# Lack of Passwords Verification Against a Set of Breached Passwords #PT12068 7

Pending Fix Informational · Server Security Misconfiguration · Aug 22, 2022

(mturk)

### Vulnerability Type

Server Security Misconfiguration > Lack of Password Confirmation

### Description

When setting a new password for a user, the application does not verify user's passwords is leaked or not.
This could make easier brute force attacks on login forms. Verifying a user's password for a complexity is not enough, application should also check for top1000 or top10,000 leaked passwords for applied input.

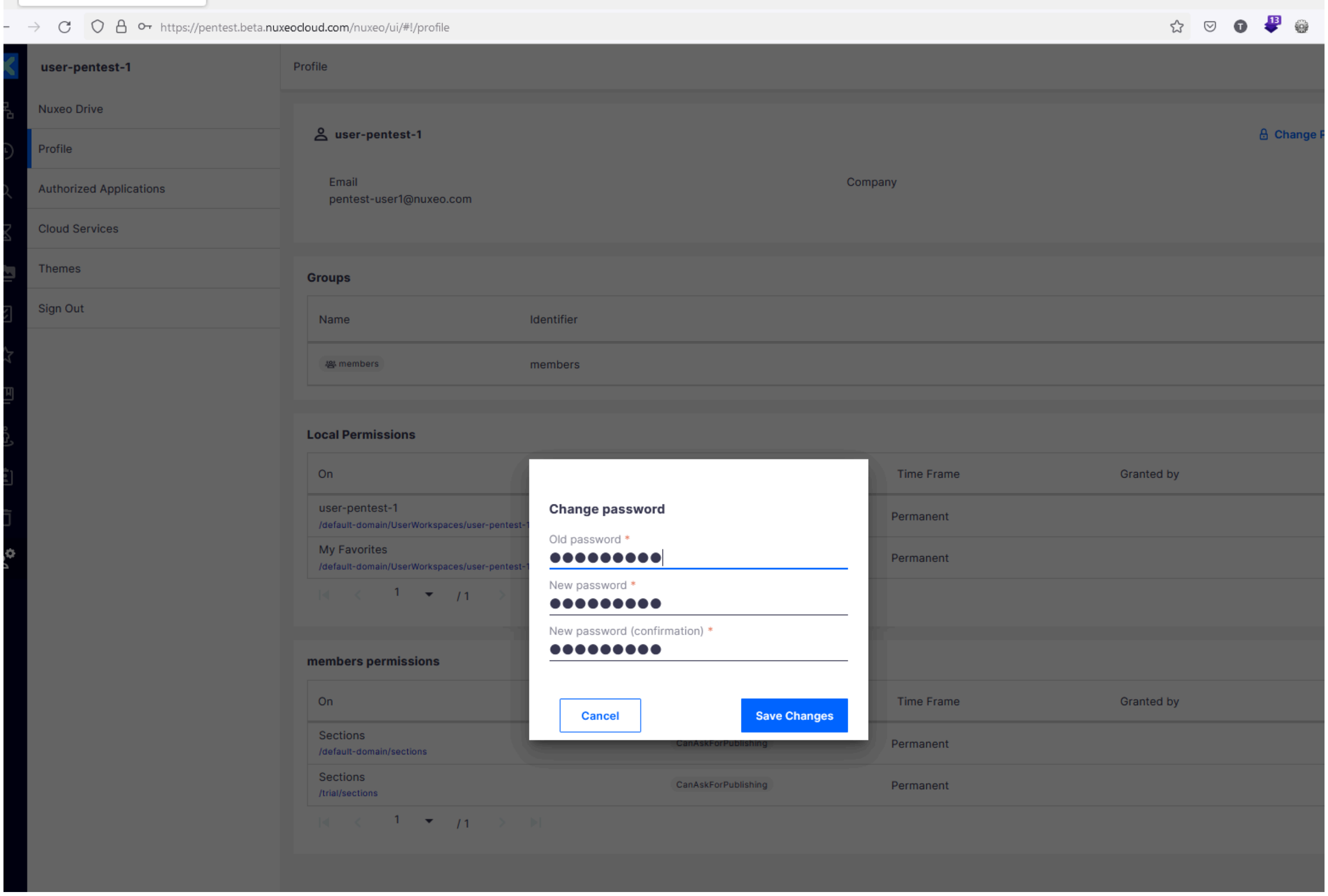
### Affected URL(s)

```
https://pentest.beta.nuxeocloud.com/nuxeo/api/v1/me/changepassword
```

