

# NEST Kali Linux Tutorial: Burp Suite

**“Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.”**

Catherine Zittlosen  
Ruth Karkiewicz  
November 2013

*<http://www.portswigger.net/burp/>*

# Introduction

- Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

# Launch Burp Suite

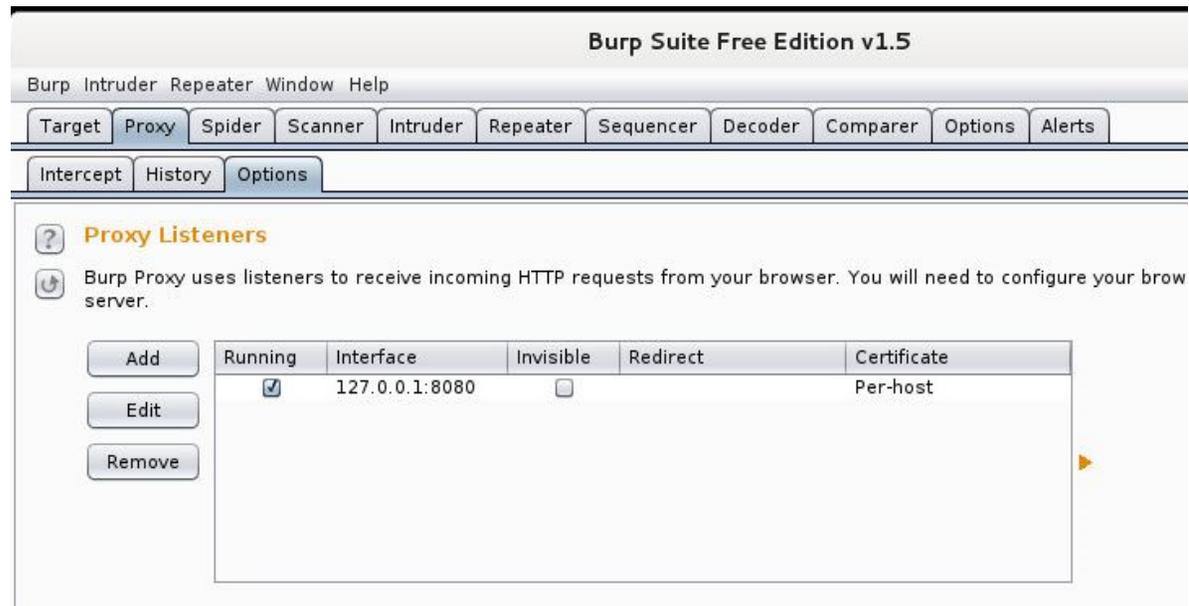
- Applications > Kali Linux > Top 10 Security Tools > burpsuite
- Accept the license agreement.



- The program will launch after a few seconds.

# Start Proxy

- Check that the proxy is running by clicking on
  - Proxy > Options
- There should be a check box under the “Running” column to indicate that the proxy is running.

