Database Vulnerabilities

Due Nov 28 by 11:59pm **Points** 100 **Submitting** a website url

Task Description

The challenge is to analyze, ethically exploit, and mitigate vulnerabilities in PHP scripts running on a Linux virtual machine.

The sequence of steps is the following:

1. Download the virtual machine image.
2. Run the virtual machine on VirtualBox, and logon as root.
3. Configure the networking between your physical machine and the virtual machine. The virtual machine is your target, while your physical machine will be used to ethically launch your exploit.
4. Open a browser on your host machine and navigate to the IP address of the VM. Browse the links on the VM's website that appear's in your host machine's browser.
5. Figure out how to perform a sql injection for the cat.php script and print the hashed password.
6. Write an exploit of the vulnerability that you found. Write the exploit in Python.
7. Your program must be developed in a git version control repository (gitlab.cs.wwu.edu). The name for your repository can be anything but files must be placed on the root directory of the repository. Set the visibility settings on **Private** and add my account (**tsikerm and stovalc**) as a **Maintainer** to your repository.
8. Your exploitation script should be named **php_exploit.py** and be written in **Python3** and placed in the root of your repository. The script should print the results of the exploitation. When pushing the version on your repository have it access the http address on localhost (**http://localhost/.. (http://localhost/..)** .).
9. The final deliverable is a working exploit that successfully exploits the sql vulnerability and prints the hashed password. The password can be inside the html source code.
10. There is a "checkpoint" deadline of this assignment upcoming **one week before it is due**. At that point you will need to have set up your repository and submitted its URL on canvas. Please verify that once you did that you have received a score from ATHINA.
11. An automated testing suite (ATHINA - **A**utomated **T**esting **H**omework **I**nterface for **N** **A**ssignments) will assist in verifying that your application is compliant with the project requirements. Once you submit the location of your files, it will test the repository and submit 80% of your grade depending on the outcome of the tests. With every new commit to your repository, it will re-evaluate and submit a

new grade. This is meant to give you immediate feedback and multiple opportunities to correct your code and get full points for the assignment.

Virtual Machine

The virtual machine is available for download from the following link:

sql_injection.iso (https://wwu.instructure.com/courses/1500739/files/81104115/download?download_frd=1)

Create a new virtual machine on virtualbox and follow the wizard for an ubuntu 64bit instance. Once completed load the iso in the optical drive slot. Then, setup the network configuration.

Network Configuration

Setup the network interface as host-only (**https://www.virtualbox.org/manual/ch06.html (https://www.virtualbox.org/manual/ch06.html)**). Type **ifconfig** once the machine boots to view the IP address that it can be accessed from (**inet addr** field).

1. Click ”File", then "Host-Network Manager". Create a new network adapter and make a note of the IP and subnet (usually 192.168.56.0/24 on linux)
2. Enable it (there is a checkbox to the right)
3. Select your virtual machine entry on the left panel, and then click on Network
4. Click on Adapter 1, and select “Host-only Adapter”, and pair it with the new adapter (usually called “vboxnet0” or a similar variant)

Useful

You will notice that cat.php gets a parameter when navigating to it from the top menu (item called test). E.g., cat.php?id=1

1 is a user parameter that is entered in a sql query that SELECT's a bunch of columns from a table based on the id. For example SELECT * FROM sometable WHERE id=1

You cannot alter what the website is printing (in other words the server side logic) but you can view at least the source elements (view source). In other words, the php scripts that run on server print a fixed

number of elements that they obtain from the select sql query.

After figuring out how to do a sql injection (should take you about a minute) your challenge will be to figure out how to use it to your advantage. Consider the use of: UNION ALL SELECT 1

This with a bit of modification should get you to identify the number of attributes that the original query expects to be returned (remember that UNION requires the number of columns to match between two queries).

Once you know the total number of attributes that you need to pass, you can use the following structure to find what tables exist on the database (show table won't work, try it out):

SELECT * FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema'

You will have to replace * with the number of columns that interest you. You primarily need table names so at least something along these lines. How would you know what attributes information_schema.columns has? (I googled this for you: **https://dev.mysql.com/doc/refman/8.0/en/columns-table.html (https://dev.mysql.com/doc/refman/8.0/en/columns-table.html)**).

Alright, so now you know what tables are out there and what columns they have! Guess which one has the password (it is obvious once you have the names). Use: UNION ALL SELECT * FROM table

Replace * and table with your desired values and make sure to match the number of columns that the union expects. If all goes well you should get something printed only to view it you will need to look at the source html in all likelihood. See a funny alphanumeric sequence? What could it be (**https://www.mobilefish.com/services/hash_generator/hash_generator.php (https://www.mobilefish.com/services/hash_generator/hash_generator.php)**)? Once you figure it out do a google search for "HASH cracker" and replace the HASH with your hash type. Literally the first or second result will be a website that can help you crack that password.

Python Implementation

Use the module requests to build your exploit. There are other modules such as curl or urllib but requests is the easiest.

Intro to Python (for Java programmers)

Guide: **Python_for_Java_developers_cheat_sheet.pdf** ⬇
(https://wwu.instructure.com/courses/1500739/files/81104122/download?download_frd=1)