Session Hijacking Attempt via Cookie Replay on Fiver

Contents

Executive Summary

This task evaluated the resilience of Fiverr's session management against cookie-based session hijacking attacks. By capturing and replaying valid session cookies from an authenticated user account, we aimed to impersonate the user on another browser instance. The objective was to determine whether Fiverr binds sessions solely to cookies or also considers additional context like IP address or device fingerprinting. Our test concluded that Fiverr's session management effectively prevents hijacking via cookie replay alone, showcasing robust security.

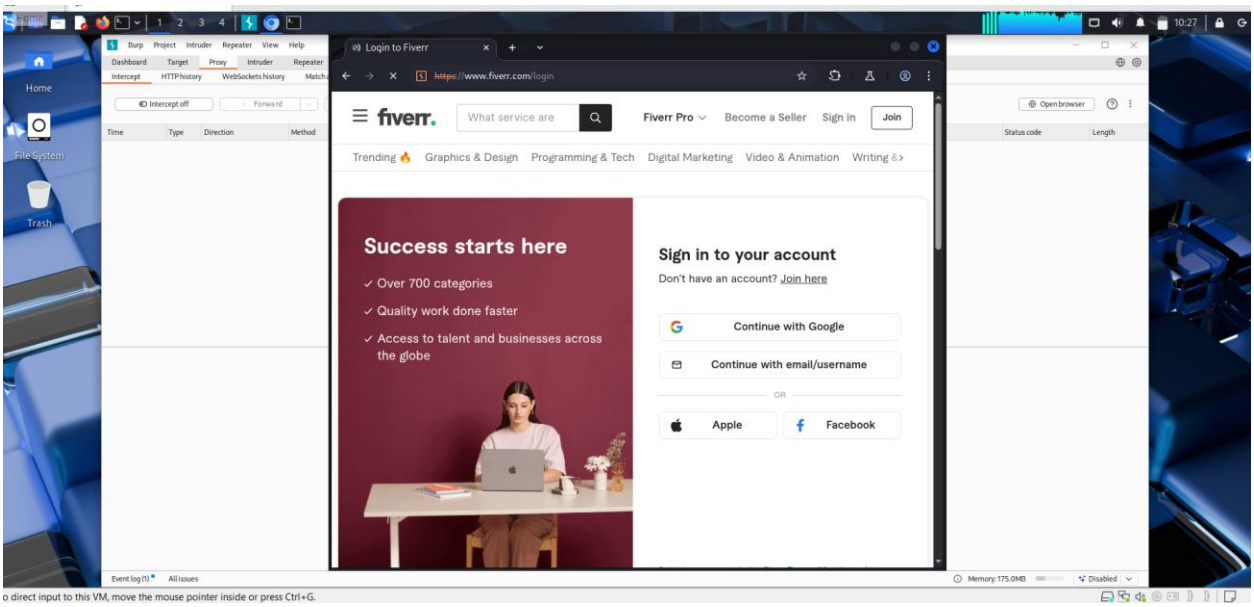
Introduction

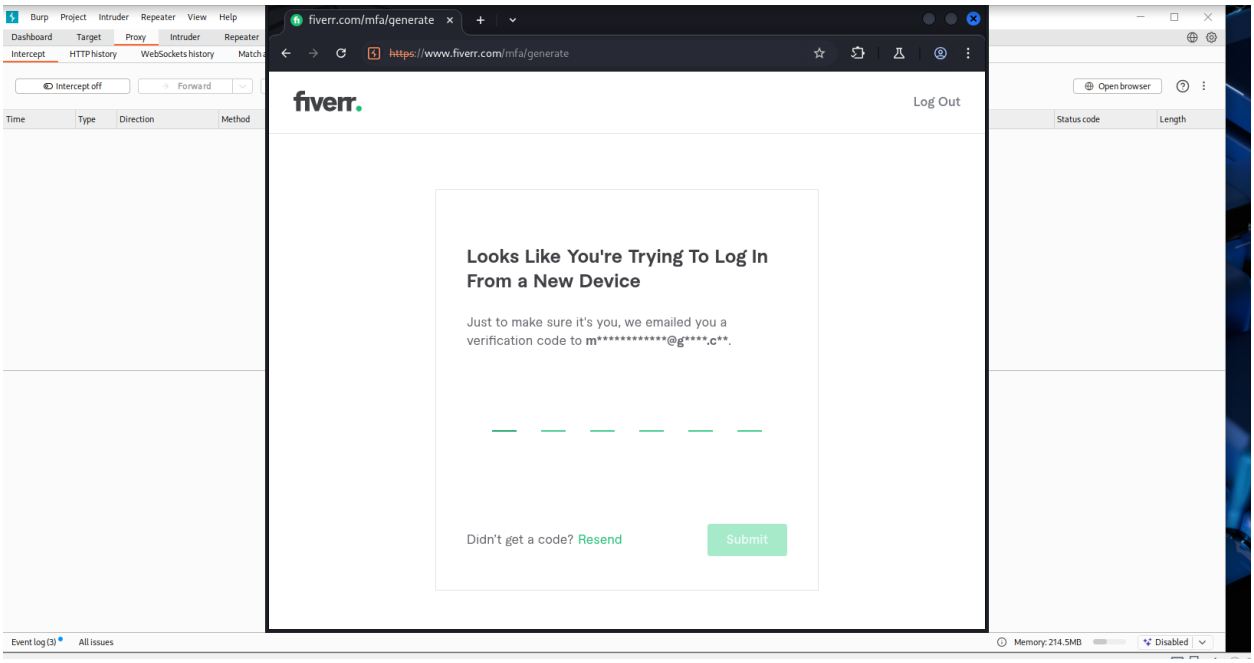
Session hijacking remains a critical threat in web security, allowing attackers to impersonate legitimate users by reusing stolen session cookies. This task involved manually capturing authenticated cookies from a valid Fiverr login and replaying them through Burp Suite to simulate a session hijack. The experiment tested whether the application solely relies on session cookies for authentication or leverages additional context, thus evaluating the effectiveness of Fiverr's session management mechanisms.OWASP ZAP: Used to intercept and analyze login traffic to Instagram.

