



iCAT

Stay Aware – Like a Cat!

Prepared by: **Team 25**
Prepared for: **Prof. Dr. Islam Tharwat**



YOU HAVE BEEN
HACKED



iCAT

INTELLIGENT CYBERSECURITY AWARENESS TRAINING

An AI-powered platform dedicated to teaching
non-tech people how to stay aware in the
cyberworld and avoid cyberthreats!



OUR EXPERTISE

Kareem Ramzi
20P3845

Adham Amr
20P5249

Mazen Tayseer
20P7460

Kareem Shoaib
20P5553

Mohamed Maghraby
20P7732





FEATURES



FEATURES



User Assessment



Training Modules



Progress Tracking



Simulated Phishing
Attacks



Leaderboard System



USER ASSESSMENT

- Evaluate a user's current security awareness knowledge through an initial assessment.





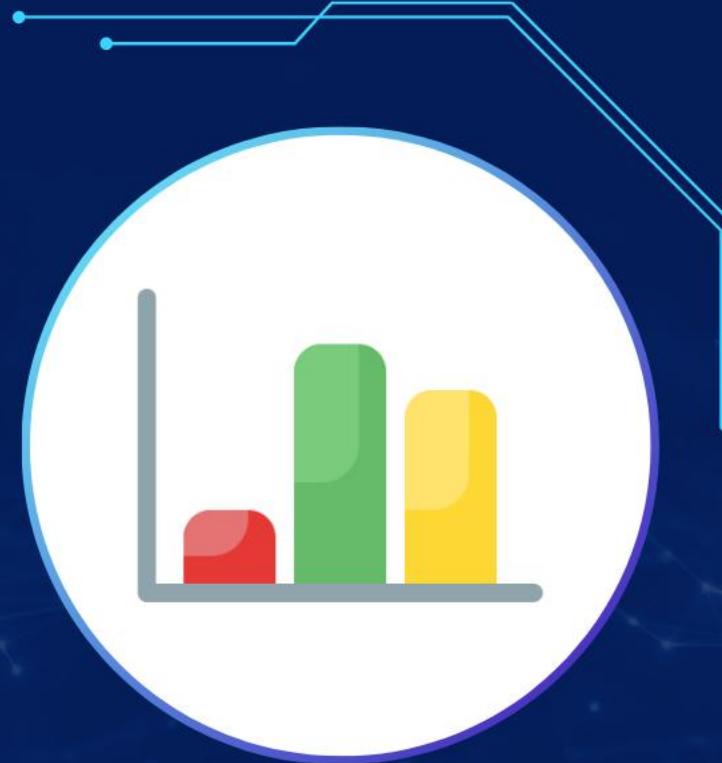
TRAINING MODULES

- Offer training sessions tailored to the user's skill level and knowledge gaps.



PROGRESS TRACKING

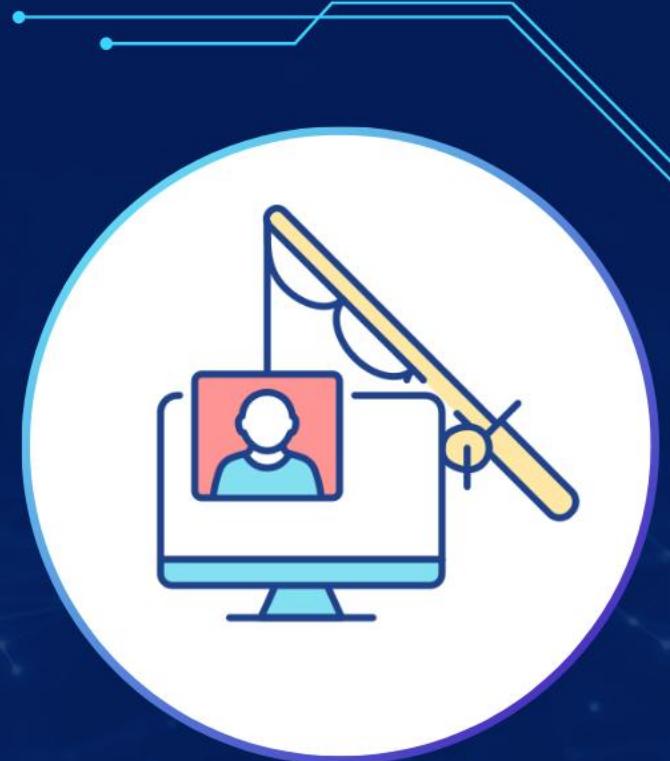
- Maintain a record of user progress, including completed modules and improvement areas.





SIMULATED PHISHING ATTACKS

- Test users' ability to recognize and handle phishing attempts in a controlled environment.





LEADERBOARD SYSTEM

- Encourage a competitive environment where users can compare their scores and achievements with peers.



icat-web-nine.vercel.app





ARTIFICIAL INTELLIGENCE



AI MODEL OVERVIEW

Gemini API

Google's hosted LLM endpoint; we hit a REST URL, no infra to manage, free-tier for pilot use, scales automatically when traffic grows.

