

ASSIGNMENT - 01

1. CWE: CWE-284: Improper Access Control

OWSAP Category: A01:2021-Broken Access Control

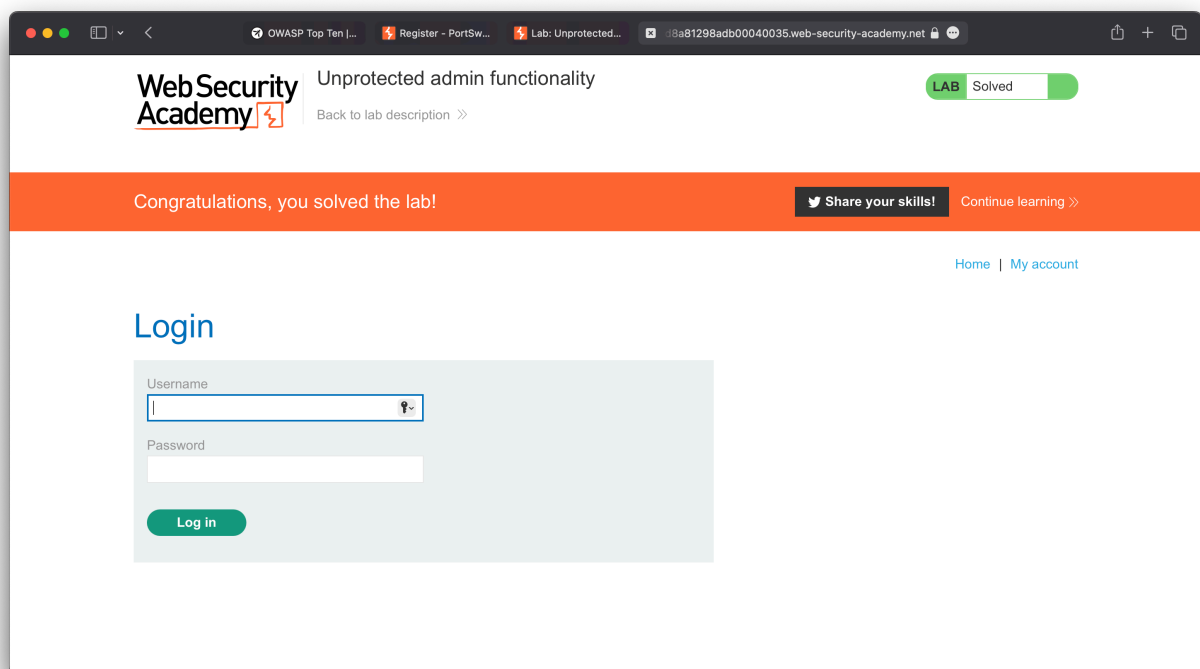
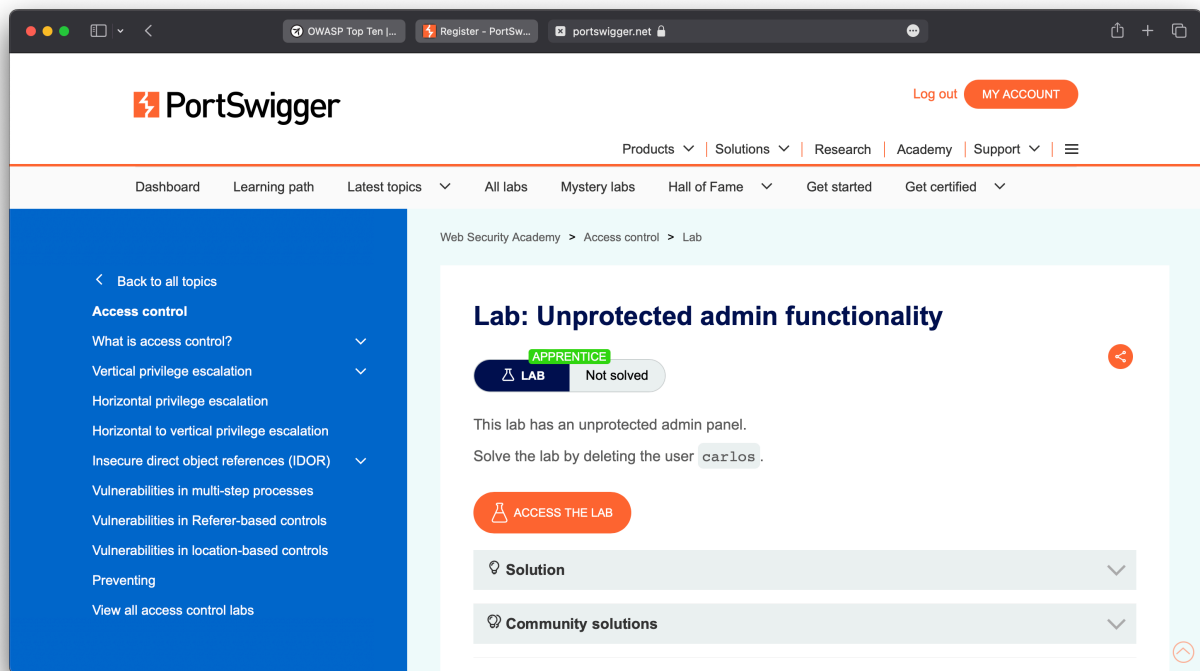
Description:

