Computer Systems Security (CS628A), Assignment - 3
Autumn 2019, IIT Kanpur

Mohit Malhotra, Krishna Kumar Tayal and Dixit Kumar

Released: 5 October 2019
Due: 22 October 2019

Credits:

The basic code of the server is based on **Dave O'Hallaron** of Carnegie Mellon University (CMU)**.** The original code can be found the following link: TinyWebServer.

NOTE:

1. **Do not use the code linked above and instead use the code in the VM provided by us.** We have made many significant modifications for the purpose of this assignment.

2. You are advised to **read the whole assignment carefully** before starting it. You **should read the submission guidelines** more than once. Submissions missing files or in the incorrect format **will not be graded**.

Baahubali - The saviour of Mahishmati

Amarendra Baahubali became the king of **Mahishmati** after ***Rajamatha*** **Sivagami** recognised his leadership qualities and announced him as the next king after he succeeded in a contest to defend the empire from Kalakeya invasion. Though **Bhallala Deva** killed the Kalakeya king Inkoshi, Baahubali was announced the next king as he showed more honor in the battle. He was envied by Bhallaladeva who then manipulated Sivagami into issuing an order to **Kattappa** to execute Baahubali for treason.

Mahendra Baahubali, the son of Amrendra and the rightful heir to the throne, was somehow saved by his grandmother, Sivagami Devi, who sacrificed her life for the cause. However, Bhallala Deva managed to capture **Devasena**, Amrendra's wife, and imprisoned her. Mahendra was raised by an educated family and was good in studies from a very young age.

Mahendra pursued his engineering degree from **IIT Kanpur** and knows how to use technology for the benefit of people. However, he did not attend **Computer Systems**

Security (CS628A) course. One day, while scrolling through his facebook feed, he saw a friend suggestion of a beautiful girl, **Avantika**, and instantly fell for her. Avantika, a student of **Mahishmati Institute of Technology (MIT)** was an intern at **RajamouliSoft**, Hyderabad. Mahendra immediately applied for an internship in the same company and was selected straightaway since he was a student of IIT Kanpur **;)** There, he started executing his master plan of wooing Avantika. She eventually fell in love with him but she had already dedicated her life for another cause, i.e. saving Devasena and Mahishmati. She discussed her plight with Mahendra. He joined her mission for her love without a second thought.

When Mahendra reached Mahishmati, Kattappa recognised him instantaneously because Mahendra looks exactly like his late father. Kattappa told the whole story to Mahendra and Mahendra decided to save his mother and the **junta** of the kingdom from the cruelties of Bhallala Deva and his men. As Mahendra cannot fight this battle alone against the professional army of Bhallala Deva, he needs to build his own army to stand a chance. Junta of Mahishmati, which was ridiculed for years, was waiting for years for their true king.

Mahendra sees this as an opportunity to get the support of the junta for the revolt. But the challenge Mahendra faces is that the people of Mahishmati are poor, unskilled and illiterate because of the high education fee in Mahishmati. Inorder to educate the junta, Mahendra builds a web portal, **Mahishmati Programme on Technology Enhanced Learning (MPTEL).** This portal can be used to teach basic arithmetic but in reality he also uses this portal to convey provoking messages against Bhalla Deva. As he is running short on money, he is using the same server to host the website and to store the secrets. These secrets include name of soldiers, their roles, strategies, date and place of attacks, etc.

Bhallala Deva comes to know about Mahendra and the web portal that he is running. So, he hires a guy, **Bhondu**, from **IIT Bombay** to hack the MPTEL server. As you know, Mahendra did not attend the **CS628A** course, he has left some vulnerabilities unknowingly while developing the server. Can you help Mahendra in finding and fixing these vulnerabilities?

Getting Started

You have been given the virtual machine being used by Baahubali to host the MPTEL server. You first need to download this VM. For this you will need to get an SSH private key that gives you access to the computer that stores the VM. Use this command to get the private key:

```
$ wget
https://web.cse.iitk.ac.in/users/spramod/courses/cs628-2019-I/id_ecdsa_anonymous
```

For private keys to work correctly, you will need to make sure they are only readable by you. So, change its permissions as follows.

```
$ chmod 600 id_ecdsa_anonymous
```

Next use this key to download the VM from the server spramod.cse.iitk.ac.in. Use the following command. The VM is a 10 GB file so the download will take a while (probably best to download using LAN rather than WiFi).

```
$ echo get cs628a-hw3.qcow2 | sftp -i id_ecdsa_anonymous
anonymous@cs628a.cse.iitk.ac.in
```

If you are on a slow connection, it may be faster to download a 7z archive of the above file.

```
$ echo get cs628a-hw3.qcow2.7z | sftp -i id_ecdsa_anonymous
anonymous@cs628a.cse.iitk.ac.in
```

You can then extract from the above archive by using

```
$ 7z e cs628a-hw3.qcow2.7z
```

You will need to install a virtual machine manager. We recommend you to use KVM. Here is how to install KVM on ubuntu:

```
$ sudo apt-get install qemu-kvm libvirt-bin bridge-utils virt-manager
```

Copy the downloaded VM to the following path: `/var/lib/libvirt/images/`

You will require root permissions for making the above operation. Now, create a new virtual machine and choose option “Import existing disk image”. If you feel lost, refer to this article. Once you are done with the installation, login into VM with the following credentials:

Username: **baahubali**
Password**: Jai_Mahishmati**

Navigate to the path “**/home/baahubali/KiliKili**” to find the MPTEL server.

