

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS E:\secure hitl employee acess>
python src/init db.py
Database initialized
PS E:\secure hitl employee acess> python src/create_user.py
user inserted successfully
PS E:\secure hitl employee acess> python -m streamlit run src/app.py

You can now view your Streamlit app in your browser.

Local URL: http://localhost:8501
Network URL: http://10.16.150.93:8501

Database initialized
```

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS E:\secure hitl employee acess> python -u "e:\secure hitl employee acess\src\test.py"
('emp01', 'employee', 'pass101', 'E001')
('emp02', 'employee', 'pass202', 'E002')
('emp03', 'employee', 'pass303', 'E003')
('emp04', 'employee', 'pass404', 'E004')
('emp05', 'employee', 'pass505', 'E005')
('emp06', 'employee', 'pass606', 'E006')
('emp07', 'employee', 'pass707', 'E007')
('emp08', 'employee', 'pass808', 'E008')
('emp09', 'employee', 'pass909', 'E009')
('emp10', 'employee', 'pass100', 'E010')
('reviewer', 'reviewer', 'review123', None)
('admin', 'admin', 'admin123', None)
PS E:\secure hitl employee acess>
```

 Login

Username

emp01

Password

pass101

Login

User: emp01

Role: employee

Logout



Employee Access Request

Employee ID: E001

Requested Access

Server_Admin

Reason for Access (optional)

Submit Request



Request sent for human review



My Access Requests



Login

Username

reviewer

Password

review123



Login

User: reviewer

Role: reviewer

Logout



Reviewer Dashboard

Request #2 | Employee E001

Department: IT

Role: Engineer

Requested Access: Server_Admin

Tenure: 6 years

Past Violations: 0



Risk Level: HIGH



Model Confidence: 0.82



Risk Factors: High access sensitivity



Approve



Reject

User: emp01

Role: employee

Logout

Submit Request

Request sent for human review

My Access Requests

	Request ID	Requested Access	Risk Level	Status	Reviewed By	Reviewed At	Risk Explanation
0	1	Source_Code_Repo	LOW	APPROVED	SYSTEM	28/01/26 15:25:19	Access aligns with role and experience
1	2	Server_Admin	HIGH	PENDING	None		High access sensitivity

Role: employee

Logout

Reason for Access (optional)

Submit Request

My Access Requests

	Request ID	Requested Access	Risk Level	Status	Reviewed By	Reviewed At	Risk Explanation
0	1	Source_Code_Repo	LOW	APPROVED	SYSTEM	28/01/26 15:25:19	Access aligns with role and experience
1	2	Server_Admin	HIGH	APPROVED	reviewer	28/01/26 15:30:42	High access sensitivity

Login

Username

admin

Password

admin123

Login

User: admin

Role: admin

Logout



Admin Dashboard



All Access Requests

	Request ID	Employee ID	Requested Access	Risk Level	Status	Reviewed By	Reviewed At
0	1	E001	Source_Code_Repo	LOW	APPROVED	SYSTEM	28/01/26 15:25:19
1	2	E001	Server_Admin	HIGH	REJECTED	admin	28/01/26 16:49:43



Override Decision ⇄

Select Request ID to Override

2

Override Selected Request

User: emp01

Role: employee

Logout

Reason for Access (optional)

Submit Request



My Access Requests

	Request ID	Requested Access	Risk Level	Status	Reviewed By	Reviewed At	Risk Explanation
0	1	Source_Code_Repo	LOW	APPROVED	SYSTEM	28/01/26 15:25:19	Access aligns with role and experience
1	2	Server_Admin	HIGH	REJECTED	admin	28/01/26 16:49:43	High access sensitivity