

**ID: 1**

**TITLE:** User data are not encrypted in LinkedIn API

**DESCRIPTION:** Using the "Login to account" functionality using the LinkedIn profile, the login and password data from the user profile are transmitted in a publicly accessible form

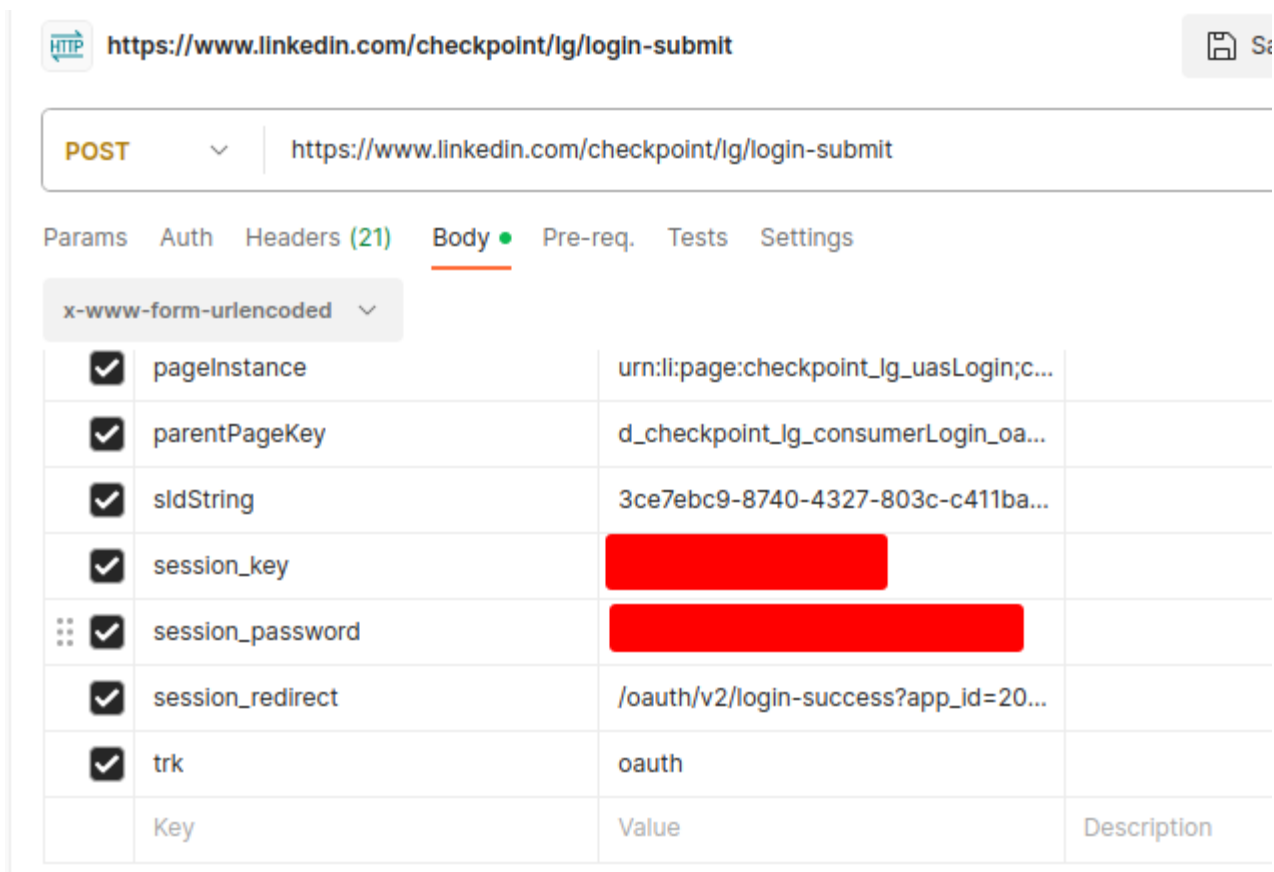
**STR:**

1. Use "Sign Up" or "Login" functionality using LinkedIn profile (on any resource, where it possible)
2. Use browser DevTools (or Postman Interceptor) and find request with method "POST" and URL:  
<https://www.linkedin.com/checkpoint/lg/login-submit>
3. Find "session\_key" and "session\_password" headers

**EXP:** Login and password from your LinkedIn account hidden or encrypted

**ACR:** NO encryption. Login and password are visible

**Environment:** xUbuntu 22.04, Chrome 115



The screenshot shows a web browser window with the URL <https://www.linkedin.com/checkpoint/lg/login-submit>. The browser's developer tools are open, displaying the network tab. A POST request to the same URL is selected. The 'Body' tab is active, showing the request body in 'x-www-form-urlencoded' format. The body contains several parameters, with 'session\_key' and 'session\_password' redacted with black boxes.

Key	Value	Description
<input checked="" type="checkbox"/> pageInstance	urn:li:page:checkpoint_lg_uasLogin;c...	
<input checked="" type="checkbox"/> parentPageKey	d_checkpoint_lg_consumerLogin_oa...	
<input checked="" type="checkbox"/> sldString	3ce7ebc9-8740-4327-803c-c411ba...	
<input checked="" type="checkbox"/> session_key	[REDACTED]	
<input checked="" type="checkbox"/> session_password	[REDACTED]	
<input checked="" type="checkbox"/> session_redirect	/oauth/v2/login-success?app_id=20...	
<input checked="" type="checkbox"/> trk	oauth	