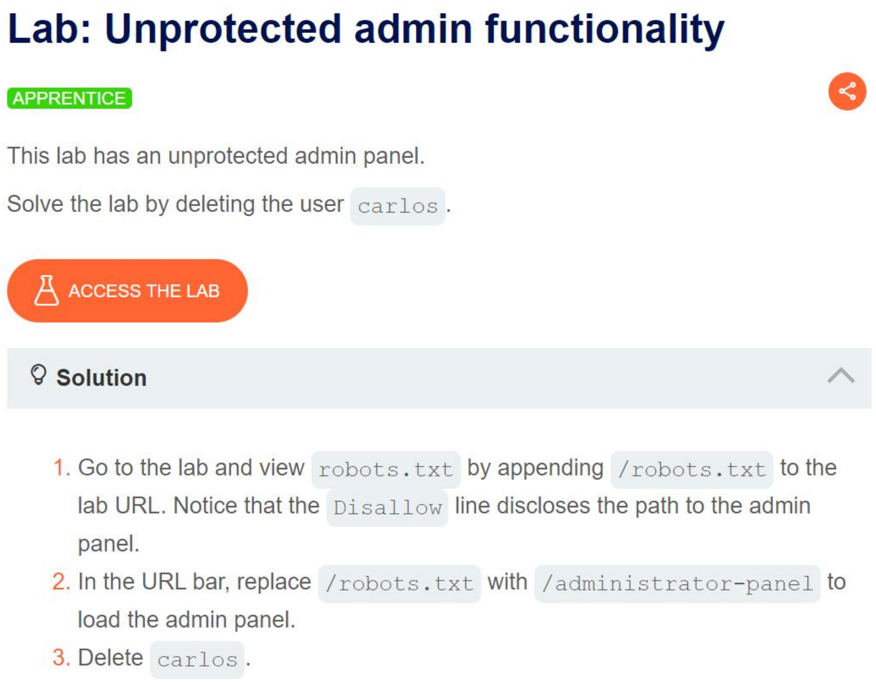
Name : Veekshitha
Reg no: 21BCE8943

ASSIGNMENT - 1

1. BROKEN ACCESS CONTROL (CWE-285)

Description:
Broken access control vulnerabilities occur when an application does not properly enforce restrictions on what authenticated users are allowed to do. This can lead to unauthorized access to certain functionalities or data.

Business Impact:
Exploiting broken access control can result in unauthorized access to sensitive functionality, data exposure, and even the compromise of user accounts. This can lead to data breaches, financial loss, and loss of user trust.



Lab: Unprotected admin functionality

APPRENTICE

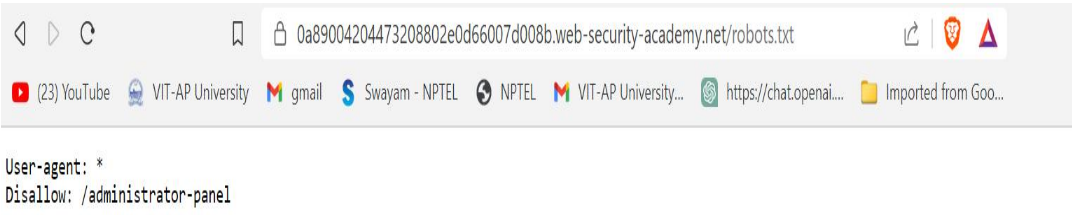
This lab has an unprotected admin panel.

Solve the lab by deleting the user `carlos`.

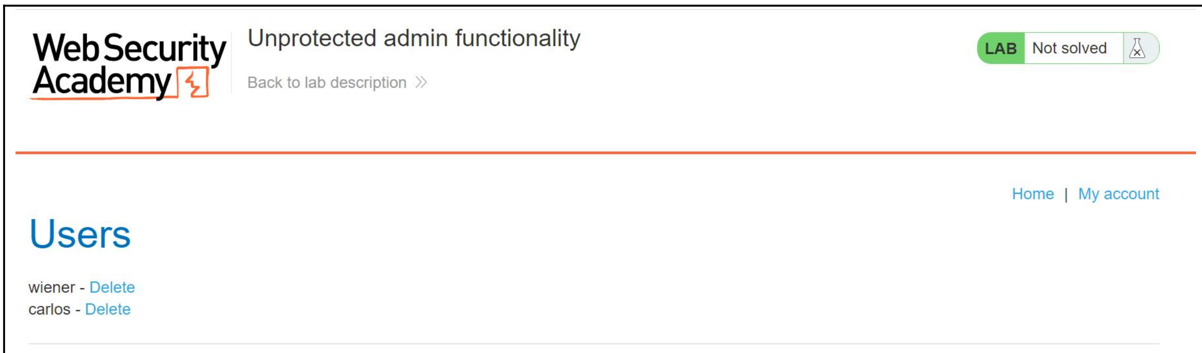
ACCESS THE LAB

Solution

1. Go to the lab and view `robots.txt` by appending `/robots.txt` to the lab URL. Notice that the `Disallow` line discloses the path to the admin panel.
2. In the URL bar, replace `/robots.txt` with `/administrator-panel` to load the admin panel.
3. Delete `carlos`.



