**ASSIGNMENT - 1**

NAME: Yelakanti Ramu

REGNO: 21BCb7046

**List of Vulnerable Parameter.**

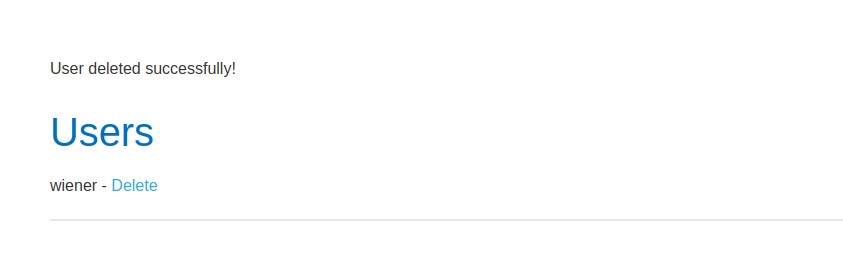
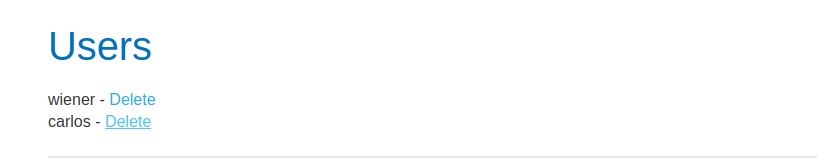
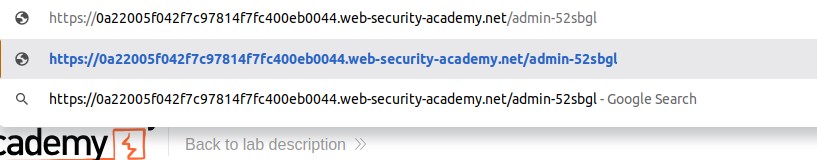
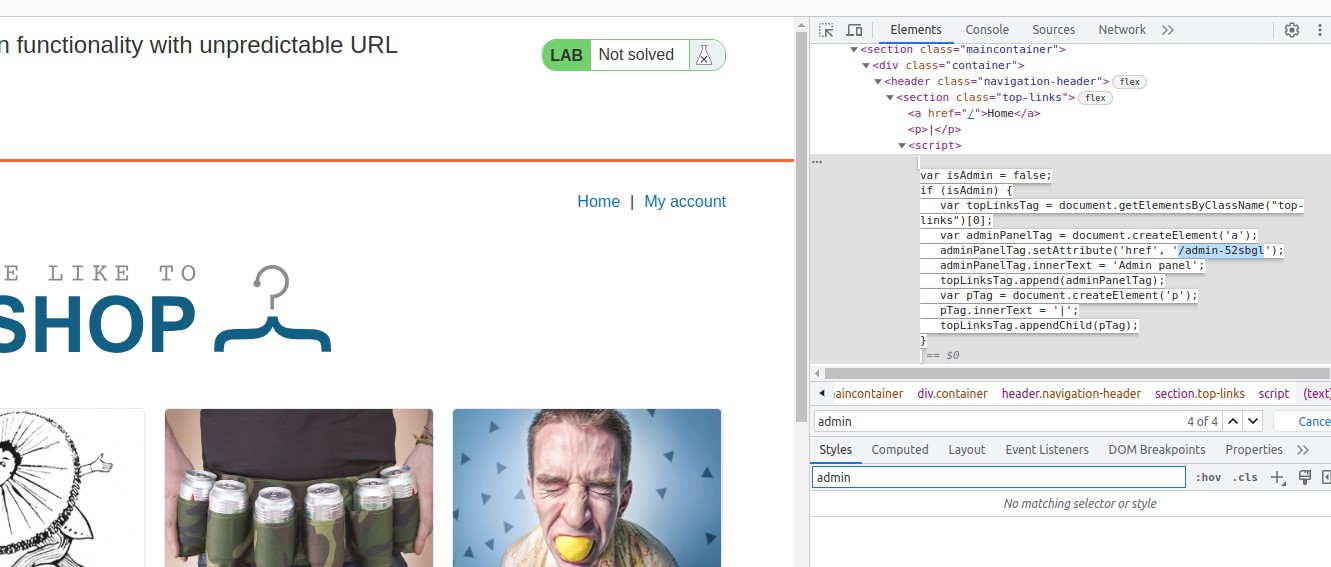
**1. CWE: CWE-284: Improper Access Control**

**OWASP CATEGORY: A01 2021 Broken Access Control**

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

**BUSINESS IMPACT:** can harm businesses by enabling unauthorized users to access sensitive data, causing data breaches, financial loss, reputation damage, legal issues, operational disruptions, intellectual property theft, and increasing insider threat risks.