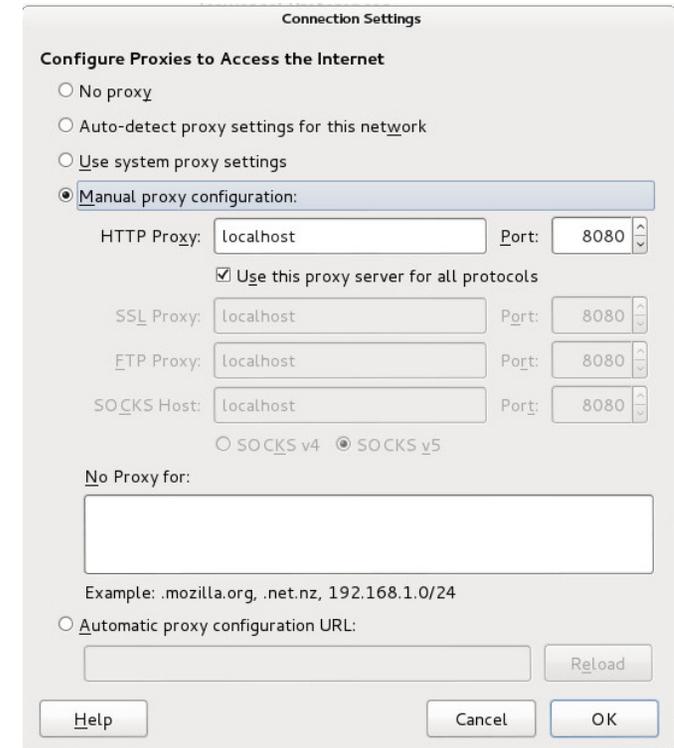


# Configure Browser

- Launch Iceweasel Internet browser
  - Applications > Internet > Iceweasel Web Browser
- In Iceweasel Web Browser go to
  - Edit > Preferences > Advanced > Network > Settings...

# Proxy Settings

- Select “Manual proxy configuration”
- Enter “localhost” in “HTTP Proxy” and set it to port “8080”
- Check “Use this proxy server for all protocols”
- Delete everything in the “No Proxy for” box.
- Select “OK” and then “Close”.



The screenshot shows the "Connection Settings" dialog box with the "Manual proxy configuration" option selected. The "HTTP Proxy" is set to "localhost" and the port is "8080". The checkbox "Use this proxy server for all protocols" is checked. The "SSL Proxy", "FTP Proxy", and "SOCKS Host" are also set to "localhost" with port "8080". The "SOCKS v5" option is selected. The "No Proxy for" field is empty. The "Automatic proxy configuration URL" field is also empty. The "Help", "Cancel", and "OK" buttons are visible at the bottom.

Connection Settings

Configure Proxies to Access the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration:

HTTP Proxy: localhost Port: 8080

Use this proxy server for all protocols

SSL Proxy: localhost Port: 8080

FTP Proxy: localhost Port: 8080

SOCKS Host: localhost Port: 8080

SOCKS v4  SOCKS v5

No Proxy for:

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

Automatic proxy configuration URL:

Reload

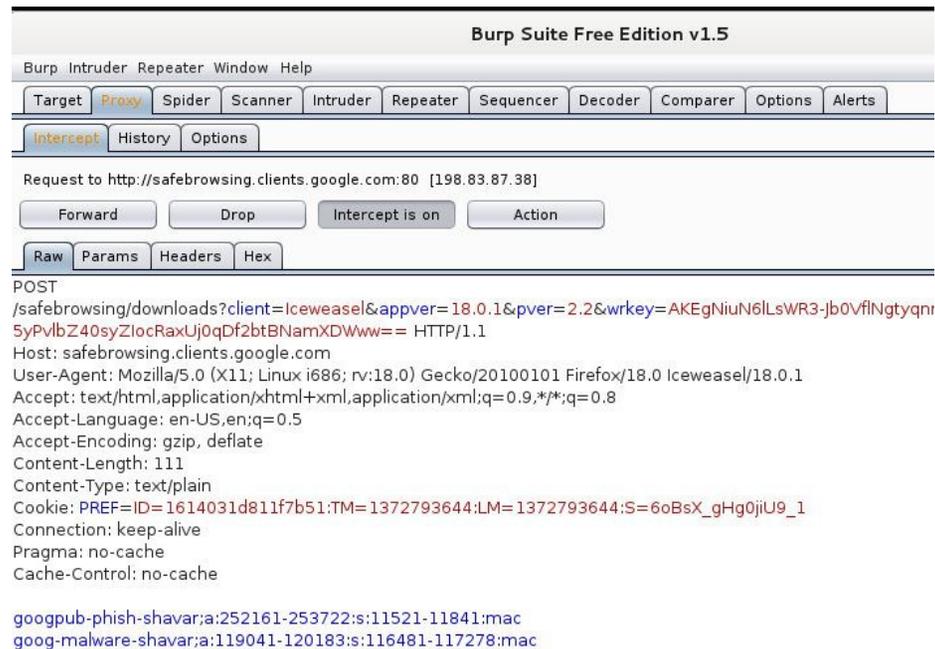
Help Cancel OK

# Test Browser

- With Burp running, in your browser go to any HTTP URL.
  - You can use “[www.thinkgeek.com](http://www.thinkgeek.com)” if you want
- Your browser should sit waiting for the request to complete.

