ASSIGNMENT - 1

NAME: RAMAR PRIYA MAHA LAKSHMI

REGNO: 21BCE7521

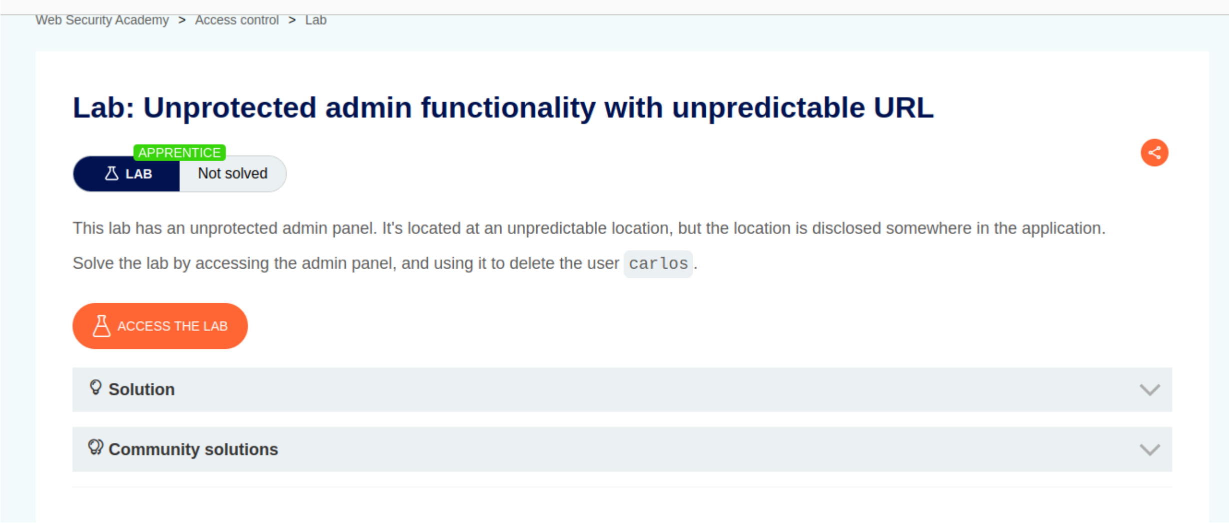
a. List of Vulnerable Parameter.

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.

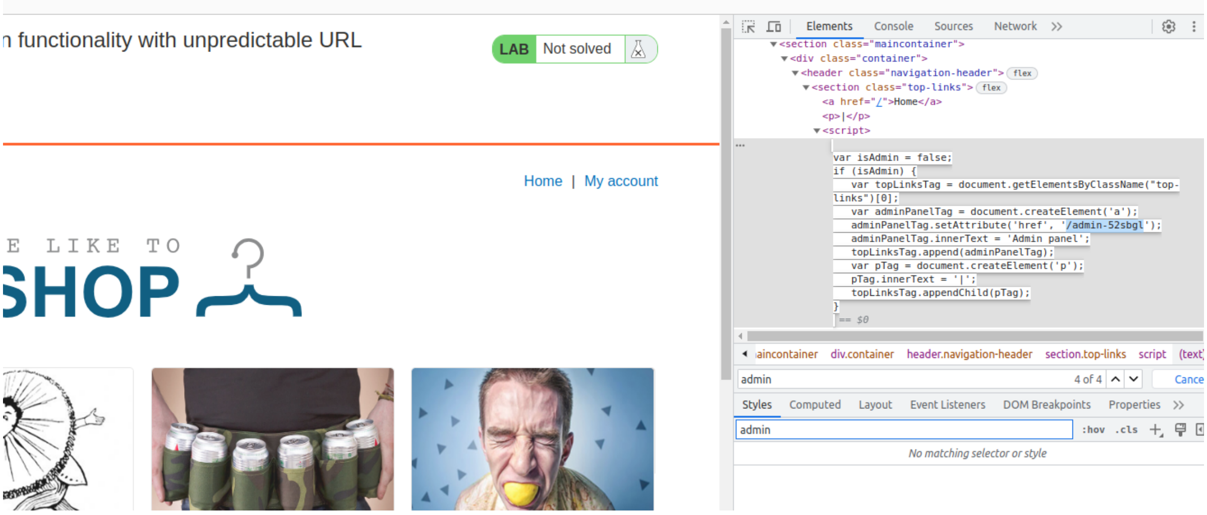


Web Security Academy > Access control > Lab

Lab: Unprotected admin functionality with unpredictable URL

This lab has an unprotected admin panel. It's located at an unpredictable location, but the location is disclosed somewhere in the application.