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



Business Impact:

When any mechanism fails then the attackers can harm the business by unauthorised access and steal sensitive information, data breaches. When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

Unprotected admin functionality.



✕ 035.web-security-academy.net/administrator-panel


Web Security Academy  Unprotected admin functionality LAB Not solved 

[Back to lab description >>](#)

[Home](#) | [My account](#)

Users

wiener - [Delete](#)
carlos - [Delete](#)

Web Security Academy  Unprotected admin functionality LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab! [Share your skills!](#) [Continue learning >>](#)

[Home](#) | [My account](#)

User deleted successfully!

Users

wiener - [Delete](#)

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:


Insecure cryptography can be exploited to expose sensitive information, modify data in unexpected ways, spoof the identities of other users or devices, or other impacts. 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

I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

Crack Hashes

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-94: Improper Control of Generation of Code('Code Injection)

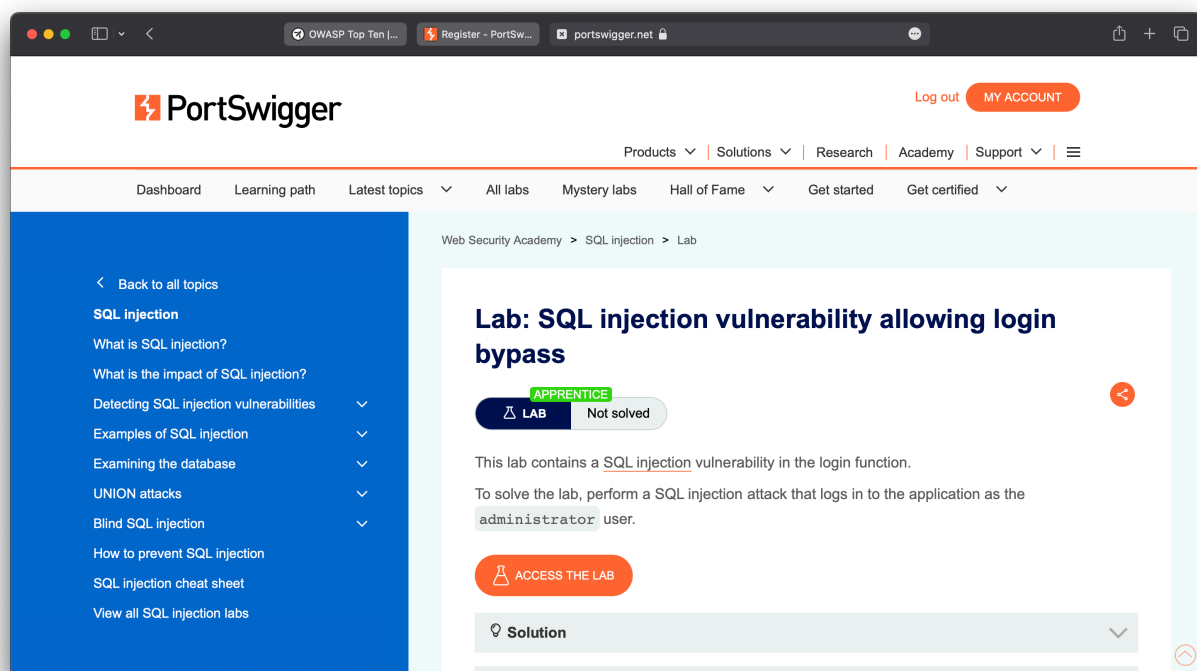
OWASP Category: A03:2021-Injection

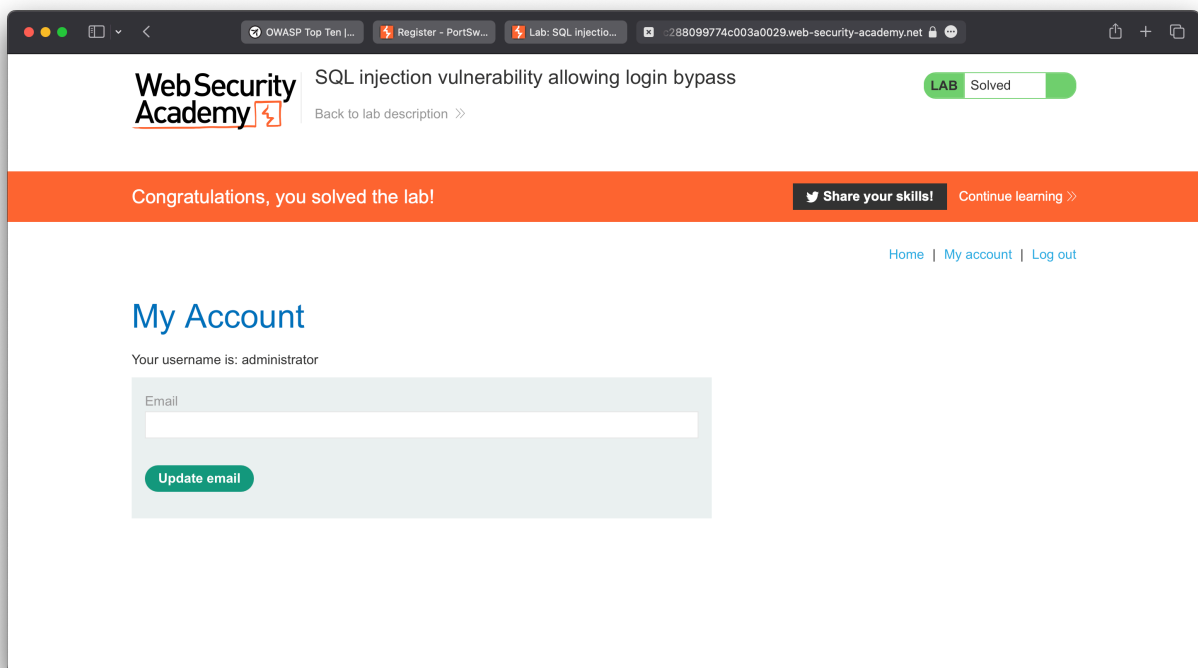
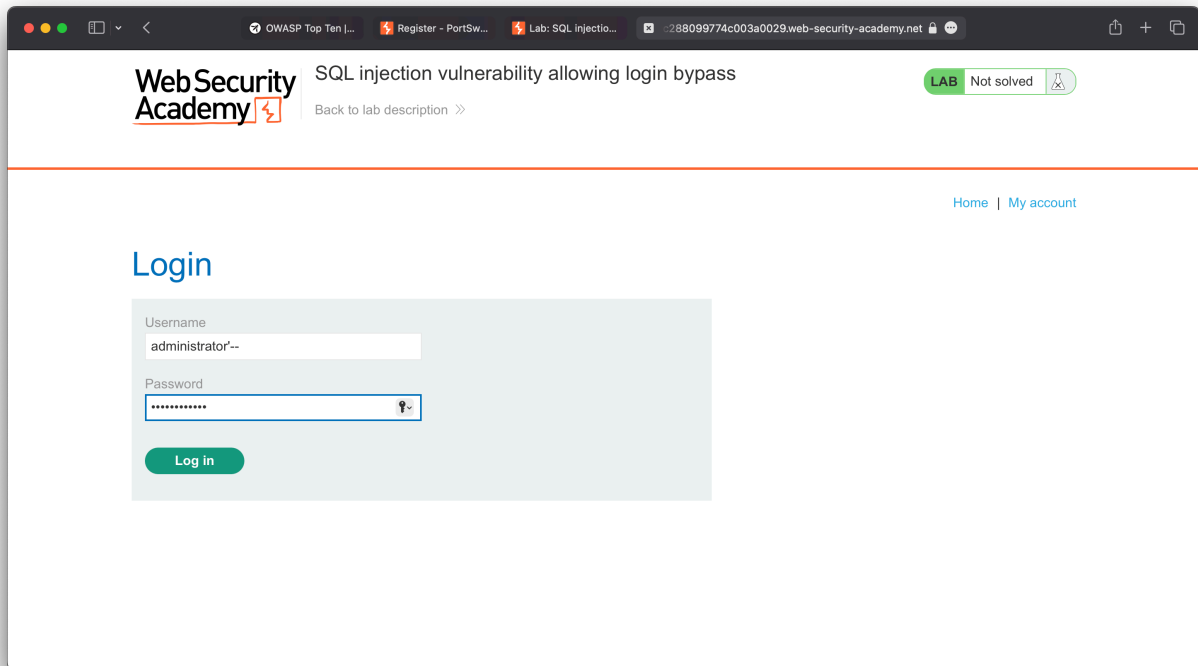
Description:

The product constructs all or part of a code segment using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralize special elements that could modify the syntax or behaviour of the intended code segment.

Business Impact:

When a product allows a user's input to contain code syntax, it might be possible for an attacker to craft the code in such a way that it will alter the intended control flow of the product. Such an alteration could lead to arbitrary code execution. Using SQL injection, attackers can retrieve and alter data, which risks exposing sensitive company data stored on the SQL server.





4. CWE: CWE-657: Violation of Secure Design Principles

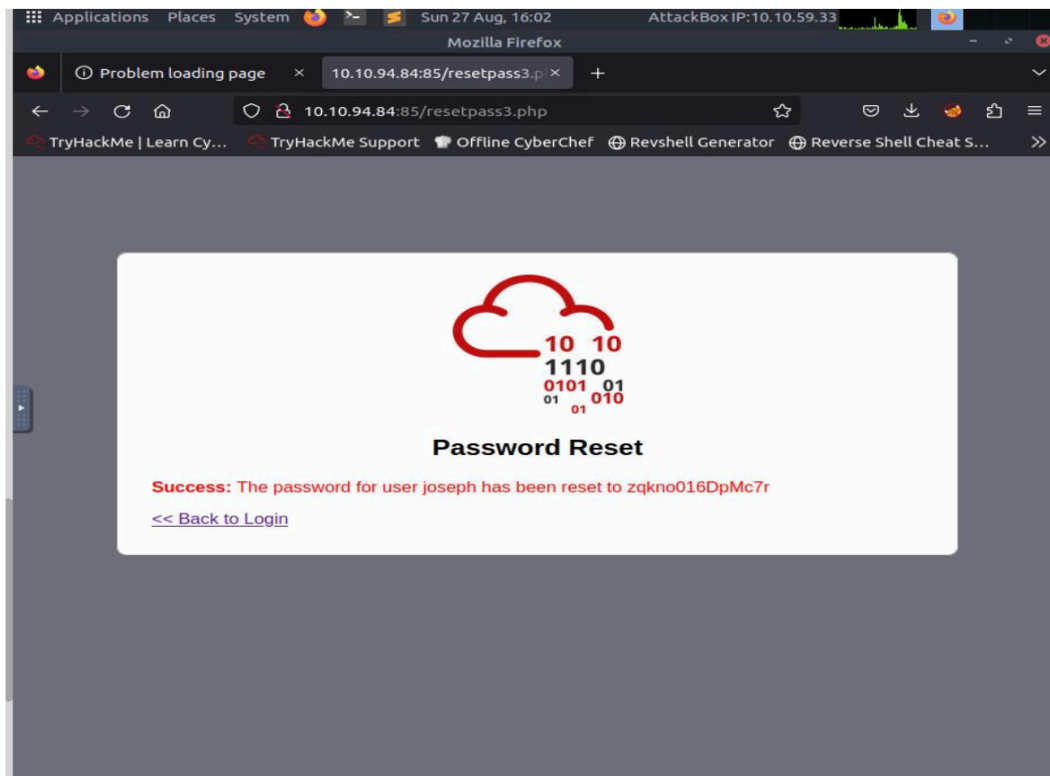
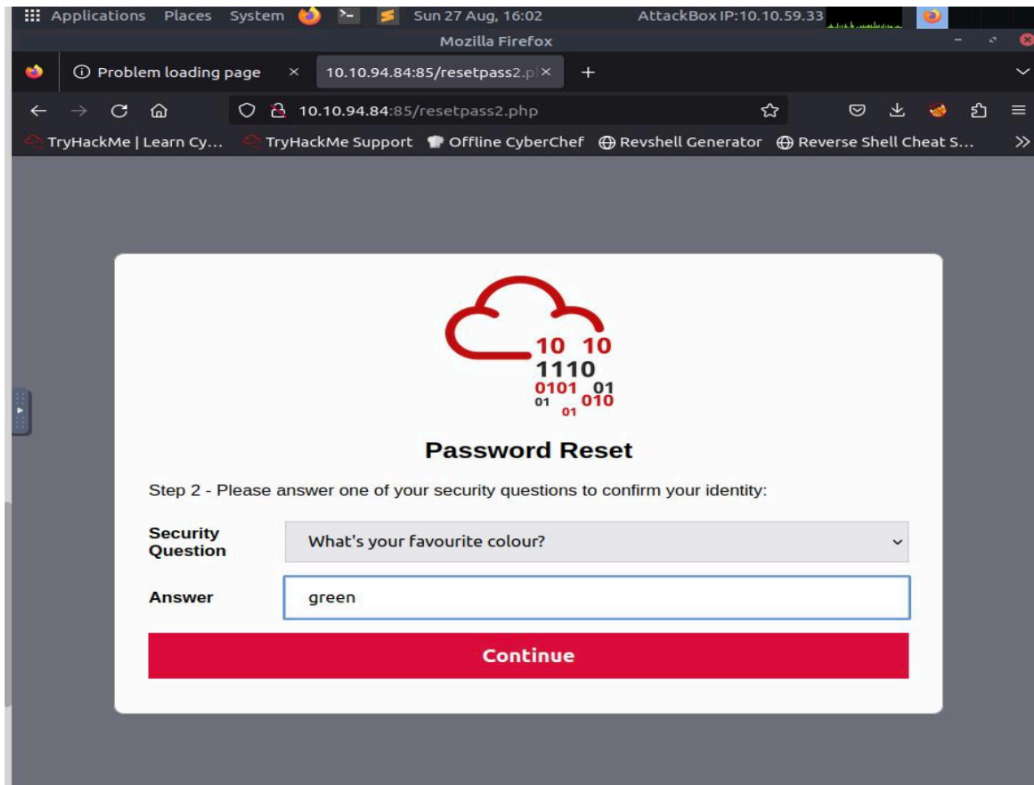
OWASP Category: A04:2021-Insecure Design

