worldskills
India

Skill India
कौशल भारत-कुशल भारत

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

Module B

IndiaSkills National Competition

Cyber Security

NASSCOM®

Description

The competition has a fixed start and finish time. You must decide how to best divide your time.

Please carefully read the following instructions!

- There are 4 parts to this Module and you have to submit a pdf report containing all 4 parts. You can make this report on Google Docs.
- The report format is provided on page 9-10.
- For each question (except in source code review), restrict yourself to 1–5-word answer wherever possible. Also provide screenshots supporting your answers. You can add explanation but only do that if you feel it is required.
- When the competition time ends, you need to submit the report on the provided Google Forms link.
- The filename of the report should be *YourState_YourName.pdf*
- Nothing would be checked on your machines and only your reports would be used for assigning marks.
- The provided tasks can be completed in any order, but have to be reported in the order the questions have been asked.
- Marking for each section has been provided in brackets

  Google Forms Link: https://forms.gle/YAnDRB7E2VXiWMCE6

Part 1: USB Forensics (9)

You are a Forensic Investigator, deputed to investigate an incident of an individual who has been misusing an organization fund and has been travelling. As part of the investigation, you have confiscated a USB drive from him for the analysis. This individual is technology savvy and has adopted few techniques for securing the evidence. As a forensic investigator, you have been given the forensic image of the USB drive for analysis. Kindly answer the below questions, based on the evidence extracted from the image. You have to load the image (present in USB Forensics folder) in AccessData Forensic Toolkit for the analysis.

1. What is the password of the zip file?
2. What is the name of the individual?
3. What is the day & month of his travel?
4. Which international destination he has visited?
5. Where was he staying?
6. What is the registration number of the taxi hired during that individual's travel destination?

Part 2: Memory Forensics (12.5)

You are provided with two memory dumps. Analyze the dumps using Volatility (present in Memory Forensics folder) and answer the following questions.

1. **mexo.vmem (5)**
   a. What is the name of the malicious process?
   b. What is the PPID of the malicious process?
   c. With which IP is communication happening at the time RAM dump was taken?
   d. With regards to the above question, also mention the other malicious IP and Port?
   e. What HTTP request(Method and URI) is the malware making at the time of RAM dump?
   f. Mention all malicious IPs you have found?
   g. Where is the malware actually stored(Give complete path)?
   h. List the mutants used by the malware?
   i. Based on the info you have gathered, what is the goal of the malware?
   j. Based on the info you have gathered, how is the process(determined in Q1) related to the malware?

2. krono.vmem (7.5)

a. What is the name of the malicious process?
b. Where did the process start running from?
c. Dump the malicious binary and provide the MD5 sum(Hint: It starts with 3D and ends with 0C)?
d. What was the IP address of the machine at the time the RAM dump was created?
e. What is the C2 domain:port for Malware?
f. What is the IP for the domain when the RAM dump was created?
g. What is the PPID of the process that launched the Malware?
h. Which other process was launched by the same PPID?
i. Which process is further launched by the malware?
j. What is the mutex used by the malware?
k. What is the file where the malware is storing its logs?
l. What kind of malicious behaviour is the malware exhibiting based on the logs?
m. Which SubKey does the malware use for Persistance?
n. What is the name of the malware?
o. What is the value of GENCODE based on the malware config?

Part 3: Network Traffic Analysis (8.5)

You are provided with two packet captures (present in Network Traffic Analysis folder). Analyze the captures using Wireshark and answer the following questions.

1. rejuve.pcapng (5)

a. How many ping requests were sent?
b. What is the IP address for the MAC 08:00:27:4b:e3:60
c. What version of Internet Group Management Protocol is in use?
d. What is the hostname of the device at 10.0.2.22?
e. What is the hostname of the device at 10.0.2.15?
f. What is the IP address of the DHCP Server?
g. What is the IP address of the attacker?
h. What was the first command run by attacker?
i. What is the process ID of the RDP session?
j. What is the source port for the RDP session?