Solve the lab by accessing the admin panel, and using it to delete the user `carlos`.



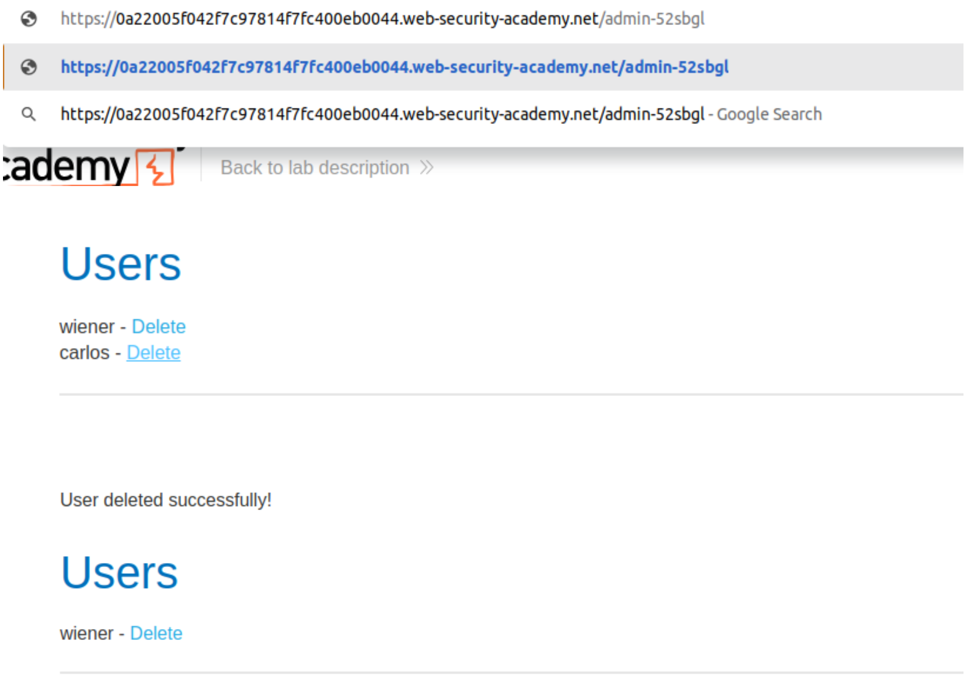
```
▼<section class="maincontainer">
  ▼<div class="container">
    ▼<header class="navigation-header"> flex
      ▼<section class="top-links"> flex
          <a href="/">Home</a>
          <p>|</p>
        ▼<script>
            var isAdmin = false;
            if (isAdmin) {
               var topLinksTag = document.getElementsByClassName("top-
            links")[0];
               var adminPanelTag = document.createElement('a');
               adminPanelTag.setAttribute('href', '/admin-52sbgl');
               adminPanelTag.innerText = 'Admin panel';
               topLinksTag.append(adminPanelTag);
               var pTag = document.createElement('p');
               pTag.innerText = '|';
               topLinksTag.appendChild(pTag);
            }
            == $0
```

aincontainer div.container header.navigation-header section.top-links script (text)

admin 4 of 4 Cance

admin :hov .cls

No matching selector or style



https://0a22005f042f7c97814f7fc400eb0044.web-security-academy.net/admin-52sbgl

https://0a22005f042f7c97814f7fc400eb0044.web-security-academy.net/admin-52sbgl

https://0a22005f042f7c97814f7fc400eb0044.web-security-academy.net/admin-52sbgl - Google Search

Users

wiener - Delete
carlos - Delete

User deleted successfully!

