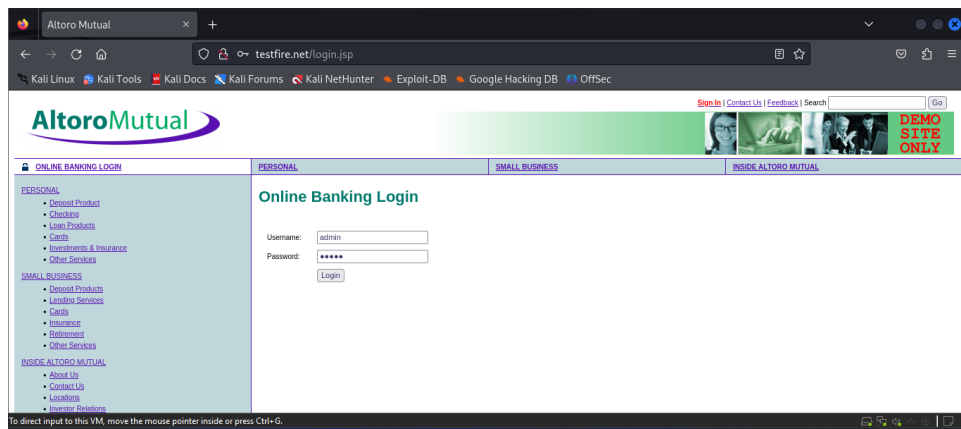
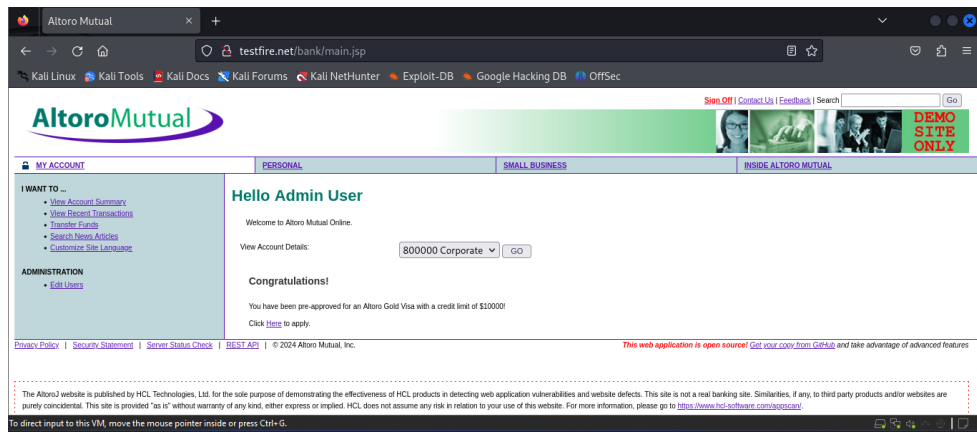


Session Hijacking

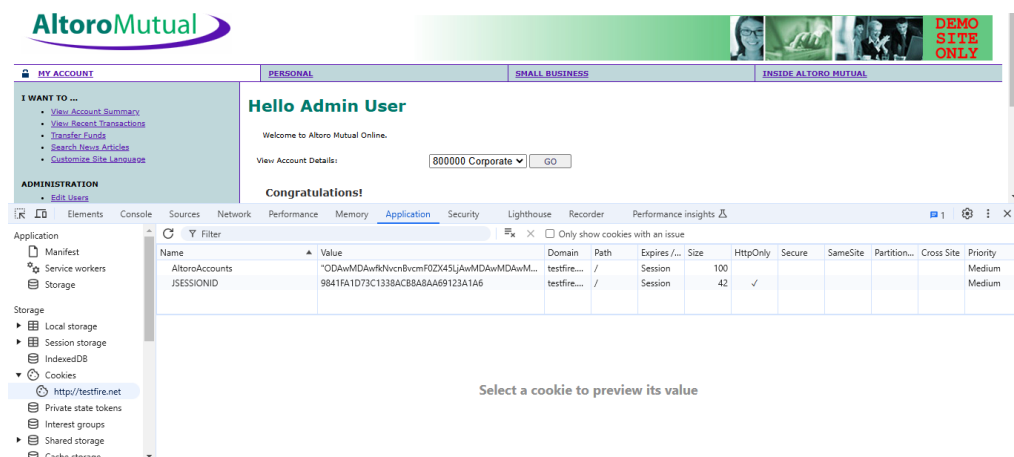
- Basic Session Hijacking:



- Logged in to the account.