2. volta.zip (3.5)

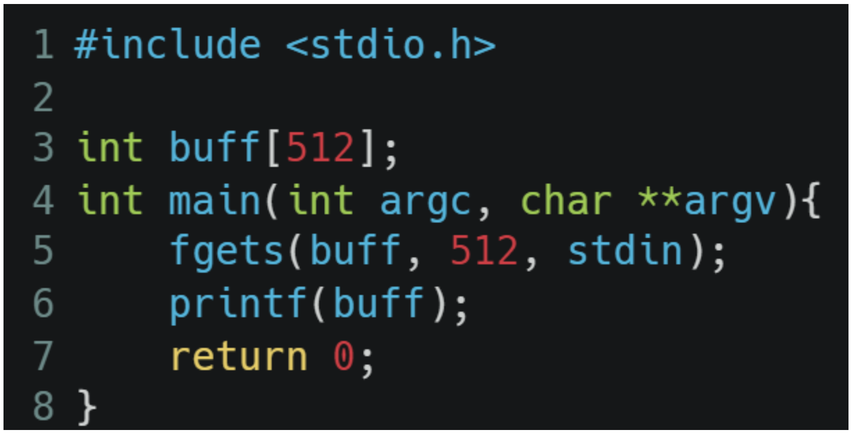
a. Identify the IP address, MAC Address, & Hostname of all 3 machines that were infected?
b. Which machine was not actually infected and was a false positive?

c. Which exploit kit was used for the infection?
d. What was the domain it was hosted on?
e. Regarding the previous question, what was the type of malware downloaded?
f. What was the infection vector for the other machine?
