Assignment – 1

AI for Cyber Security

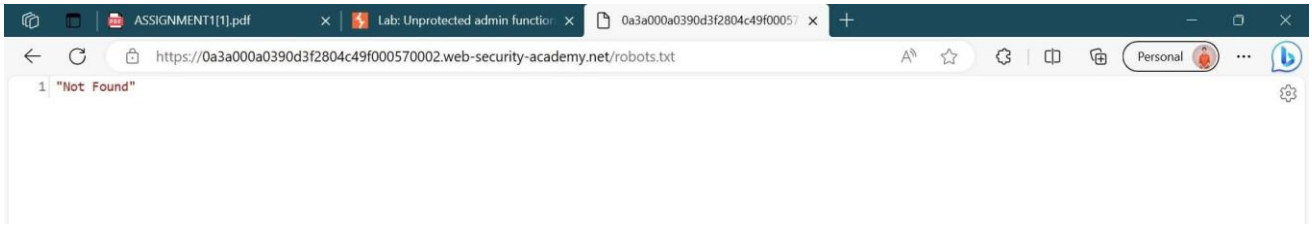
Name: P. Monish

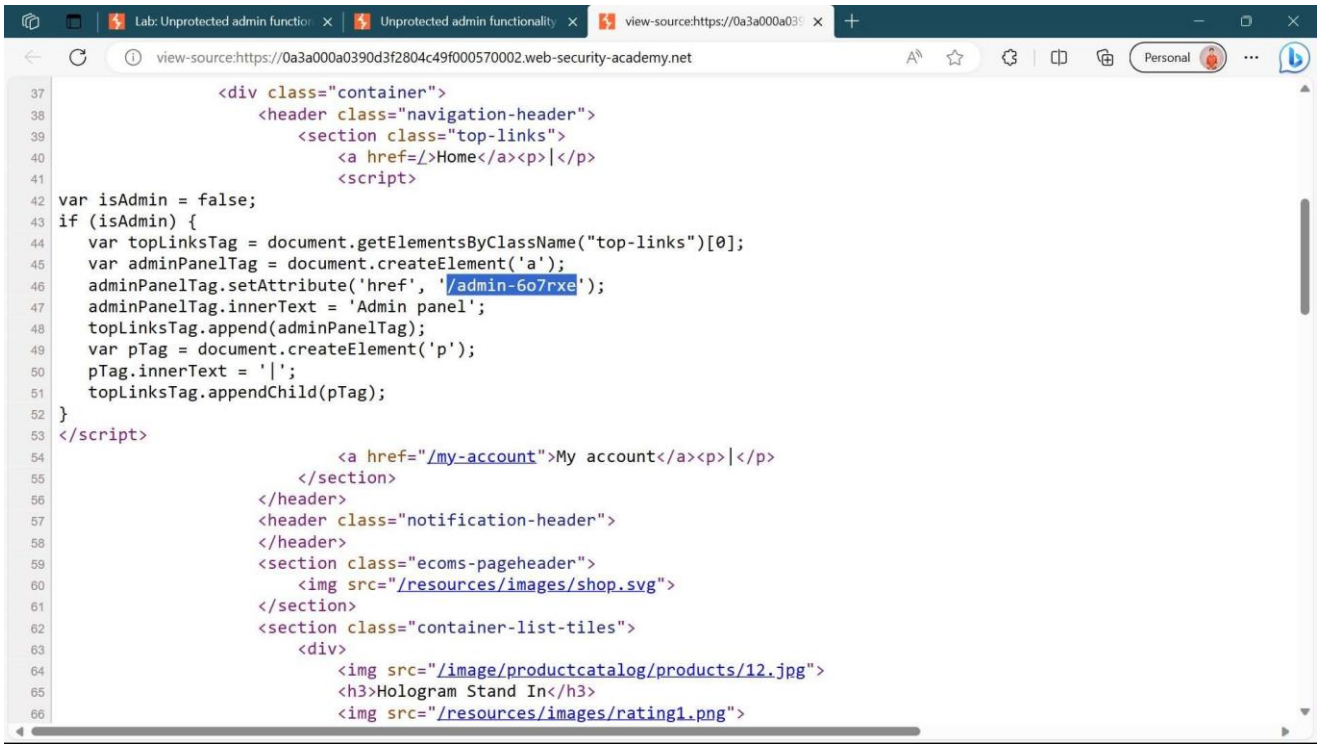
Reg No: 21BCE9517

List of Vulnerable Parameter

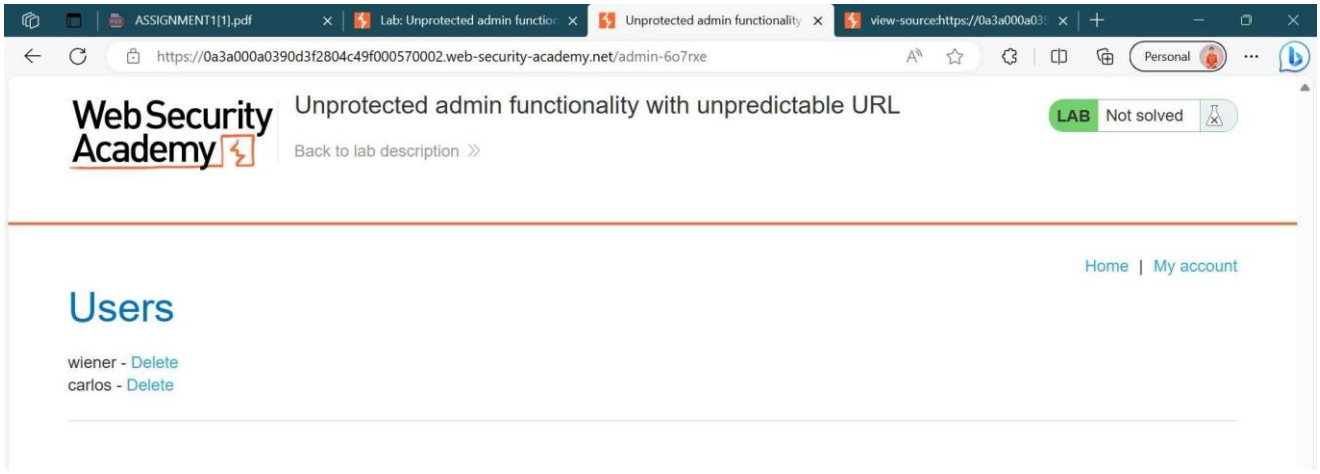
1. **OWASP CATEGORY: A01 2021 Broken Access Control**
   CWE-284: Improper Access Control