• Improper access controls can help attacker in altering or permanently deleting an existing user.

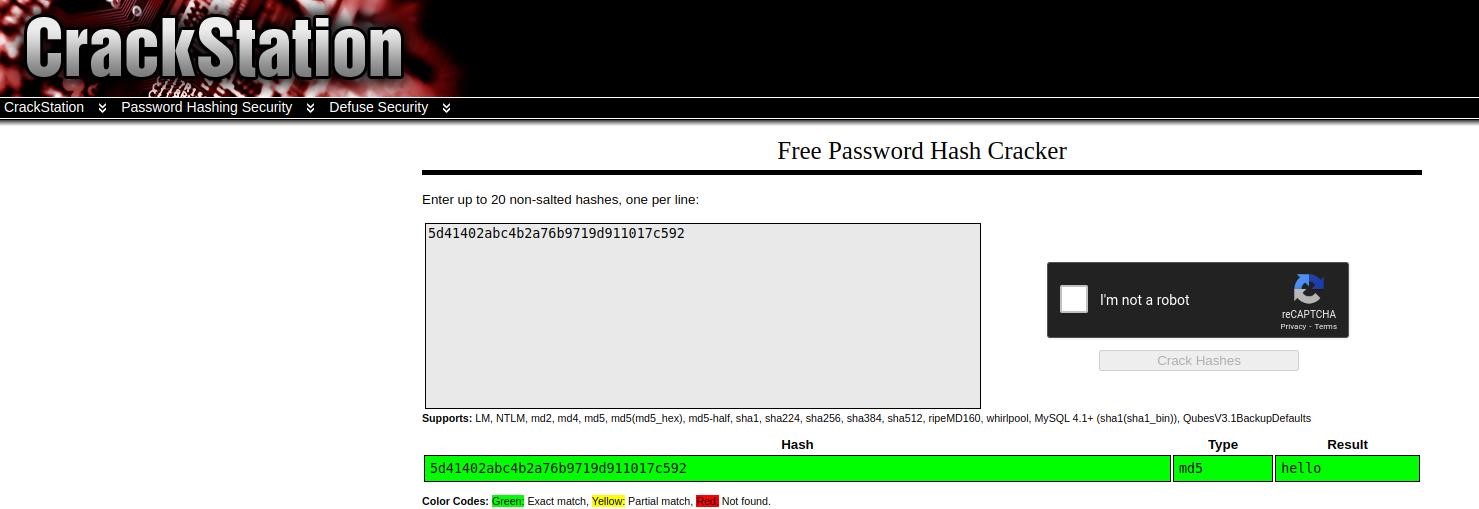
1. **CWE: CWE-327: Use of a Broken or Risky**

**Cryptographic Algorithm**

**OWASP CATEGORY: A02 2021 Cryptographic Failures**

**DESCRIPTION:** The product uses a broken or risky cryptographic algorithm or protocol.

**BUSINESS IMPACT:** can seriously impact businesses by compromising data security, leading to potential breaches, loss of trust, regulatory penalties, and operational disruptions.