g. What was the type of file downloaded, what was its actual extension?

Part 4: Source Code Analysis (7.5)

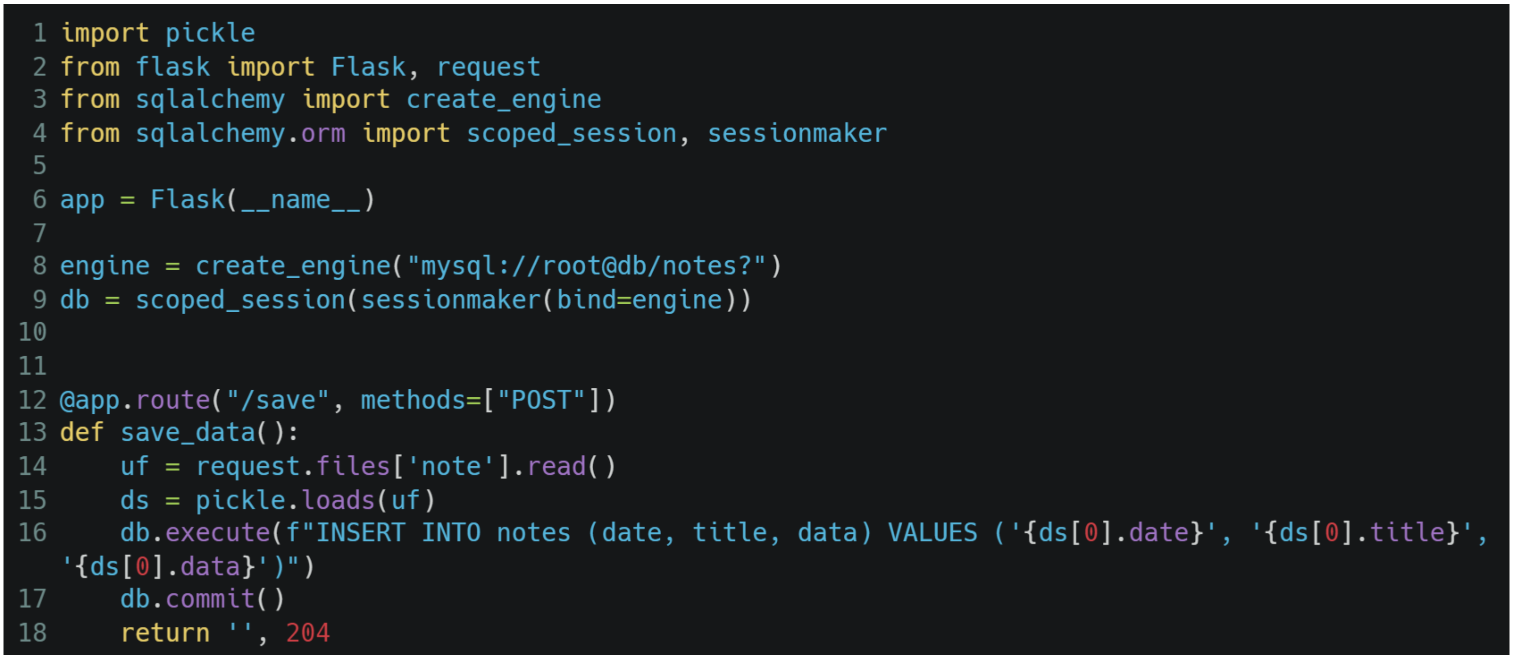
You are provided with 5 code snippets (present in Source Code Review folder) in different languages. Identify the vulnerabilities in all the snippets and mention the line number, the name of the vulnerability, the impact it can have and provide the fixed code snippet

