Lack of Throttling on Email Functionality

#PT12068 4

Pending Fix Low · Server Security Misconfiguration · Aug 11, 2022

(pranavhivar...)

Vulnerability Type

Server Security Misconfiguration > No Rate Limiting on Form > Email-Triggering

Description

The software does not properly limit the number or frequency of interactions that it has with an actor, such as the number of incoming requests.

This can allow the actor to perform actions more frequently than expected. The actor could be a human or an automated process such as a virus or bot. This could be used to cause a denial of service, compromise program logic (such as limiting humans to a single vote), or other consequences. For example, an authentication routine might not limit the number of times an attacker can guess a password. Or, a web site might conduct a poll but only expect humans to vote a maximum of once a day.

The email functionality of the https://pentest.beta.nuxeocloud.com/ application is not throttled when a user sends out notification emails. This allows an attacker to use the forge web application to send excessive mail volume to unsuspecting people.

Affected URL(s)

```
https://pentest.beta.nuxeocloud.com/nuxeo/ui/#!/browse/default-domain/sections/test.html?p=permissions
```


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.

Proof of Concept

1] Login into your admin account on https://pentest.beta.nuxeocloud.com
2] Create a file and go to the permissions tab.
Eg. https://pentest.beta.nuxeocloud.com/nuxeo/ui/#!/browse/default-domain/sections/test.html?p=permissions
3] Now, share the file with an external user and add

```
email
```

