

## 1.1 Cleartext Submission of Password

Here is the process:

- To capture a login request using Burp Suite, follow these detailed steps. Begin by accessing the URL <https://api.iob.in> in your browser. Next, you need to configure the browser's proxy settings to route traffic through Burp Suite. To do this, go to the browser's proxy settings and set the address to 127.0.0.1 with the port number 8080, then save these settings.
- After configuring the browser, open the Burp Suite application. Within Burp Suite, navigate to the Proxy tab and select Options. Here, click on the "Add" button to create a new proxy listener. In the dialog that appears, set the port to 8080 and the IP address to 127.0.0.1, then save these changes.
- Next, go to the Intercept tab within Burp Suite and ensure that intercept mode is turned on. This mode allows Burp Suite to capture and display the HTTP requests sent from your browser.
- With these settings in place, return to your browser and navigate to the web application where you need to provide your login details. Enter the required information and click the sign-in button. Because intercept mode is enabled, Burp Suite will capture the login request, allowing you to inspect and analyze the details of the request.
- By following these steps, you can effectively capture and analyze the login request using Burp Suite, which is useful for various security testing purposes



```
Request to https://api.iob.in:443 [202.54.204.229]
Forward Drop Intercept is on Action Open Browser
Inspector HTTP/1.1
Pretty Raw Hex
POST /user/login HTTP/1.1
Host: api.iob.in
Cookie: portal_web=1703934549.464.26.4447261b7a84c6aaaf064576eca883c32ba21ff; SSES876433e58e180d3be0fc76fa87023c6b5 =E2hk59P6b6h85u42Cfc69i154gA05s0VvWkTFpY91y1VegfmQ
Content-Length: 215
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A_Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://api.iob.in
Dat: 1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://api.iob.in/user/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
registry_url=%2Fconsumer-api%2Fuser-registries%2F6b70a45-3734-40be-9981-4e82401f1c00 &name=mathish&pass=mathish440123 &op=SignIn&form_build_id=
form-pSjT50PEIIN110x002w56fhwmm0J0CjtInC66aV8g &form_id=user_login_form
```