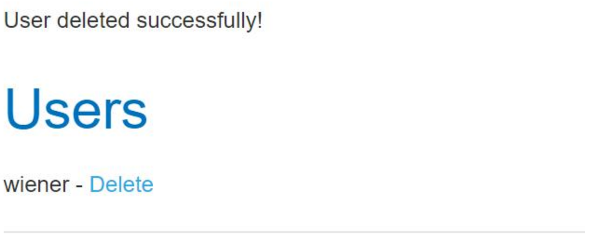
```
User-agent: *
Disallow: /administrator-panel
```



Unprotected admin functionality

Users

wiener - Delete
carlos - Delete



User deleted successfully!

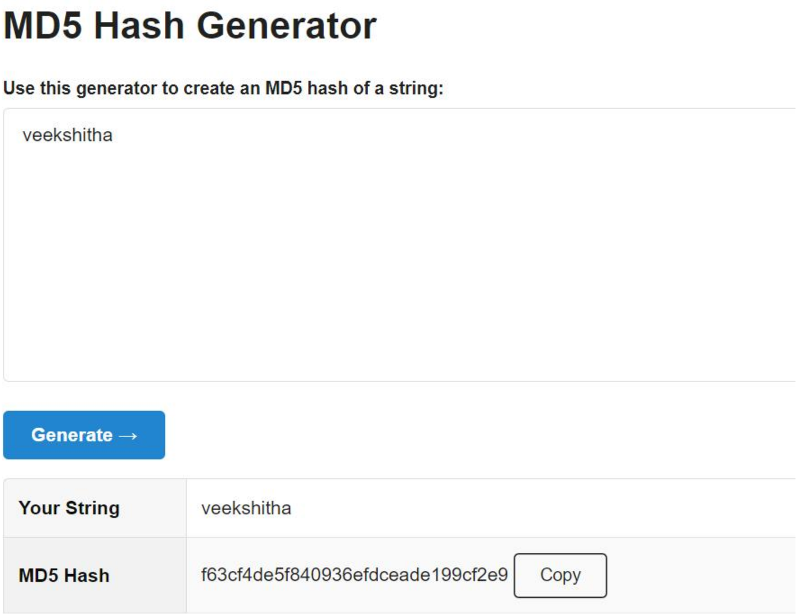
Users

wiener - Delete

2.CRYPTOGRAPHIC FAILURES (CWE-310)

Description:
Cryptographic failures refer to vulnerabilities related to the incorrect use or implementation of cryptographic algorithms. This can lead to weaknesses in data protection and encryption mechanisms.

Business Impact:
Exploiting cryptographic failures can lead to the compromise of sensitive data, including passwords and other confidential information. This can result in data breaches, regulatory non-compliance, and reputational damage.