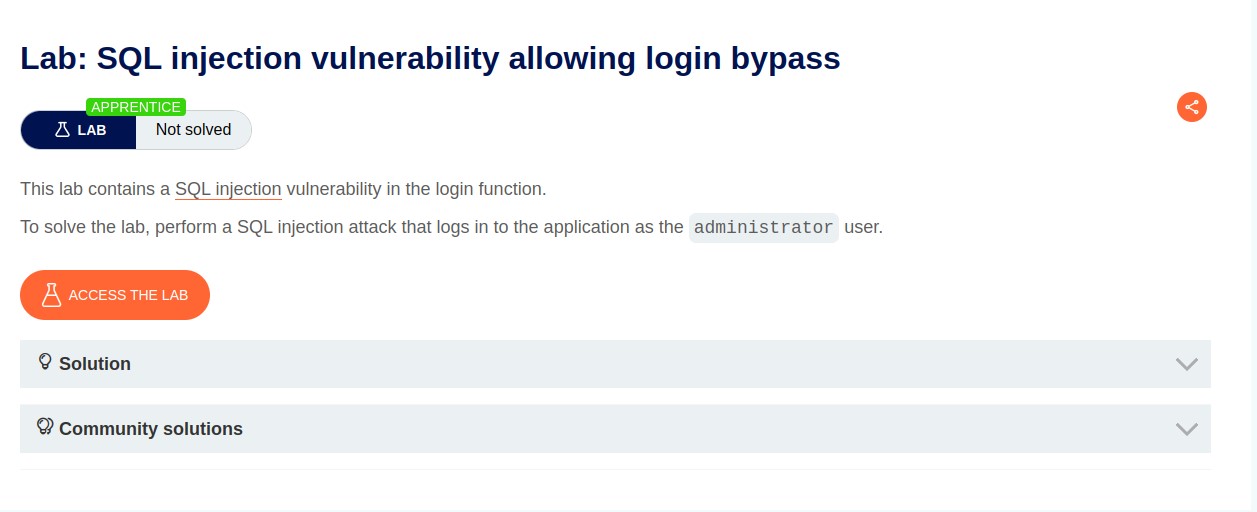


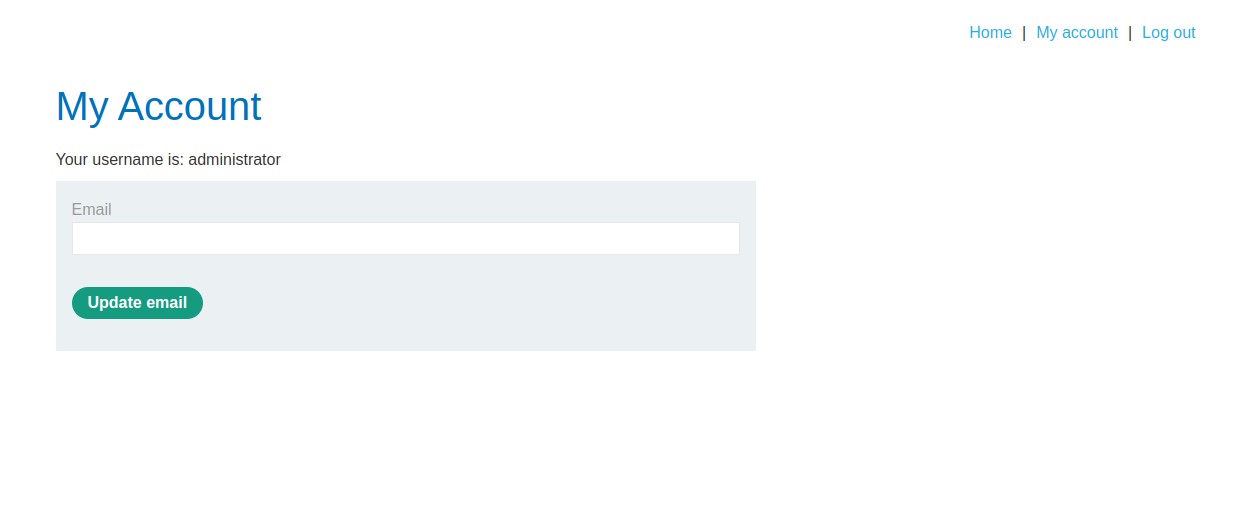
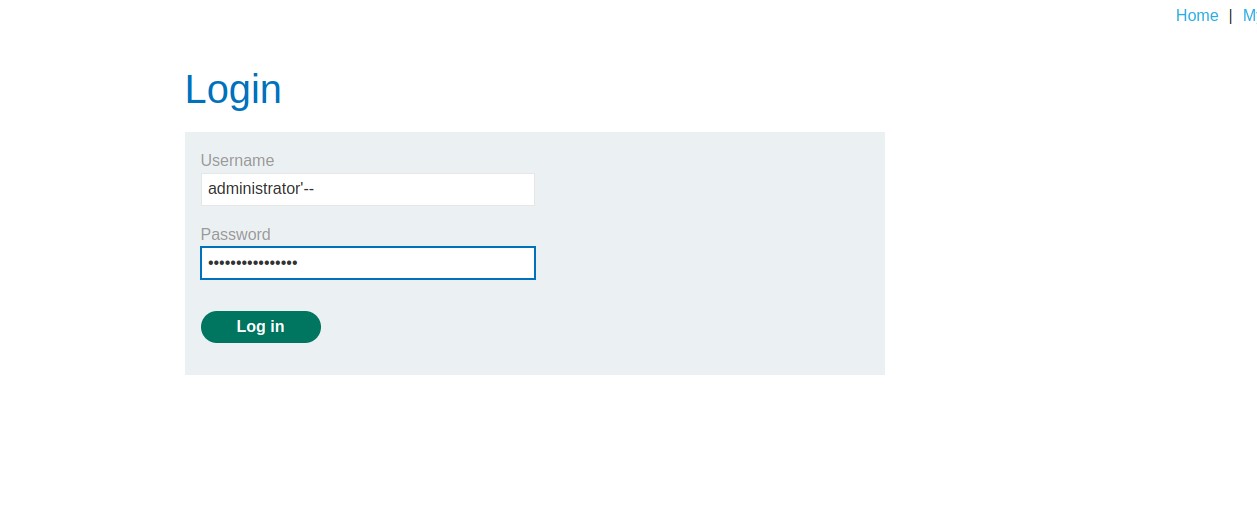
1. **CWE: CWE-564: SQL Injection: Hibernate**