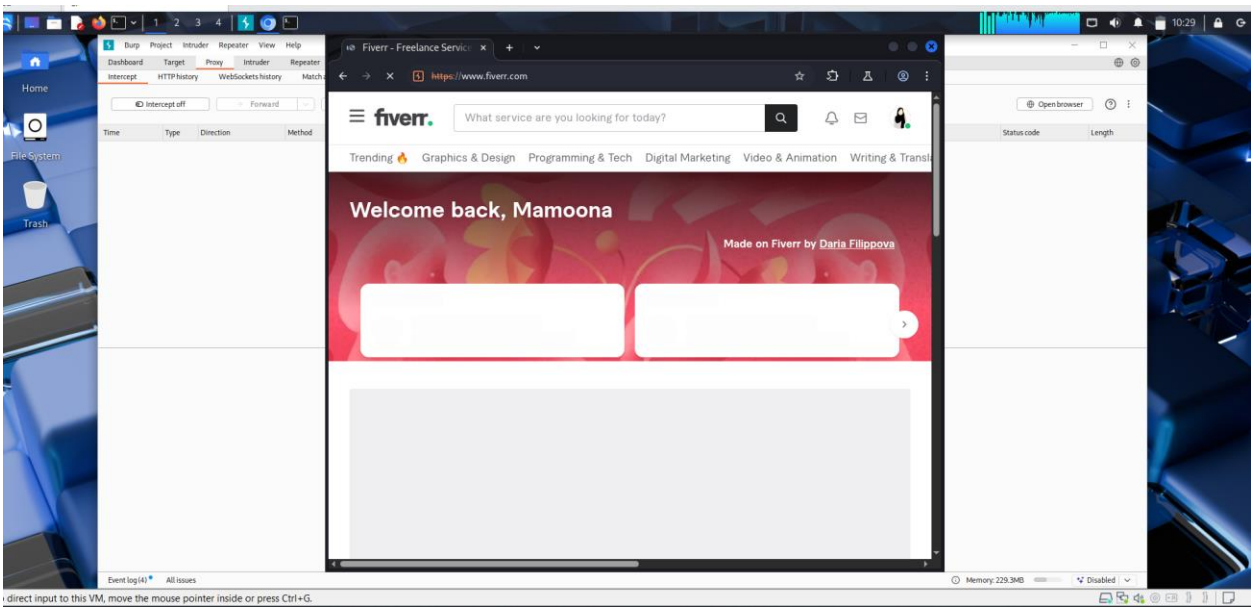
Task Details and Working

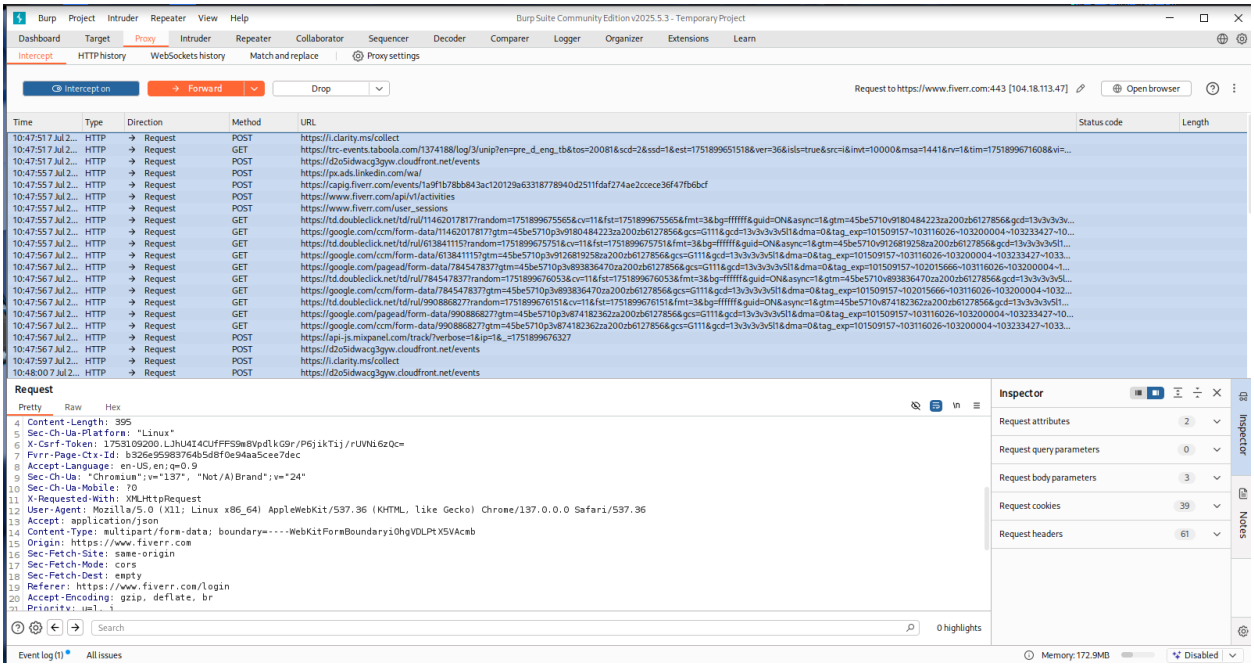
Capturing Cookies

- Intercepted the HTTP POST request to /user_sessions while logging in with the first account.