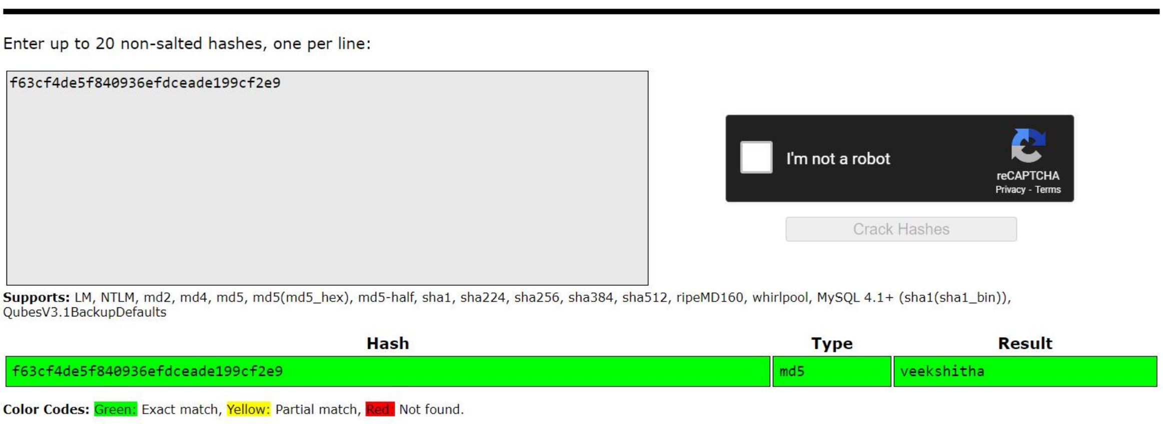


MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

veekshitha

Your String	veekshitha
MD5 Hash	f63cf4de5f840936efdceade199cf2e9


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

```
f63cf4de5f840936efdceade199cf2e9
```

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

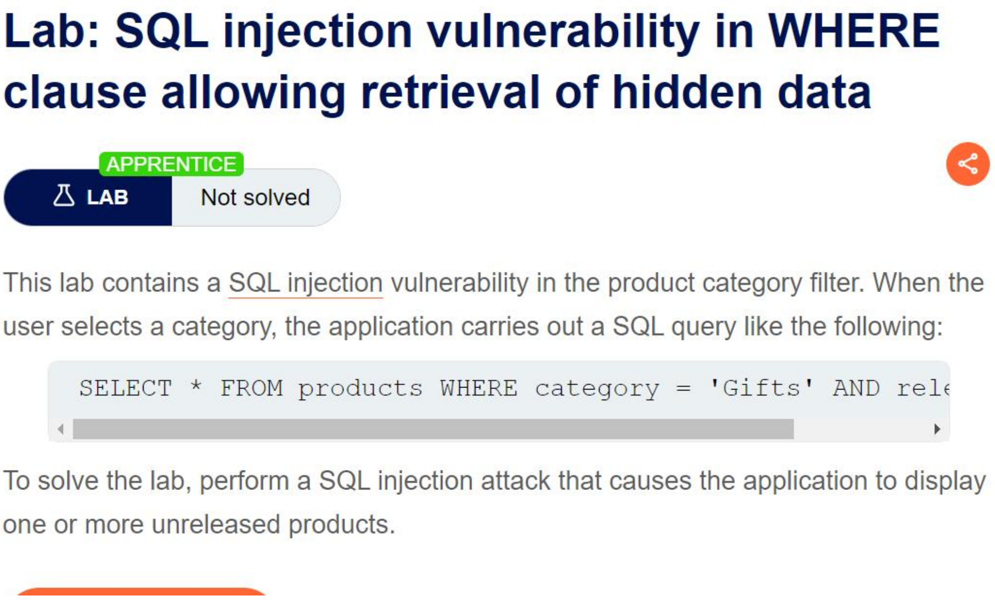
Hash	Type	Result
f63cf4de5f840936efdceade199cf2e9	md5	veekshitha

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

3.INJECTION (CWE-89)

Description:
Injection vulnerabilities occur when untrusted data is inserted into an application and is executed as code. This can allow attackers to manipulate the application's behavior or access unauthorized data.

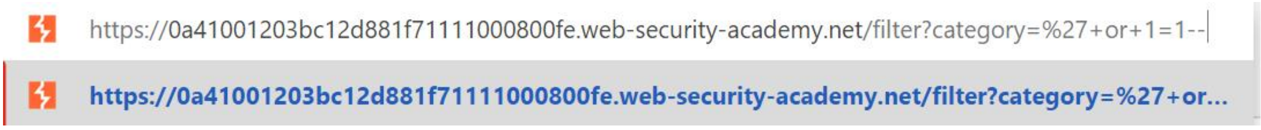
Business Impact:
Successful exploitation of injection vulnerabilities can lead to unauthorized data access, data manipulation, and even remote code execution. This can result in data breaches, system compromise, and financial loss.


