Content Spoofing Via Emails #PT12068 3

Pending Fix Low · Server-Side Injection · Aug 11, 2022

(pranavhivar...)

Vulnerability Type

Server-Side Injection > Content Spoofing > Email Hyperlink Injection Based on Email Provider

Description

Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Content spoofing, also referred to as content injection, "arbitrary text injection" or virtual defacement, is an attack targeting a user made possible by an injection vulnerability in a web application. When an application does not properly handle user-supplied data, an attacker can supply content to a web application, typically via a parameter value, that is reflected back to the user. This presents the user with a modified page under the context of the trusted domain.
This attack is typically used as, or in conjunction with, social engineering because the attack is exploiting a code-based vulnerability and a user's trust. As a side note, this attack is widely misunderstood as a kind of bug that brings no impact.

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.

Affected URL(s)

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

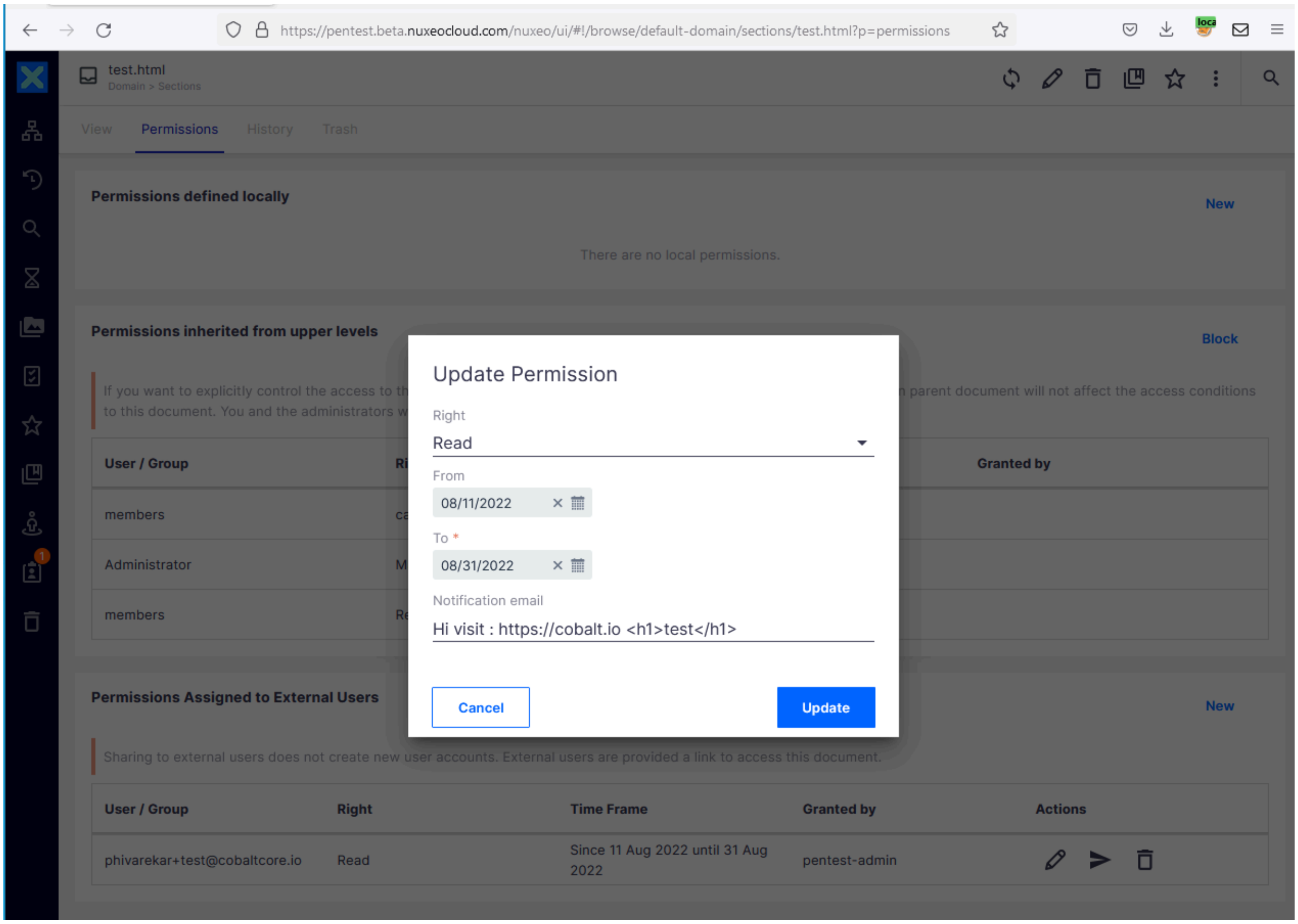
Proof of Concept

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

```
email
```

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.

and your message to be sent in email. Add some links or edit my file as follows:



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

test.html
Domain > Sections

Permissions defined locally New

There are no local permissions.