1.c



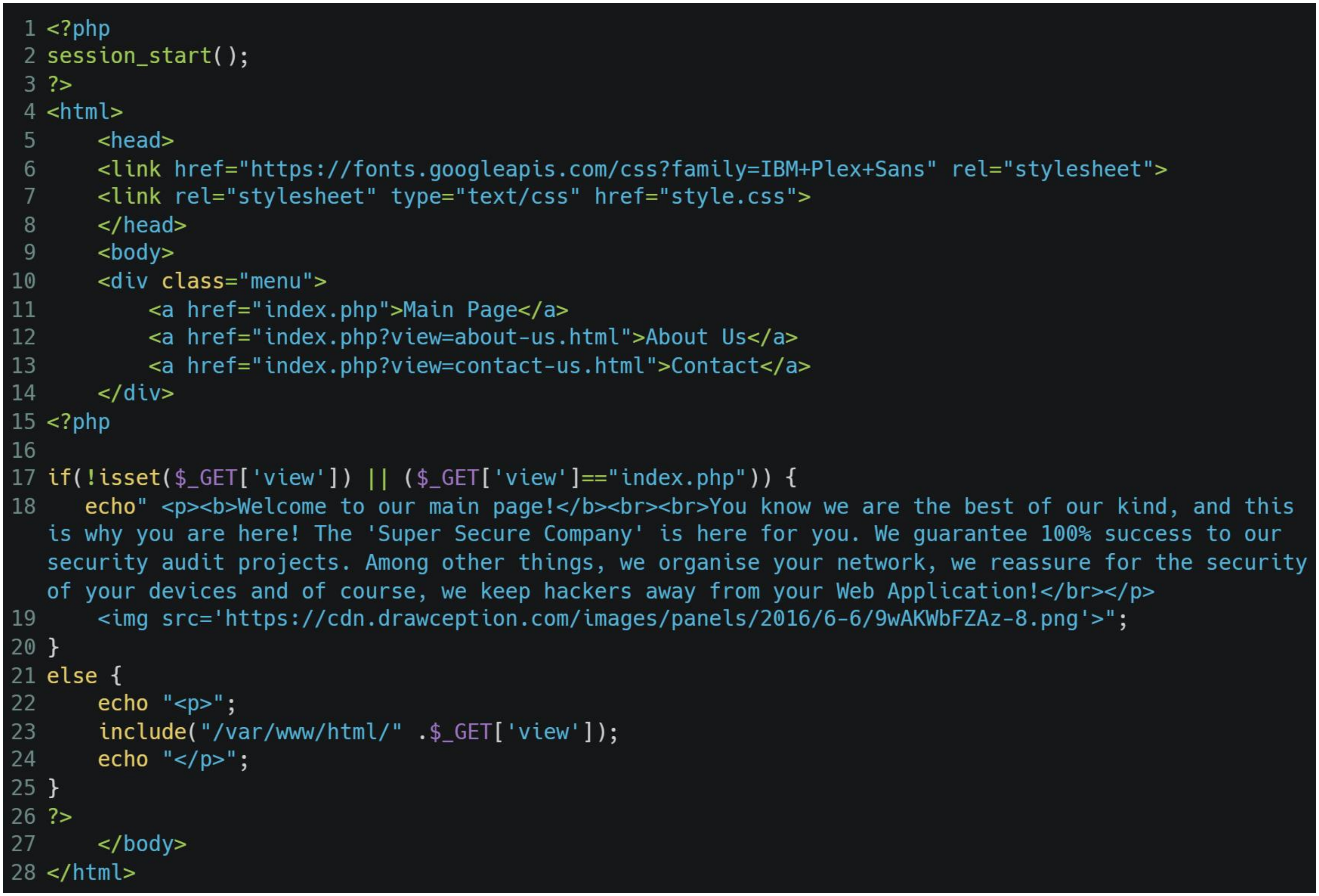
```c
1 #include <stdio.h>
2
3 int buff[512];
4 int main(int argc, char **argv){
5     fgets(buff, 512, stdin);
6     printf(buff);
7     return 0;
8 }
```