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

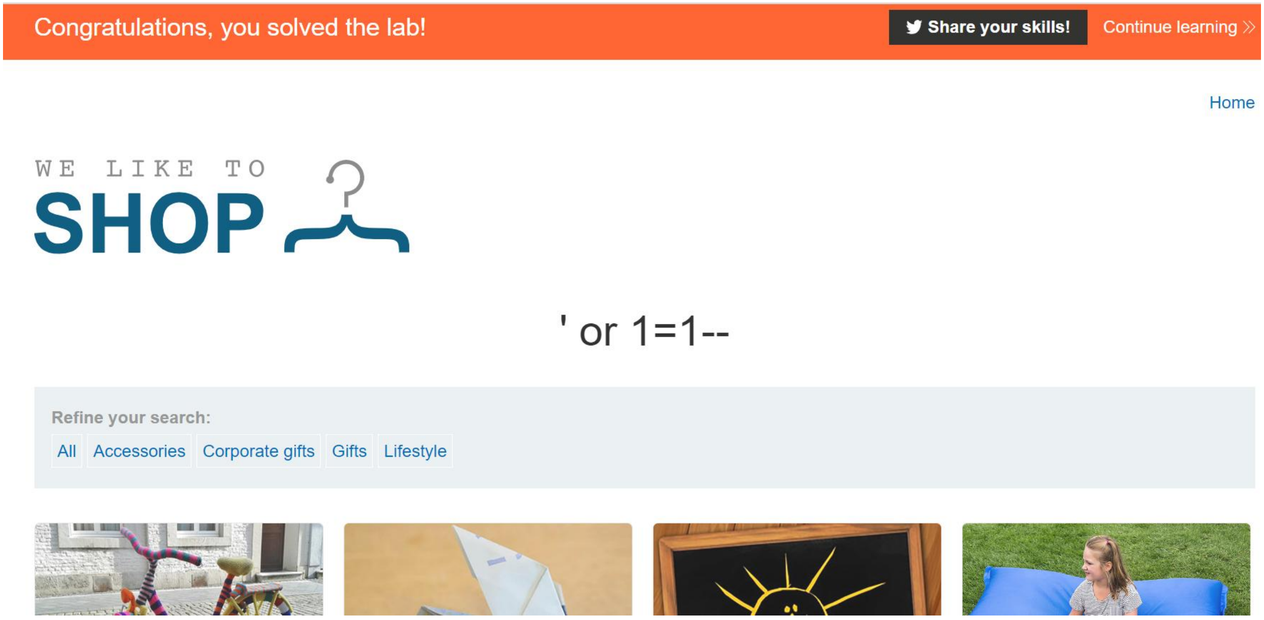
This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

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

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


https://0a41001203bc12d881f71111000800fe.web-security-academy.net/filter?category=%27+or+1=1--

https://0a41001203bc12d881f71111000800fe.web-security-academy.net/filter?category=%27+or...

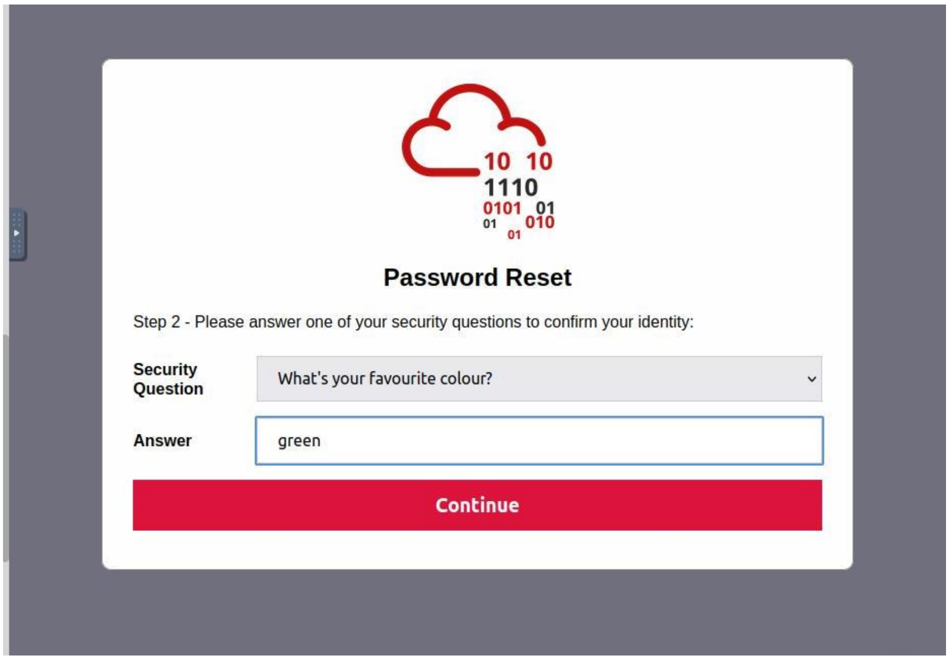

Congratulations, you solved the lab!

' or 1=1--

4.INSECURE DESERIALIZATION (CWE-502)

Description:
Insecure deserialization vulnerabilities happen when an application processes untrusted serialized data. Attackers can exploit this to execute arbitrary code or cause unintended behavior.

