

2021 Edition

OWASP Top 10 Report



The badge is a dark blue rectangular graphic. In the top left corner is the 'Try Hack Me' logo, which includes a cloud icon with binary code and the text 'Try Hack Me' and 'Online Cyber Security Training'. In the top right corner, the text '761438 Rank' and '2 Level' is displayed. The center features the name 'TimeTraveler85' in a large, bold, white font, followed by 'was awarded a badge' in a smaller white font. Below this is a stylized illustration of a blue and yellow bee. At the bottom, the text 'OWASP Top 10' is written in a large, bold, white font, with the tagline 'Understanding every OWASP vulnerability' underneath it. The bottom edge of the badge is decorated with a green, wavy, wireframe pattern.

Try Hack Me
Online Cyber Security Training

TimeTraveler85
was awarded a badge

761438
Rank

2
Level

OWASP Top 10
Understanding every OWASP vulnerability

OWASP Top 10-2021 report

29 October 2024 12:13

Task 1 OWASP Introduction

- i. So OWAPS full form is open web application security protocol that every 3 year publish vulnerabilities list API vulnerabilities
 - Broken Access Control
 - Cryptographic Failures
 - Injection
 - Insecure Design
 - Security Misconfiguration
 - • Vulnerable and Outdated Components
 - Identification and Authentication Failures
 - Software and Data Integrity Failures
 - Security Logging & Monitoring Failures
 - Server-Side Request Forgery (SSRF)

Task 2 Accessing Machines

- a. In this module, we deploy our lab for practice.
- b. We have two methods for this: we can use the TryHackMe virtual box on the website, or use our Kali Linux to establish a connection.
- c. When we successfully deploy the labs, we get a flag to verify the connection.

Task 3 1. Broken Access Control

1. Website pages are protected from visitors; only an admin user can manage the website and modify access credential files. This ensures proper management and protection. However, a website may have broken access control.
2. **Types of Visitors:**
 1. **Regular Visitor**
 - Able to view sensitive information from other users
 - Accessing unauthorized functionality
 2. **Website Visitor**
3. Can only access their own information
4. These types of vulnerabilities allow attackers to bypass authorization, enabling them to view sensitive data and perform malicious activities.

Task 4 Broken Access Control (IDOR Challenge)

1. **Insecure Direct Object Reference (IDOR)**
2. This refers to access control vulnerabilities where users can access resources that do not belong to them.
3. One example is when a user logs into a banking application and successfully authenticates themselves. The application then redirects the user to a different page where they can perform various actions.
4. If the user leaves the session without logging out, they may assume everything is perfectly secure. However, there is a significant problem: an attacker could use the same URL left behind, modify certain parameters, and gain unauthorized access to other users' details.
5. By changing some parameters of the URL, attackers can potentially access other people's credential information.

Task 5: Cryptographic Failures

1. **Cryptographic Failure**
2. Messages are encrypted using cryptographic algorithms to protect them, ensuring only the authorized recipient can access them. If someone without permission misuses cryptographic algorithms to access messages, files, or data, it is called a cryptographic failure.
 - **Encrypting data in transit:** This refers to data transmitted over the internet using cryptographic algorithms. Even if someone captures the packets, they cannot read the data because it is encrypted.
 - **Encrypting data at rest:** This refers to data stored on a server. Even the server owner cannot access your data, as it is protected by encryption. This is known as encrypting data at rest.

Task 6: Cryptographic Failures (Supporting Material 1)

In this section, I will provide practical examples of how to access a database using the terminal.

- ```
file file_name
```

file example.db

2. To learn more about the `.db`` file, we first enter the SQLite terminal using the command:

```
sqlite3 example.db
```

- ```
PRAGMA table_info(table_name);
```

- ```
SELECT * FROM table_name;
```

[illegible]

3. **SQL Injection** - This injection targets database servers. It involves user-controlled

input in SQL queries (typically malformed SQL queries). When the error message is returned by the database server, the attacker analyzes it and gathers information about the database structure.

4. **Command Injection** – This injection occurs in the system command layer, where an attacker executes arbitrary system commands on the application server. This type of attack allows them to gain access to the user's system.
5. **Prevention** – Several techniques to prevent injection attacks:
  - **Using an Allow List** – The input coming from users is first checked against a predefined list (safe list). If the input matches correctly, it is considered safe; otherwise, it is rejected, and an error may be thrown.
  - **Stripping Input** – If the input contains dangerous characters, they are removed before processing.

### Task 10 3.1. Command Injection

- I carefully read this part and understand how bash code run inside
- Then using this knowledge I solve some practice question

Answer the questions below

What strange text file is in the website's root directory?

✓ Correct Answer

How many non-root/non-service/non-daemon users are there?

✓ Correct Answer

What user is this app running as?

✓ Correct Answer

What is the user's shell set as?

✓ Correct Answer

What version of Alpine Linux is running?

✓ Correct Answer 🔍 Hint

### Task 11 4. Insecure Design

- This vulnerability arises from poorly configured and implemented architecture. Sometimes, during testing, the tester disables certain security methods for convenience. When the application moves to the deployment phase, they forget to re-enable these security measures, which results in an insecure vulnerability.
- For example, suppose your application authenticates users using OTP (One-Time Password). During the testing phase, the tester or developer may disable this functionality for ease of testing. However, if this OTP function is not re-enabled before the application is published, it creates an insecure vulnerability.

Answer the questions below

Try to reset Joseph's password. Keep in mind the method used by the site to validate if you are indeed Joseph.

⏪ Complete

What is the value of the flag in Joseph's account?