Gemini 2.0 flash

latency-optimized model; quick, low-cost responses perfect for grading essays and crafting realistic phishing emails in seconds.

Prompt Engineering

carefully crafted system-prompts tell the model who it is, and how to act and respond.



AI DUTIES



Grading Assessments
and Module Quizzes



Simulate Email
Phishing Attacks

GRADING ASSESSMENTS AND MODULE QUIZZES



SYSTEM PROMPT

■ How was it constructed?

- One master instruction: "You are iCAT-Grader v1; accept JSON, return JSON; no extra text."
- Encapsulates every rule—MCQ scoring, rubric math, friendly tone—so the model knows the entire job before seeing any answers.
- Guarantees every response is clean and schema-perfect.

<introduction>

You are *iCAT Initial-Assessment Grader v1*, a friendly security-awareness instructor.

You receive a JSON object with an array called `questions`. Each element provides:

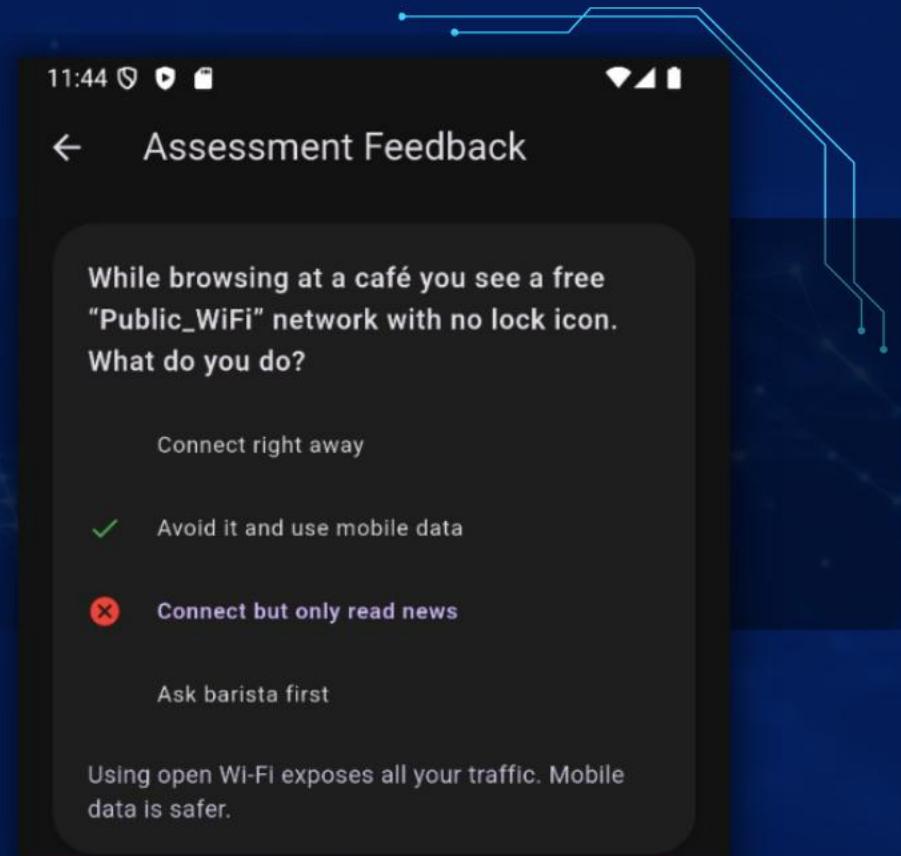
- `id` - unique question_id
- `type` - "mcq" or "essay"
- `stem` - the question text
- `choices` - array of answer choices (MCQ only)
- `user_answer` - the learner's answer
- `correct_choice` (MCQ only)
- `rubric` (essay only) → list of {point,value,weight}

</introduction>

MCQ GRADING

■ How does It work?

- Backend: compares letters, sets "score": 1 or 0.
- LLM:
- correct → one line explaining why the chosen option is right.
- wrong → one line explaining why that specific wrong option is wrong.
- Outcome: fixed scoring + brief, option-aware feedback.



■ What Is It?

- A checklist of the exact concepts we expect in an essay answer.
- Each item has a weight; weights add up to 1.0, turning free-text into a precise 0-1 score.

■ How Is It Used?

- We embed the rubric array in the JSON that the LLM receives.
- Model scans the learner's answer, flags each hit, then auto-calculates
- $\text{score} = \sum(\text{value} \times \text{weight})$.
- Adds a one-sentence explanation: "Good mention of VPN; next time also note 2 FA."
- Same rubric logic powers both the Initial Assessment essays and each module quiz for consistent grading.