# Test Browser Cont.

- In Burp, go to Proxy > Intercept
- These tabs should be highlighted, and there should be an HTTP request showing in the main panel.



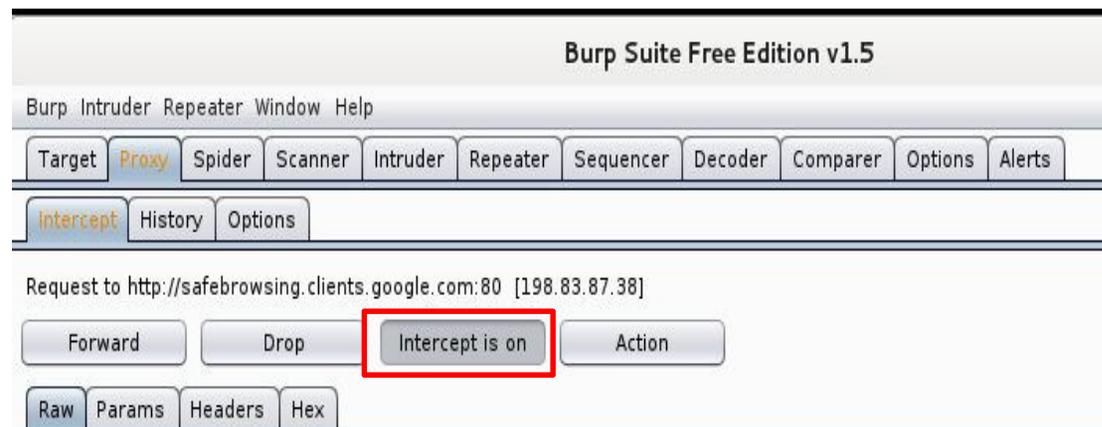
The screenshot shows the Burp Suite Free Edition v1.5 interface. The 'Proxy' tab is selected in the top menu, and the 'Intercept' sub-tab is active. The main panel displays an intercepted HTTP request to 'http://safebrowsing.clients.google.com:80 [198.83.87.38]'. The request is a POST method with the following details:

```
POST
/safebrowsing/downloads?client=iceweasel&appver=18.0.1&pver=2.2&wrkey=AKEgNiuN6LSWR3-jb0VfINgtyqnr
5yPvIbZ40syZlocRaxUj0qDf2btBNamXDwww== HTTP/1.1
Host: safebrowsing.clients.google.com
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 iceweasel/18.0.1
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
Content-Length: 111
Content-Type: text/plain
Cookie: PREF=ID=1614031d811f7b51:TM=1372793644:LM=1372793644:S=6oBsX_gHg0jiU9_1
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

googpub-phish-shavar;a:252161-253722:s:11521-11841:mac
goog-malware-shavar;a:119041-120183:s:116481-117278:mac
```

# Test Browser Cont.

- Click on the "Intercept is on" button so that it says "Intercept is off".
- Go back to your browser, and you should (shortly) see the URL you requested being loaded in the normal way.



# Using Burp Proxy

- Each HTTP request made by your browser is displayed in the Intercept tab. You can view each message, and edit it.
- Click on the “Intercept is on” button in Burp Suite
- Browse to “nest.unm.edu” in Iceweasel
- You can view the request in Burp Suite.
- Click through each of the message editor tabs (Raw, Headers, etc.) to see the different ways of analyzing the message.

# Forward Request

- Click the "Forward" button to send the request on to the destination web server (repeat if necessary).
- In most cases, your browser will make more than one request in order to display the page (for images, etc.). Look at each subsequent request and then forward it to the server. When there are no more requests to forward, your browser should have finished loading the URL you requested.
- You can toggle the "Intercept is on / off" button in order to browse normally without any interception.

