YOUSSEF KANDEEL

+201066276067 | youssefkandeel16@gmail.com | linkedin.com/in/youssef-kandeel-12a508263/ | GitHub

EDUCATION & CERTIFICATES

- Arab Academy for Science, Technology and Maritime Transport
  College of Computing and Information Technology
  Major in Cybersecurity (AASTMT) GPA: 3.4 — September 2022–June 2026
- eJPT v1 Prep From Netriders Academy — September 2024
- Security+ From Netriders Academy — February 2025
- CYBERSECURITY L1 | Google Cybersecurity From Google — August 2024
- Jr Penetration Tester From TryHackMe — June 2024–July 2024

PROJECTS & RELEVENT EXPERIENCE

Juice-Shop (SQL-injection) May 2024

- Gained access to the **admin** account using the SQL injection payload ' or 1=1 -- to bypass login authentication.
- Discovered SQL injection vulnerability in the search functionality using the payload '))--.
- Identified susceptibility to union select attacks, enabling further database queries.
- Exploited SQLite's sqlite_schema table to access the database schema, including table definitions, indexes, and triggers.
- Refined union select query ')) UNION SELECT '1', '2', '3', '4', '5', '6', '7', '8', '9' FROM sqlite_schema--) to match the column count of the product table, retrieving key database structure details.
- Developed a Python script to fetch hashed passwords from the database via an API and format the output into a text file compatible with **John the Ripper** for brute-force cracking attempts.
- Tools used in the Attack (Burp suite, John the Ripper, python scripting)

Juice-Shop (XSS and CSRF Attack)

- Identified the victim's account before any attack, with no alterations made to the profile.
- Crafted an XSS attack that triggers a CSRF exploit to manipulate the victim's profile.
- Uploaded a product titled "Click Me 9," which contained a malicious payload to execute the attack when clicked by the victim.
- XSS and CSRF payload allowed the following actions
  - Changed the victim's username to "HACKED" via a POST request to /profile.
  - Updated the victim's profile image by sending a POST request to /profile/image/url, using a URL of a selected image.
  - Altered the victim's password by sending a GET request to /rest/user/change-password?new=hacked&repeat=hacked, utilizing the victim's authentication token stored in localStorage.
- When the victim clicked on the "Click Me 9" product, the **attack was triggered**, successfully changing the username, profile image, and password, confirming the exploit's effectiveness.
- Tools used in the Attack (Burp suite, Postman)

CTF player (TryHackMe)

- Solved exactly 40 CTF rooms, gaining hands-on experience in various security challenges.
- Developed expertise in Linux privilege escalation techniques, including SUID, GUID, scheduled tasks & cron jobs, kernel exploits, hunting for SSH keys, and sudo privilege escalation.
- TryHackMe Account