and your message to be sent in email. Click

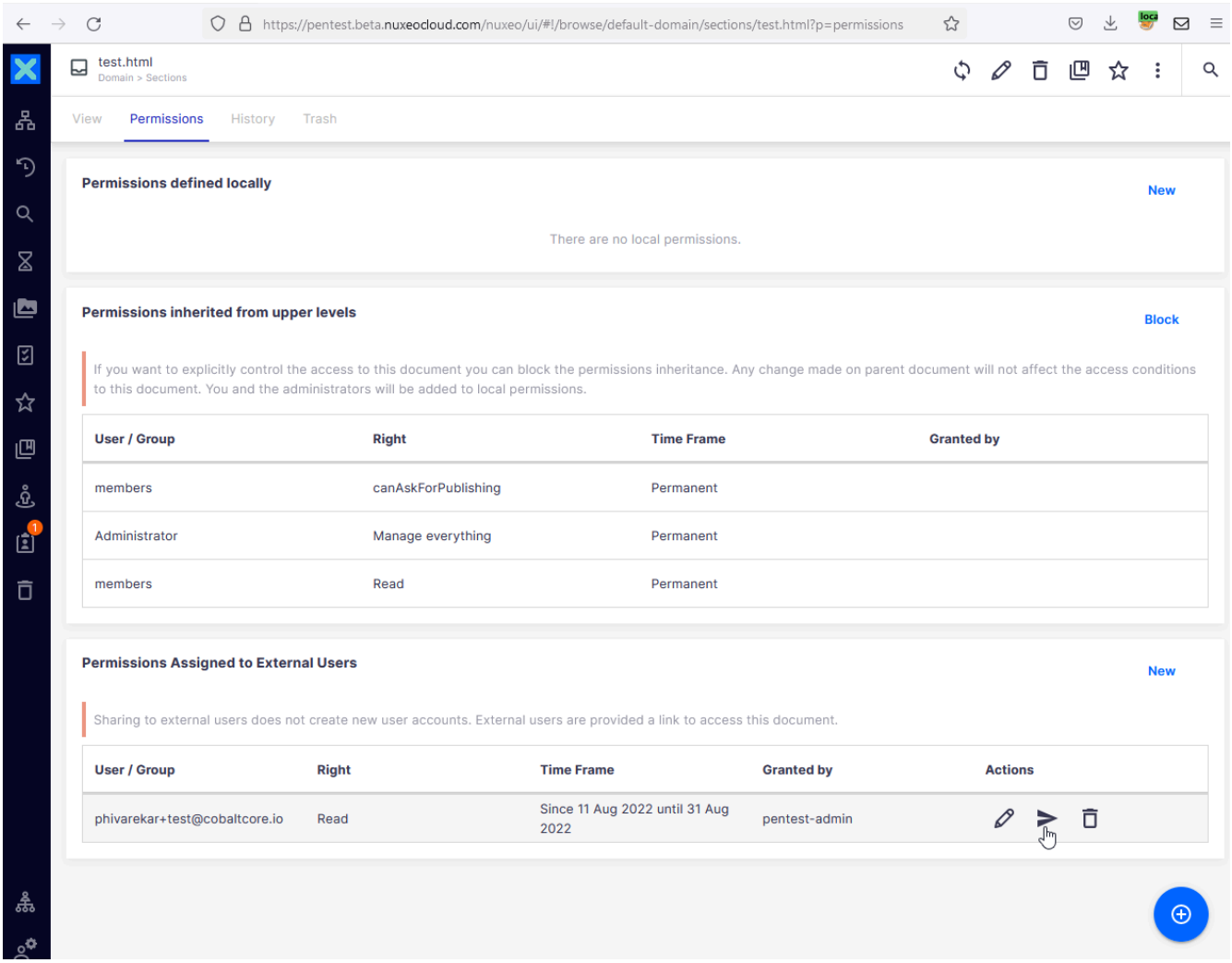
```
Send email
```

from

```
Actions
```

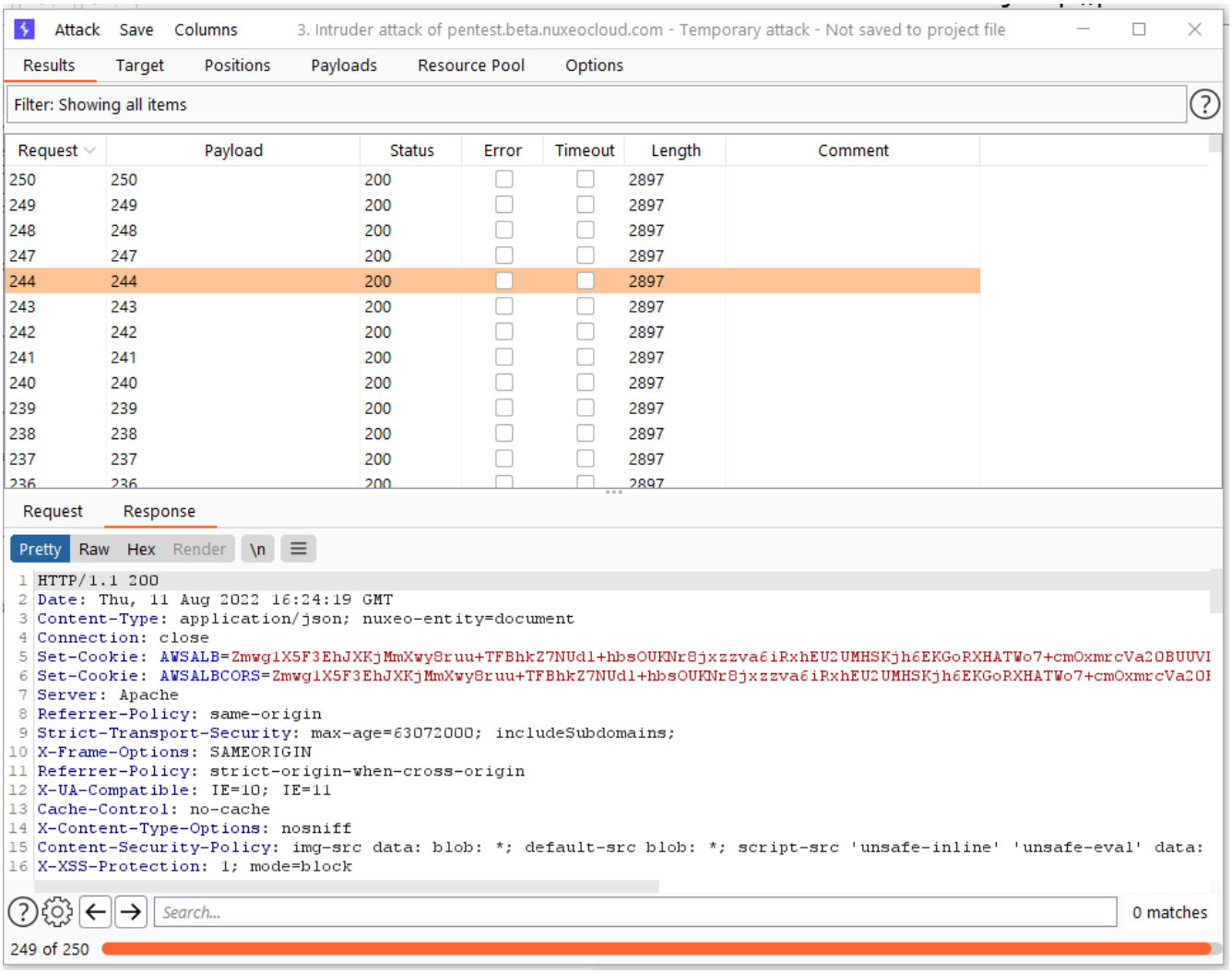
as shown in image.