MPTEL Server

MPTEL server is a tiny web server which serves static and dynamic GET requests **only**. It uses the GET method to serve static content (text, HTML, GIF, and JPG files) out of ./ and to serve dynamic content by running CGI programs out of ./cgi-bin. Dynamic content includes addition, multiplication and division only. Study the source code to understand the working of tiny server.

How to run Tiny:

- ‘`make`’ to compile the code.
- Run "./`tiny <port>`" on the server machine to start the server.
  e.g., "`./tiny 8000`".

GET request using browser:

Static content: **http://<host>:8000**
Dynamic content: **http://<host>:8000/cgi-bin/adder?1&2**

GET request using command line:

Execute the python script **exploit.py**. Read and understand the script. It may help you to write exploits.

PART A

1. ***soldier*** is a file that contains the details of all the soldiers, their roles and skills. Deleting this file may dismantle the whole plan of action. Some vulnerabilities in server can allow Bhondu to delete this file. One possibility may be using **return-to-libc** attack to make the "**unlink**" system call.

   Write a script named **exploit_A1.py** which will use above mentioned attack to delete the file ***soldier***. The script must run on the unchanged code present in VM. Also, briefly explain how you made this exploit in **answers_A.txt**

2. Another possible attack to delete the file ***soldier*** is to use **shellcode injection** technique.
   a. Write an assembly code **'unlink.S'** to delete the file ***soldier***. You will need to make a call to **'unlink'** system call in your "unlink.S" file. System call number of unlink is **10** or **'\n',** this may complicate things. Take care of it while writing your assembly code. Also keep in mind that your shellcode must run on a **32 bit machine**. Remember this assembly code is meant to be **injected into another program**. Use command **'nasm unlink.S'** to generate the shellcode. We have provided a program **run_shellcode.c** to test your shellcode. You can use it as follows:

      - `$ ./run_shellcode ./unlink`

      After executing your shellcode, ***soldier*** is supposed to be deleted.

      Submission: /home/baahubali/KiliKili/unlink.S

      Resources: "0x500, shellcode" from the book "Hacking, The Art of Exploitation" can be very helpful in writing the shellcode.

   b. Try to inject this shellcode into the webserver using **GET** request and get the file deleted. Write this exploit in a script named **exploit_A2.py**. The script must run on the unchanged code present in the VM.

      Also, briefly explain how you made this exploit in **answers_A.txt**

3. How can you prevent these attacks? Discuss at least 2 points about Question A1 and A2 each. Write your answer in **answers_A.txt**

PART B

1. Baahubali wants to find the best way to place soldiers in his troops. Every soldier is unique in terms of skills and abilities. **Brigadier Mohit**, has developed an algorithm to compute the troop placement strategy, but this algorithm needs heavy computation. Mohit has implemented the algorithm and has started the execution of this process on the same server.

   There is another vulnerability in the server which may allow Bhondu to execute **Linux commands** on server side by using just GET requests. Bhondu wants to find the name of the above mentioned process and kill the same. Your job is to find the vulnerability in the server.

   Write a script **exploit_B1.py** to automatically kill this process. Also, briefly explain how you made this exploit in **answers_B.txt**
   (**HINT : try to execute "ps -ef" command).**

2. This server is supposed to serve static and dynamic GET requests only. Client must not be able to send files to the server side. Bhondu wants to replace **"index.html"** with provoking speeches against Baahubali. Can you find the vulnerability before Bhondu misuses it?

   Write exact steps and commands in **answers_B.txt** that you used to replace **index.html (NOTE : Do not assume anything about the size of the file).**
   (HINT : Read about 'nc' command)

3. You can prevent above mentioned attacks using **input sanitization technique**. Implement this fix. You must return **'INVALID INPUT'** in case if input is not valid.

   We have made another directory **KiliKili_B3** which is an exact copy of original KiliKili. You should save all the code changes for this question(**B-3**) in this directory only.

4. You can also use one more concept discussed in the class, called **namespaces** to fix above mentioned attacks. Implement the fix of **Part B, Q1**.

   We have made another directory **KiliKili_B4** which is an exact copy of original KiliKili. You should save all the code changes for this question(**B-4**) in this directory only.

   Which namespace(s) prevented the attack and how? Discuss in **answers_B.txt.**

   Resources: Good understanding of the code explained in the class.

5. Implement the fix of **Part B-Q2** using namespaces.

   We have made another directory **KiliKili_B5** which is an exact copy of original KiliKili. You should save all the code changes for this question(**B-5**) in this directory only.

   Which namespace(s) prevented the attack and how? Discuss in **answers_B.txt**

6. We should be happy after sanitizing the input, so why do we still need this namespace business? Can you think of an attack scenario that cannot be prevented by input sanitization, but is prevented by namespaces. Discuss in **answers_B.txt**.

Submission Guidelines

1. Run your server on **port 8000**, since our test scripts have been written for that.
2. Save all **exploit_*** scripts, **unlink.S,** and **answers_*.txt** files in **KiliKili** directory**.** Do not change the location of **KiliKili_*** directories.

3. Run script **make_submission.sh** with your roll number as argument. This script will automatically create **<rollno>.tar** in **home/baahubali** directory. Submit this tar file.

   NOTE: You must still check the correct submission by extracting the tar file. You must not blame the script for wrong submission. Checklist of submission - KiliKili, KiliKili_B3, KiliKili_B4, KiliKili_B5; such that all the scripts and text files are present at their expected location.