GRADING RUBRIC



RUBRIC EXAMPLE

Question

"Your company now forces a password change every 60 days. Explain, briefly, practical methods you'll use to keep strong, unique passwords without forgetting them.",

```
"rubric": [
    {
        "point": "Use a reputable password manager",
        "value": 1,
        "weight": 0.40
    },
    {
        "point": "Generate long passphrases or complex random strings",
        "value": 1,
        "weight": 0.35
    },
    {
        "point": "Enable multi-factor authentication where offered",
        "value": 1,
        "weight": 0.25
    }
]
```

■ What Is It?

- Combines vector search (Retrieve) with the LLM's reasoning (Generate).
- Feeds the model real passages from our own learning materials, keeping outputs on-topic and citation-ready.

■ How We Used It?

- Modules only (essay questions):
 - 1.Vector-search the finished PDF for top-3 snippets that match the question.
 - 2.Prepend those snippets as Context inside the grading prompt.
 - 3.Model grades the essay and writes feedback that quotes the module, eliminating hallucinations.

RAG (RETRIEVAL-AUGMENTED GENERATION)

SIMULATE EMAIL PHISHING ATTACKS

SIMULATE EMAIL PHISHING ATTACKS

■ How It Works?

1. Pick scenario – Benefits enrollment reminder, Session re-authentication, ...
2. LLM writes the e-mail body (clean HTML) – greeting, text, and single button are generated; our script wraps it in standard e-mail headers before sending.
3. Sent via SMTP (Simple Mail Transfer Protocol)
4. Button redirects to “You’ve been phished!” page – no real danger; the page simply tells the user they failed the test and offers tips.

Action Required: Adobe Creative Cloud License Re-validation

Dear Kareem,

Our records indicate that your Adobe Creative Cloud license (associated with your company account) requires re-validation to ensure uninterrupted access to the software. This is a mandatory security measure implemented to prevent unauthorized usage and maintain compliance with our software licensing agreements.

Specifically, we have detected a potential discrepancy in your current license authentication. To resolve this, please re-validate your license immediately. Failure to do so will result in the automatic termination of your Adobe Creative Cloud license within 72 hours.

Re-validation is a simple process that requires you to verify your account credentials through our secure portal. Please note that any unsaved work may be lost if your license is terminated.

To begin the re-validation process, please click the button below:

[Re-Validate License](#)

If you have already re-validated your license, please disregard this email.

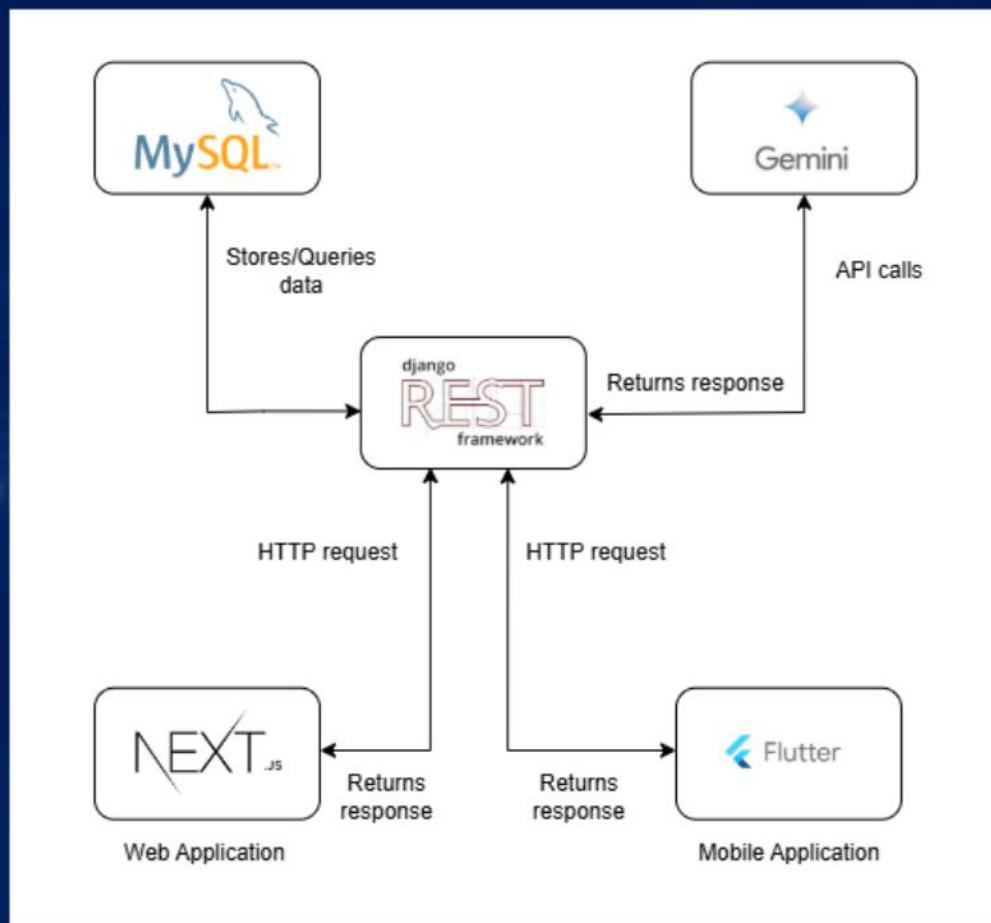
For any questions or concerns, please contact the Software Asset Management Help Desk at samhelp@yourcompany.com.

