Arvest Bank Cyber Security Tabletop Web Application

Presented By:

Zachary Chapman, Jacob Smith, Matthew Mclendon, Ashwin Prakash, and Rudy Ramirez

Problem

- Cyber security training scenarios require time and experience to create.
- Repetitive scenarios lead to weakening defense teams.
- Generated scenarios risk not simulating real-world conditions.



Objective

- To create a web application to be used to create dynamic cyber security training scenarios.
 - Generate a random scenario from nothing or generate a scenario based off a threat.
 - Store components of scenarios within database.



High-Level Architecture

- The database was created using SQL and MySQL.
- Python was used to build the API.
- The web application manager was built using PHP and CSS.
- The web application will also take care of the security aspects.
- Users will have 2 different roles, manager and employee.





Database Schema

- Threats
- Targets
- Vulnerabilities
- Impact
- Injects
- Scenarios Generated
- Users



User Roles

Manager Role

- Can access the database and make changes by adding and deleting aspects.
- Can do everything that an employee can do.

Employee Role

 Can create scenarios that get saved into their account in order to make sure duplicate scenarios don't get generated

Login

- Manager users can log in and modify the database. They can also update user roles
- Employees can log in and enter the Scenario Generator Page
- Managers & Admin will sign up Employees and other Managers into the system

Arvest Cyber Security Exercise



Username	
Enter Username	

Password Enter Password



Sign-up

- Managers can sign up users or give access to employees to sign up and register a login account.
- It checks for already entered usernames, improper emails, or mismatched passwords.

Arvest Cyber Security Exercise Sign up



Database Modification

- All 5 scenario attributes can be viewed, added, and deleted.
- This is where a manager can add components to the tool to generate more scenarios
- A manager can gain access to the scenario generator through this page.



Scenario Generator

- Generates Scenario based on selected threat
- Scenario Contents:
 - Threat
 - Target
 - Vulnerability
 - Impact
 - Inject
- Current Version allows access to Database Modification Page

Security Scenario Generator

Threat: Making someone think there is something wrong. Offering clean up software. V



Enter Database Modification

Demo Recording



Results & Potential Developments

Results

- Web Application with integrated login system.
- Functional Database Management System
- Generator Page that displays randomized cyber security scenarios

Potential Developments

- Creating Scenarios from random threats.
- Implementing Difficulty Levels when generating exercises.
- Saving generated scenarios into database table for statistical purposes.
- "Gameifying" the tool to incorporate user responses and scoring correct responses.
- Transforming tool into mobile training app.