Users

wiener - Delete

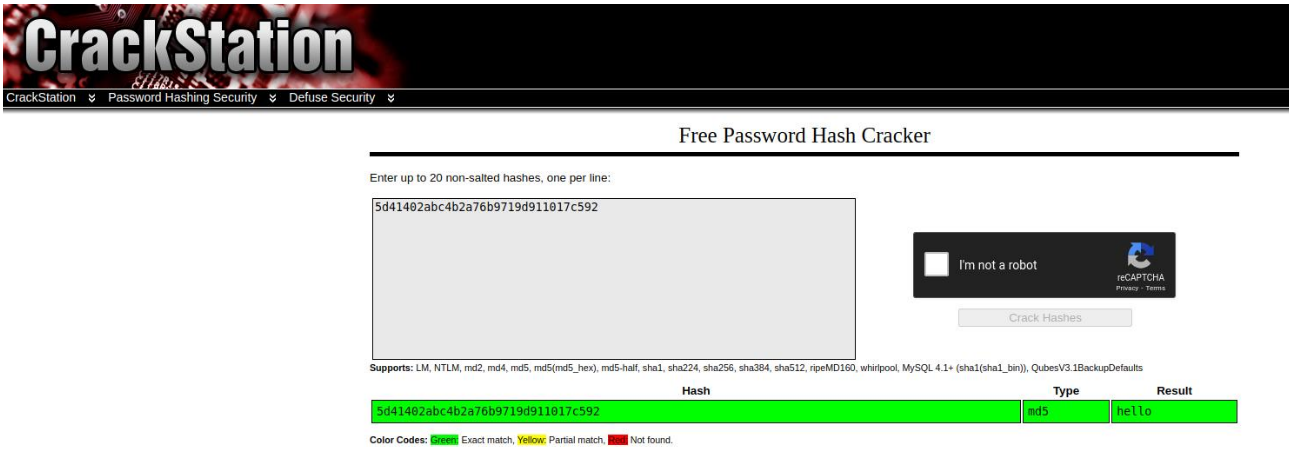
- Improper access controls can help attacker in altering or permanently deleting an existing user.

2. 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.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5d41402abc4b2a76b9719d911017c592
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5d41402abc4b2a76b9719d911017c592	md5	hello

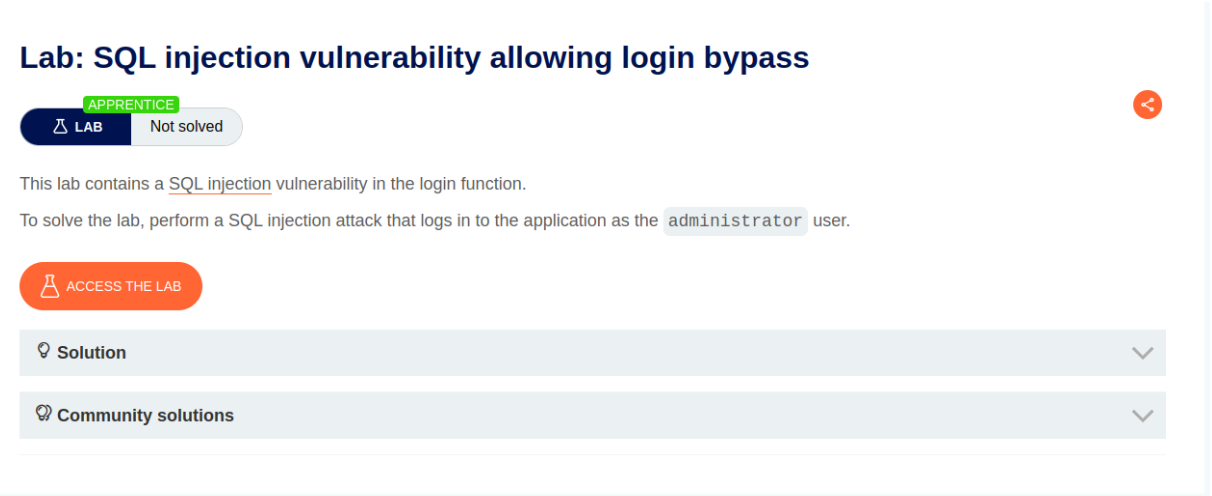
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

3. 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.