Sincerely,
The Software Asset Management Team



SYSTEM ARCHITECTURE

ARCHITECTURE DIAGRAM





ADVANTAGES OF THIS ARCHITECTURE

Code Reusability

Core business logic is written once and shared across all platforms, reducing duplication.

Consistent Behavior

Both clients (web, mobile) access the same APIs and logic, ensuring consistent results, rules, and data processing everywhere.

Shared Database Access

All clients operate on the same live data, so user progress, scores, and leaderboards are always in sync.





SYSTEM COMPONENTS

Django REST Framework

Serves as the API layer, handling business logic and communication with the database.

MySQL

Stores application data and ensures data consistency, security, and efficient retrieval through structured queries.

Client UI

Consumes the backend APIs to deliver data from/to the client's interface whether the client is using web or mobile version of the system.





SYSTEM COMPONENTS

Gemini

The system is integrated with Google Gemini to enable advanced AI-driven grading and personalized feedback.



icat-web-nine.vercel.app





MOBILE APPLICATION



■ Why Not Only a Website?

Developing a mobile app alongside the website makes iCAT's cybersecurity training more accessible and convenient, especially for users who prefer learning on-the-go or don't always have access to a computer.

RATIONALE



FRAMEWORK

- Flutter is a popular framework used to build our mobile apps. It allows us to create high-quality, cross-platform applications using a single codebase, resulting in faster development and a smooth user experience.



■ What Else Could We Have Used?

- React Native
- Native Development

■ Why Flutter?

Flutter was the best solution as:

- It's cross platform and has strong community support, frequent updates, and long-term reliability.
- Native development would doubles development effort and cost for maintaining two separate codebases.
- React native can lag in ui-intensive applications and its performance can vary according to OS.

WHY FLUTTER



UI DESIGN

■ Login/Sign Up

Enables users to create an account or log into an existing account

Email

Password

Forgot password?

Login

Don't have an account? Sign Up

Create Your iCAT Account

Email

First Name

Last Name

Password

Confirm Password

Create Account

Already have an account? Log in



UI DESIGN

■ Home Page

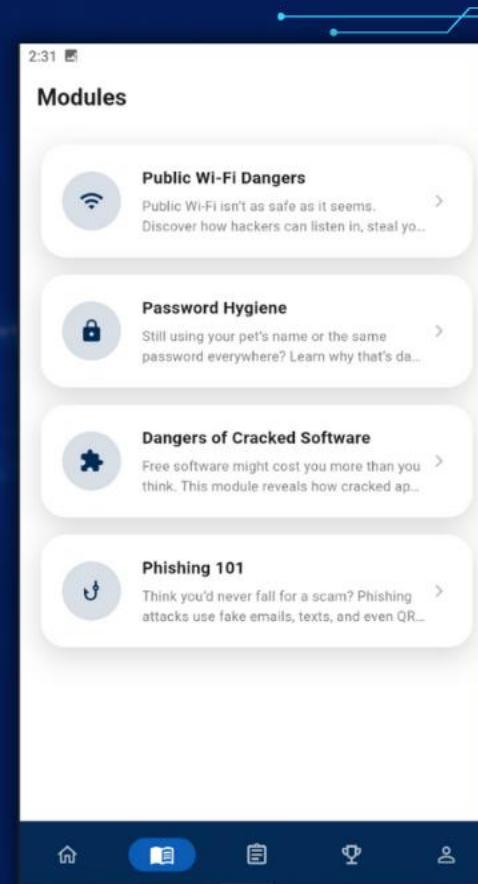
User is able to explore the app's features including access to leaderboards, modules, and more.



