV dataset and generates charts/graphs.
    - Produces an HTML report (`report.html`) that displays:
        - Failed login attempts over time.
        - Most common usernames used.
        - Most common passwords attempted.
        - IP addresses generating suspicious activity.
6. **`report.html`**
    - A dashboard that can be accessed directly in the browser (e.g., `http://18.191.248.36/report.html`).
    - Shows real-time attack data and graphs.

## Workflow

1. A bot or attacker visits the login page.
2. They enter credentials → `login.py` logs the attempt.
3. The attempt is saved into `sample_credentials.txt` (raw log).
4. Running `parse_logs.py` processes this log into `dataset.csv`.
5. Running `visualize.py` updates `report.html` with graphs.
6. The dashboard can then be viewed in a browser for analysis.

## Key Concepts Learned

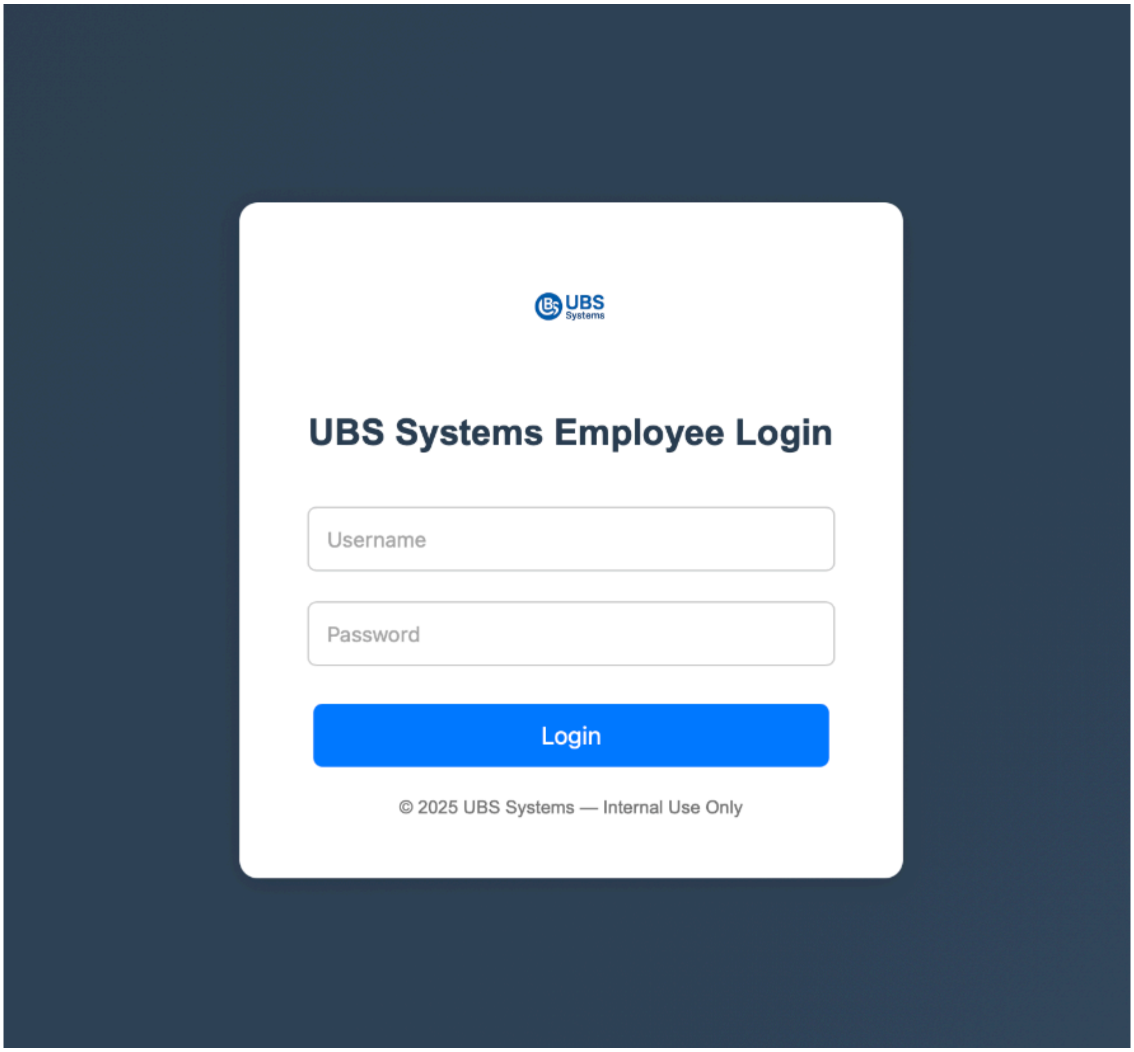
- **AWS EC2**: Hosting a web server in the cloud.
- **Security Concepts**: Understanding brute-force login attempts and how attackers target weak credentials.
- **Python Programming**: Building scripts for logging, parsing, and visualizing data.
- **Data Handling**: Converting logs into structured CSV for analysis.
- **Visualization**: Generating graphs and dashboards to make security data understandable.
- **Web Hosting**: Serving dynamic and static files (`index.html` and `report.html`) via Apache/Nginx on AWS.