- Goto Inspect page → Application → Cookies. Copy the session Id.



- Goto other browser and paste the **session Id** in Inspect page → Application → Cookies.

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

Application

Filter

Name	Value	Domain	Path	Expires...	Size	HttpOnly	Secure	SameSite	Partition...	Cross Site	Priority
AltoroAccounts	*ODAwMDAwRkRlc3RlbnVudmF0ZXA5UjAwMDAwMDAwM...	testfire...	/	Session	100						Medium
JSESSIONID	9841FA1D73C1338ACB8AA69123A1A6	testfire...	/	Session	42	✓					Medium

Select a cookie to preview its value

Brief Demo using Wireshark:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.80.129 && http

No.	Time	Source	Destination	Protocol	Length	Info
83	7.995245967	192.168.80.129	65.61.137.117	HTTP	390	GET / HTTP/1.1
93	8.610870450	65.61.137.117	192.168.80.129	HTTP	1851	HTTP/1.1 200 OK (text/html)
95	8.727426326	192.168.80.129	65.61.137.117	HTTP	386	GET /style.css HTTP/1.1
99	8.732155994	192.168.80.129	65.61.137.117	HTTP	405	GET /images/header_pic.jpg HTTP/1.1
102	8.732678960	192.168.80.129	65.61.137.117	HTTP	402	GET /images/pf_lock.gif HTTP/1.1
108	9.083569554	65.61.137.117	192.168.80.129	HTTP	1446	HTTP/1.1 200 OK (text/css)
112	9.197848003	65.61.137.117	192.168.80.129	HTTP	354	HTTP/1.1 200 OK (GIF89a)
129	14.549308418	192.168.80.129	65.61.137.117	HTTP	483	GET /login.jsp HTTP/1.1
131	14.956278538	65.61.137.117	192.168.80.129	HTTP	8588	HTTP/1.1 200 OK (text/html)
142	17.927413907	192.168.80.129	23.212.50.219	OCSP	470	Request
144	18.028698827	23.212.50.219	192.168.80.129	OCSP	944	Response
150	23.295544258	192.168.80.129	65.61.137.117	HTTP	626	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
152	23.660279585	65.61.137.117	192.168.80.129	HTTP	318	HTTP/1.1 302 Found

Frame 83: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on 0

Ethernet II, Src: VMware_b8:05:77 (00:0c:29:b8:05:77), Dst: VMware_e8:6a

Internet Protocol Version 4, Src: 192.168.80.129, Dst: 65.61.137.117

Transmission Control Protocol, Src Port: 44726, Dst Port: 80, Seq: 1, Acl

Hypertext Transfer Protocol

Hypertext Transfer Protocol: Protocol

Packets: 246 - Displayed: 17 (6.9%)

Profile: Wireshark Masterclass

- Goto the website and login to the account. Track the packets using wireshark. Apply the filter (target ip, http).
- Search for the POST method after filtering packets.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.80.129 && http

No.	Time	Source	Destination	Protocol	Length	Info
150	23.295544258	192.168.80.129	65.61.137.117	HTTP	626	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
152	23.660279585	65.61.137.117	192.168.80.129	HTTP	318	HTTP/1.1 302 Found

Frame 150: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on 0

Ethernet II, Src: VMware_b8:05:77 (00:0c:29:b8:05:77), Dst: VMware_e8:6a

Internet Protocol Version 4, Src: 192.168.80.129, Dst: 65.61.137.117

Transmission Control Protocol, Src Port: 41144, Dst Port: 80, Seq: 430,

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "uid" = "admin"
- Form item: "passw" = "admin"
- Form item: "btnSubmit" = "Login"

HTML Form URL Encoded (urlencoded-form), 37 bytes

Packets: 707 - Displayed: 23 (3.3%)

Profile: Wireshark Masterclass

We got the Username and Password.