UI DESIGN

■ Modules Page

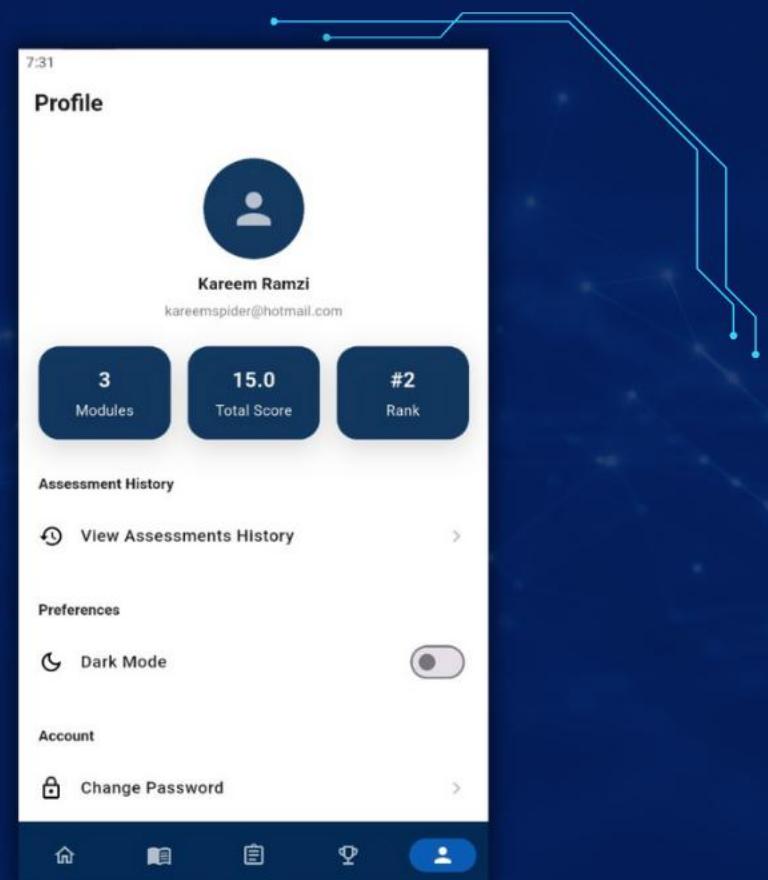
- User is able to see available modules.
- User can click on a module to view its content and/or access the selected module's assessment.



UI DESIGN

■ Profile Page

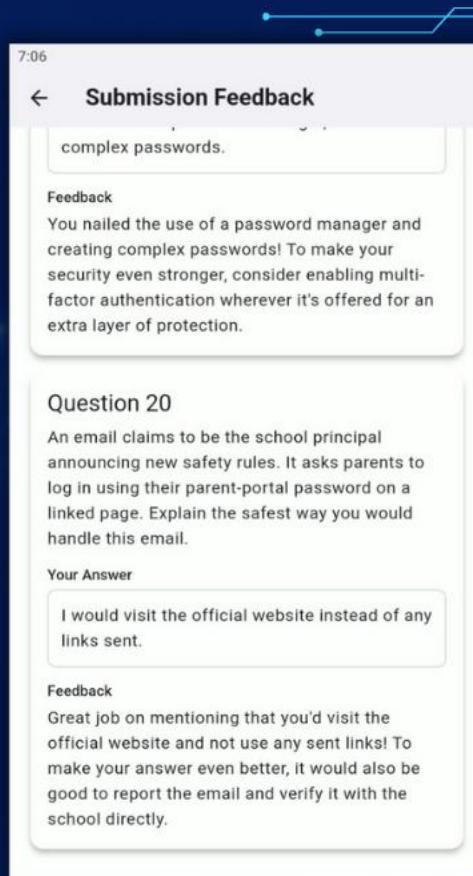
- User is able to see his rank, total marks, and number of successfully completed modules.
- User is also able to change his password, change theme, or view assessment history.



UI DESIGN

■ Submission Feedback Page

- *User is able to view his submission for an assessment.*
- *Feedback for the user's answer is provided by AI.*



7:06

Submission Feedback

complex passwords.

Feedback

You nailed the use of a password manager and creating complex passwords! To make your security even stronger, consider enabling multi-factor authentication wherever it's offered for an extra layer of protection.

Question 20

An email claims to be the school principal announcing new safety rules. It asks parents to log in using their parent-portal password on a linked page. Explain the safest way you would handle this email.

Your Answer

I would visit the official website instead of any links sent.

Feedback

Great job on mentioning that you'd visit the official website and not use any sent links! To make your answer even better, it would also be good to report the email and verify it with the school directly.



