Offensive Security

OSWE Exam Documentation

v1.0

bing.ecnu@gmai.com
OS@111111

Contents

1 Offensive-Security OSWE Exam Documentation

https://github.com/madneal/oswe-report-teplate

The Offensive Security OSWE exam documentation contains all efforts that were conducted in order to pass the Offensive Security Web Expert exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has the technical knowledge required to pass the qualifications for the Offensive Security Web Expert certification.
The student will be required to fill out this exam documentation fully and to include the following sections:

- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 192.168.XX.XX

2.1 Local.txt / Proof.txt

Provide the contents of local.txt and proof.txt

2.2 Vulnerability 1

Provide the method and code used to find the vulnerability 1.

2.3 Vulnerability 2

Provide the method and code used to find the vulnerability 2.

2.4 Vulnerability X

Provide the method and code used to find the vulnerability X

2.5 PoC Code

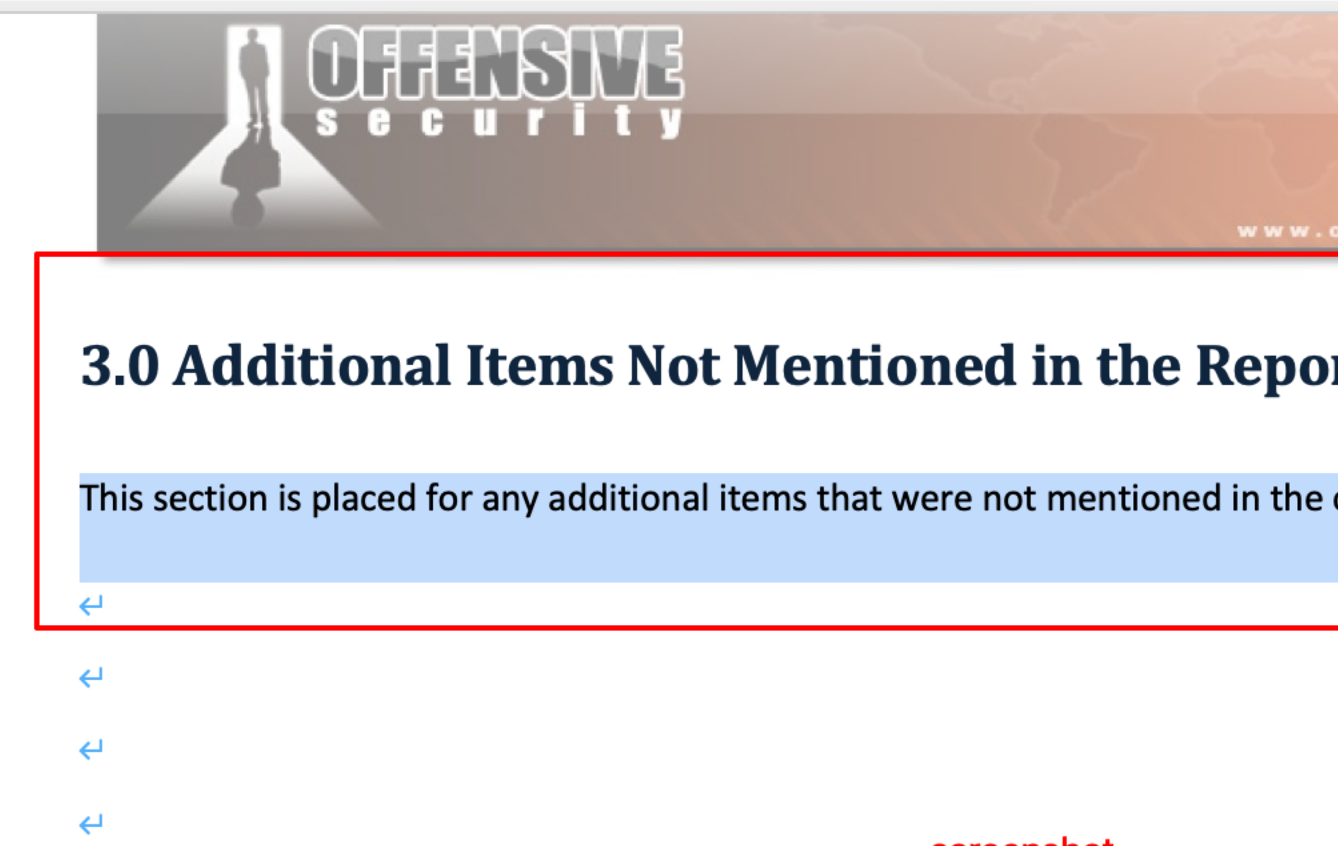
Provide the final proof of concept code used to gain access to the server.

```
import numpy as np

def incmatrix(genl1,genl2):
    m = len(genl1)
    n = len(genl2)
    M = None #to become the incidence matrix
    VT = np.zeros((n*m,1), int) #dummy variable

    #compute the bitwise xor matrix
    M1 = bitxormatrix(genl1)
    M2 = np.triu(bitxormatrix(genl2),1)

    for i in range(m-1):
        for j in range(i+1, m):
            [r,c] = np.where(M2 == M1[i,j])
            for k in range(len(r)):
                VT[(i)*n + r[k]] = 1;
                VT[(i)*n + c[k]] = 1;
                VT[(j)*n + r[k]] = 1;
                VT[(j)*n + c[k]] = 1;

                if M is None:
                    M = np.copy(VT)
                else:
                    M = np.concatenate((M, VT), 1)

                VT = np.zeros((n*m,1), int)
    return M
```

```
import java.util.Scanner;

blic class HelloWorld {

  public static void main(String[] args) {

      // Creates a reader instance which takes
      // input from standard input - keyboard
      Scanner reader = new Scanner(System.in);
      System.out.print("Enter a number: ");

      // nextInt() reads the next integer from the keyboard
      int number = reader.nextInt();

      // println() prints the following line to the output screen
      System.out.println("You entered: " + number);
  }
```

2.6 Screenshots

Provide screenshots of local.txt and proof.txt contents as stated in the Exam Control Panel Objectives.



3.0 Additional Items Not Mentioned in the Repo

This section is placed for any additional items that were not mentioned in the

screenshot

2.7 Steps

Provide a detailed account of your methodology in creating the exploits. The steps taken should be able to be easily followed and reproducible if necessary.

3 Additional Items Not Mentioned in the Report

This section is placed for any additional items that were not mentioned in the overall report.