Improper/Weak Input Sanitizing for HTML/ JavaScript Injection #PT12068 8

Pending Fix Informational · Client-Side Injection · Aug 22, 2022

(mturk)

Vulnerability Type

Client-Side Injection

Description

Client side injection may result in the execution of malicious code on the web application. Typically, this malicious code is provided in the form of data that the threat agent inputs to the web application form through a number of different means. Here, a malicious user can inject HTML/JavaScript code to some web pages. Because of HTML codes are not being executed on web pages vulnerability effect is lowered as result. But HTML codes should not be allowed even if they are not permitted to be executed. In feature a bypass method can be revealed, and attackers can use those techniques to execute their HTML codes on web application.
HTML injection is a type of injection vulnerability that occurs when a user can control an input point and is able to inject arbitrary HTML code into a vulnerable web page. This vulnerability can have many consequences, like disclosure of a user's session cookies that could be used to impersonate the victim, or, more generally, it can allow the attacker to modify the page content seen by the victims.

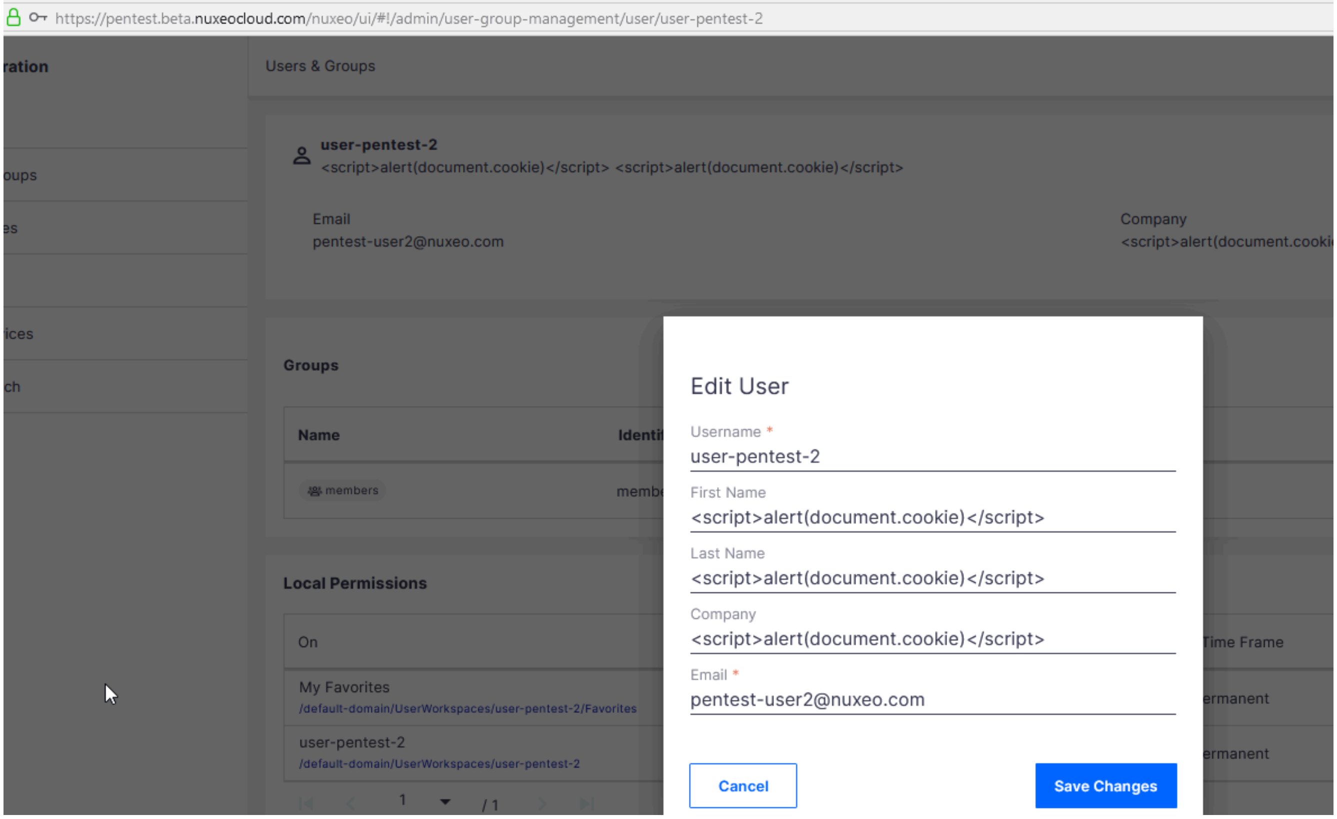
This vulnerability occurs when user input is not correctly sanitized, and the output is not encoded. An injection allows the attacker to send a malicious HTML page to a victim. The targeted browser will not be able to distinguish (trust) legitimate parts from malicious parts of the page, and consequently will parse and execute the whole page in the victim's context.