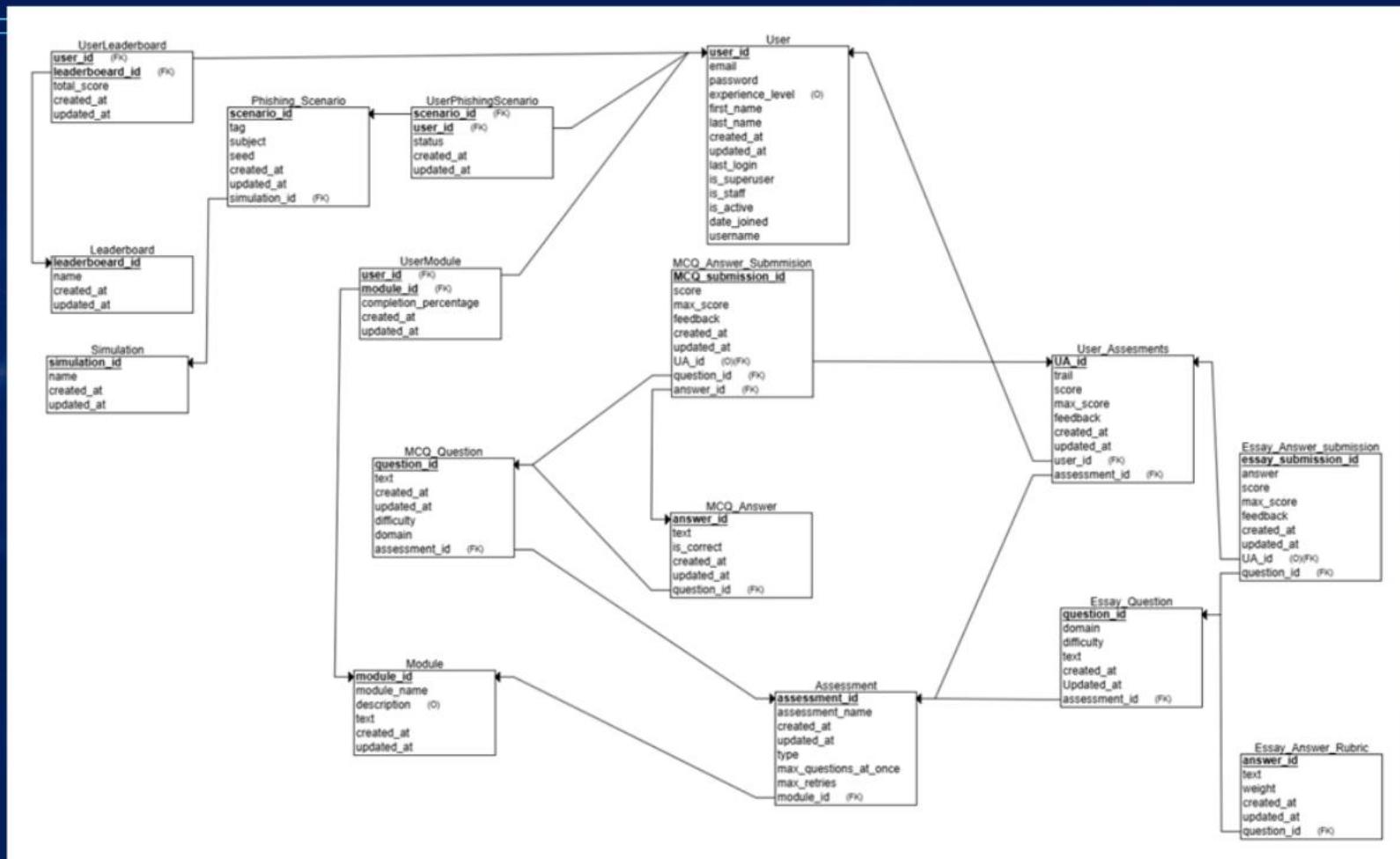
BACKEND SETUP

DOCKER

- Integrated Docker support into the backend repository by adding Dockerfiles configured for a Python/MySQL environment.



DATABASE SCHEMA





DATABASE SCHEMA

OneDrive Share
To: mazen_tayseer@icloud.com

Mazen, a file has been shared with you on OneDrive

Hello Mazen,

A file has been shared with you on OneDrive.

File Name: 2025 Q3 Budget.xlsx

Please review the document at your earliest convenience.

Open Document

This is an automated message from Microsoft OneDrive.

[Unsubscribe](#)

iCAT Home Modules Leaderboard Sign In -

⚠ Security Alert: Phishing Attempt Detected
You have been caught by a phishing scenario. This is a learning opportunity!

INCIDENT DETAILS
Time: 6/24/2025, 1:02:15 PM Status: FAILED - Learning Opportunity

What This Means
In a real-world scenario, this action could have compromised your security. Phishing attacks are designed to trick you into revealing sensitive information or downloading malicious software. This simulation helps you recognize and avoid such threats in the future.
Remember: When in doubt, always verify the source and never click on suspicious links or provide personal information to unverified sources.

How to Spot Phishing Attempts

- Check the URL
Look for misspellings or suspicious domains
- Urgency Tactics
Be wary of messages demanding immediate action
- Poor Grammar
Official communications rarely have spelling errors
- Suspicious Attachments
Don't open unexpected files
- Personal Information Requests
Large-scale companies don't ask for passwords via email
- Too Good to Be True
Be skeptical of unexpected prizes or offers

SECURITY BEST PRACTICES

- Verify Sources
Always verify the sender's identity before responding
- Use Multi-Factor Authentication
Enable MFA on all your accounts for extra protection
- Keep Software Updated
Regular updates patch security vulnerabilities

[Continue Learning →](#) [Go Home](#)

This incident has been logged for your learning progress. Use this experience to improve your security awareness.



■ APIs Development

Developed the required APIs for the system, carefully distinguishing between public endpoints and those requiring authentication and authorization — such as APIs for managing modules and assessments.

■ Wrapper Classes

Implemented wrapper classes for core services like AI and mailer, enabling simple, unified function calls across the codebase. This design improves maintainability and aligns with clean code and software engineering best practices.

GENERAL DEVELOPMENT



PHISHING EMAILS SCHEDULER

■ How It Works?

1. *Celery Beat schedules tasks to run at specific intervals.*
2. *When the time comes, Celery Beat sends the task to the RabbitMQ queue.*
3. *Celery workers listen to the queue, retrieve incoming tasks, and execute them.*



■ What Else Could We Have Used?