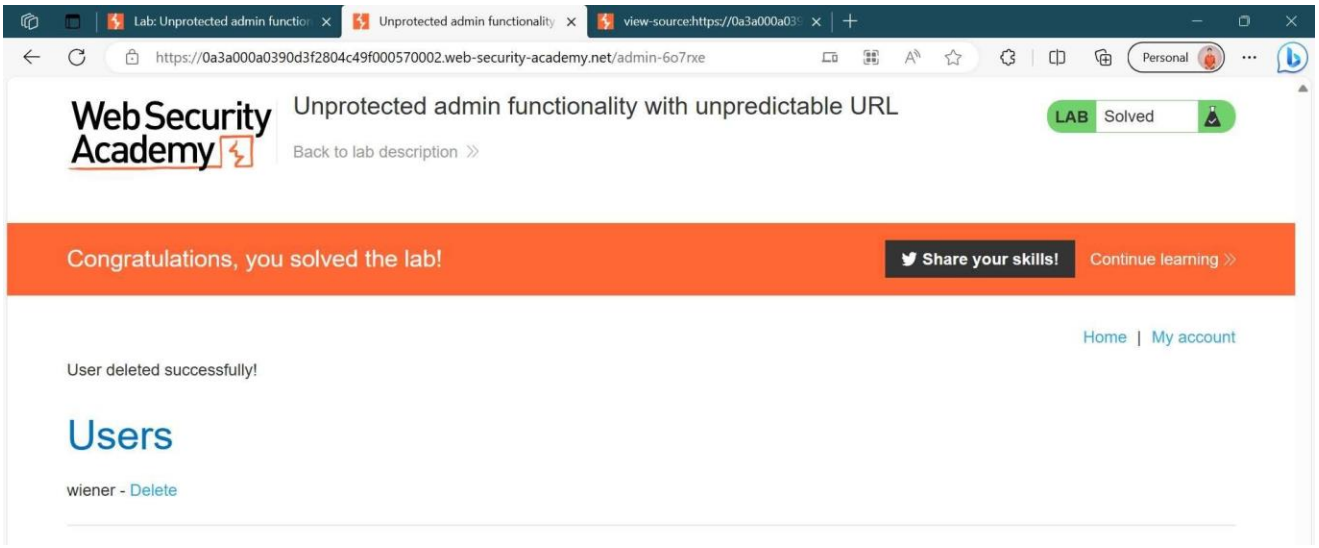
Solving the Lab:






```
                <div class="container">
                    <header class="navigation-header">
                        <section class="top-links">
                            <a href=/>Home</a><p>|</p>
                            <script>
var isAdmin = false;
if (isAdmin) {
   var topLinksTag = document.getElementsByClassName("top-links")[0];
   var adminPanelTag = document.createElement('a');
   adminPanelTag.setAttribute('href', '/admin-6o7rxe');
   adminPanelTag.innerText = 'Admin panel';
   topLinksTag.append(adminPanelTag);
   var pTag = document.createElement('p');
   pTag.innerText = '|';
   topLinksTag.appendChild(pTag);
}
</script>
                            <a href="/my-account">My account</a><p>|</p>
                        </section>
                    </header>
                    <header class="notification-header">
                    </header>
                    <section class="ecoms-pageheader">
                        <img src="/resources/images/shop.svg">
                    </section>
                    <section class="container-list-tiles">
                        <div>
                            <img src="/image/productcatalog/products/12.jpg">
                            <h3>Hologram Stand In</h3>
                            <img src="/resources/images/rating1.png">
```





Description:

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

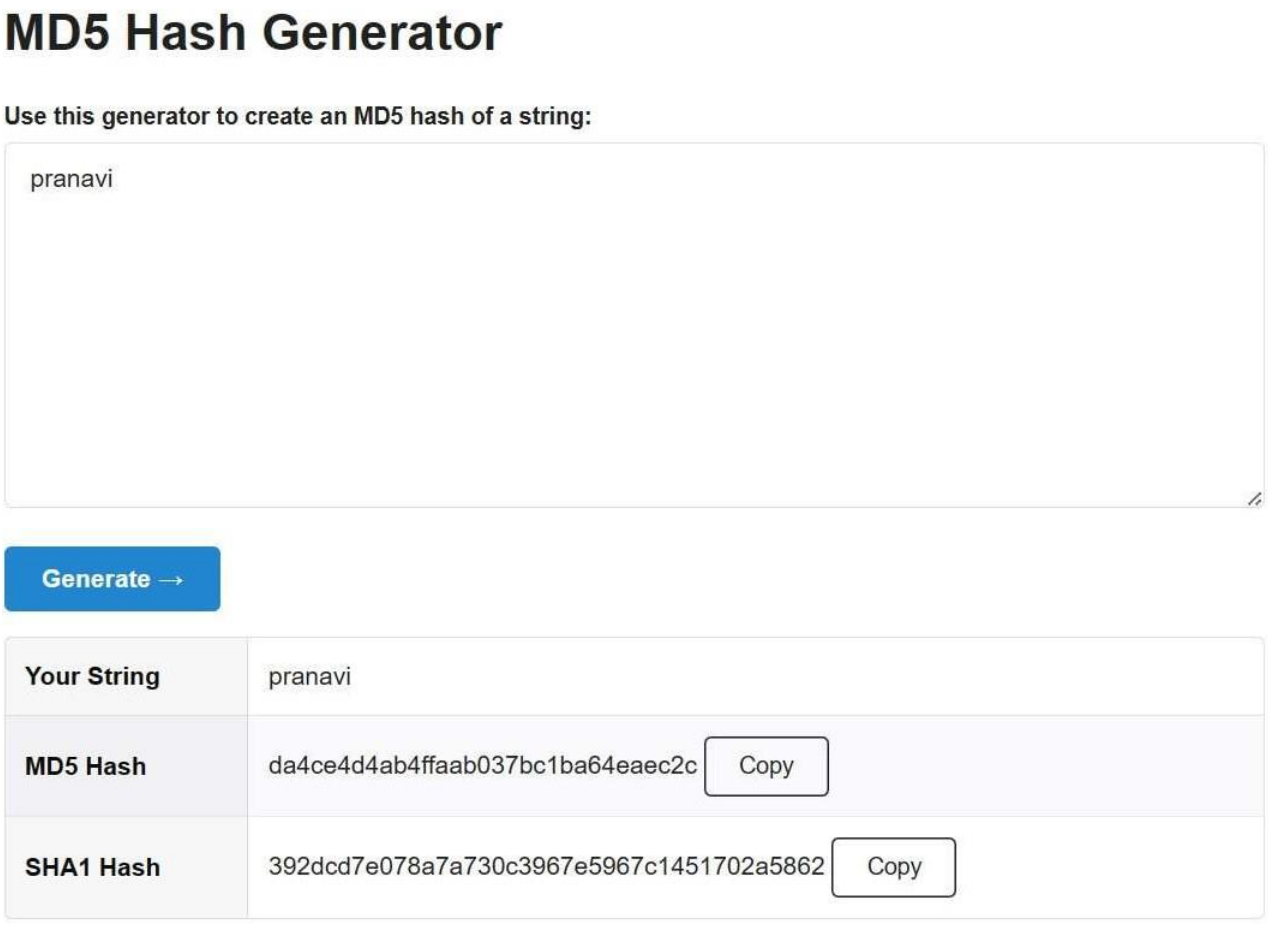
Business Impact:

