Login page vulnerable to bruteforce attacks

#PT12068 6

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

(mturk)

Vulnerability Type

Server Security Misconfiguration > No Rate Limiting on Form > Login

Description

A brute force attack can manifest itself in many different ways, but primarily consists in an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response. For the sake of efficiency, an attacker may use a dictionary attack (with or without mutations) or a traditional brute-force attack (with given classes of characters e.g.: alphanumeric, special, case (in)sensitive). Considering a given method, number of tries, efficiency of the system which conducts the attack, and estimated efficiency of the system which is attacked the attacker is able to calculate approximately how long it will take to submit all chosen predetermined values.

Affected URL(s)

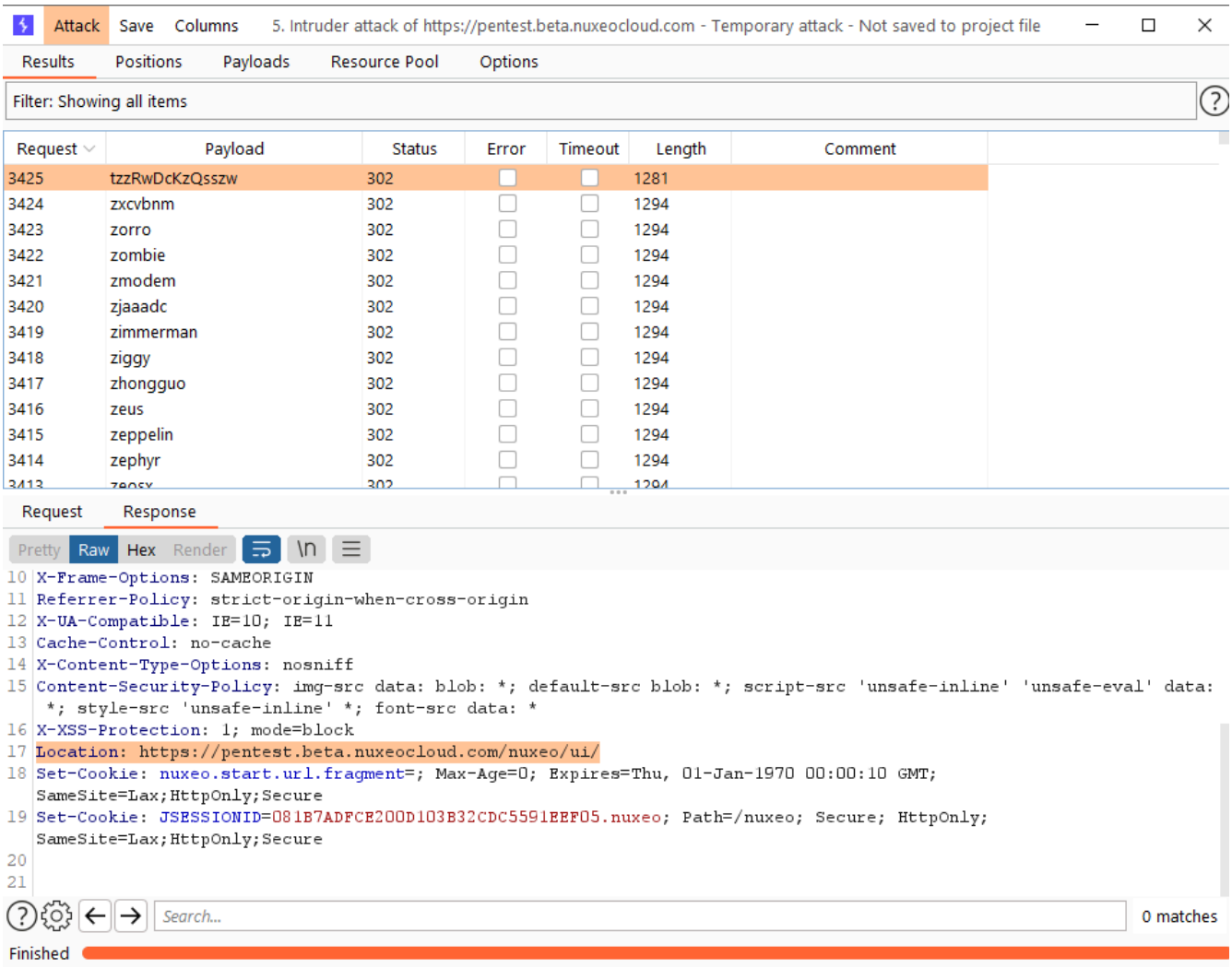
```
https://pentest.beta.nuxeocloud.com/nuxeo/login.jsp
```

Proof of Concept

1. Browse "https://pentest.beta.nuxeocloud.com/nuxeo/login.jsp" URL for login attempt
2. Place a rondom username and password in username and password areas,

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.

3. Use a proxy tool like burpsuite to intercept HTTP traffic.
4. Click "Log in" button on login page.
5. Intercept and send the request to the Intruder module on burpsuite tool.
6. Clear all reference point and place only a reference on "password" parameter.
7. On Payloads tab, use wordlist
8. Start attack and you will realize that login form is vulnerable to the brute force attack.
   A screenshot is given below to show 3425 times login attempts.



Severity

Whole users can be affected by this vulnerability.

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.

Suggested Fix

- Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks.
- Do not ship or deploy with any default credentials, particularly for admin users.
- Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords.
- Align password length, complexity and rotation policies with NIST 800-63 B's guidelines in section 5.1.1 for Memorized Secrets or other modern, evidence based password policies.
- Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes.
- Limit or increasingly delay failed login attempts. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.
- Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL, be securely stored and invalidated after logout, idle, and absolute timeouts.

HTTP Request

```
POST /nuxeo/startup HTTP/1.1
Host: pentest.beta.nuxeocloud.com
Cookie: JSESSIONID=AF71EC05F11890E6C29EE68795526BC1.nuxeo;
AWSALB=vlVM8OJtPstmPZteNWqz0wzKNtF9O6VAzrnheneyonNA2cOE2lhayzQKaFYx
zftqFkDbCXpOSZOqieP2F0bgxNmr79mFyo6WKvCVQvVcvQNJIdxoLoT/MgKEjXv2;
AWSALBCORS=vlVM8OJtPstmPZteNWqz0wzKNtF9O6VAzrnheneyonNA2cOE2lhayzQK
aFYxzftqFkDbCXpOSZOqieP2F0bgxNmr79mFyo6WKvCVQvVcvQNJIdxoLoT/
MgKEjXv2; 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
```


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.

```
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://pentest.beta.nuxeocloud.com/nuxeo/
login.jsp?requestedUrl=ui%2F
Content-Type: application/x-www-form-urlencoded
Content-Length: 143
Origin: https://pentest.beta.nuxeocloud.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

user_name=user-
pentest-1&user_password=tzzRwDcKzQsszw1&language=en&requestedUrl=ui
%2F&forceAnonymousLogin=&form_submitted_marker=&Submit=Log+In
```


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.