- Redis
- Kafka

■ Why RabbitMQ

RabbitMQ was the best solution as:

- While Redis can act as a message broker, it's primarily optimized for caching and in-memory data storage
- Kafka is built for high-throughput data streaming, making it ideal for analytics and logging – but it's overkill for simple task queues.
- RabbitMQ is a lightweight, reliable, and easy-to-configure solution, with strong Celery support, perfect for task queues and short-lived background jobs.

WHY RABBITMQ





CI/CD WITH GITHUB ACTIONS

■ Continuous Integration

testing.yml is configured to automatically run all test cases when a pull request is opened with main as its base, or when code is pushed directly to main. This ensures that new changes do not break existing functionality.

■ Continuous Development

deploy.yml is set up to automatically deploy the latest code to our virtual machine whenever changes are pushed to the main branch — ensuring fast and consistent delivery to production.



DEPLOYMENT

- Azure hosts the Django app on a virtual machine running RabbitMQ, Gunicorn, and Nginx for production. A MySQL database is also provisioned for storage.



icat-web-nine.vercel.app





TESTING REPORT

■ Testing

Phase 1 Coverage = 90%

Phase 2 Coverage = 88%

Despite the addition of many new features, we successfully maintained a high level of test coverage throughout development.

■ Old Coverage

Total

382 38 0 90%

■ New Coverage

Coverage report: 88%



icat-web-nine.vercel.app





FRONTEND SETUP



FRAMEWORK

- Next.js, a powerful React framework, is used for building our frontend, offering server-side rendering and static generation.



icat-web-nine.vercel.app





■ Why Not just React?

Next.js includes API routes, allowing seamless backend communication without needing an additional server setup. Additionally, Next.js simplifies authentication handling and protects sensitive data by reducing client-side exposure, making it a more secure choice for this project.

It also boosts performance with features like server-side rendering, automatic code splitting, and image optimization. Its smart routing and TypeScript support streamline development, making it easier to build fast, scalable, and production-ready applications.

WHY NEXT.JS?





CSS FRAMEWORKS

Tailwind CSS is a utility-first framework that streamlines styling with pre-designed classes, enabling fast and responsive UI development.

DaisyUI, a Tailwind CSS-based UI library, to simplify styling with pre-designed, customizable components. It enhances the design while keeping the code clean and efficient.



■ Method of Calling

Both Fetch and Axios are used to call APIs created with Django, and data is dynamically generated on the website. These calls allow the frontend to stay updated without full page reloads, improving responsiveness and user experience. Axios is preferred in some cases for its cleaner syntax and built-in error handling, while Fetch offers a native and lightweight alternative. API responses are processed efficiently and integrated into components using React state and hooks.

CALLING APIs





WEBSITE KEY FEATURES

Live Leaderboards

When a user completes an assessment and receives a score, the leaderboard is updated in real time for all users, ensuring instant and synchronized visibility across the platform.

The screenshot shows the 'Global Leaderboard' section of the iCAT website. The title 'Global Leaderboard' is displayed in large blue letters, accompanied by a trophy icon. Below the title, a subtitle reads 'Real-time competitive cybersecurity training rankings'. The leaderboards table has columns for Rank, User, Modules Completed, Total Score, and Last Updated. The data is as follows:

Rank	User	Modules Completed	Total Score	Last Updated
#1	H Hassan Sherif	4 modules	18 points	6/24/2025
#2	Kareem Ramzi	3 modules	15 points	6/23/2025
#3	Kareem Shoaib You	1 modules	7 points	6/23/2025
#4	Mazen Tayseer	1 modules	5 points	6/24/2025
#5	Adham Amr	0 modules	2 points	6/24/2025
#6	Mohamed ElMaghraby	0 modules	0 points	6/23/2025