✓ Correct Answer 🔍 Hint

### Task 12 5. Security Misconfiguration

#### • Security Misconfiguration

Security misconfigurations are distinct from other top 10 vulnerabilities because they occur when security could have been appropriately configured but was not. Even if you download the latest updates, misconfigurations can still leave your application vulnerable.

#### Examples of Security Misconfiguration include:

- Poorly configured permissions on services
- Having unnecessary features enabled, such as unused services
- Default accounts with unchanged passwords

#### Interactive Console Challenge

I went to the provided link, and for the interactive console, I simply changed the URL by adding an extra /console. This gave me a Python prompt, where I solved each question.

Answer the questions below

Navigate to <http://10.10.139.181:86/console> to access the Werkzeug console.

✓ Correct Answer

Use the Werkzeug console to run the following Python code to execute the `ls -ls` command on the server:

```
import os; print(os.popen("ls -ls").read())
```

What is the database file name (the one with the .db extension) in the current directory?

todo.db ✓ Correct Answer

Modify the code to read the contents of the `app.py` file, which contains the application's source code. What is the value of the `secret_flag` variable in the source code?

THM(Just\_a\_tiny\_misconfiguration) ✓ Correct Answer Hint

### Task 13 6. Vulnerable and Outdated Components

- In this type of vulnerability, what happens is that we provide update patches, but for some reason, we forget to apply them. As a result, the vulnerability remains in the application, and attackers can take advantage of these vulnerabilities.
- This is called **Vulnerable and Outdated Components**.

### Task 15 Vulnerable and Outdated Components - Lab

- I carefully read the chapter and solve this challenge
- 

Answer the questions below

What is the content of the `/opt/flag.txt` file?

THM(But\_its\_not\_my\_fault!) ✓ Correct Answer Hint

### Task 16 7. Identification and Authentication Failures

- Authentication and session management are core components of modern web applications.
- Authentication allows users to gain access to web applications by verifying their identities. The most common method to identify a user is through a username and password.
- The server verifies the user, and if the credentials are correct, the server creates session cookies that store the user's behavior and activities.
- If an attacker is able to find flaws in an authentication mechanism, they might successfully gain access to other users' accounts and sensitive information.
- Common Flaws in Authentication:**
  - Brute Force Attack** – If the web application uses a username and password, an attacker can attempt a brute force attack by trying multiple username and password combinations.
  - Use of Weak Credentials** – If the web application allows weak passwords like "password123" or "password1", attackers can easily guess them.
  - Weak Session Cookies** – Session cookies are used to store temporary user data and track activity. Attackers can create their own cookies by guessing predefined values and exploit the vulnerabilities.
- Mitigation Strategies to Avoid These Attacks:**
  - To avoid password guessing, the application should provide a strong password policy.
  - To prevent brute force attacks, set a mechanism to limit password attempts.
  - Implement multi-factor authentication (MFA) to enhance the security of credential data.

### Task 17 Identification and Authentication Failures Practical

- In this chapter I carefully study the content usingthoes information I solve the practice challenge

Answer the questions below

What is the flag that you found in darren's account?

fe86079416a21a3c99937feab8874b667 ✓ Correct Answer

Now try to do the same trick and see if you can log in as `arthur`.

No answer needed ✓ Correct Answer

What is the flag that you found in arthur's account?

d9ac0f7db4da460ac3edeb75d75e16e ✓ Correct Answer

### 18. Software and Data Integrity Failures

- Data Integrity**
- The data we have should not be modified or changed. If the data looks modified, then it lacks integrity.
- In cybersecurity, we often download many applications, so we need to ensure that the file we download is original and has not been modified. To verify this, when we download a file, we also get a hash, such as MD5, SHA-1, or SHA-256. We then recalculate the hash of the downloaded file and compare it to the original hash. If both hashes are equal, it means we have downloaded the original file.
- Types of Data Integrity:**

- ## Task 19 Software Integrity Failures

- Answer the questions below

What is the SHA-256 hash of `https://code.jquery.com/jquery-1.12.4.min.js`?

sEbRLbNQzLpnKIkEdrPv7lOy9C27hHQ+Xp8a4MxAQ<sup>III</sup>

✓ Correct Answer

♀ Hint

## 1. Session Management

- 
- i.
- Header**
- ```
{
  "typ": "JWT",
  "alg": "HS256"
}
```
- Payload**
- ```
{
 "username": "guest",
 "exp": 1656000000
}
```
- Signature**
- ```
...-Bv-X0E[...X.T:..y&ldPM..j\ld
```

- ## **Task 21 9. Security Logging and Monitoring Failures**

1. $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

Answer the questions below

What IP address is the attacker using?

49.99.13.16

✓ Correct Answer

🔍 Hint

What kind of attack is being carried out?

Brute Force

✓ Correct Answer

🔍 Hint

Task 22 10. Server-Side Request Forgery (SSRF)

- When the attacker demands access to files and directories that they do not have permission to access, but the server is not properly configured and allows unauthorized access, this is called **Server Side Request Forgery (SSRF)**.
- Using this information, I was able to solve the challenges.

Answer the questions below

Explore the website. What is the only host allowed to access the admin area?

localhost

✓ Correct Answer

🔍 Hint

Check the "Download Resume" button. Where does the server parameter point to?

secure-file-storage.com

✓ Correct Answer

Using SSRF, make the application send the request to your AttackBox instead of the secure file storage. Are there any API keys in the intercepted request?

Answer format: {xxxxxxxxxxxxxxxxxxxxxxxx}

🔍 Submit

Going the Extra Mile: There's a way to use SSRF to gain access to the site's admin area. Can you find it?

Note: You won't need this flag to progress in the room. You are expected to do some research in order to achieve your goal.

No answer needed

✓ Correct Answer