# History

- As you browse via Burp, the Proxy history keeps a record of all requests and responses.
- Go to Proxy > History

The screenshot shows the Burp Suite Proxy History window. The main table lists the following requests:

#	Host	Method	URL	Params	Modifi...	Status	Length	MIME type	Extension	Title
1	http://safebrowsing.clients...	POST	/safebrowsing/downloads?client...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	4437	script		
2	http://thinkgeek.com	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	302	117			
3	http://www.thinkgeek.com	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	200	68837	HTML		ThinkGeek :: Stuff fo...
4	http://safebrowsing-cache...	GET	/safebrowsing/rd/ChNnb29nLW1h...	<input type="checkbox"/>	<input type="checkbox"/>	200	85324			
5	http://safebrowsing-cache...	GET	/safebrowsing/rd/ChNnb29nLW1h...	<input type="checkbox"/>	<input type="checkbox"/>	200	152966			
12	http://www.thinkgeek.com	GET	/js/jquery-1.5.2.min.js	<input type="checkbox"/>	<input type="checkbox"/>	200	86294	script	js	
13	http://www.thinkgeek.com	GET	/js/global.js	<input type="checkbox"/>	<input type="checkbox"/>	200	4785	script	js	
14	http://www.thinkgeek.com	GET	/js/sku_picker.js?v=2013060701	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	4931	script	js	
15	http://www.thinkgeek.com	GET	/js/testing/mbox.js?v=2013050701	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	25298	script	js	
16	http://www.thinkgeek.com	GET	/js/jquery/jquery.cookie.js	<input type="checkbox"/>	<input type="checkbox"/>	200	2300	script	js	
17	http://www.thinkgeek.com	GET	/js/jquery/jquery.fancybox.pack.js	<input type="checkbox"/>	<input type="checkbox"/>	200	15093	script	js	
18	http://www.thinkgeek.com	GET	/js/omniture.js	<input type="checkbox"/>	<input type="checkbox"/>	200	47587	script	js	
37	http://www.thinkgeek.com	GET	/js/carousel.js?v=20111015	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	6274	script	js	
38	http://www.thinkgeek.com	GET	/js/jquery/jquery.ui.1.8.6.custom	<input type="checkbox"/>	<input type="checkbox"/>	200	162724	script	js	

The selected request (row 14) is shown in the Request/Response pane:

```
GET /javascript/esapi4js/resources/Base.esapi.properties.js?v=9.1.110082.0-3 HTTP/1.1
Host: learn.unm.edu
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://learn.unm.edu/
Cookie: __utma=6691053.1318864966.1380144972.1380144972.1380144972.1;
__utmz=6691053.1380144972.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); JSESSIONID=0655ED445F6B4AAB5CD2161C5CA189F6.root;
session_id=E14ACC090267E9AB8E29DA0946DCE88F; s_session_id=5BE2EFFB7EFDCA6E2D4F4183361E09DD; Oreo=3276908736.20480.0000
Connection: keep-alive
```

# History Cont.

- You can review the series of requests you have made.
- Click on a column header in the Proxy history to sort.
- Select an item in the table and view the full messages in the Request and Response tabs.

# Site Map

- Also, as you browse, Burp builds up a site map of the target application.
- Go to Target > Site map

The screenshot shows the Burp Suite Free Edition v1.5 interface. The 'Site map' tab is active, displaying a list of discovered hosts. The list includes various domains such as a.adroll.com, a.mobify.com, access.blackboard.com, admin6.testandtarget.omniture.com, analytics.twitter.com, bugzilla.mozilla.org, cdn.mobify.com, cm.g.doubleclick.net, code.jquery.com, computing.unm.edu, counsel.unm.edu, creativecommons.org, d.adroll.com, dean.edwards.name, directory.unm.edu, edge, edge.quantserve.com, esurvey.unm.edu, fancybox.net, fastinfo.unm.edu, fortawesome.github.com, get.adobe.com, github.com, google.unm.edu, ib.adnxs.com, it.unm.edu, jquery.com, jquery.org, kyruus.com, learn.unm.edu, learn.unm.edu, learnaboutlearn.unm.edu, localhost, metrics.thinkgeek.com, my.unm.edu, and nest.unm.edu.