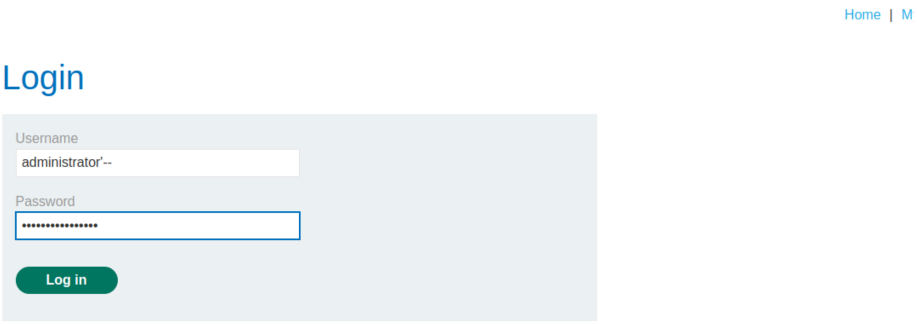
BUSINESS IMPACT: allows attackers to manipulate database queries through vulnerabilities in Hibernate, potentially leading to unauthorized data access, breaches, financial losses, legal issues, and reputation damage.



Lab: SQL injection vulnerability allowing login bypass

This lab contains a SQL injection vulnerability in the login function.

To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user.



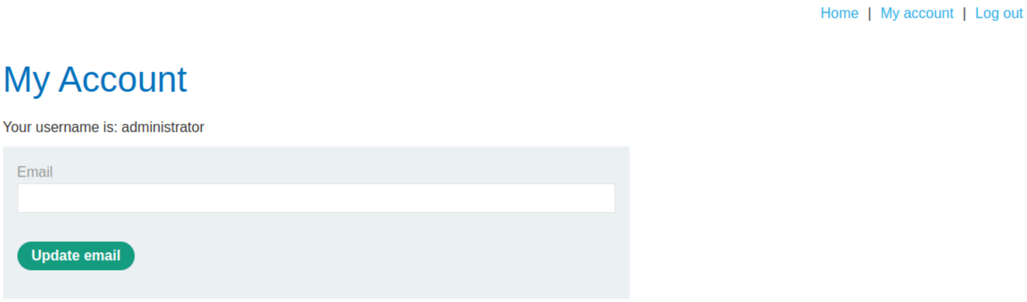
Login

Username

administrator'--

Password

••••••••••••••••



My Account

Your username is: administrator

Email

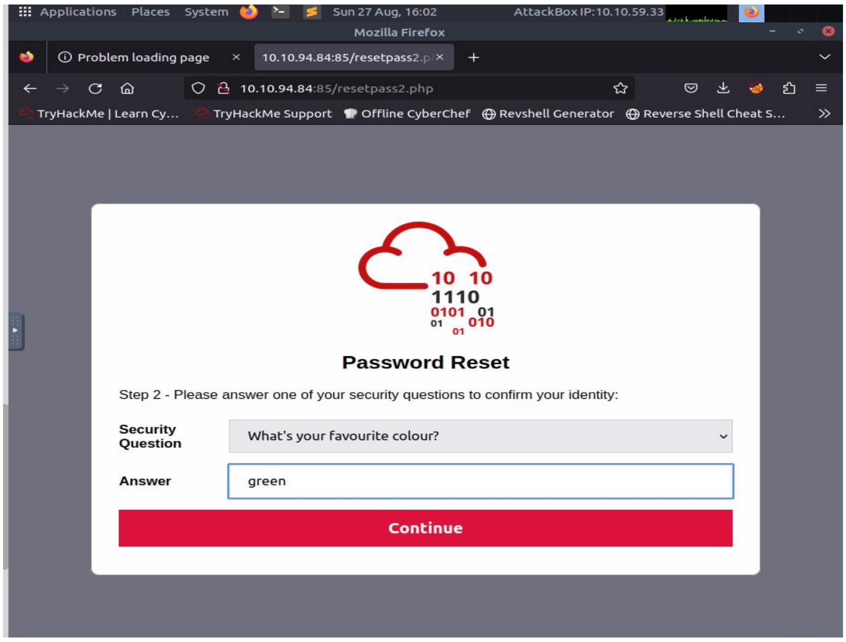
- SQL Statements can be used to modify the table and gain access to users' data.