Permissions inherited from upper levels Block

If you want to explicitly control the access to th… parent document will not affect the access conditions to this document. You and the administrators w…

User / Group	Ri…	Granted by
members	ca…	
Administrator	M…	
members	Re…	

Update Permission

Right
Read

From
08/11/2022

To *
08/31/2022

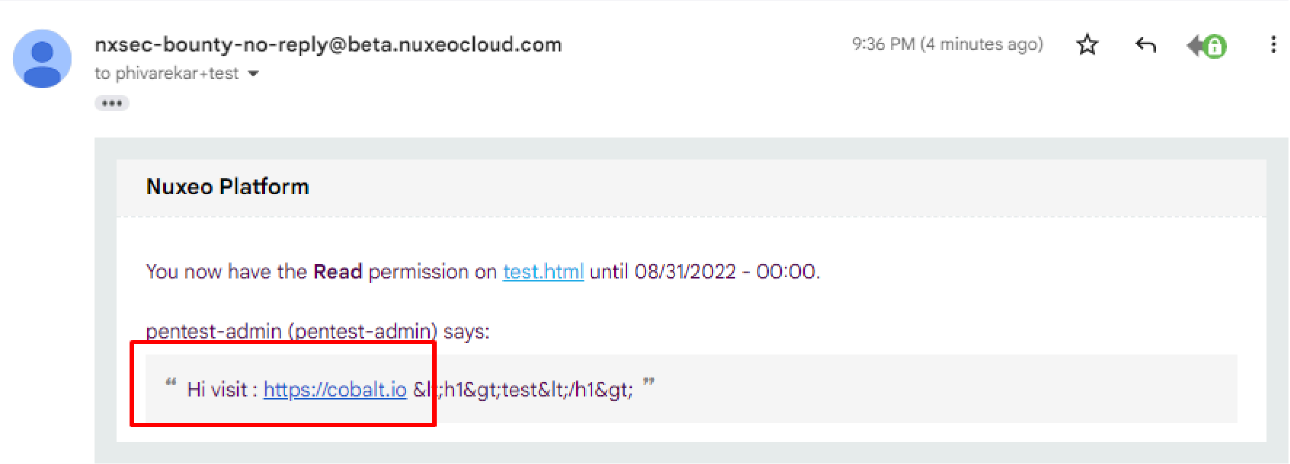
Notification email
Hi visit : https://cobalt.io <h1>test</h1>

Permissions Assigned to External Users New

Sharing to external users does not create new user accounts. External users are provided a link to access this document.

User / Group	Right	Time Frame	Granted by	Actions
phivarekar+test@cobaltcore.io	Read	Since 11 Aug 2022 until 31 Aug 2022	pentest-admin	

4] This triggers an email and link in the email is rendered.



nxsec-bounty-no-reply@beta.nuxeocloud.com
to phivarekar+test

9:36 PM (4 minutes ago)

Nuxeo Platform

You now have the **Read** permission on test.html until 08/31/2022 - 00:00.

pentest-admin (pentest-admin) says:

“ Hi visit : https://cobalt.io <h1>test</h1> ”

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

Attackers can abuse the functionality and can conduct phishing attacks against users of the application.

Suggested Fix

Always ensure that email contents cannot be tampered with. Limit what the user can insert into the email by filtering special characters and limiting the amount of characters that can be inserted. Filter out any URLs as they are often rendered as links by email providers.

HTTP Request

```
POST /nuxeo/api/v1/automation/Document.ReplacePermission HTTP/1.1
Host: pentest.beta.nuxeocloud.com
Cookie: JSESSIONID=9AD55F87B462297FAA8C94DD3DD2C6A7.nuxeo;
AWSALB=YB1oBSln7VT+82FDZXLybAAwC9tv50LkLvIyhacXyvFQ3KtUHFEglU2z293A
cRPozSBPsZVJ7FqSyTuArH2+zEXBBn+e2l/tN7lg/rf1l/0ijHIL+ZUkdeRPKb/a;
AWSALBCORS=YB1oBSln7VT+82FDZXLybAAwC9tv50LkLvIyhacXyvFQ3KtUHFEglU2z
293AcRPozSBPsZVJ7FqSyTuArH2+zEXBBn+e2l/tN7lg/rf1l/0ijHIL+ZUkdeRPKb/
a; 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
Content-Type: application/json
Content-Length: 407
Properties: *
X-Nxrepository: default
Origin: https://pentest.beta.nuxeocloud.com
```

```
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

{"params":{"users":[],"username":"transient/
phivarekar+test@cobaltcore.io","email":null,"permission":"Read","be
gin":"2022-08-11T05:30:00+05:30","end":"2022-08-31T05:30:00+05:30",
"notify":true,"comment":"Hi visit : https://cobalt.io
<h1>test</h1>","id":"transient/
phivarekar+test@cobaltcore.io:Read:true:pentest-
admin:1660156200000:1661884200000"},"context":{},"input":"d79a30e2-
80e8-466b-b258-4a21fff0b0f0"}
```