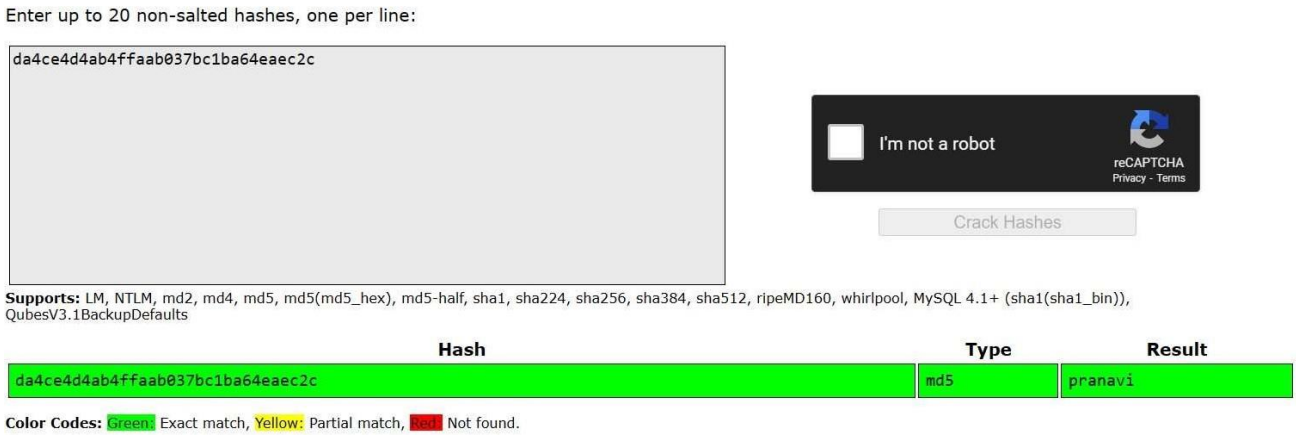
"Improper Access Control," represents a significant threat to businesses. This vulnerability arises when systems fail to enforce proper restrictions on user access to resources. Exploiting this flaw can lead to unauthorized data exposure, alterations, or even complete system compromise. Business consequences include breaches of sensitive information, loss of intellectual property, regulatory penalties, legal actions, erosion of customer trust, and reputational damage. Additionally, addressing this issue demands substantial investments in code review, security architecture, and access management solutions, diverting resources

from core business activities and hindering innovation while striving to ensure robust access controls.

In the above experiment we have clearly seen that we have gained access to the admin panel by just seeing the java script code and using the URL we can be able to gain unauthorized access and deleted the user.

2. **OWASP CATEGORY: A02 2021 Cryptographic Failures**
   CWE-259: Use of Hard-coded Password





Description:

The product contains a hard-coded password, which it uses for its own inbound authentication or for outbound communication to external components.

Business Impact:

"Use of Hard-coded Password," poses a substantial business risk by embedding passwords directly into code or configuration files. This practice can lead to unauthorized access, data breaches, and compromised systems. If exploited, attackers can gain control over critical assets, manipulate sensitive data, disrupt operations, and compromise customer trust. Business impact includes financial losses due to data loss or theft, regulatory fines for noncompliance, legal liabilities, reputational damage, and operational downtime. Mitigation efforts require resources for code review, password management, and system updates, impacting development timelines and diverting focus from innovation to security remediation.

In the above experiment we have cracked the password by using md5 hash of that password. This comes under one of the cryptographic failure.

