

## **Learn Ethical Hacking By Solving Real Security Challenges**

**Student Name**  
**Mr.DhavanthRao J,**  
**(M.SC ISCF)**

**Guide Name**  
**Ms.Kanimozhi V,**  
**M.E., (PhD)**  
**Faculty/IT**

# Problem Statement

- It can be difficult for any teacher to **introduce Security concepts** to students who have little or no technical expertise.
- **Gamification** is a term that has lately been used to describe a **strategy for motivating students** that involves incorporating various **game-based strategies into instructional modules**.
- This idea has led to the discovery that **capture the flag (CTF)-style** competitions are an effective approach to introduce students to a number of technical ideas within the **traditional Cyber Security curriculum**.
- A CTF was conducted at numerous Cyber camps across the nation with the **main objective of educating high school students** to **various computer security** and **digital forensics issues** without necessitating any prior knowledge on the part of the students.
- I discovered that this approach of breaking things down into **discrete problems** and linking these difficulties together in a competitive setting was **remarkably successful** at not just introducing kids to these concepts but also inspire students to **learn security concepts very enthusiastically**.

# Literature Review

Year	Title	Objective	Existing	Future Enhancement
2015	Randomized virtualized scenarios	Computer security students benefit from having hands-on experience with hacking tools.	Further vulnerability definitions not developed.	Developing with all new vulnerabilities according to owasp top 10 vulnerabilities.
2016	A CTF-Based Approach in Information Security Education	A CTF-based educational framework that allows students to gain more practical skills	Static challenges.	Implementing the latest vulnerabilities.

# Literature Review

Year	Title	Objective	Existing	Future Enhancement
2017	A Framework for Generating Randomly Vulnerable Rich-scenario VMs	Generating random vulnerable machine.	Only has few random scenarios and consumes more ram, not compatible for old personal computers.	Enhancing the complexity of the scenarios and hints generation in web application.
2019	VulnerVAN: A Vulnerable Network Generation Tool	Generating random vulnerable networks for practice ethical hacking.	Only has few random scenarios which has no hints on how to solve the hack when we stuck in-between.	Enhancing the complexity of the network defence according our new security protocols.

# Literature Review

Year	Title	Objective	Existing	Future Enhancement
2019	Hackerbot: Attacker Chatbots for Randomised and Interactive Security Labs, Using SecGen.	Hackerbot teaches computer security students interact with a malicious attacker Chatbot.	Remote access via VPN often dropped connections(leading to the introduction of RDP as an alternative).	Providing the uninterrupted service.
2021	Automatic Generation of Randomized Cyber Range Scenarios	The cyber range used in information security exercises is a system that allows students to learn knowledge and skills efficiently	Consumes more space and takes more time to generate the scenario.	enriching the random scenarios, applying to online exercise and testing their educational effectiveness.

# Existing system

- **TryHackMe** is a free online platform for learning cyber security, **using hands-on exercises** and labs, **all through your browser**.
- **PICOCTF** is a free computer security education program with original content built on a **capture-the-flag framework** created by security and privacy experts.
- **CTFd** is a Capture The Flag (CTF) framework designed for ease of use for both administrators and users.

# Project Goals

- **Capture the Flag (CTF)** is a very interesting way to learn **Ethical Hacking** very **Enthusiastically**.
- The **project goal** is to create a **web application** for the **universities or schools** which contains the **security challenges**.
- **Security challenges** helps students to **learn ethical hacking** and **cyber forensics** in a **very interesting way**.
- Compacting everything inside a web helps students access the challenges very easily. They **only need a browser** with a internet connection.
- They can access this web application from their campus computer lab itself.

# Algorithms and highlights of the Proposed System

- **Docker:** It is an open platform for developing, shipping, and running your applications separate from your infrastructure.
- **Container:** A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.
- **Parameterisation:** all of the elements should be able to be configured (for example, the ports services should use, strength of passwords, theme of the scenario), and this configuration will be randomizable.



# Summaries the Ultimate Findings of the Project

- **Capture the flag (CTF)** is a type of cyber security game which involves **collecting flags** by **solving security challenges**.
- By this **teaching cyber security** concepts to **students** is **very simplified**.
- **Gamification** is the key to learn **new things** very **quickly and easy**.
- Students love these types of **Hands-on-classes** rather than a **boring theory class**.

# Explanation of Code

- **There is mainly three part in source code:**

- Source code
- Dockerfile
- Shell script

- **Source code:**

```
include_once "includes/encrypt.php";
$username = $_POST["username"];
$password = $_POST["password"];
$error = "";
if(isset($username) && isset($password)) {
    if($username != "" && $password != "") {
```

# Explanation of Code

- **Source code:**

- `if ctype_alnum($username) && ctype_alnum($password)) {`
- `setcookie("ID", encrypt($username, $password));`
- `}`
- `else {`
- `$error="alpha_num";`
- `}`
- `}`
- `else {`
- `$error="empty_params";`
- `}`

# Explanation of Code

## Dockerfile:

- FROM tutum/apache-php
- RUN apt-get update && apt-get upgrade -y
- RUN apt-get install -y libapache2-mod-php5 php5-mysql

## Shell script:

### To Start:

- docker-compose build
- docker-compose up -d

### To Stop:

- docker-compose down

# Publication Details

## **Journal / Conference Name:**

IEEE PRESS, WILEY : Digital Twins in industrial Production and Smart Manufacturing: An Understanding of Principles, Enhancers and Obstacles.