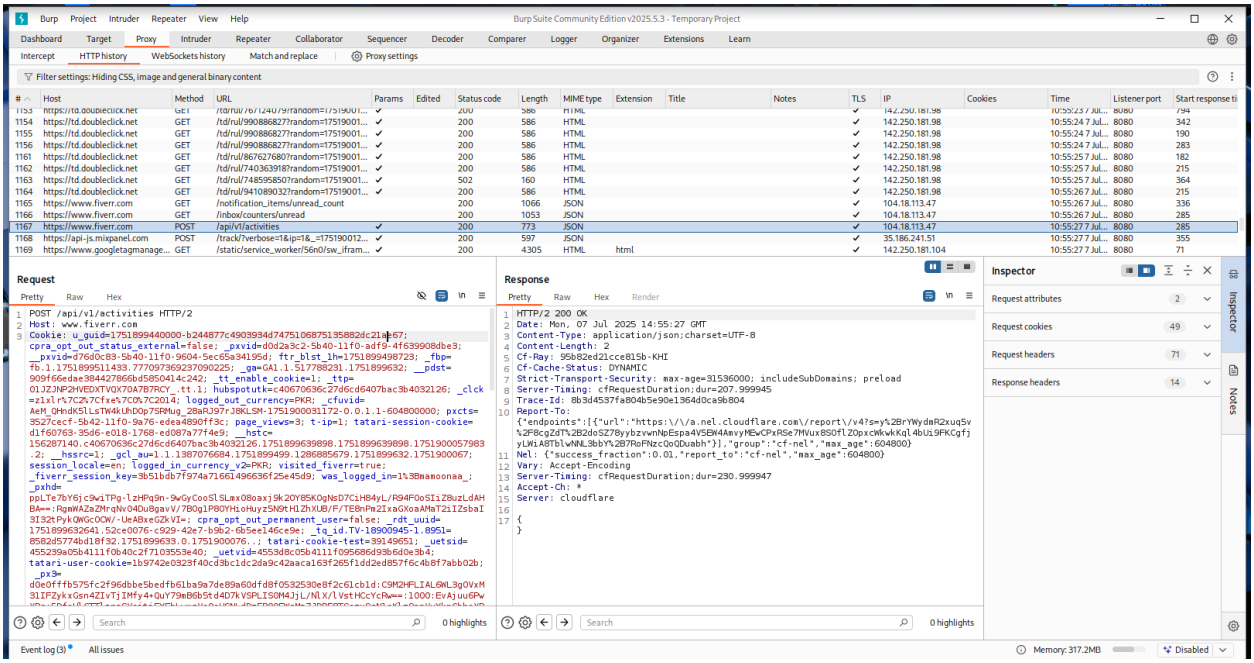

Login to Fiverr
https://www.fiverr.com/login
fiverr.
What service are
Fiverr Pro
Become a Seller
Sign in
Join
Trending
Graphics & Design
Programming & Tech
Digital Marketing
Video & Animation
Writing &
Success starts here
Over 700 categories
Quality work done faster
Access to talent and businesses across the globe
Sign in to your account
Don't have an account? Join here
Continue with Google
Continue with email/username
OR
Apple
Facebook


fiverr.com/mfa/generate
https://www.fiverr.com/mfa/generate
fiverr.
Log Out
Looks Like You're Trying To Log In From a New Device
Just to make sure it's you, we emailed you a verification code to m**********@g****.c**.
Didn't get a code? Resend
Submit