3. OWASP CATEGORY: A03 2021 Injection
CWE-564: SQL Injection: Hibernate

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

APPRENTICE

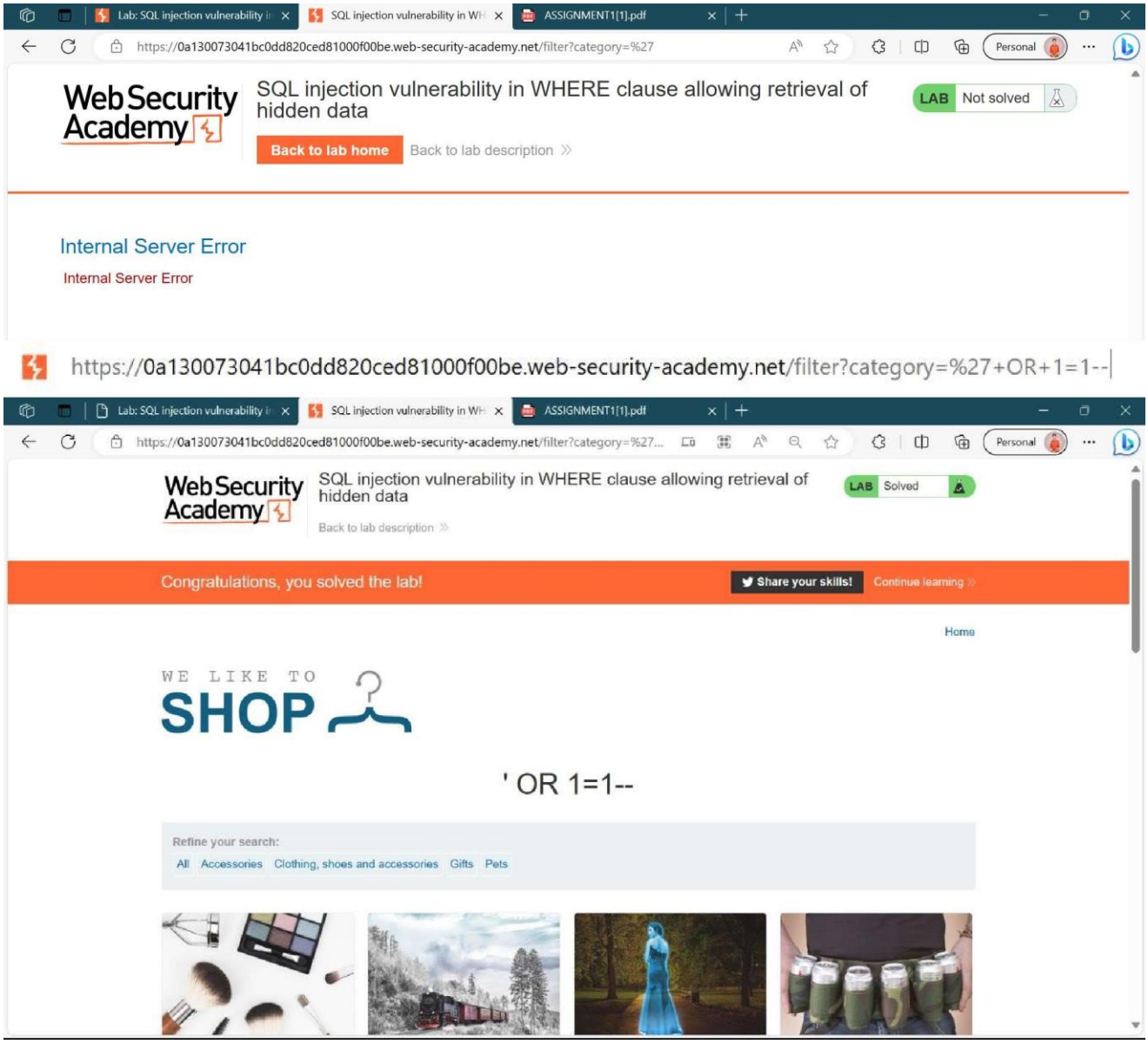
LAB ✓ Solved

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND rel
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

Solving the Lab:



SELECT * FROM Products WHERE category = ‘ ‘ OR 1 = 1 - - ’ Description:

Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

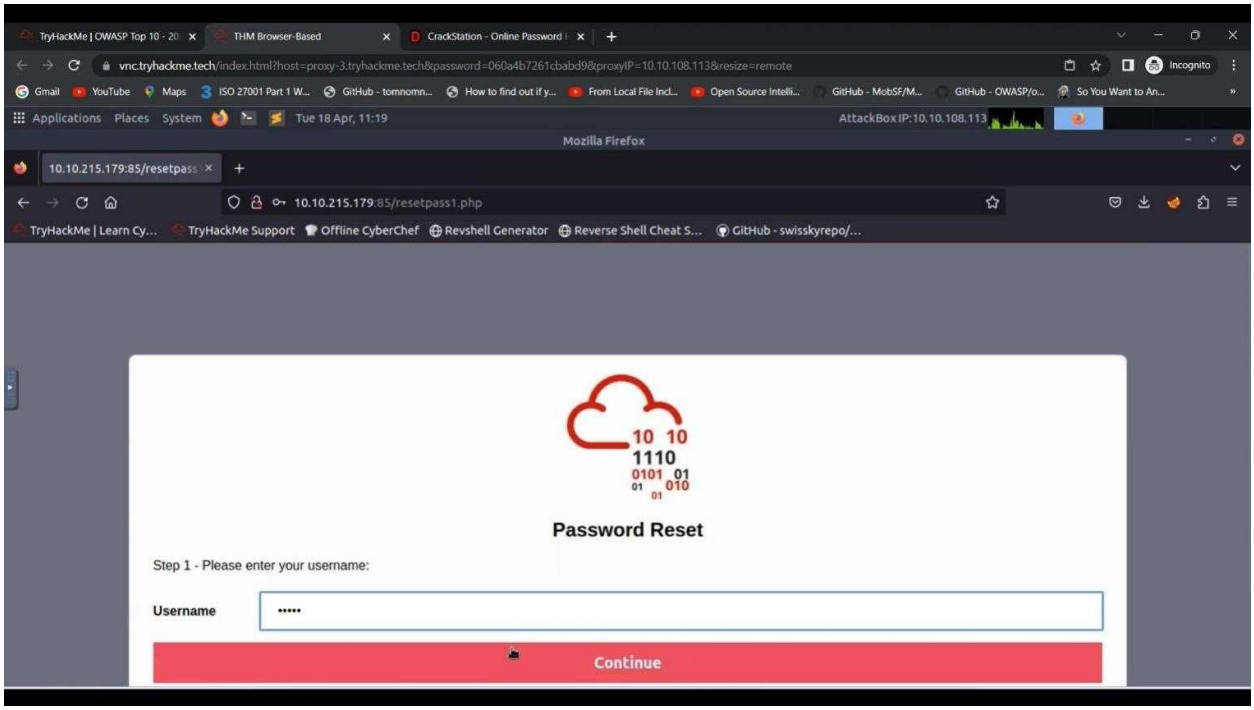
Business Impact:

