Pakistan Cyber Security Challenge (PCC)

This Contest consists of two events: the first is a distributed, wide-area security exercise, whose goal is to test the security skills of the participants (the "**qualification stage**"). From this first exercise PCC management will select a number of finalists to compete in an **on-site contest** where selected teams will compete to solve another set of challenges in a fast-paced setting.

Term of qualification stage: The Contest begins at 14:00:00 (2:00:00 P.M.) PST on ****July 21st 2022**** and ends at 17:00:00 (5:00:00 P.M.) PST on ****July 21 2022**** This CTF is Jeopardy Style CTF.

Rules and Regulations

---

1. Following categories exists for this CTF:
   - Binary Exploitation (PWN)
   - Cryptography
   - Forensics
   - OSINT
   - Malware Analysis
   - Reversing
   - Steganography
   - Web
   - Misc.

   NOTE: For Malware Analysis challenges, please setup an isolated VM (Preferably FLARE VM).

2. Each category would have 3 different difficulty levels
   - Easy – 50-100 points
   - Medium – 150-250 points
   - Hard – 300+ Points.

   NOTE: All challenges are completely solvable, the mentality of **TRY HARDER** may help

3. The time schedule must be **STRITCLY** followed as the flag submission would close after the time is reached.
4. In case of two teams having the same score; although the platform manages it on its own, but just to be sure, the time would be matched and the team that summitted the flag first would be declared the winner.
5. You are **NOT** allowed to share the flags with anyone. If found cheating, the team will be **DISQUALIFIED** on spot.
6. Teams may not interfere with the progress of other Teams, nor with the operation of the Competition's infrastructure. More specifically, attacking the scoring server, other Teams, or machines not explicitly designated as targets will be considered as **cheating** and is **STRICTLY PROHIBITED**. This includes both breaking into such machines, and denying others access to them or the ability to solve problems (for example, by altering a key or ping-flooding). Sharing keys or providing overly-revealing hints with other teams is **cheating**, as is being directly assisted by personnel outside the Team (using tools from the internet is OK; asking people on the internet to help solve the problem is not). Any sort of communication (whether it be WHATSAPP, DISCORD or anything) is stronglyprohibited, if found, the team will be **DISQUALIFIED** on spot.
7. **NO Challenge** requires any sort of brute-forcing, if someone is found brute-forcing, first they'llbe warned and then they will be disqualified (Brute-forcing include use of **Hydra** to crack SSH credentials, use of Gobuster to find a certain subdomain/directory.
8. Answers to problems may not be publicly posted or otherwise shared with anyone outside of your Team members until after the Competition is over.
9. You are solely responsible for keeping your account names and passwords confidential. You are responsible for activity that takes place under your account (including but not limited to activity that may affect your eligibility for prizes). If you believe that your account has been or may be compromised, you must notify management by contacting **info@nccs.pk** (or Discord: https://discord.gg/p2hUjgmvCH) as soon as possible.
10. PCC management reserves the right to verify the identity and eligibility of all Participants and Teams at any time.
11. Competition problems or other content on the PCC site remains the property of NCCS/AirOverFlow. You may not use the PCC CTF 2022 site or any materials on it for any unauthorized purpose.
12. PCC management will determine participation eligibility, declare winners and award prizes in its sole and absolute discretion.

Good Luck!

In case of any query, you may contact us on the following:

Discord: **https://discord.gg/p2hUjgmvCH**
E-Mail: **info@nccs.pk**
Location: **Air University, E-9 Islamabad**