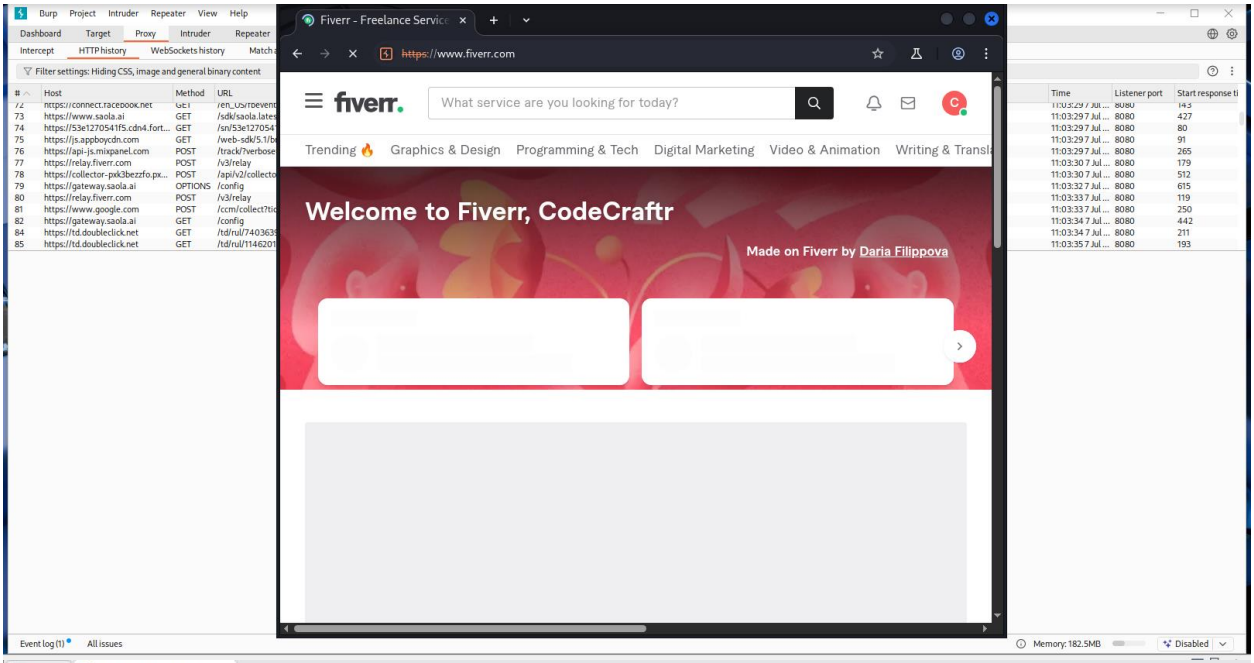


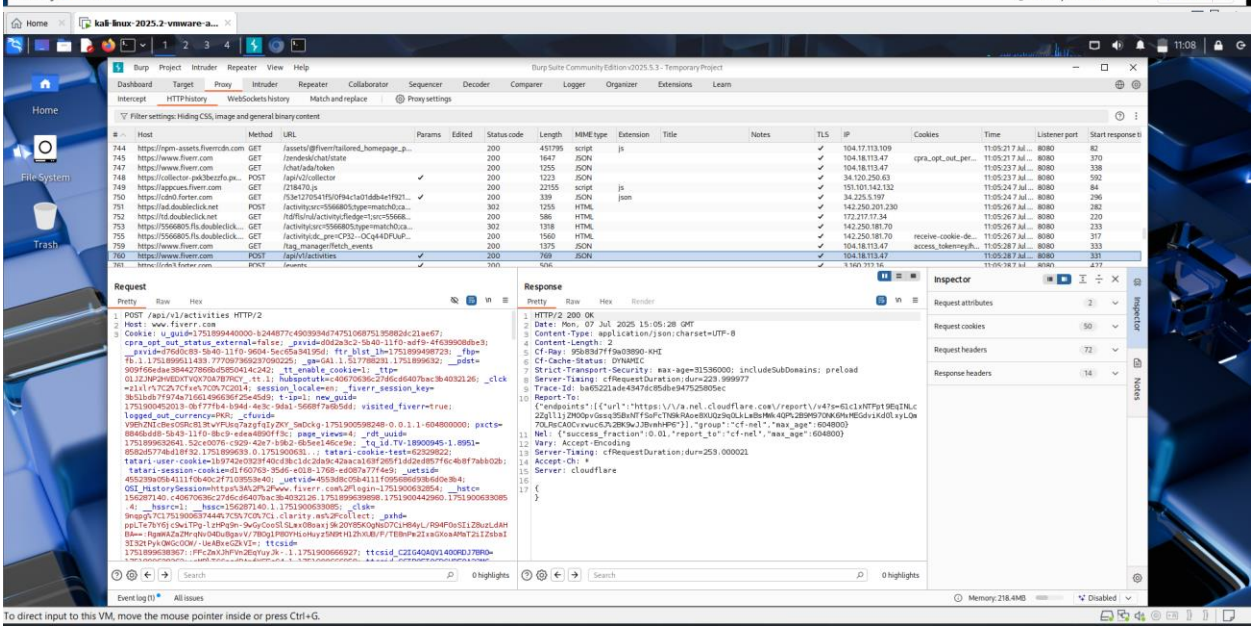
- Saved the Cookie header containing session-related tokens (e.g., u_guid, fiverr_session_key, access_token).