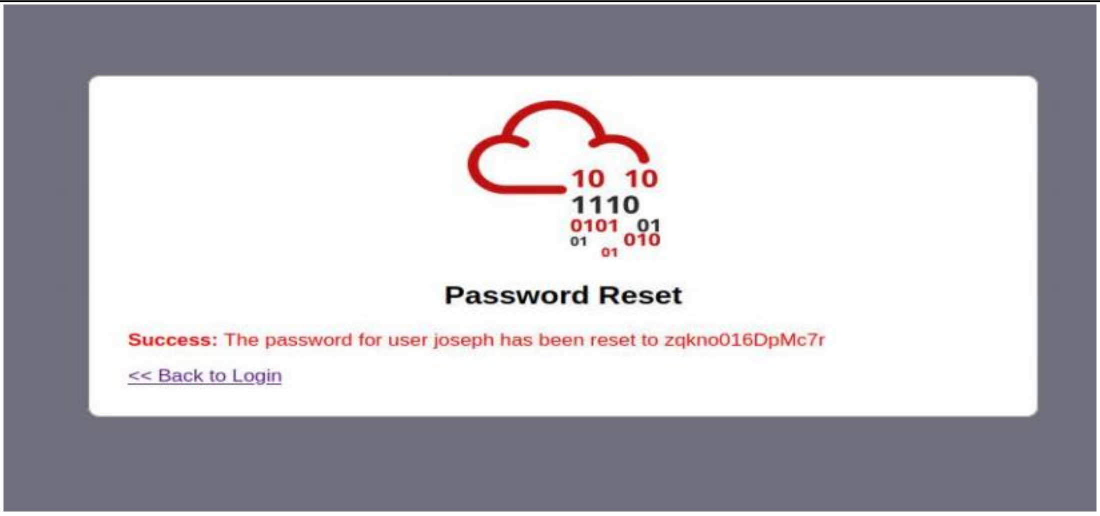
Business Impact:
Exploiting insecure deserialization can lead to remote code execution, denial of service, and potentially full compromise of the application. This can result in system downtime, data loss, and reputational damage.


Password Reset

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

Security Question: What's your favourite colour?

Answer: green



Password Reset

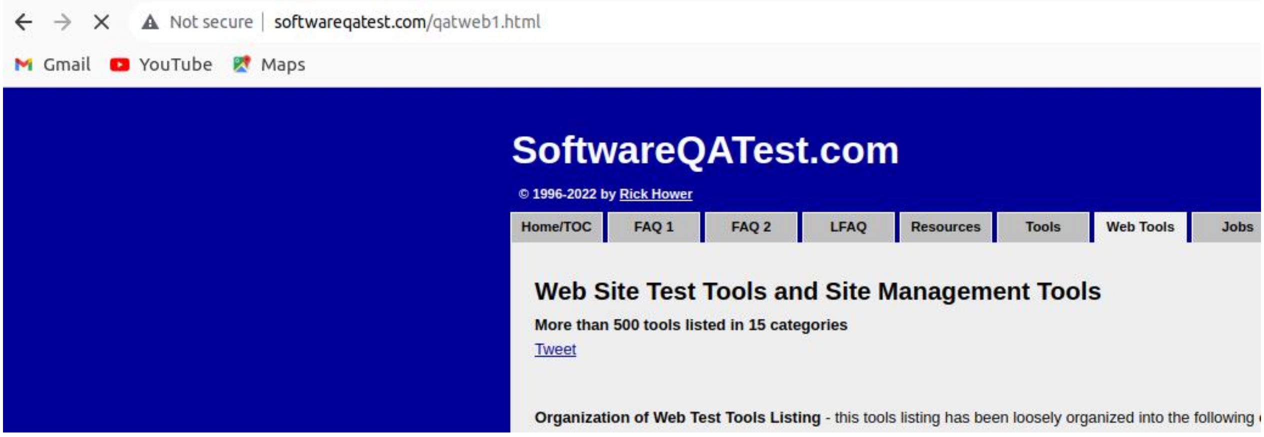
Success: The password for user joseph has been reset to zqkno016DpMc7r

<< Back to Login

5.SECURITY MISCONFIGURATION (CWE-396)

Description:
Security misconfiguration vulnerabilities occur when security settings are not properly configured, leaving potential vulnerabilities exposed. This can include default credentials, unnecessary features, and more.

Business Impact:
Exploiting security misconfigurations can lead to unauthorized access, data exposure, and other security breaches. This can result in data leaks, financial losses, and damage to an organization's reputation.



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