### Proof of Concept

1. Login to application with a privileged user account.
2. Navigate to "User Settings" -> "Profile"
3. Try to change user's password
4. While setting password process give leaked password (here I used one in top1000 leaked passwords: "Password1" this password is got from Seclists, https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top1000.txt),

5. See application will be accepting the given password.
   A screenshot is given below to show password setting process with a leaked one.



user-pentest-1

Email
pentest-user1@nuxeo.com

Company

Groups

| Name | Identifier |
|---|---|
| members | members |

Local Permissions

| On | | Time Frame | Granted by |
|---|---|---|---|
| user-pentest-1<br>/default-domain/UserWorkspaces/user-pentest-1 | | Permanent | |
| My Favorites<br>/default-domain/UserWorkspaces/user-pentest-1 | | Permanent | |

Change password

Old password *
●●●●●●●●●

New password *
●●●●●●●●●

New password (confirmation) *
●●●●●●●●●

members permissions

| On | | Time Frame | Granted by |
|---|---|---|---|
| Sections<br>/default-domain/sections | CanAskForPublishing | Permanent | |
| Sections<br>/trial/sections | CanAskForPublishing | Permanent | |

## Severity

Whole users can be affected with this vulnerability.

## Suggested Fix

1. Allow all characters to be used for passwords to avoid shortening the key space for brute-force guessing.

Prepared for Hyland. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Hyland. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.

2. Do not impose character restrictions such as "must have at least X number of specific character type" in the password. This will shorten the key space for brute-force guessing.
3. Disallow short password lengths. 12 characters is generally considered a good minimum password length.
4. Allow for a large maximum password length.
5. Do not advertise the maximum password length as this will shorten the key space for brute-force guessing.
6. Disallow previous passwords from being used.
7. Disallow the password being the same as the email or username.
8. Check given password for leaked password lists for at least top1000.

**HTTP Request**

```
PUT /nuxeo/api/v1/me/changepassword HTTP/1.1
Host: pentest.beta.nuxeocloud.com
Cookie: JSESSIONID=1E01E0BDD947F281E2A1B80A64D0C984.nuxeo;
AWSALB=bWIbK8TV1av7qINJTPPZQt2AbwonQoV1HTATKlYuxqm0awDZCVoS/
tQS+nfTBJQKO/+/OrSdhIyE3T/
SfB+xrhJKiIoe+S7lV4mirVlgBoFpSGgPqgZehTKsr6ZM;
AWSALBCORS=bWIbK8TV1av7qINJTPPZQt2AbwonQoV1HTATKlYuxqm0awDZCVoS/
tQS+nfTBJQKO/+/OrSdhIyE3T/
SfB+xrhJKiIoe+S7lV4mirVlgBoFpSGgPqgZehTKsr6ZM;
org.jboss.seam.core.TimeZone=Europe/Istanbul;
nuxeo.start.url.fragment=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
Gecko/20100101 Firefox/103.0
Accept: text/plain,application/json, application/json
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 59
Properties: *
Origin: https://pentest.beta.nuxeocloud.com
```

Prepared for Hyland. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Hyland. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.

```
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer: https://pentest.beta.nuxeocloud.com/nuxeo/ui/
Te: trailers
Connection: close

{"oldPassword":"tzzRwDcKzQsszw1","newPassword":"Password1"}
```

Prepared for Hyland. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Hyland. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.