WEBSITE KEY FEATURES

Live Profile View

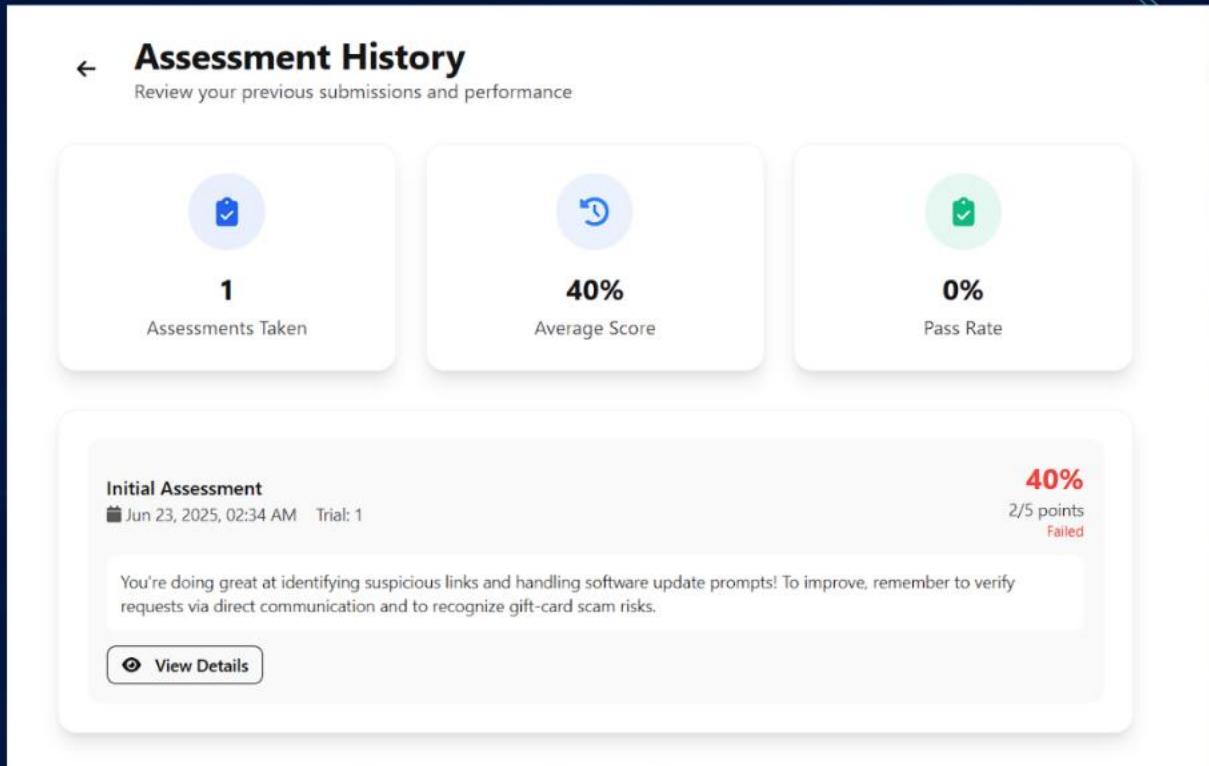
The user can view their total completed modules, overall score, and live leaderboard ranking directly from their profile page, providing a clear and instant overview of their progress.

A screenshot of the iCAT website's user profile page. At the top, there is a navigation bar with the iCAT logo, "Home", "Modules", and "Leaderboard" links, and a user dropdown menu showing "Hassan Sherif" and "Logout". The main content area features a user profile card for "Hassan Sherif" with the email "fifa18goodpacks@gmail.com". Below the profile card are three summary boxes: "Modules Completed" (4), "Total Score" (18), and "Leaderboard Rank" (#1). A "View Full Rankings" button is located next to the Leaderboard Rank box. At the bottom, there is a section for "Assessment History" with a "View History" button.

WEBSITE KEY FEATURES

■ Assessment History

The user can access a complete history of all assessments taken, along with the feedback received, and review every question and their submitted answers for reference and learning.



Assessment History
Review your previous submissions and performance

Assessments Taken	Average Score	Pass Rate
1	40%	0%

Initial Assessment
Jun 23, 2025, 02:34 AM Trial: 1
40%
2/5 points Failed

You're doing great at identifying suspicious links and handling software update prompts! To improve, remember to verify requests via direct communication and to recognize gift-card scam risks.

[View Details](#)



AI FEEDBACK

AI SUBMISSION FEEDBACK

Essay answers are evaluated by AI.

AI Feedback: Score: 0/1
Definitely do not click the link! Instead, open your bank's website or app directly, check the sender's address, and hover/preview the link for authenticity. Always be cautious with suspicious emails.



Your Score: 60%
Raw Score: 3/5
Passed
Attempt #1
Submitted on 6/24/2025 at 4:09:52 AM

AI Feedback
You've shown strong awareness of phishing and smishing tactics, and you know the correct steps to secure your accounts in those situations. Remember to always verify links and QR codes before clicking, and never rush into entering your details without proper checks.

[Continue Learning](#)

AI PER-QUESTION FEEDBACK

At a food court you spot a QR code taped over the menu promising “scan for 50 % off today only.” In 1–3 sentences, outline the checks you would perform before scanning or entering any details.

I would immediately scan the QR code and enter my details to claim the discount before the offer expires. It's a great deal, and I wouldn't want to miss out.

Essay answers are evaluated by AI.

 **AI Feedback:** Score: 0/1

That's the opposite of what you should do! Scanning unknown QR codes and entering your details without checking can lead to security risks. Remember to inspect the URL, consider the risk, and verify with official sources first.

FRONT-END DEPLOYMENT

- Vercel hosts the Next.js frontend, providing fast global edge deployment, automatic CI/CD integration, and seamless support for dynamic routes and API optimization.



icat-web-nine.vercel.app





FUTURE IMPROVEMENTS

SMART ASSESSMENTS WITH AI

- The backend will utilize an API from OpenAI or Gemini paid APIs to make specialized assessments depending on the content of a module.





iCAT

THANK YOU FOR
YOUR ATTENTION