**OWASP CATEGORY: A03 2021 Injection**

**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:** allows attackers to manipulate database queries through vulnerabilities in Hibernate, potentially leading to unauthorized data access, breaches, financial losses, legal issues, and reputation damage.





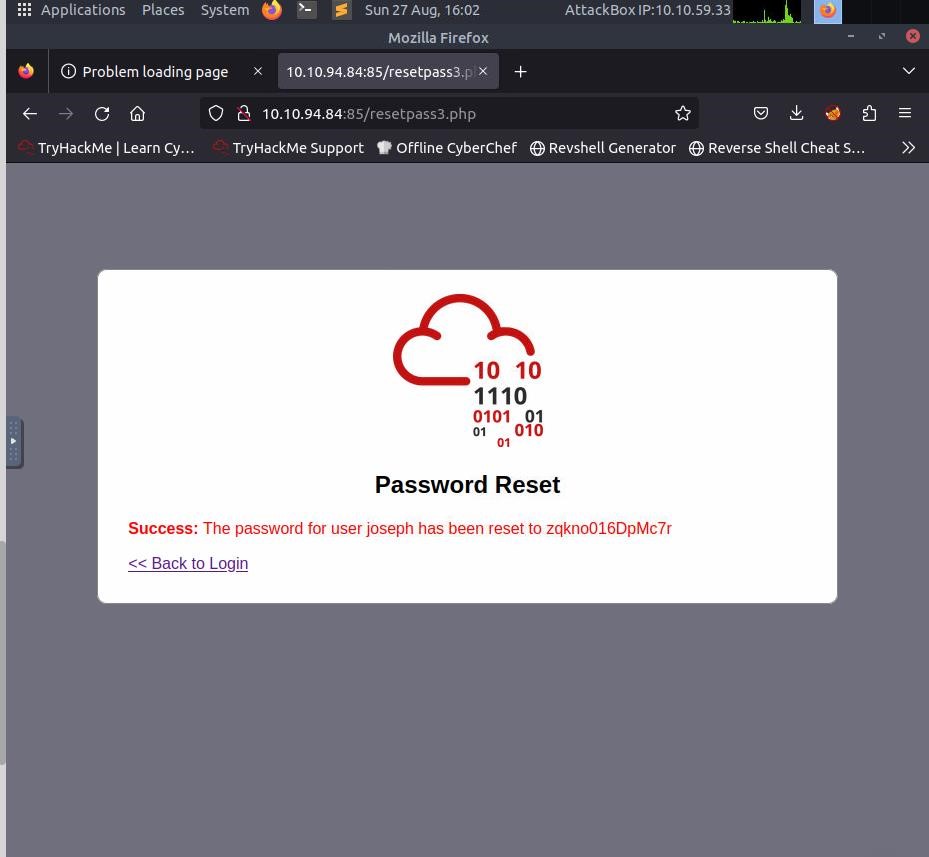
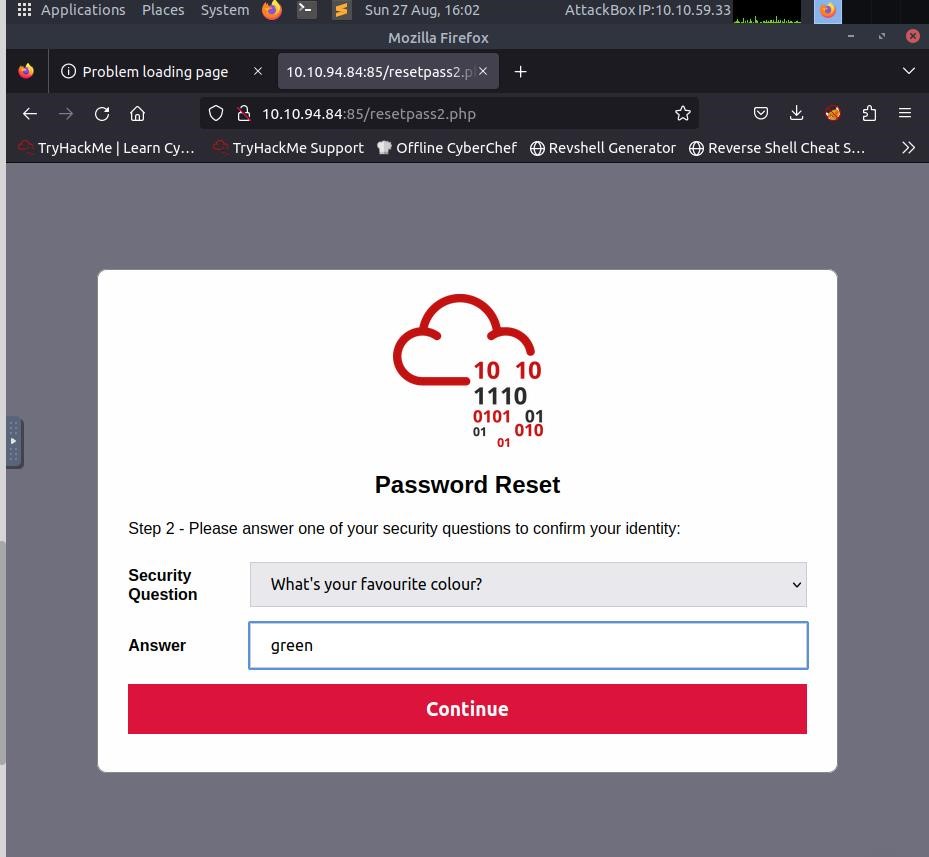
* + SQL Statements can be used to modify the table and gain access to users' data.