The detailed view shows a request for a.html from a.mobify.com. The request details are as follows:

Host	Method	URL	Params	Stat...	Length	MIME type
http://a.mobify.com	GET	/thinkgeek-tablet/a.h...		200	2938	HTML
http://a.mobify.com	GET	/thinkgeek-tablet/a.js		200	4269	script
http://a.mobify.com	GET	/thinkgeek-tablet/wo...		200	40666	script

The request details are:

```
GET /thinkgeek-tablet/a.html HTTP/1.1
Host: a.mobify.com
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.
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://www.thinkgeek.com/
Connection: keep-alive
```

# Site Map Cont.

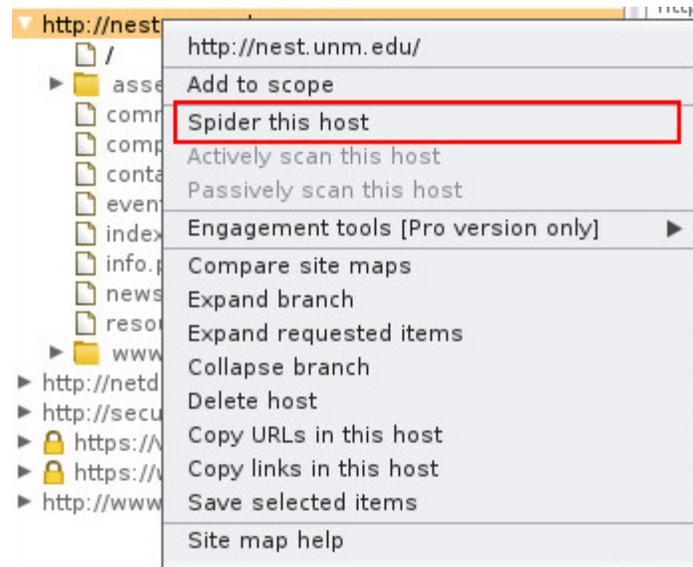
- The site map contains all of the URLs you have visited in your browser, and also all of the content that Burp has inferred from responses to your requests (e.g. by parsing links from HTML responses).
- Items that have been requested are shown in black, and other items are shown in gray.
- You can expand branches in the tree, select individual items, and view the full requests and responses (where available).

# Burp Spider

- Burp Spider uses various techniques to crawl application content, and by default it will follow all in-scope links, submit forms with dummy data, and make additional requests (for robots.txt, directory roots, etc.).

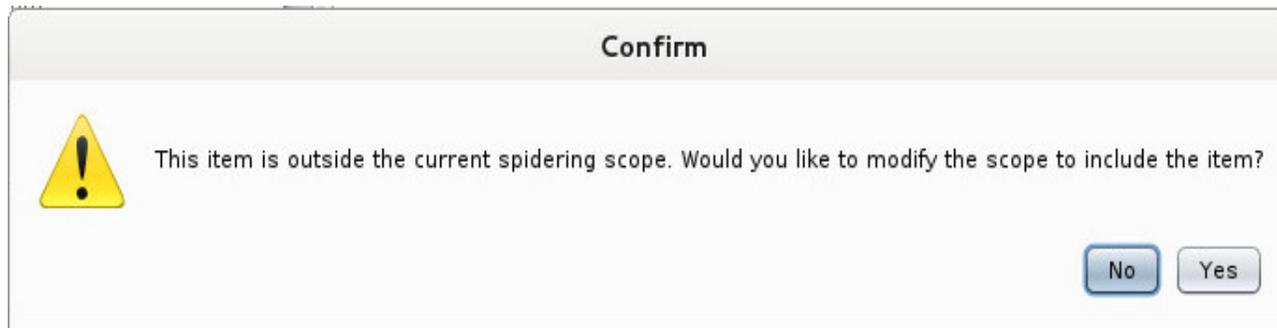
# Initiating the Spider Cont.

