

Hacking Websites

Objectives:

The primary goals include understanding potential weaknesses in web systems, assessing the impact of these vulnerabilities, and providing recommendations for mitigation. By conducting controlled security assessments, the project aims to contribute to the broader objective of enhancing website security and safeguarding user data.

Methodology:

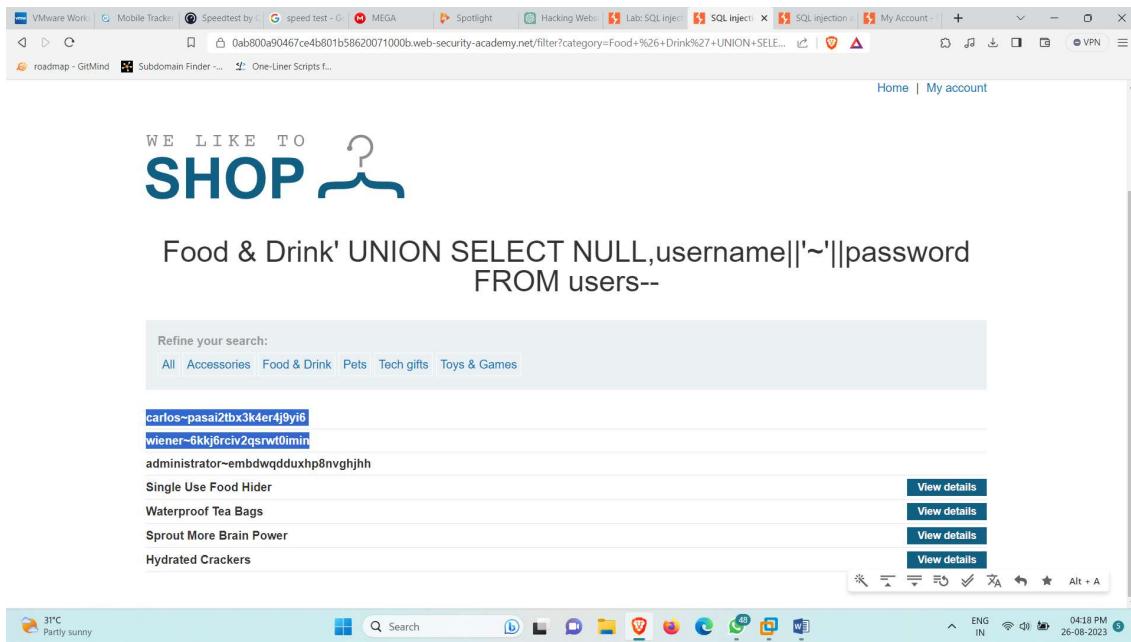
1. Script Kiddies
 - Keylogger
 - Phishing
2. Offensive Hacking
 - Kali Linux
 - Scripting

Tools:

- SQL Injection attack

Proof of concept (POC):

The screenshot shows a browser window with multiple tabs open. The active tab displays a proof-of-concept (POC) for a SQL injection vulnerability on a website called "Web Academy". The URL in the address bar is <https://0ab800a90467ce4b801b58620071000b.web-security-academy.net/filter?category=Food+%26+Drink>. The page content shows a search bar with the query "Food & Drink" and a dropdown menu with options like "Waterproof Tea Bags", "Single Use Food Hider", "Hydrated Crackers", and "Sprout More Brain Power". To the right of each item is a "View details" button. At the bottom of the page, there is a navigation bar with links for "Home" and "My account", along with system status indicators for battery level, signal strength, and date/time (04:18 PM, 26-08-2023).



Conclusion:

In summary, ethical hacking stands as a proactive defense strategy. By identifying vulnerabilities, evaluating risks, and fortifying web systems, it safeguards data, maintains trust, and fosters cybersecurity awareness. Adhering to legal and ethical guidelines, ethical hacking contributes to a secure digital landscape and a culture of protection.