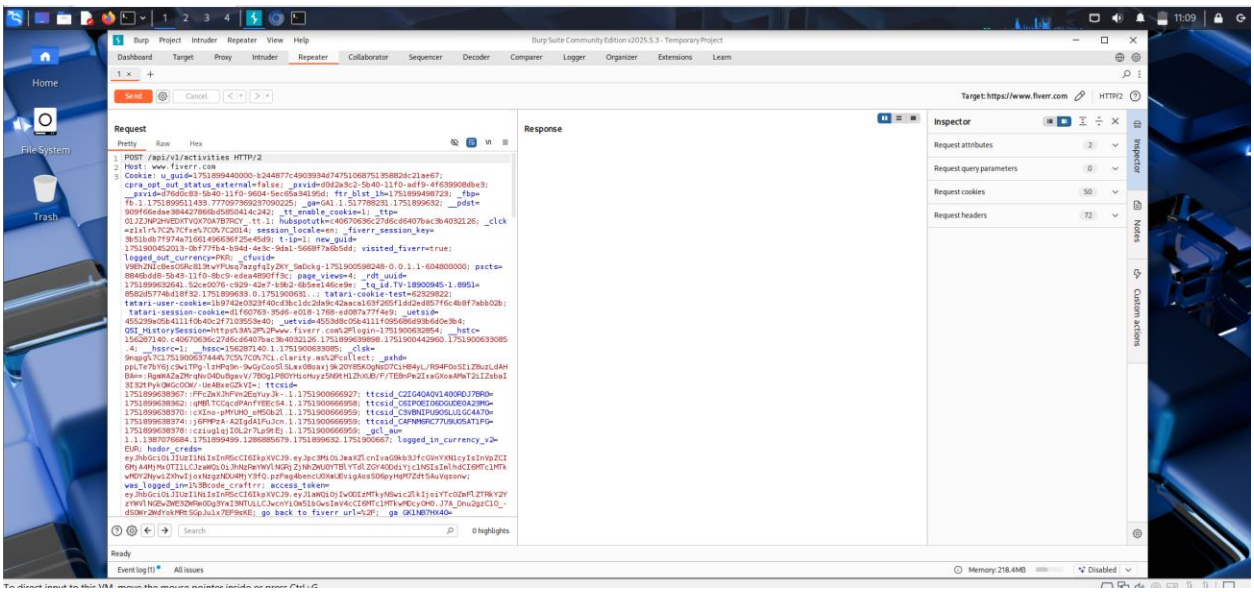


Cookie: u_guid=1751899440000-b244877c4903934d74751068751358 82dc21ae67; cpra_opt_out_status_external=false; _pxvid=d0d2a3c2-5b40-11f0-adf9-4f639908dbe3; __pxvid=d76d0c83-5b40-11f0-9604-5ec65a34195d; ftr_blst_1h=1751899498723; _fbp=fb.1.1751899511433.777097369237090225; _ga=GA1.1.517788231.1751899632; __pdst=909f66edae384427866bd5850414c242; _tt_enable_cookie=1; _ttp=01JZJNP2HVEDXTVQX70A7B7RCY_.tt.1; hubspotutk=c40670636c27d6cd6407bac3b4032126; _clck=z1xlr%7C2%7Cfxe%7C0%7C2014; logged_out_currency=PKR; _cfuvid=AeM_QHndK5lLsTW4kUhDOp7SRMug_28aRJ97rJ8KLSM-1751900031172-0.0.1.1-604800000; pxcts=3527cecf-5b42-11f0-9a76-edea4890ff3c; page_views=3; t-ip=1; tatari-session-cookie=d1f60763-35d6-e018-1768-ed087a77f4e9; __hstc=156287140.c40670636c27d6cd6407bac3b4032126.1751899639898.1751899639898.1751900057983.2; __hssrc=1; _gcl_au=1.1.1387076684.1751899499.1286885679.1751899632.1751900067; session_locale=en; logged_in_currency_v2=PKR; visited_fiverr=true; _fiverr_session_key=3b51bdb7f974a71661496636f25e45d9; was_logged_in=1%3Bmamoonaa_; _pxhd=ppLTe7bY6jc9wiTPg-lzHPq9n-9wGyCooSlSLmx08oaxj9k2OY85KOgNsD7CiH84yL/R94FOoSIiZ8uzLdAHBA==:RgmWAZaZMrqNv04Du8gavV/7BOg1P8OYHioHuyz5N9tH1ZhXUB/F/TE8nPm2IxaGXoaAMaT2iIZsbaI3I32tPykQWGcOCW/-UeABxeGZkVI=; cpra_opt_out_permanent_user=false; _rdt_uuid=1751899632641.52ce0076-c929-42e7-b9b2-6b5ee146ce9e; _tq_id.TV-18900945-1.8951=8582d5774bd18f32.1751899633.0.1751900076..; tatari-cookie-test=39149651; _uetsid=455239a05b4111f0b40c2f7103553e40; _uetvid=4553d8c05b4111f095686d93b6d0e3b4; tatari-user-cookie=1b9742e0323f40cd3bc1dc2da9c42aaca163f265f1dd2ed857f6c4b8f7abb02b; _px3=d0e0fffb575fc2f96dbbe5bedfb61ba9a7de89a60dfd8f0532530e8f2c61cb1d