Simulating Cyber-Attacks:

A Practical Exploration of Vulnerabilities and Defenses in Web Security

Abstract

This project explores how simulated cyber-attacks can help identify vulnerabilities in poorly secured web applications and test the effectiveness of common defenses. Using a Django-based web app, I developed two contrasting versions: one with intentional security flaws, and one incorporating key security best practices. Through this, I demonstrate how attackers exploit weak spots and how better security design can prevent breaches

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks. These attacks often aim to access, change, or destroy sensitive information or disrupt services. Common threats include phishing, malware, SQL injection, and brute-force attacks.

Questions

- **How can attackers exploit insecure websites, and how can better coding practices stop them?**
- Approach:
  - I built two sites—one intentionally insecure, one secured with Django features like CSRF protection and input validation—and tested common web attacks.
- Findings:
  - Attacks like SQL injection and brute-force worked on the insecure site but failed on the secured one. Simple security measures made a big difference.

Kai Francis
Advised by Dr. Heather Guarnera

Real Hackers & Groups

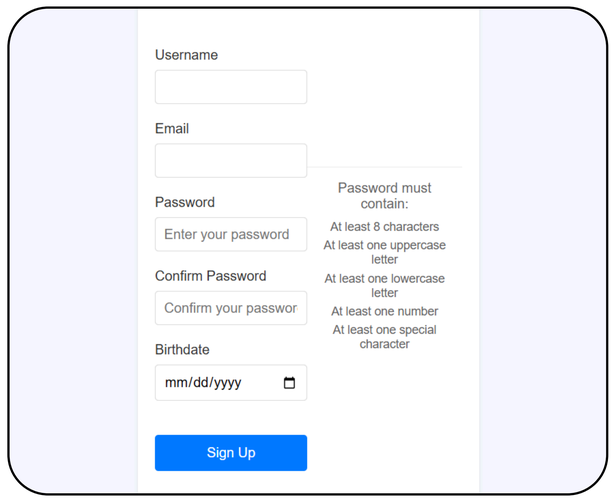
Gary McKinnon
McKinnon accessed U.S. military and NASA systems in search of UFO evidence, exploiting weak passwords and poor system security

Kevin Mitnick
One of the most infamous hackers in history, Mitnick used social engineering and software exploits to breach networks like Motorola and Nokia.

The Legion of Doom
An elite hacking group from the 1980s–90s known for exploiting early phone and computer networks. They shaped hacker culture and inspired future generations of cyber activists.

Photos

Website sign up



Results

- Simulated brute-force attacks were successful on the insecure site.
- SQL injection exposed admin credentials.
- All simulated attacks failed on the secured version.
- Feedback from peers showed increased trust in the secure version's layout and messaging.

Future Works

- Expand simulated attacks to include phishing scenarios.
- Add encryption and 2FA features to the secure site.
- Develop a teaching module based on this simulation for beginner cybersecurity learners.
- Host site with real-time vulnerability scanner demo.