JAVA BANKING MANAGEMENT AND SECURITY

**Users**

* User Registration
* User forgot Password
* After login user can lodge complaint
* Complaint History
* Profile Management
* Change Password
* Dashboard

Malware reverse engineering, on the other hand, is the process of breaking down malware into low-level lines of code, usually assembly code, to fully understand its function. It requires that you can read and understand low-level code. This is where knowledge of assembly language becomes crucial. It is needed to decipher and read low-level code. Without this knowledge, it will be impossible to trace each line of code’s execution flow let alone understand what each line of code actually means.

**Ransomware:** Ransomware is a type of a malware that restricts access to the computer system’s files and folders and demands an online ransom payment to the malware

The following are the activities of the adversary:

o Downloading and installing malicious software such as backdoors

o Gaining remote access to the target system

o Leveraging various methods to keep backdoor hidden and running

o Maintaining access to the target system

while($row = mysql\_fetch\_array($result, MYSQL\_ASSOC))

{

// display the results to the browser

echo “Description : {$row[‘ProductDescription’]} <br>”.

“Product ID : {$row[‘ProductID’]} <br>”.

“Price : {$row[‘Price’]} <br><br>”;

}

**HTTP User Agent**

In HTTP-based communication, the server identifies the connected HTTP client using the

user agent field. An adversary modifies the content of the HTTP user agent field to

communicate with the compromised system and to carry further attacks. Therefore,

security professionals can identify this attack at an initial stage by checking the content

of the user agent field.

The URL examples in this chapter use *GET* parameters instead of

*POST* parameters for ease of illustration. *POST* parameters are just

as easy to manipulate; however, this usually involves the use of

something else, such as a tra􀉽c manipulation tool, Web browser

plug-in, or inline proxy application.

This time, however, you are going to attempt to inject your own

SQL commands by appending them to the input parameter *val*. You

can do this by appending the string *􀂶OR 􀂶1’= 􀂶1* to the URL:

“AND password = ‘$\_GET[“password”]’”;

// execute the query against the database

$result = mysql\_query($query);

// check to see how many rows were returned from the database

$rowcount = mysql\_num\_rows($result);

// if a row is returned then the credentials must be valid, so

// forward the user to the admin pages

if ($rowcount ! = 0){header(“Location: admin.php”);}

// if a row is not returned then the credentials must be invalid

else {die(‘Incorrect username or password, please try again.’)}

**sGray Hats**: Gray hats are the individuals who work both offensively and defensively at

various times. Gray hats might help hackers to find various vulnerabilities in a system or

network and, at the same time, help vendors to improve products (software or

hardware) by checking limitations and making them more secure.

**Password Attacks**: Authentication systems are always a go-to attack vector. Many useful

tools can be found here, from online password attack tools to offline attacks against the

encryption or hashing systems