



Format String

“A good old exploit”

The background of the image is a circular emblem. It features a dark blue field with a network of light blue lines and dots, resembling a globe or a data network. In the center is a shield-shaped area containing a stylized map of France composed of small white dots. The shield is flanked by two curved arrows pointing outwards. The entire emblem is set against a dark background with a subtle French flag (blue, white, red) at the bottom. The text "COMCYBER" and "CTF de l'été" is centered over the shield.

COMCYBER

CTF de l'été

LE COMBAT COMMENCE ICI

[Accueil](#)[ExploitMe](#)[Classement](#)

ÉPREUVES 68.4%

1615 POINTS



Cette session est actuellement fermée ! Vous ne pourrez pas valider d'épreuves.

ExploitMe

Validation par flag



Challenge ExploitMe

150 Points

Moyen



Vous avez complété cette épreuve avec succès.

Rétro-ingénierie

Exploitation

31 validations



26 juillet 2020 à 18:37

Description

Dans le cadre d'un CTF organisé pour entraîner les cybercombattants du ministère, une des équipes a mis en place un service sans procéder à son audit préalable.

Auditez leur application et, si vous trouvez une vulnérabilité, nous vous autorisons à l'exploiter.

Exploit

Afficher via `*printf`
des données utilisateur
non contrôlées

Démo

Ressources

- https://owasp.org/www-community/attacks/Format_string_attack
- Write-up du challenge “ExploitMe”:
<https://cotonne.github.io/binary/2020/07/14/format-string.html>