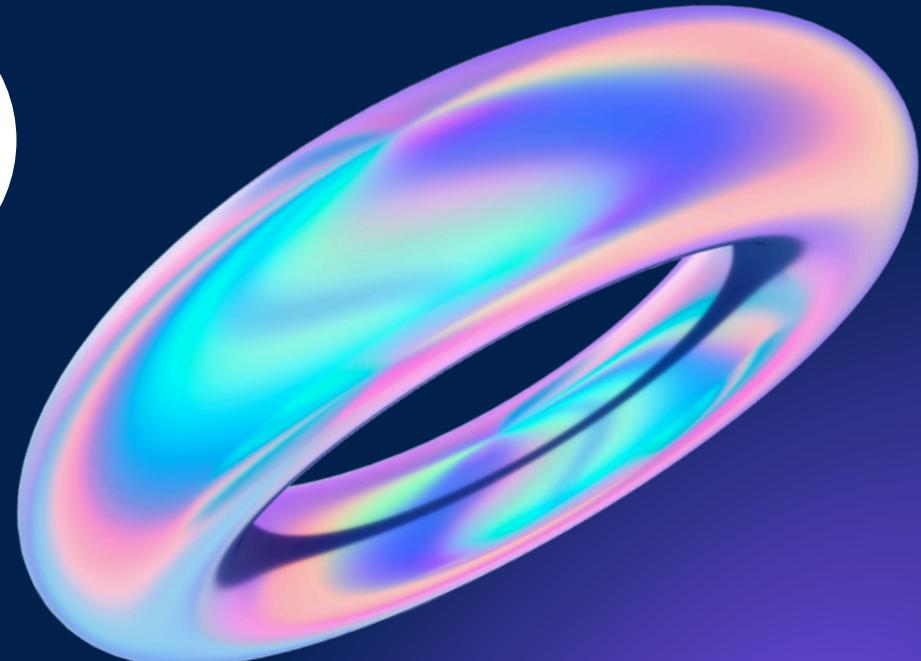


Mercredi 3 Décembre 2025

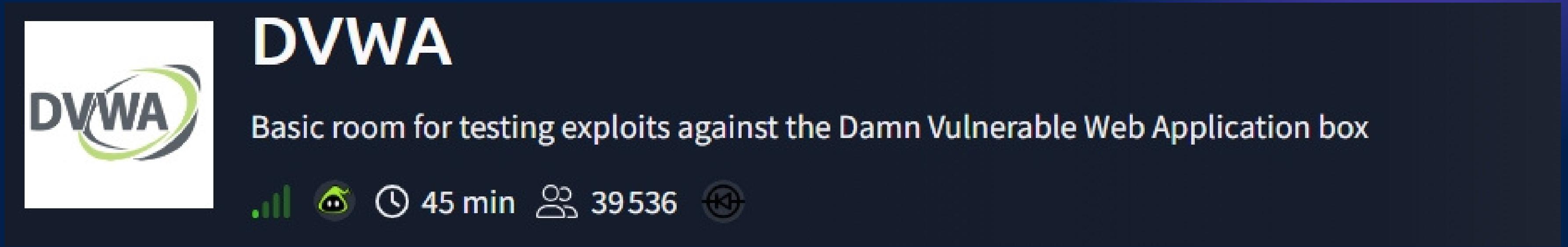


Bienvenue!

SÉANCE 09: DVWA (Partie 1) : File
Inclusion



La room du jour



A screenshot of a TryHackMe room card for the DVWA room. The card has a dark background with a large image of a blue and purple abstract shape on the right. The room name "DVWA" is displayed in large white letters. Below it is a description: "Basic room for testing exploits against the Damn Vulnerable Web Application box". On the left, there is a logo for DVWA featuring the letters in a stylized font inside a green and grey swoosh. To the right of the description are several icons: a signal strength icon, a green alien head icon, a clock icon with "45 min", a people icon with "39536", and a circular icon with a key symbol.

DVWA

Basic room for testing exploits against the Damn Vulnerable Web Application box

45 min 39536

<https://tryhackme.com/room/dvwa>

File inclusion :

Machine potentiellement vulnérable : Applications exécutant des scripts au runtime (ex : php, javascript).

Si mal sécurisé, il peut être possible de contrôler le fichier exécuté sur la cible

LFI : Local File Inclusion

Le fichier est sur la machine cible.

Exemples d'utilisation :

- Récupérer des données sensibles sur la machine cible - Attaque par **directory traversal**
- Exécuter un code injecté par une autre vulnérabilité (ex : File Upload)

RFI : Remote File Inclusion

Le fichier est téléchargé depuis un serveur distant puis exécuté par la machine cible. Exemples d'utilisation :

- Obtenir un reverse shell
- ...

Mais, Souvent une RFI est impossible

DVWA : Damn Vulnerable Web Application

DVWA : Un environnement didactique (sur une VM ou en local)

Trois niveaux de difficulté :
Low / Medium / High
(+Impossible)

Une multitude de vulnérabilités :
-File injection
-Brute force
-File upload
-SQL injection

...



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Navigation menu:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Outils utiles :

Liste de PHP wrapper :

file:// — Accessing local filesystem

http:// — Accessing HTTP(s) URLs

ftp:// — Accessing FTP(s) URLs

php:// — Accessing various I/O streams

data:// — Data (RFC 2397)

glob:// — Find pathnames matching pattern

expect:// — Process Interaction Streams

Encoder un fichier en base 64 avec des wrapper:

php://filter/convert.base64-encode/resource= [Fichier]

Root par défaut d'un serveur web : /var/www/html

Exemple d'attaque par directory traversal :

http://exemple.com/?page=../../../../../../../../etc/passwd

Création d'un serveur python dans le répertoire local:

python -m http.server [port]

Ecouter sur un port :

nc -lvp [port]

Merci et à la semaine prochaine !



La séance sur notre Github:
<https://github.com/CyberMines-Nancy/SEANCES>



@cyber.mines