## Takeaways

- This honeypot project demonstrates how a simple web page can be used to **attract and monitor attackers**.
- It shows the importance of **logging and analyzing security events**.

## Diagram:

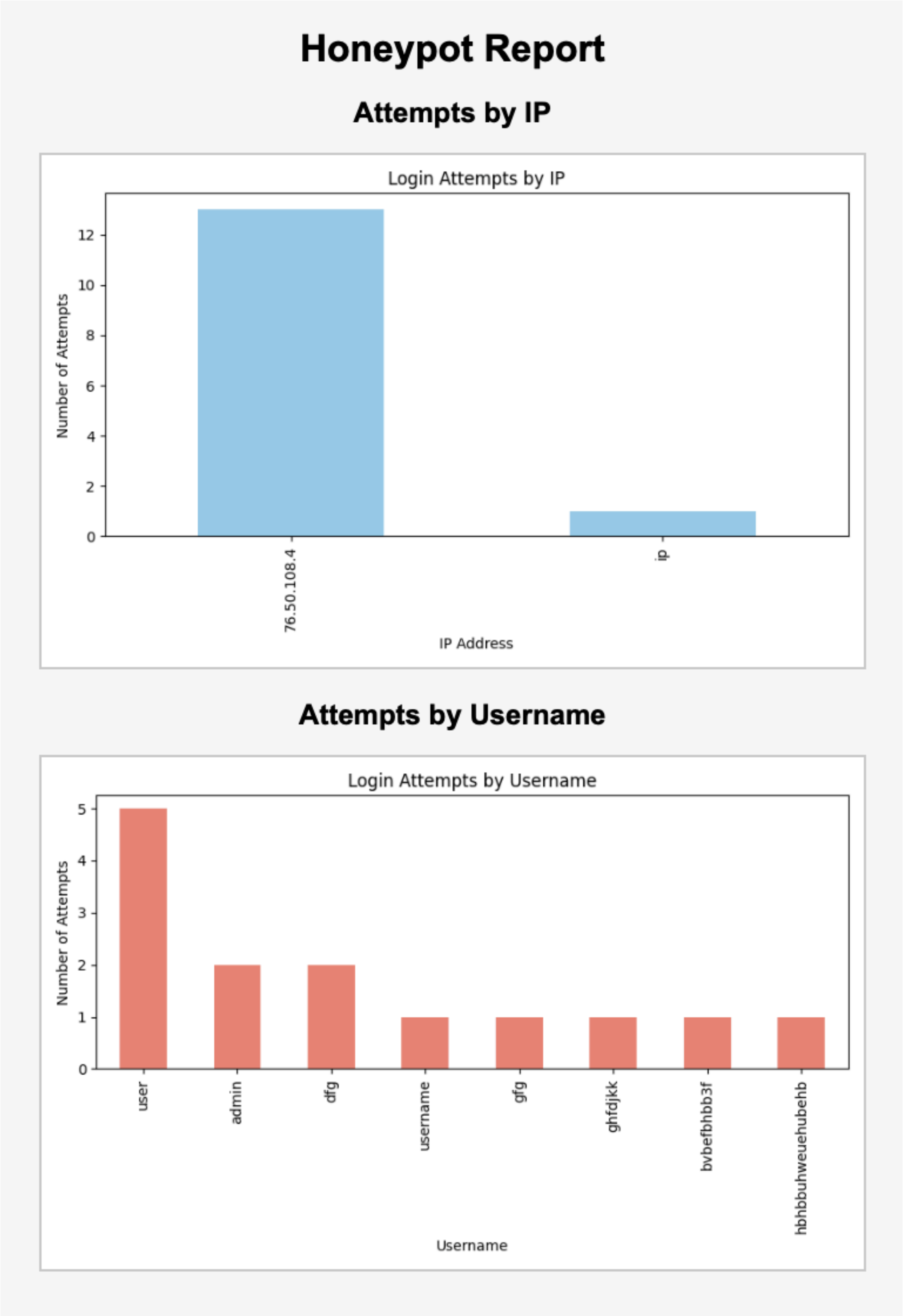
```
[Attacker's Browser]
       |
       ▼
  1. Attacker visits fake login page
     (index.html hosted on Apache)

       |
       ▼
  2. index.html -> sends credentials
     (username, password, etc.)
     ▼
     login.py (CGI script in /usr/lib/cgi-bin)
        - Logs the attempt with timestamp, IP, user-agent
        - Saves data into sample_credentials.txt

       |
       ▼
  3. parse_logs.py
        - Reads sample_credentials.txt
        - Converts log data → structured dataset.csv
        - Format: timestamp, IP, username, password, user-agent

       |
       ▼
  4. visualize.py
        - Reads dataset.csv
        - Creates charts (failed attempts, IP distribution, etc.)
        - Exports report.html with graphs

       |
       ▼
  5. Apache Server
        - Serves both index.html (login page)
        - AND report.html (real-time dashboard)

       |
       ▼
[You / Viewer]
  - Can access http://<EC2-IP>/index.html
    (fake login page)
  - Can access http://<EC2-IP>/report.html
    (dashboard with charts)
```



