Technical affairs- IIITDM Kancheepuram

Day - 16

Cybersecurity CTF Hackathon

Date : 16/07/2025

Duration : 24 Hours

Challenge Brief

(We made a website just for the community: https://ctf-platform-mu.vercel.app/

All CTFs, including this one, will be hosted here ~ check it out!)

Many of you want to get into cybersecurity, but don't know where to start. This is a simple CTF, which explores topics such as Ethical Hacking, Web Security, Forensics and Cryptography - which will help you get the feel of what cybersecurity is about.
A CTF (Capture The Flag) is a challenge where a person has to find a hidden string - a "flag", in a vulnerable file/program/website. The aim of this CTF is to introduce absolute beginners to some of the basic methods of analysis to exploit vulnerabilities, which serves as a foundation for the real world.

Objective

Questions can be found here once you create an account with your institute mail ID - https://ctf-platform-mu.vercel.app/

Try to find the flag in each of the 10 questions.

It's not straightforward, but no prior cybersecurity experience is needed to find them. You may use whatever online tools/LLMs you find. Solving these questions will give you the basic competency to attempt future CTFs.

General Guidelines

- *Please register with your institute email account*. We only consider them because it is easier for us to keep track!
- Once you create your account, you can check your dashboard which contains the challenges.
- Click on '*View Challenge*' under any question to get a detailed view, along with a text-box where you can *Submit the Flag*.
- Flags are in the format: **CTF{*<some_alphanumeric_string>*}**

- Some of these questions may contain files which are better accessed on a Linux Machine. A Virtual Machine or WSL works perfectly fine as well.
- Questions have HINTS which make your life easier.
- Try to solve them all, they aren't difficult or time consuming, all you have to do is read the questions carefully. We've made sure they are beginner friendly.
- remember to have fun

Deliverables

- flags

Evaluation Criteria

The CTF has a total of 10 questions (400 points in total). A question can have one of three difficulty levels:

- Easy: 20 points (3 questions)
- Medium: 40 points (4 questions)
- Hard: 60 points (3 questions)

The person with the highest points out of 400 wins.

Addition resources or dataset if required

These might help you with the questions:

- https://www.realisable.co.uk/support/documentation/iman-user-guide/DataConcepts/WebRequestAnatomy.htm
- https://developer.chrome.com/docs/devtools/open/
- https://www.postman.com/what-is-an-api/#history-of-apis
- https://learning.postman.com/docs/sending-requests/requests/
- https://www.ibm.com/docs/en/aix/7.2.0?topic=s-strings-command
- https://www.geeksforgeeks.org/python/substitution-cipher/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://owasp.org/www-community/attacks/xss/
- https://cyberchef.io/

Support

For any queries, reach out to:

Email: cybersec.comm@gmail.com

Name & contact:
Dharun & 9390211782
Neha & 7730065218
Rohan & 7975009603

WhatsApp Community: https://chat.whatsapp.com/CEjhrp1QolYLs1m4OgslMT

Submission

- Submit the flags for each question within the CTF Platform website itself.

Provide Your valuable Feedback Here
https://forms.gle/UC3RbHfAPRZMuAyZ6

Connect Us On Various Platforms
https://linktr.ee/iiitdm.technical

TECH AFFAIRS
IIITDM