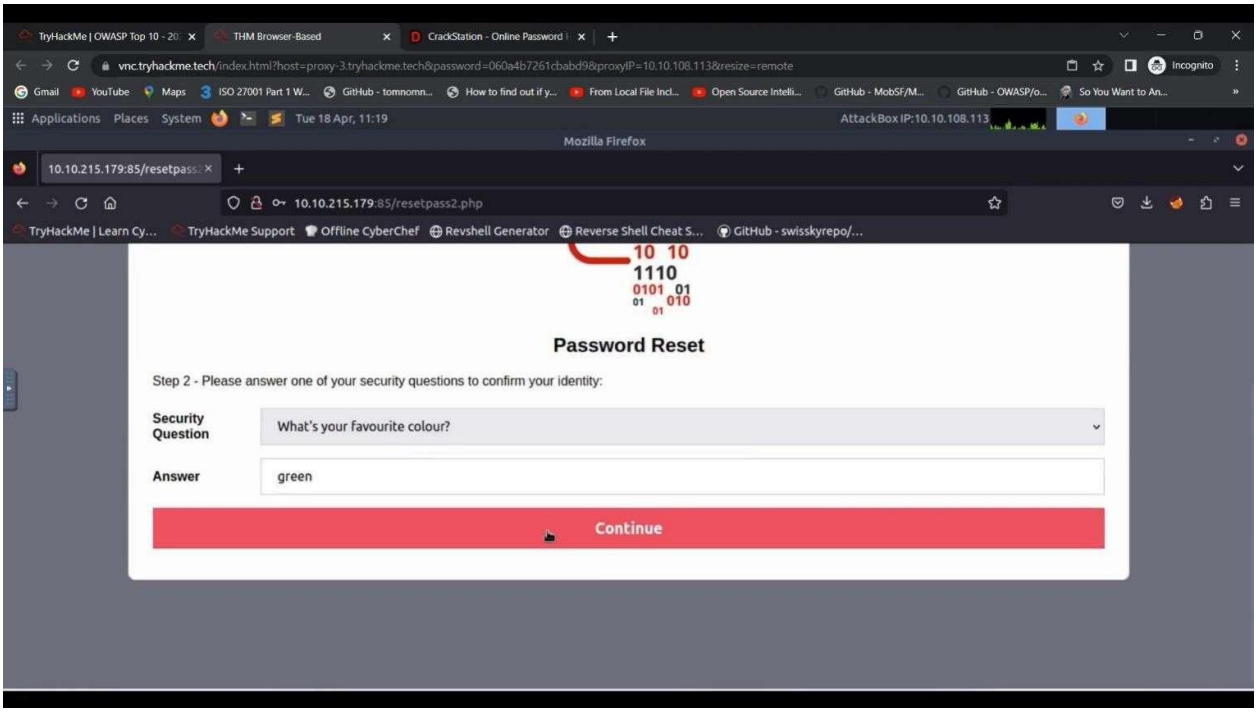
SQL Injection in Hibernate can have severe business impact. Attackers exploit vulnerabilities in Hibernate ORM framework to inject malicious SQL queries, potentially leading to unauthorized access, data leakage, or manipulation of sensitive data stored in the database. This can compromise data integrity, breach user privacy, and result in financial losses, legal

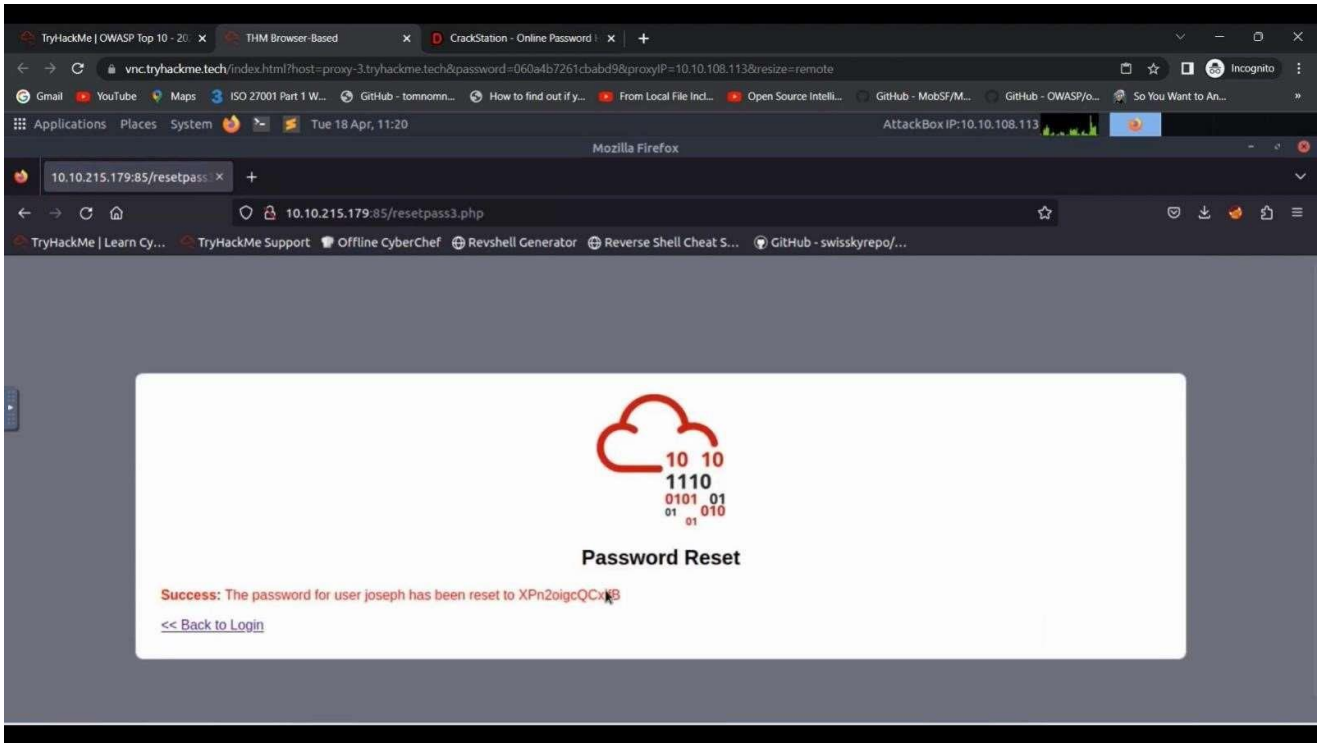
liabilities, and reputational damage. Promptly addressing this vulnerability is crucial to safeguarding the application's security and maintaining trust among users and stakeholders.