4. 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.

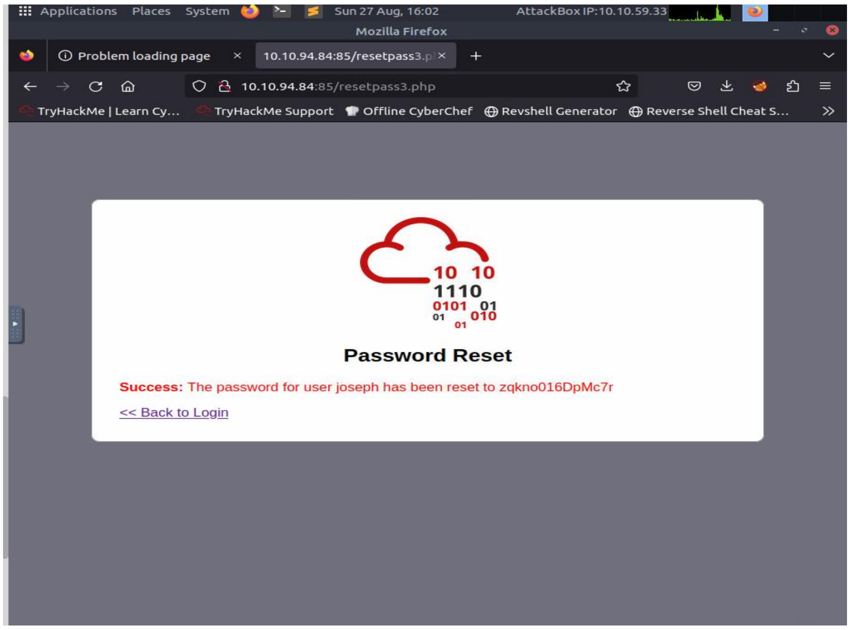


Password Reset

Step 2 - Please answer one of your security questions to confirm your identity:

Security Question	What's your favourite colour?
Answer	green

Continue



Password Reset

Success: The password for user joseph has been reset to zqkno016DpMc7r

<< Back to Login

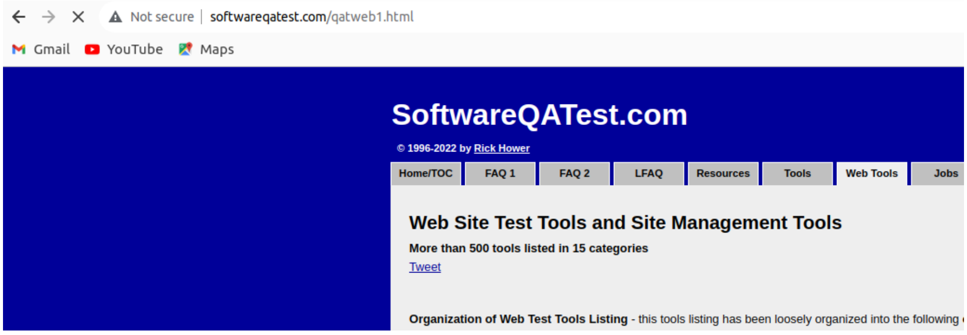
- Violation of security design principles includes poor security designing.
- The chances of an attacker stealing passwords is higher when poor security related questions are set.

5. CWE: CWE-319: Cleartext Transmission of Sensitive Information

OWASP CATEGORY: A05 2021 Security Misconfiguration

DESCRIPTION: The product transmits sensitive or security-critical 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.



SoftwareQATest.com

© 1996-2022 by Rick Hower

Web Site Test Tools and Site Management Tools

More than 500 tools listed in 15 categories

Tweet

Organization of Web Test Tools Listing - this tools listing has been loosely organized into the following

- 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.