- In the Site Map, find 'http://nest.unm.edu/'
- Right click and select 'Spider this host'



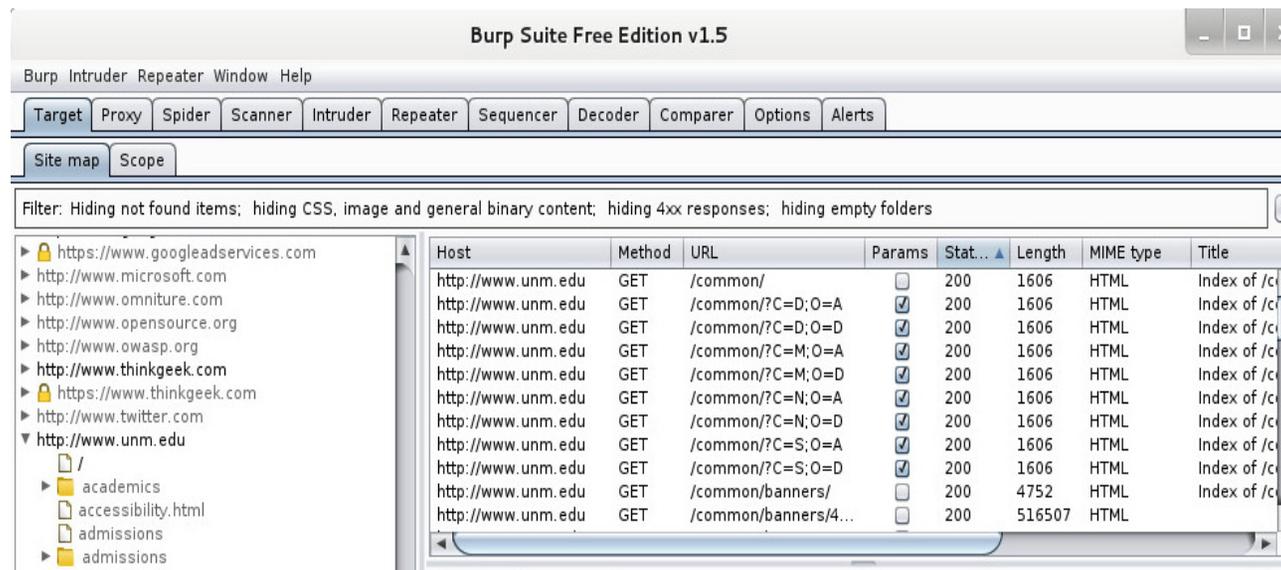
# Confirm Scope

- If you get the following message
  - Click “Yes”



# Spider Results

- Once the spider starts, it will display all the pages. You will see them in the main window to the right.



The screenshot shows the Burp Suite Free Edition v1.5 interface. The 'Spider' tab is active, displaying a list of discovered URLs and a table of request details. The left pane shows a site map for 'http://www.unm.edu' with folders for 'academics', 'admissions', and 'admissions'. The main pane shows a table of requests with columns for Host, Method, URL, Params, Status, Length, MIME type, and Title.

Host	Method	URL	Params	Stat...	Length	MIME type	Title
http://www.unm.edu	GET	/common/	<input type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=D;O=A	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=D;O=D	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=M;O=A	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=M;O=D	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=N;O=A	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=N;O=D	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=S;O=A	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/?C=S;O=D	<input checked="" type="checkbox"/>	200	1606	HTML	Index of /c
http://www.unm.edu	GET	/common/banners/	<input type="checkbox"/>	200	4752	HTML	Index of /c
http://www.unm.edu	GET	/common/banners/4...	<input type="checkbox"/>	200	516507	HTML	Index of /c

# References

- <http://geekyshow.blogspot.com/2013/07/how-to-use-maltego-in-kali-linux.html>
- [http://portswigger.net/burp/help/proxy\\_gettingstarted.html](http://portswigger.net/burp/help/proxy_gettingstarted.html)
- [http://portswigger.net/burp/help/spider\\_using.html](http://portswigger.net/burp/help/spider_using.html)