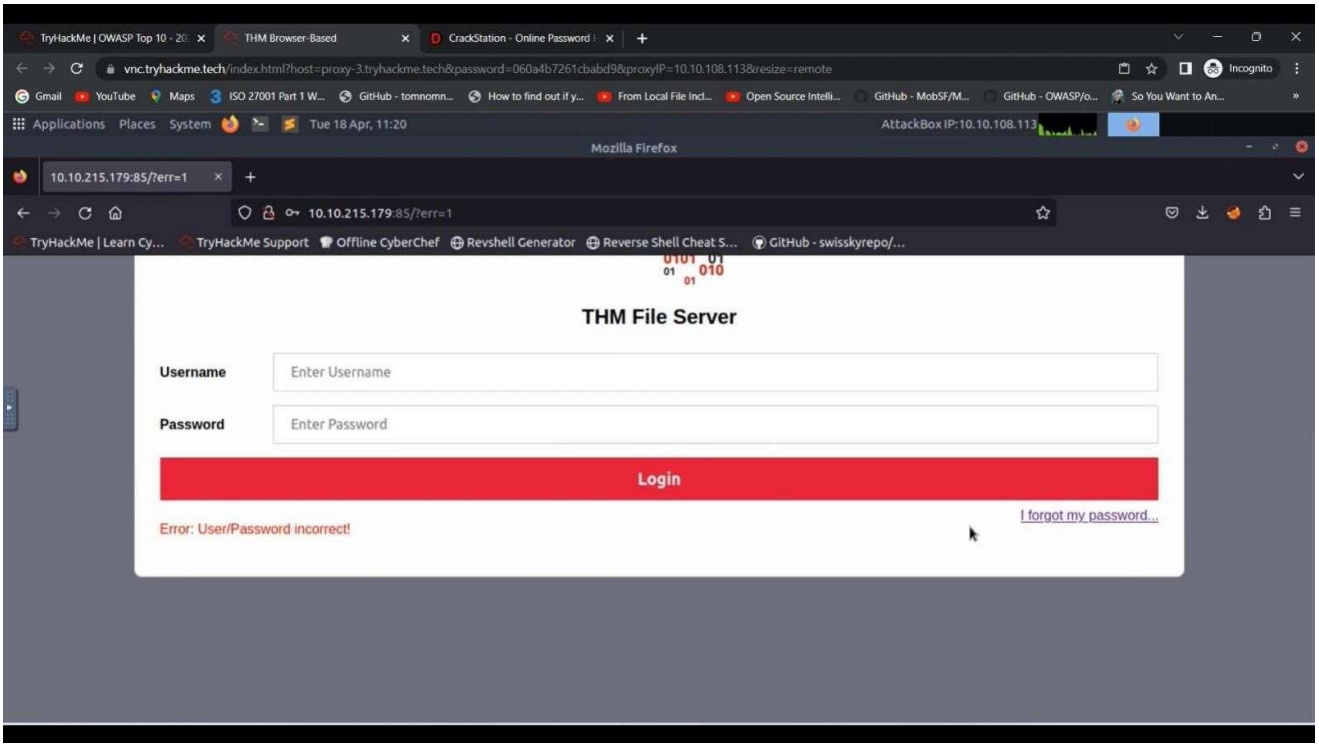
In the above experiment we have modified the SQL statement and displayed all the products in the category whether they are released or not. This is known as SQL Injection.

4. **OWASP CATEGORY: A04 2021 Insecure Design CWE-657: Violation of Secure Design Principles**


TryHackMe | OWASP Top 10 - 20
THM Browser-Based
CrackStation - Online Password
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=060a4b7261cbabd98&proxyIP=10.10.108.113&resize=remote
Incognito
Gmail
YouTube
Maps
ISO 27001 Part 1 W...
GitHub - tomnomn...
How to find out if y...
From Local File Incl...
Open Source Intelli...
GitHub - MobSF/M...
GitHub - OWASP/o...
So You Want to An...
Applications
Places
System
Tue 18 Apr, 11:19
AttackBox IP:10.10.108.113
Mozilla Firefox
10.10.215.179:85/resetpass
10.10.215.179:85/resetpass1.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
Password Reset
Step 1 - Please enter your username:
Username
Continue


TryHackMe | OWASP Top 10 - 20
THM Browser-Based
CrackStation - Online Password
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=060a4b7261cbabd98&proxyIP=10.10.108.113&resize=remote
Incognito
Gmail
YouTube
Maps
ISO 27001 Part 1 W...
GitHub - tomnomn...
How to find out if y...
From Local File Incl...
Open Source Intelli...
GitHub - MobSF/M...
GitHub - OWASP/o...
So You Want to An...
Applications
Places
System
Tue 18 Apr, 11:19
AttackBox IP:10.10.108.113
Mozilla Firefox
10.10.215.179:85/resetpass
10.10.215.179:85/resetpass2.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
Password Reset
Step 2 - Please answer one of your security questions to confirm your identity:
Security Question
What's your favourite colour?
Answer
green
Continue