2.py



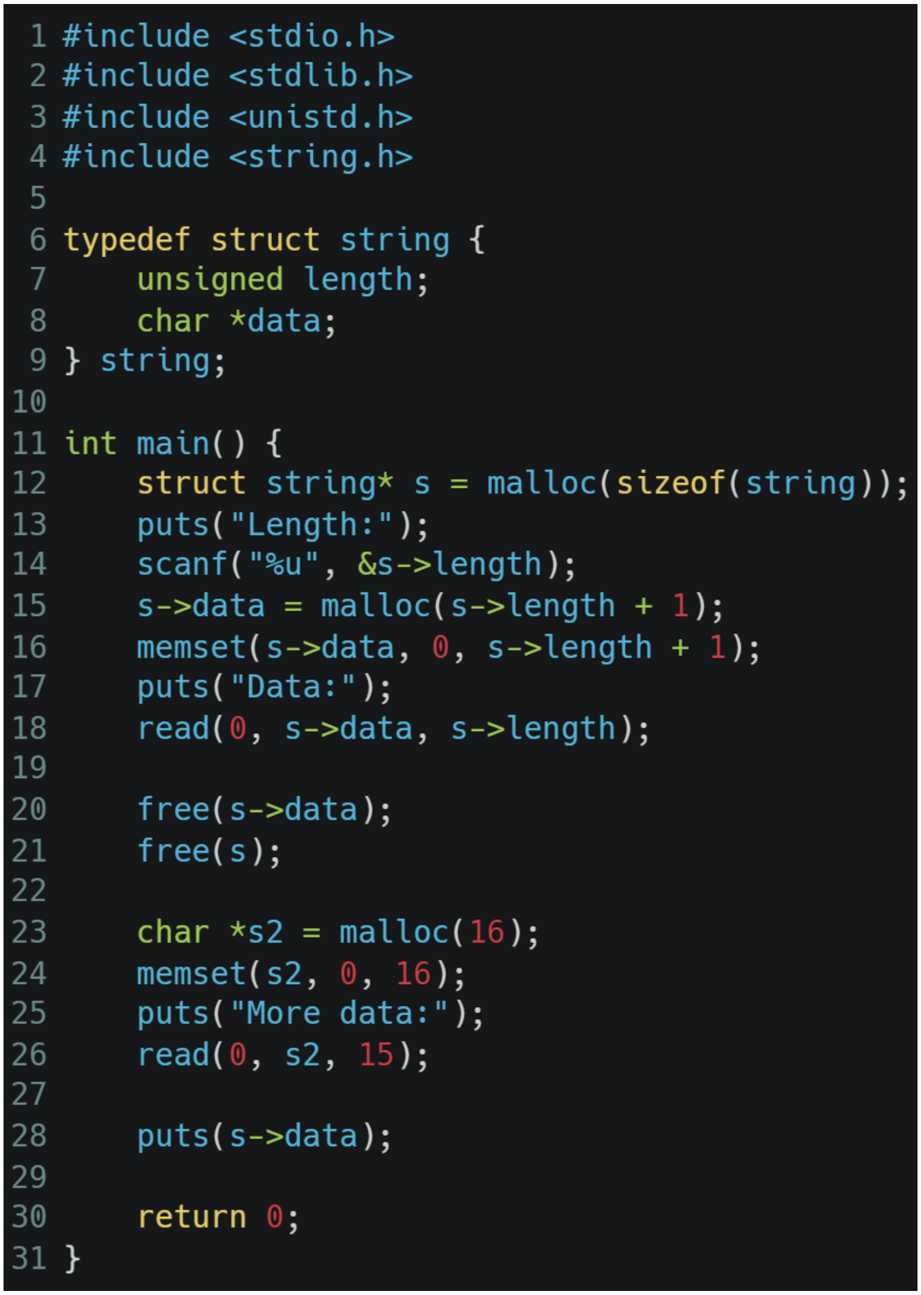
```python
 1 import pickle
 2 from flask import Flask, request
 3 from sqlalchemy import create_engine
 4 from sqlalchemy.orm import scoped_session, sessionmaker
 5
 6 app = Flask(__name__)
 7
 8 engine = create_engine("mysql://root@db/notes?")
 9 db = scoped_session(sessionmaker(bind=engine))
10
11
12 @app.route("/save", methods=["POST"])
13 def save_data():
14     uf = request.files['note'].read()
15     ds = pickle.loads(uf)
16     db.execute(f"INSERT INTO notes (date, title, data) VALUES ('{ds[0].date}', '{ds[0].title}', '{ds[0].data}')")
17     db.commit()
18     return '', 204
```