1. **CWE: CWE-657: Violation of Secure Design Principles**

**OWASP CATEGORY: A04 2021 Insecure Design**

**DESCRIPTION:** The product violates well-established principles for secure design.

**BUSINESS IMPACT:** has substantial business implications due to its potential to result in vulnerabilities and weak security structures. This can lead to data breaches, financial losses, reputational damage, and regulatory penalties.



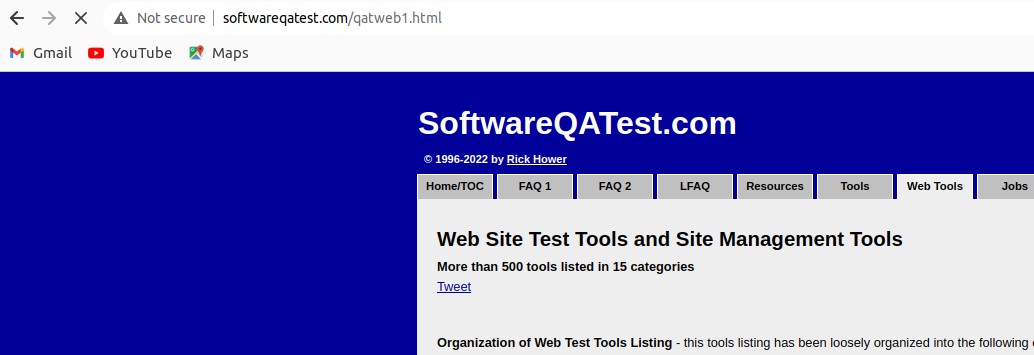
* + Violation of security design principles includes poor security designing.
  + The chances of an attacker stealing passwords is higher when poor security related questions are set.

1. **CWE: CWE-319: Cleartext Transmission of Sensitive**

**Information**

**OWASP CATEGORY: A05 2021 Security Misconfiguration DESCRIPTION:** The product transmits sensitive or securitycritical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

**BUSINESS IMPACT:** can harm businesses by exposing confidential data during transmission, leading to data breaches, compromised customer trust, regulatory violations, and potential legal consequences.



* + Websites with http allows attackers to steal sensitive information.
  + In the absence of an SSL certificate, all your communications are not encrypted at all. Meaning attackers have access to all the data.
  + Sensitive Information must only be channelled through HTTPS communicatons.