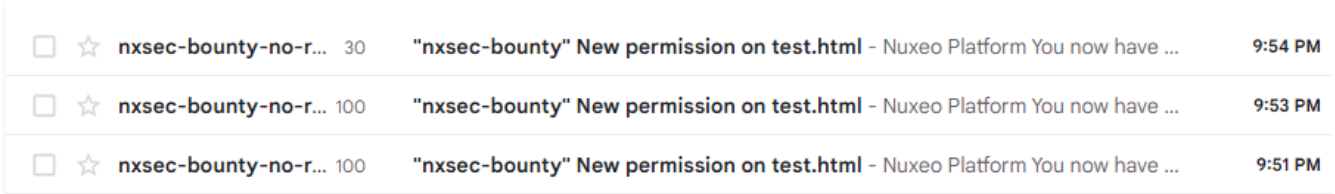
Prepared for Hyland. For informational purposes only and may not be relied upon for any other purpose. To be shared only with permission from Hyland. Cobalt disclaims all liability to any third party arising from this letter. Subject to Cobalt terms of use on https://cobalt.io.



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.

4] Intercept the request and send it to the intruder and repeat for many times. It will send that many emails to the user.





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.

Severity

All users of the application are vulnerable to this vulnerability. An attacker needs a victim's valid email address to flood the victim inbox, which can harm the Nuxeo's reputation.

Suggested Fix

1. Use a
2. `CAPTCHA`
   to limit email triggering requests.
3. Use a rate limit per IP address to throttle the amount of email triggering requests that can be made in a certain amount of time.

HTTP Request

```
POST /nuxeo/api/v1/automation/
Document.SendNotificationEmailForPermission HTTP/1.1
Host: pentest.beta.nuxeocloud.com
Cookie: JSESSIONID=9AD55F87B462297FAA8C94DD3DD2C6A7.nuxeo;
AWSALB=BC79j20BcH4t000zuxMuj7ZmFFWwMI/
u+hjoLDwyn4sys9ZHicNteWi6xAU4s2Bry4HNdk0RaDr0vyrW/
MN0lbLkUnB5Ma4gnf8ho2q8IXLSYcSoeNIHgyvuzz+v;
AWSALBCORS=BC79j20BcH4t000zuxMuj7ZmFFWwMI/
u+hjoLDwyn4sys9ZHicNteWi6xAU4s2Bry4HNdk0RaDr0vyrW/
MN0lbLkUnB5Ma4gnf8ho2q8IXLSYcSoeNIHgyvuzz+v;
org.jboss.seam.core.TimeZone=Asia/Kolkata;
nuxeo.start.url.fragment=!%2Fadmin%2Fanalytics
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
Gecko/20100101 Firefox/103.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```


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.

```
Content-Type: application/json
Content-Length: 171
Properties: *
X-Nxrepository: default
Origin: https://pentest.beta.nuxeocloud.com
Sec-Fetch-Dest: 103
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer: https://pentest.beta.nuxeocloud.com/nuxeo/ui/
Te: trailers
Connection: close

{"params":{"id":"transient/
phivarekar+test@cobaltcore.io:Read:true:pentest-
admin:1660156200000:1661884200000"},"context":{},"input":"d79a30e2-
80e8-466b-b258-4a21fff0b0f0"}
```


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.