3.php



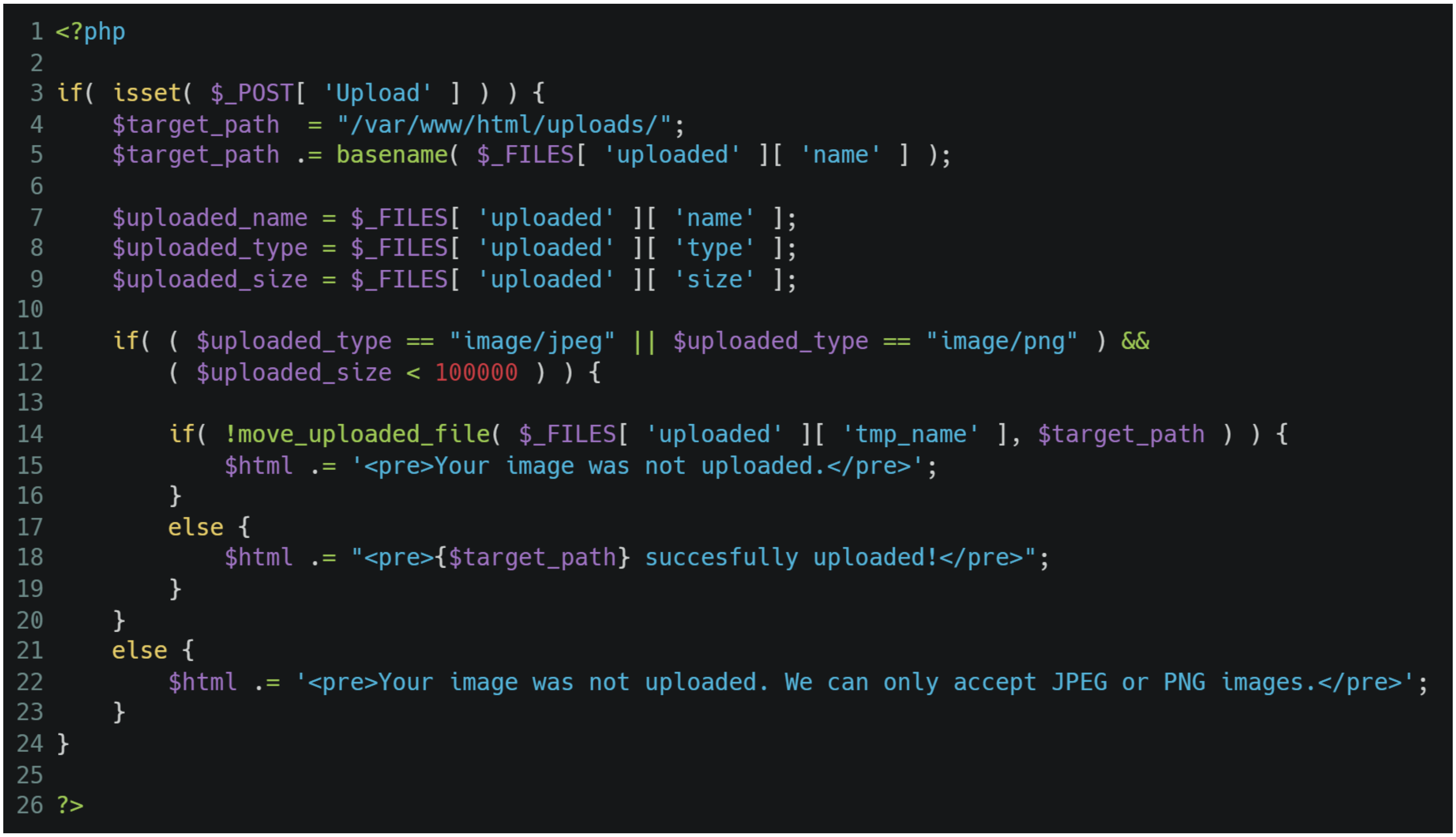
```
<?php
session_start();
?>
<html>
    <head>
    <link href="https://fonts.googleapis.com/css?family=IBM+Plex+Sans" rel="stylesheet">
    <link rel="stylesheet" type="text/css" href="style.css">
    </head>
    <body>
    <div class="menu">
        <a href="index.php">Main Page</a>
        <a href="index.php?view=about-us.html">About Us</a>
        <a href="index.php?view=contact-us.html">Contact</a>
    </div>
<?php

if(!isset($_GET['view']) || ($_GET['view']=="index.php")) {
   echo" <p><b>Welcome to our main page!</b><br><br>You know we are the best of our kind, and this is why you are here! The 'Super Secure Company' is here for you. We guarantee 100% success to our security audit projects. Among other things, we organise your network, we reassure for the security of your devices and of course, we keep hackers away from your Web Application!</br></p>
    <img src='https://cdn.drawception.com/images/panels/2016/6-6/9wAKWbFZAz-8.png'>";
}
else {
    echo "<p>";
    include("/var/www/html/" .$_GET['view']);
    echo "</p>";
}
?>
    </body>
</html>
```

