

Ryan Brodsky

ICS 482

11/25/2019

InfoSec Lab: Reflected XSS Mitigation and URL Encoding

The screenshot displays the InfoSec Learning lab interface for the 'Reflected XSS Mitigation and URL Encoding' challenge. The interface is split into two main sections, each showing a different challenge.

Challenge #1: The left window shows the 'Final_Alice_DT_32bit' challenge. The terminal window displays the setup of a web server (phpmyadmin) on a Kali VM. The output shows the creation of config files, setting up php5-gd, php5-mcrypt, and phpmyadmin, and the successful creation of the database.

```
support@Web: ~
Creating config file /etc/php5/cli/php.ini with new version
update-alternatives: using /usr/bin/php5 to provide /usr/bin/php (php) in auto mode.
Setting up php5-gd (5.3.10-1ubuntu1) ...
Setting up php5-mcrypt (5.3.5-0ubuntu1) ...
Setting up phpmyadmin (4:3.4.10-1) ...
dbconfig-common: writing config to /etc/dbconfig-common/phpmyadmin.conf
Creating config file /etc/dbconfig-common/phpmyadmin.conf with new version
Creating config file /etc/phpmyadmin/config-db.php with new version
granting access to database phpmyadmin for phpmyadmin@localhost: success.
verifying access for phpmyadmin@localhost: success.
populating database phpmyadmin: success.
populating database via sql... done.
dbconfig-common: flushing administrative password
* Reloading web server config apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
Processing triggers for libc-bin ...
libc6: deferred processing now taking place
support@Web:~$
```

Challenge #2: The right window shows the 'Final_Kali-2.0' challenge. The terminal window displays the setup of a web server (SimpleHTTPServer) on a Kali VM. The output shows the configuration of the network interface (eth0) and the successful setup of the SimpleHTTPServer.

```
root@Hacker: ~
root@Hacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::250:56ff:fe9a:42e8 prefixlen 64 scopeid 0x20<link>
    ether 08:50:56:9a:42:e8 txqueuelen 1000 (Ethernet)
    RX packets 94 bytes 6852 (6.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 76 bytes 5771 (5.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 18 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 23 bytes 1471 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 1471 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

https://lab.infoseclearing.com/lab/reflected-xss-mitigation-and-uri-encoding

Reflected XSS Mitigation and URL Encoding

```
#!/usr/bin/perl
if ($REQUEST{'myusername'}) {
    echo str_replace($script, null, $REQUEST{'myusername'});
} else {
    echo 'Please login';
}
```

4 Press and hold the Ctrl key and the x key (Ctrl-x).

5 Press the y key.

6 Press Enter.

7 Click the close button on the VM window.

Final_Alice_DT_32bit - Internet Explorer

support@Web: ~

```
GNU nano 2.2.6 File: /var/www/WeBServer/index.php Modified
<?php
session_start();
?>
<!DOCTYPE html>
<html>
<head>
<title>UrBank</title>
<meta name="description" content="UrBank online banking">
</head>
<body>
<div style="text-align:right; width:95%;">
<?php
if ($REQUEST{'myusername'}) {
    echo str_replace($script, null, $REQUEST{'myusername'});
} else {
    echo 'Please login';
}
```

Alice.urbank.
com.11.26.2019

https://lab.infoseclearing.com/lab/reflected-xss-mitigation-and-uri-encoding

Reflected XSS Mitigation and URL Encoding

7 Click the close button on the VM window.

Final_Alice_DT_32bit - Internet Explorer

support@Web: ~

```
update-alternatives: using /usr/bin/php5 to provide /usr/bin/php (php) is auto
code.
Setting up php5-gd (5.3.10-1ubuntu3) ...
Setting up php5-mcrypt (5.3.5-0ubuntu1) ...
Setting up phpmyadmin (4:3.4.10.1-1) ...
dbconfig-common: writing config to /etc/dbconfig-common/phpmyadmin.conf
Creating config file /etc/dbconfig-common/phpmyadmin.conf with new version
Creating config file /etc/phpmyadmin/config-db.php with new version
granting access to database phpmyadmin for phpmyadmin@localhost: success.
verifying access for phpmyadmin@localhost: success.
creating database phpmyadmin: success.
populating database via sql... done.
dbconfig-common: flushing administrative password
* Reloading web server config apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
support@Web:~# sudo nano -c /var/www/WeBServer/index.php
support@Web:~#
```

FINISHED WITH UBUNTU

Challenge #3

https://lab.infoseclearning.com/lab/reflected-xss-mitigation-and-uri-encoding

Reflected XSS Mitigation and URL Encoding

Save Page As...
View Background Image
Select All
View Page Source
View Page Info
Inspect Element (G)

VIEWING INDEX.PHP CLIENT-SIDE FILE

Note: We can analyze what occurred in the client-side file.

```
6 </head>
7 <body>
8 <div style="text-align:right; width:95%;">
9 <>alert('Owned')</></div>
10 </div>
11 <br><br><br>
```

RESULT

Challenge #4

6 Close the VM window.

Final_Kali-2.0 - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1129810/Final_Kali-2.0

Final_Kali-2.0

Applications Places Iceweasel Tue 00:45

http://urbank.com/?myusername=%3Cscript%3Ealert(%27Owned%27)%3C/script%3E - Iceweasel

view-source: http://urbank.com/?myusername=<sc

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>UrBank</title>
5 <meta name="description" content="UrBank online banking">
6 </head>
7 <body>
8 <div style="text-align:right; width:95%;">
9 <>alert('Owned')</></div>
10 </div>
11 <br><br><br>
12 <center>
13 <h1> Welcome to UrBank </h1><br>
14 </center>
15 <table width="301" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCC">
16 <tr>
17 <form name="form1" method="post" action="checklogin.php">
18 <table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="FFFFFF">
19 <tr>
20 <tr>
21 <td colspan="3">Login </td></tr>
22 <tr>
23 <tr>
24 <td width="78">Username</td>
25 <td width="6"></td>
26 <td width="294"><input name="myusername" type="text" id="myusername"></td>
27 </tr>
```

https://lab.infoseclearning.com/lab/reflected-xss-mitigation-and-uri-encoding

Reflected XSS Mitigation and URL Encoding

OPENING A BROWSER

15 Type **urbank.com** to the browser's search field and **press Enter**. Type the query parameter **?myusername=<>alert('Ryan Was Here')** and append your SCRIPT element and **press Enter**.

UrBank - Iceweasel

urbank.com/?myusername=<>alert('Ryan Was Here')

Please login

Welcome to UrBank

Login

Username :

Password :

Login

PENTESTING

There are two ways to tell if your attack was successful:

- If the JavaScript executes
- If the complete SCRIPT element is injected

16 When you are done pentesting, please remember to click **stop** button in the topology.

Final_Kali-2.0 - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1129810/Final_Kali-2.0

Final_Kali-2.0

Applications Places Iceweasel Tue 00:47

UrBank - Iceweasel

urbank.com/?myusername=<>alert('Ryan Was Here')

<>alert('Ryan Was Here')

Welcome to UrBank

Login

Username :

Password :

It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!