:C9M2HFLIAL6WL3gOVxM31IFZykxGsn4ZIvTjIMfy4+QuY79mB6b5td4D7kVSPLIS0M4JjL/NlX/lVstHCcYcRw==:1000:EvAjuu6PwXPr+5DfoHlGTTlannSVejtjEYFbLwxsVo0eUSNLdDzFB00FWrMa7JDPF8TSozu9cN1eKlz9pnVuYkpCbheXRRZd9tjUMrsF/F0ZUTiidt/roZalByuPD/hmDE7WIyG+EMma7UshIoRJs2yZ7halrSu5zy+8hukaV909nILKygf48NrZAXMdrYPCrb0P7FfLolkC719XuoUODoh+YaQ5WEohrl9ua1v2tyQ=; QSI_HistorySession=https%3A%2F%2Fwww.fiverr.com%2Flogin~1751900054337%7Chttps%3A%2F%2Fwww.fiverr.com%2Fmfa%2Fgenerate~1751900087714; ttcsid=1751899638367::FFcZmXJhFVn2EqYuyJk-.1.1751900095156; __hssc=156287140.2.1751900057983; _clsk=9nqpg%7C1751900098055%7C2%7C0%7Ci.clarity.ms%2Fcollect; ttcsid_C2IG4QAQV140ORDJ7BR0=1751899638362::qMBlTCCqcdPAnfYEEcS4.1.1751900109713; ttcsid_C6IPOEIO6DGUDE0A23MG=1751899638370::cXIno-pMYUH0_oM5Ob2l.1.1751900109714; ttcsid_C3VBNIPU9OSLU1GC4A70=1751899638374::j6FMPzA-A2IgdA1FuJcn.1.1751900109714; ttcsid_CAFNM6RC77U9UO5AT1FG=1751899638378::cziug1qjI0L2r7Lp9tEj.1.1751900109714; hodor_creds=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJmaXZlcnIvaG9kb3JfcGVnYXN1cyIsInVpZCI6MTczMzQyMTgyLCJzaWQiOiJlMmVkMDAwMTUwYzRmZjY2NDFjNmIwYTg5MTlkNzcxMyIsImlhdCI6MTc1MTkwMDEwOSwiZXhwIjoxNzgzNDU3NzA5fQ.qwWYvngptfdL0LSKOLEid2oAsWVzKGOjISiDdeDYO1M; access_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1aWQiOjE3MzM0MjE4Miwic2lkIjoiZTJlZDAwMDE1MGM0ZmY2NjQxYzZiMGE4OTE5ZDc3MTMiLCJwcnYiOm51bGwsImV4cCI6MTc1MTkwMDE3MH0.7H4OKYNxki5btmWOIMieWGlRThRfOH4K1YSmIW0fSHY; go_back_to_fiverr_url=%2F; _ga_GK1NB7HX40=GS2.1.s1751899632$o1$g1$t1751900111$j35$l0$h0; _pxde=b7f1e174b89b59d87660f735853da9c1e7c439e0702191c946e796334d975ad2:eyJ0aW1lc3RhbXAiOjE3NTE5MDAxMTY2MDYsImZfa2IiOjAsImlwY19pZCI6W119; forterToken=0f94c1a01ddb4e1f9214235e29cb4e4c_1751900115776__UDF43_17ck