Affected URL(s)

```
https://pentest.beta.nuxeocloud.com/nuxeo/api/v1/user/{username}
```

Proof of Concept

1. Login to the application with privileged user.
2. While a privileged user edits a user's details from "Administration -> Users & Groups" page, a HTML/JavaScript codes can be placed as user's "First Name", "Last Name", "Company" information.
   A screenshots are given below to show editing process.



user-pentest-2
<script>alert(document.cookie)</script> <script>alert(document.cookie)</script>

Email
pentest-user2@nuxeo.com

Company
<script>alert(document.cooki

My Favorites
/default-domain/UserWorkspaces/user-pentest-2/Favorites

user-pentest-2
/default-domain/UserWorkspaces/user-pentest-2

Edit User

Username *
user-pentest-2

First Name
<script>alert(document.cookie)</script>

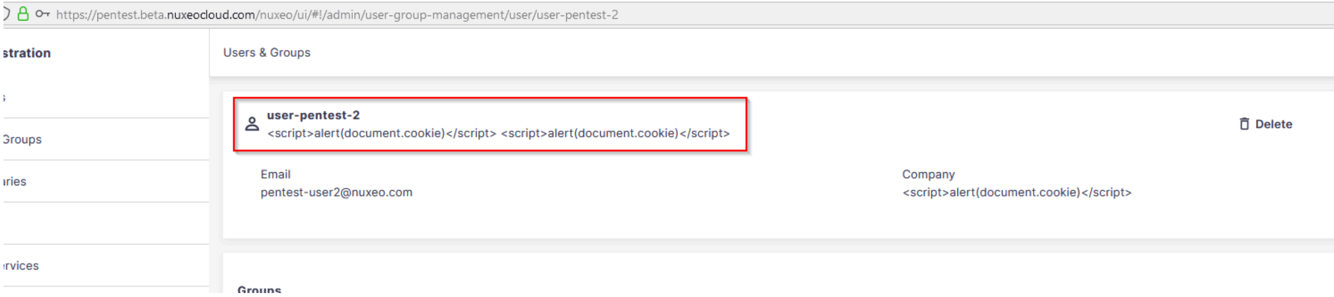
Last Name
<script>alert(document.cookie)</script>

Company
<script>alert(document.cookie)</script>

Email *
pentest-user2@nuxeo.com

A screenshot is given below to show HTML/JavaScript codes can be accepted by application.

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.



https://pentest.beta.nuxeocloud.com/nuxeo/ui/#!/admin/user-group-management/user/user-pentest-2

user-pentest-2
<script>alert(document.cookie)</script> <script>alert(document.cookie)</script>

Email
pentest-user2@nuxeo.com

Company
<script>alert(document.cookie)</script>

Severity

Whole authenticated users can be effected.
Exploitation of this vulnerability is not easy, evasion tecniques required at this stage.
With a successful exploitation, attackers can

- get web application's page content
- run malicious javascript codes on victim's browser.

Suggested Fix

Certain types of HTML tags and JavaScript codes should not be allowed as filename, user profile's info.

HTTP Request

```
PUT /nuxeo/api/v1/user/user-pentest-1 HTTP/1.1
Host: pentest.beta.nuxeocloud.com
Cookie: JSESSIONID=72B1C869D9B064B27F5620EB12D10F93.nuxeo;
AWSALB=gGw1Vn6o217UnFz9qcWMoD9Rl975WKZ5fOwY/7l6Gk334guvH4D89kpG/
8o+/BdAGmKQXB5Kkq7KeUOBEhB7sdguVIANxhtg8q9taFZKW7yY6pdwUAGgxNmWzGsE
; AWSALBCORS=gGw1Vn6o217UnFz9qcWMoD9Rl975WKZ5fOwY/
7l6Gk334guvH4D89kpG/
8o+/BdAGmKQXB5Kkq7KeUOBEhB7sdguVIANxhtg8q9taFZKW7yY6pdwUAGgxNmWzGsE
```

```
; org.jboss.seam.core.TimeZone=Europe/Istanbul;
nuxeo.start.url.fragment=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0)
Gecko/20100101 Firefox/91.0 Waterfox/91.5.0
Accept: text/plain,application/json, application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 360
Properties: *
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

{"entity-type":"user","id":"user-
pentest-2","properties":{"firstName":"","lastName":"<script>alert(d
ocument.cookie)</script>","tenantId":null,"groups":["members"],"com
pany":"","email":"pentest-user2@nuxeo.com","username":"user-
pentest-2"},"extendedGroups":[{"name":"members","label":"members","
url":"group/members"}],"isAdministrator":true,"isAnonymous":false}
```