Description:

The product violates well-established principles for secure design.

Business Impact:

This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centred around design, it can be resource-intensive to fix design problems. It 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.



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

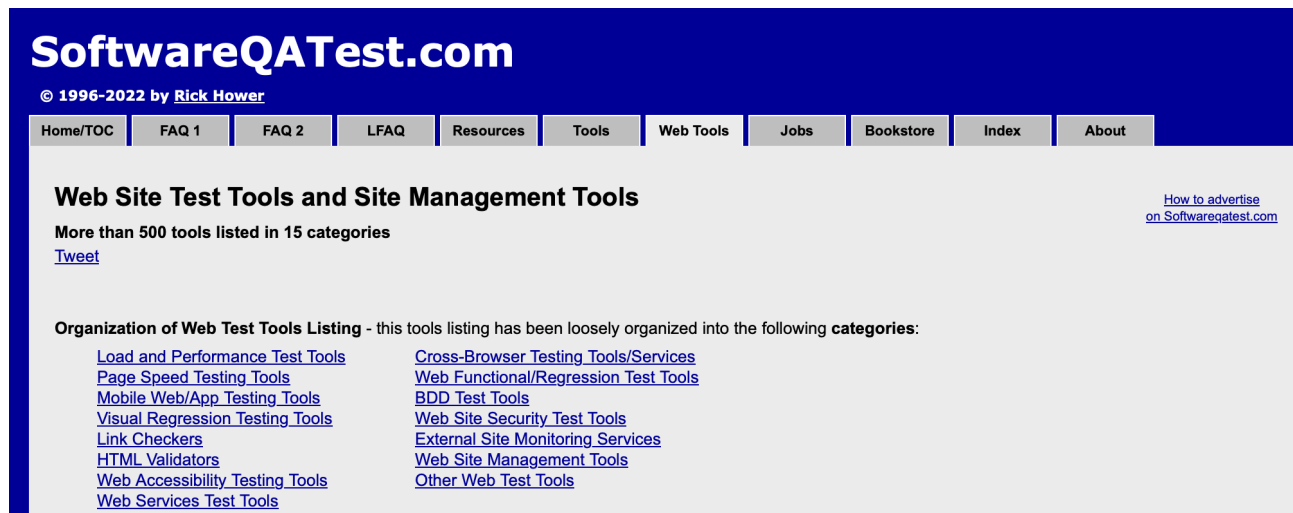
OWASP Category: A05:2021 - Security Misconfiguration

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

Home/TOC | FAQ 1 | FAQ 2 | LFAQ | Resources | Tools | Web Tools | Jobs | Bookstore | Index | About

Web Site Test Tools and Site Management Tools

More than 500 tools listed in 15 categories
[Tweet](#)

[How to advertise on Softwareqatest.com](#)

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

Load and Performance Test Tools	Cross-Browser Testing Tools/Services
Page Speed Testing Tools	Web Functional/Regression Test Tools
Mobile Web/App Testing Tools	BDD Test Tools
Visual Regression Testing Tools	Web Site Security Test Tools
Link Checkers	External Site Monitoring Services
HTML Validators	Web Site Management Tools
Web Accessibility Testing Tools	Other Web Test Tools
Web Services Test Tools	