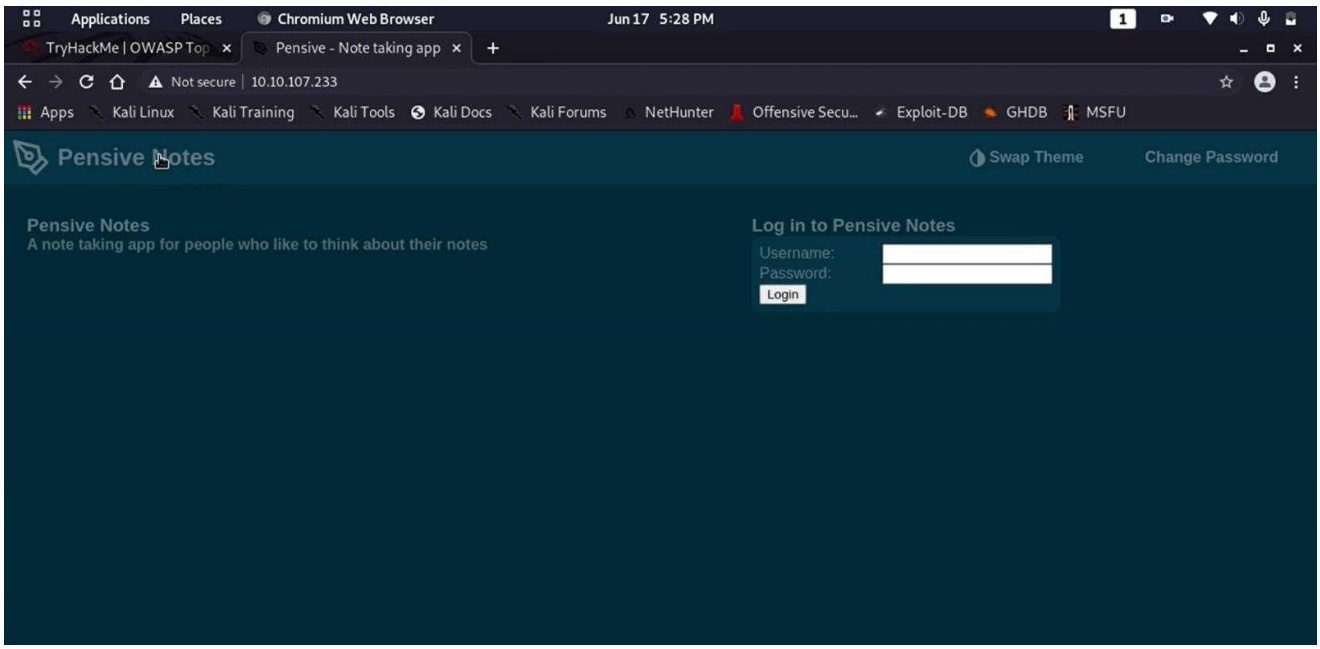
Description:

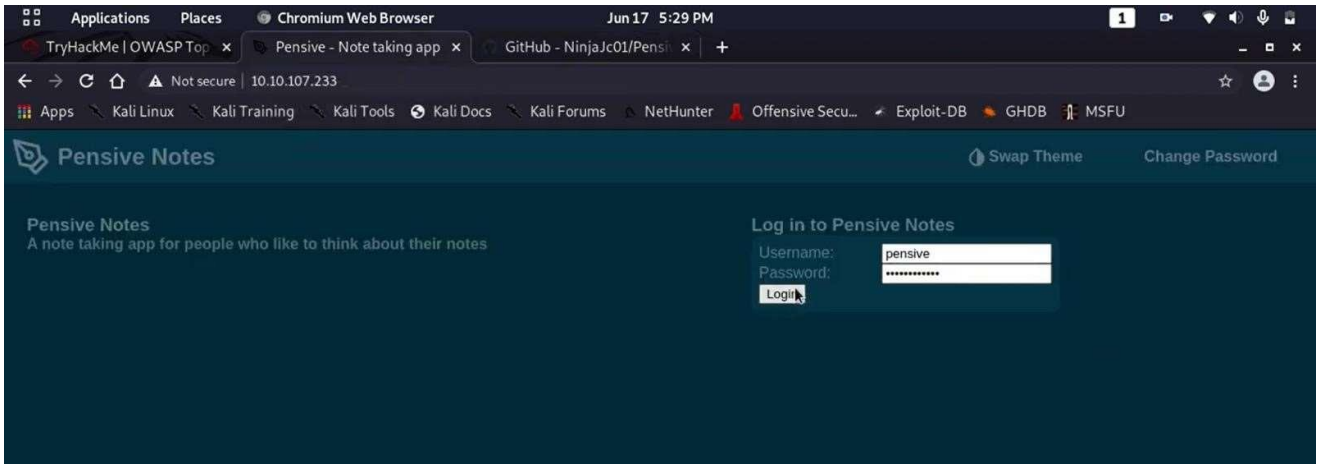
The product violates well-established principles for secure design.

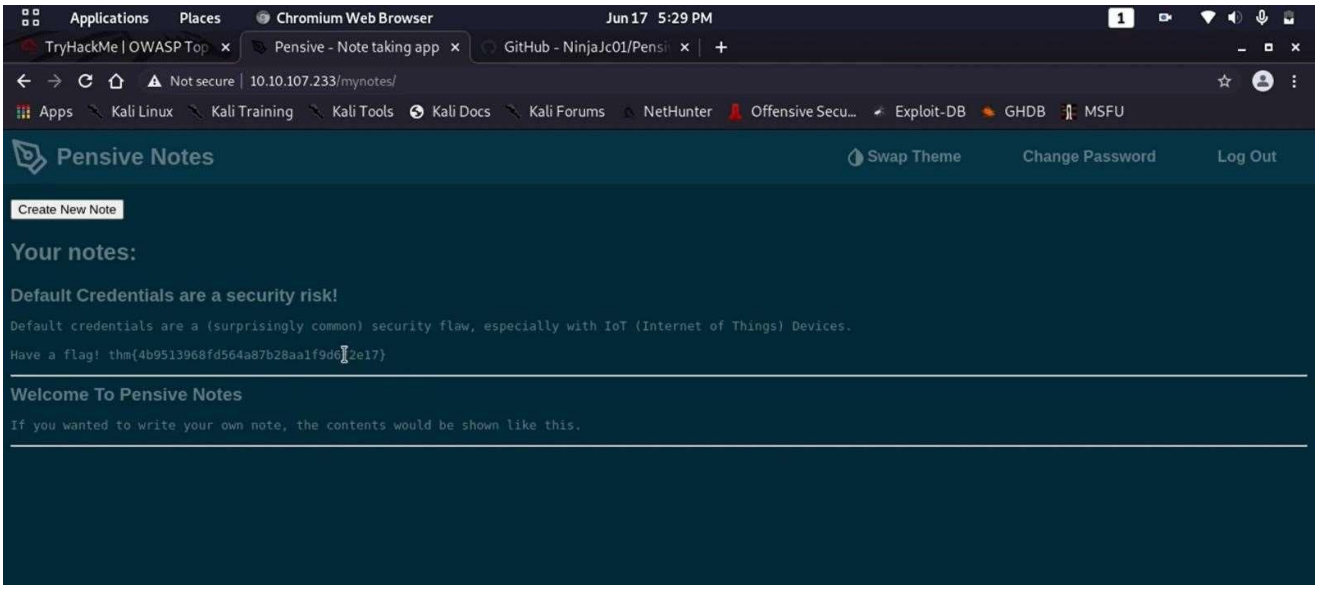
Business Impact:

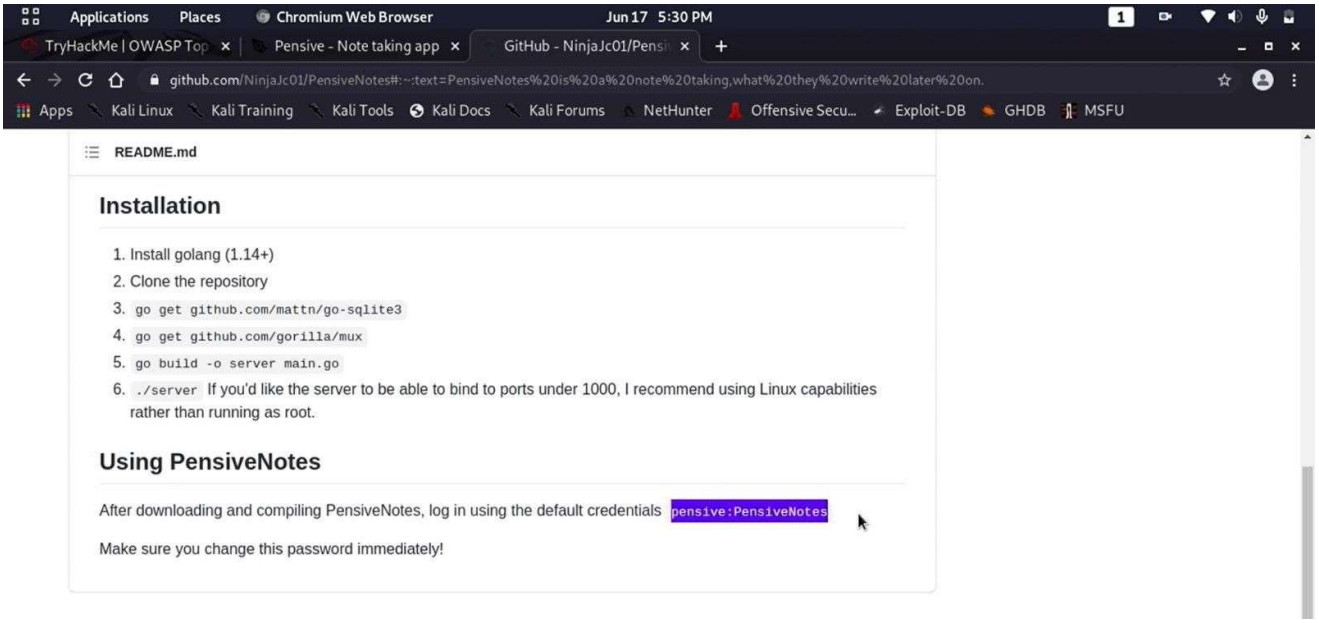
"Violation of Secure Design Principles," presents a critical risk to businesses. This vulnerability emerges when software systems are developed without following established security best practices and design principles. As a result, applications become susceptible to various attacks and breaches. Exploiting this flaw can lead to unauthorized access, data breaches, system compromise, and operational disruptions. The business impact encompasses financial losses, regulatory penalties, legal actions, reputational damage, erosion of customer trust, and increased security-related development costs. Addressing this issue necessitates reevaluating and retrofitting the software's design, diverting resources from innovation and development efforts, potentially delaying project timelines and undermining competitiveness.

5. OWASP CATEGORY: A05 2021 Security Misconfiguration
CWE-11: ASP.NET Misconfiguration: Creating Debug Binary




Applications Places Chromium Web Browser Jun 17 5:29 PM
TryHackMe | OWASP Top
Pensive - Note taking app
GitHub - NinjaJc01/Pensi
Not secure | 10.10.107.233
Apps Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Secu... Exploit-DB GHDB MSFU
Pensive Notes
Swap Theme
Change Password
Pensive Notes
A note taking app for people who like to think about their notes
Log in to Pensive Notes
Username: pensive
Password:
Login


Applications Places Chromium Web Browser Jun 17 5:29 PM
TryHackMe | OWASP Top
Pensive - Note taking app
GitHub - NinjaJc01/Pensi
Not secure | 10.10.107.233/mynotes/
Apps Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Secu... Exploit-DB GHDB MSFU
Pensive Notes
Swap Theme
Change Password
Log Out
Create New Note
Your notes:
Default Credentials are a security risk!
Default credentials are a (surprisingly common) security flaw, especially with IoT (Internet of Things) Devices.
Have a flag! thm{4b9513968fd564a87b28aa1f9d62e17}
Welcome To Pensive Notes
If you wanted to write your own note, the contents would be shown like this.


Applications Places Chromium Web Browser Jun 17 5:30 PM
TryHackMe | OWASP Top
Pensive - Note taking app
GitHub - NinjaJc01/Pensi
github.com/NinjaJc01/PensiveNotes#:~:text=PensiveNotes%20is%20a%20note%20taking,what%20they%20write%20later%20on.
Apps Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Secu... Exploit-DB GHDB MSFU
README.md
Installation
1. Install golang (1.14+)
2. Clone the repository
3. go get github.com/mattn/go-sqlite3
4. go get github.com/gorilla/mux
5. go build -o server main.go
6. ./server If you'd like the server to be able to bind to ports under 1000, I recommend using Linux capabilities rather than running as root.
Using PensiveNotes
After downloading and compiling PensiveNotes, log in using the default credentials pensive:PensiveNotes
Make sure you change this password immediately!

Description:

The product transmits sensitive or security critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact:

Security Misconfiguration can harm businesses by exposing confidential data during transmission, leading to data breaches, compromised customer trust, regulatory violations, and potential legal consequences.

In the above experiment we have noticed that credentials are available online for the website and anyone can have access to it. All the confidential details are exposed to everyone by which anyone can have access to data.