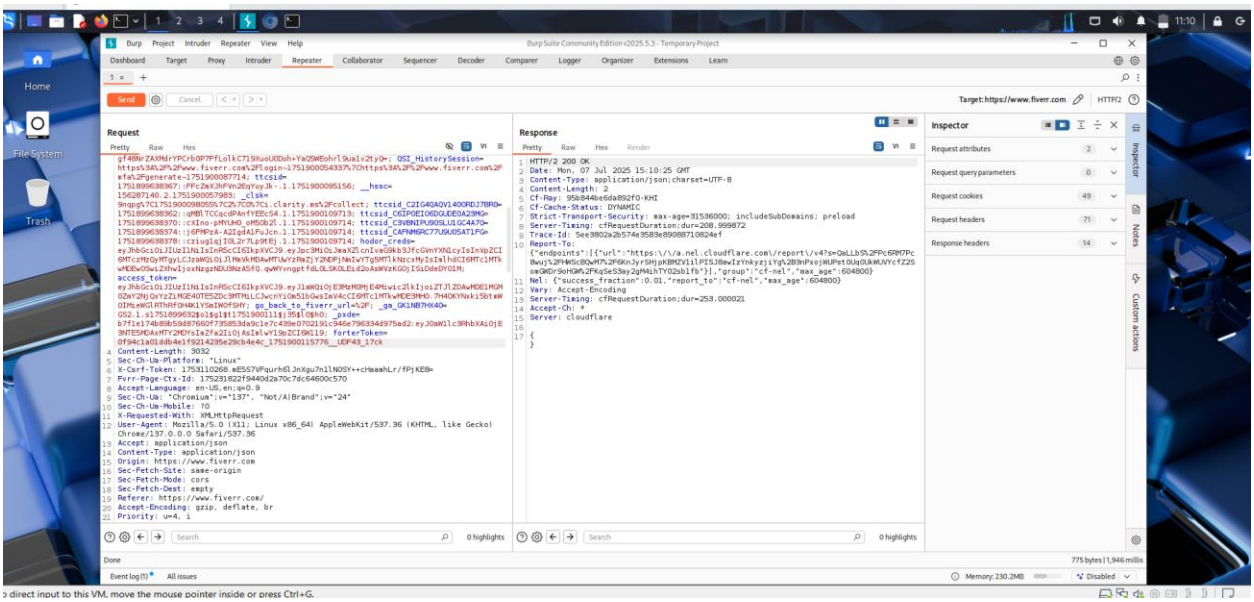
Preparing Replay

- Logged in with a second account in the Burp browser.
- Intercepted a request to a protected endpoint (e.g., /api/v1/activities) after login.
- 

- 



- Replaced the second account's Cookie header in this request with the first account's cookies.



- Received an **HTTP/2 200 OK** response with an **empty JSON body** {}.
- This indicated the request was accepted syntactically but **no user data was returned**, confirming the hijack attempt failed.
- **Inference:** Fiverr enforces session binding beyond cookie presence, likely checking IP, device fingerprint, or behavioral patterns.

Learning Outcomes

- Understood the process of **manual session hijacking via cookie replay**.
- Learned how **Burp Suite** can intercept and modify HTTP requests to simulate attack scenarios.
- Realized that **modern web apps implement multi-factor session binding** (IP, device, or fingerprint) to thwart hijacking.
- Gained practical experience in testing **session management vulnerabilities**.

Conclusion

The test demonstrated that Fiverr's session management system successfully mitigates cookie-based session hijacking attacks by binding sessions to more than just cookie values. Despite presenting a valid session cookie from another device, the server refused to return personalized or sensitive data. This shows Fiverr's effective defense-in-depth approach, ensuring user sessions remain secure even if cookies are compromised.