UBS Systems Employee Login

© 2025 UBS Systems — Internal Use Only

```
timestamp,ip,username,password,user_agent
2025-08-16 21:04:29,76.50.108.4,admin,user123,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-16 21:04:33,76.50.108.4,admin,user123,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-16 21:04:41,76.50.108.4,dfg,hfg,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-16 22:26:18,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-16 22:28:52,76.50.108.4,dfg,hfg,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 01:36:55,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 01:37:31,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 01:46:06,76.50.108.4,gfg,hjfg,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 01:50:40,76.50.108.4,ghfdjkk,ugbduhi23hioh3oihoi,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 01:56:22,76.50.108.4,bvbefbhbb3f,hu3ehfuwbuewj,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 01:59:13,76.50.108.4,hbhbbuhweuehubehb,uheuwbufebuhguh3b,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 01:59:20,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-17 02:08:03,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-19 01:22:30,76.50.108.4,hello,123,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-19 01:26:15,76.50.108.4,admin1234,admin2345,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
2025-08-19 02:17:30,76.50.108.4,user123,admin1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
```



# Honeypot Report

## Attempts by IP

## Attempts by Username

# Example Dataset:

## Timestamp, IP, Username, Password, User_Agent

```
2025-08-16 22:28:52,76.50.108.4,dfg,hfg,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-17 01:36:55,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-17 01:37:31,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-17 01:46:06,76.50.108.4,gfg,hjfg,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/18.6 Safari/605.1.15"

2025-08-17 01:50:40,76.50.108.4,ghfdjkk,ugbduhi23hioh3oihoi,"Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-17 01:56:22,76.50.108.4,bvbefbhbb3f,hu3ehfuwbuewj,"Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-17 01:59:13,76.50.108.4,hbhbbuhweuehubehb,uheuwbufebuhguh3b,"Mozilla/5.0 (Macintosh;
Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-17 01:59:20,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-17 02:08:03,76.50.108.4,user,1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-19 01:22:30,76.50.108.4,hello,123,"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-19 01:26:15,76.50.108.4,admin1234,admin2345,"Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"

2025-08-19 02:17:30,76.50.108.4,user123,admin1234,"Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.6 Safari/605.1.15"
```