4.c



```c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>

typedef struct string {
    unsigned length;
    char *data;
} string;

int main() {
    struct string* s = malloc(sizeof(string));
    puts("Length:");
    scanf("%u", &s->length);
    s->data = malloc(s->length + 1);
    memset(s->data, 0, s->length + 1);
    puts("Data:");
    read(0, s->data, s->length);

    free(s->data);
    free(s);

    char *s2 = malloc(16);
    memset(s2, 0, 16);
    puts("More data:");
    read(0, s2, 15);

    puts(s->data);

    return 0;
}
```

5.php



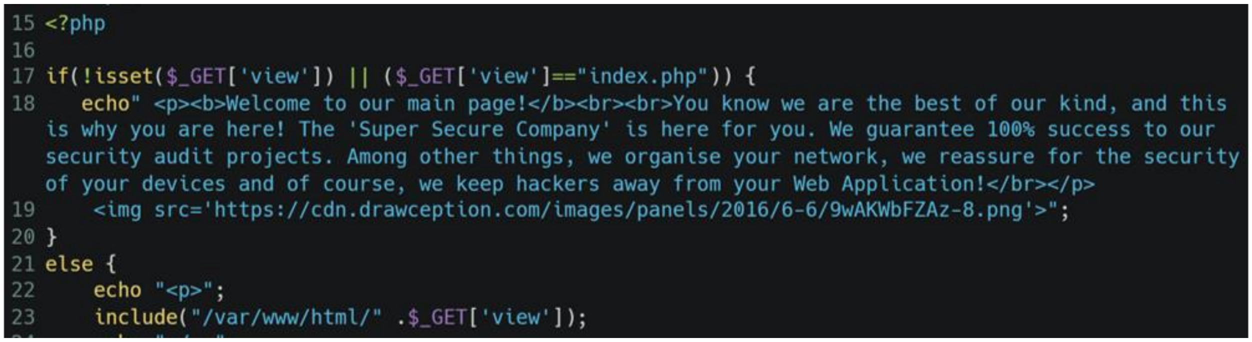
```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    $target_path  = "/var/www/html/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];

    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
        ( $uploaded_size < 100000 ) ) {

        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            $html .= '<pre>Your image was not uploaded.</pre>';
        }
        else {
            $html .= "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        $html .= '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

Module B Report by mention Name

Category: USB Forensics

1. Write your answer

   Attach screenshot(s if needed) for the answer

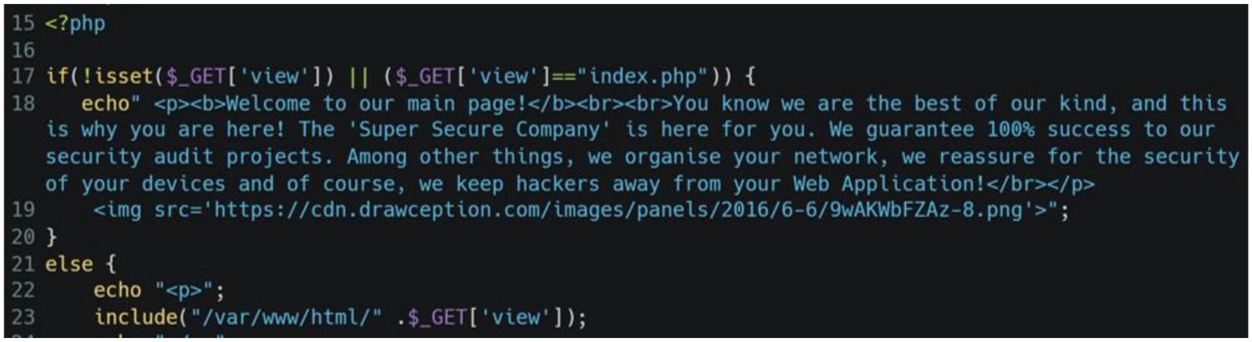


```
<?php

if(!isset($_GET['view']) || ($_GET['view']=="index.php")) {
   echo" <p><b>Welcome to our main page!</b><br><br>You know we are the best of our kind, and this is why you are here! The 'Super Secure Company' is here for you. We guarantee 100% success to our security audit projects. Among other things, we organise your network, we reassure for the security of your devices and of course, we keep hackers away from your Web Application!</br></p>
    <img src='https://cdn.drawception.com/images/panels/2016/6-6/9wAKWbFZAz-8.png'>";
}
else {
    echo "<p>";
    include("/var/www/html/" .$_GET['view']);
```

   Write explanation if any

2. Write next answer

   Attach screenshot(s if needed) for the answer



```
<?php

if(!isset($_GET['view']) || ($_GET['view']=="index.php")) {
   echo" <p><b>Welcome to our main page!</b><br><br>You know we are the best of our kind, and this is why you are here! The 'Super Secure Company' is here for you. We guarantee 100% success to our security audit projects. Among other things, we organise your network, we reassure for the security of your devices and of course, we keep hackers away from your Web Application!</br></p>
    <img src='https://cdn.drawception.com/images/panels/2016/6-6/9wAKWbFZAz-8.png'>";
}
else {
    echo "<p>";
    include("/var/www/html/" .$_GET['view']);
```

   Write explanation if any

Category: Repeat for all categories except Source Code Review

Category: Source Code Review

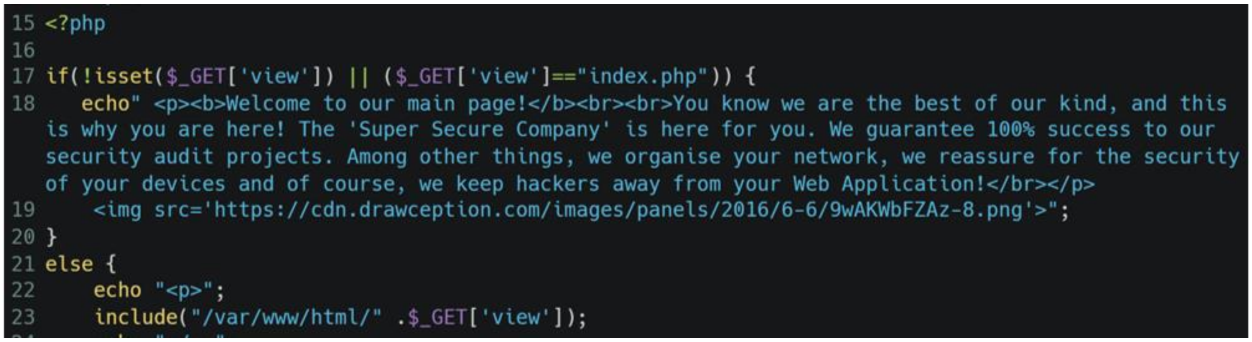
Filename: lol.py

Name of vulnerability

Impact it can have and how

How can it be prevented?

Add screenshot of fixed code snippet (if possible)



```
<?php

if(!isset($_GET['view']) || ($_GET['view']=="index.php")) {
   echo" <p><b>Welcome to our main page!</b><br><br>You know we are the best of our kind, and this is why you are here! The 'Super Secure Company' is here for you. We guarantee 100% success to our security audit projects. Among other things, we organise your network, we reassure for the security of your devices and of course, we keep hackers away from your Web Application!</br></p>
    <img src='https://cdn.drawception.com/images/panels/2016/6-6/9wAKWbFZAz-8.png'>";
}
else {
    echo "<p>";
    include("/var/www/html/" .$_GET['view']);
```

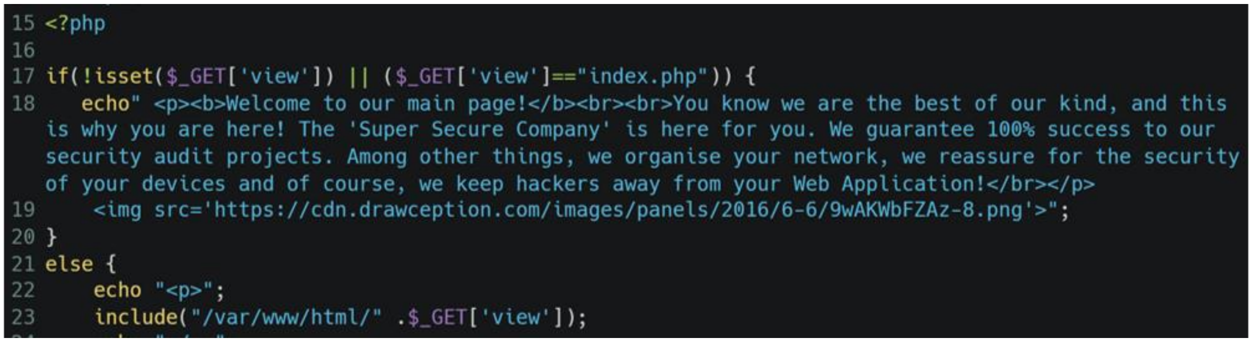
Filename: Repeat for next file.c

Name of vulnerability

Impact it can have and how

How can it be prevented?

Add screenshot of fixed code snippet



```
<?php

if(!isset($_GET['view']) || ($_GET['view']=="index.php")) {
   echo" <p><b>Welcome to our main page!</b><br><br>You know we are the best of our kind, and this is why you are here! The 'Super Secure Company' is here for you. We guarantee 100% success to our security audit projects. Among other things, we organise your network, we reassure for the security of your devices and of course, we keep hackers away from your Web Application!</br></p>
    <img src='https://cdn.drawception.com/images/panels/2016/6-6/9wAKWbFZAz-8.png'>";
}
else {
    echo "<p>";
    include("/var/www/html/" .$_GET['view']);
```