Task 6

A) Find the Flag {******} that is in the Vulnerable System

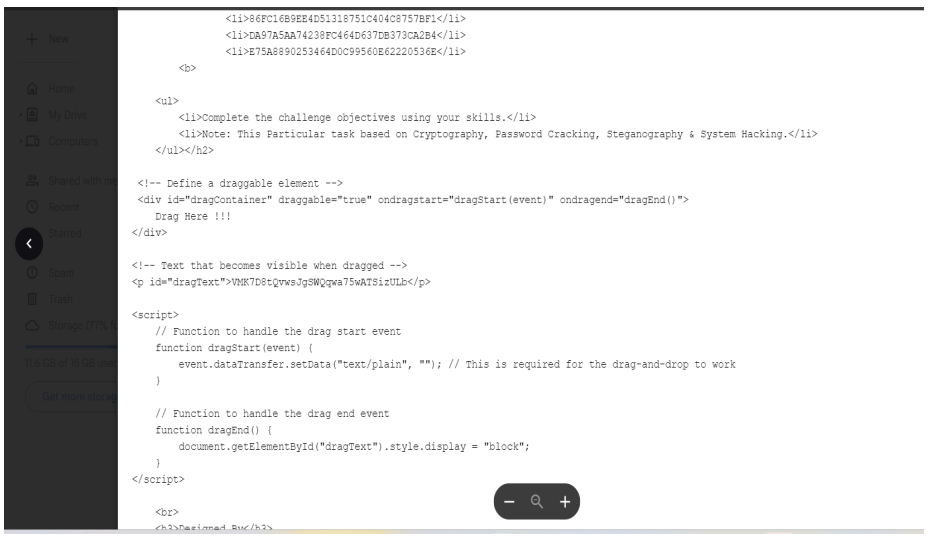
Identify the hidden message in the README file Decrypt the Secret Data to get a link

Download the OVA file from the link

Import the OVA file

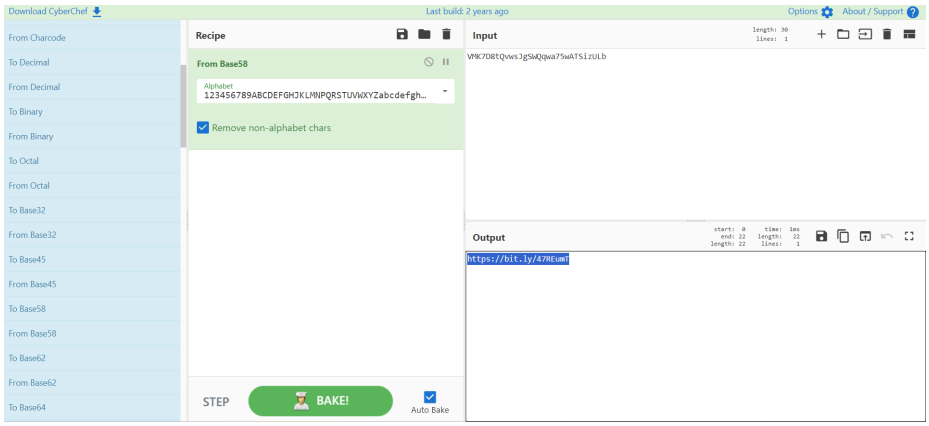
Tools used : cyberchef.io

Step 1 : Open the Readme file first and carefully read the hidden message

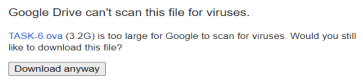


```
                <li>86FC16B9EE4D51318751C404C8757BF1</li>
                <li>DA97A5AA74238FC464D637DB373CA2B4</li>
                <li>E75A889025346 4D0C99560E62220536E</li>
        <b>

    <ul>
        <li>Complete the challenge objectives using your skills.</li>
        <li>Note: This Particular task based on Cryptography, Password Cracking, Steganography & System Hacking.</li>
    </ul></h2>

 <!-- Define a draggable element -->
 <div id="dragContainer" draggable="true" ondragstart="dragStart(event)" ondragend="dragEnd()">
    Drag Here !!!
</div>

<!-- Text that becomes visible when dragged -->
<p id="dragText">VMK7D8tQvwsJgSWQqwa75wATSizULb</p>

<script>
    // Function to handle the drag start event
    function dragStart(event) {
        event.dataTransfer.setData("text/plain", ""); // This is required for the drag-and-drop to work
    }

    // Function to handle the drag end event
    function dragEnd() {
        document.getElementById("dragText").style.display = "block";
    }
</script>

    <br>
```

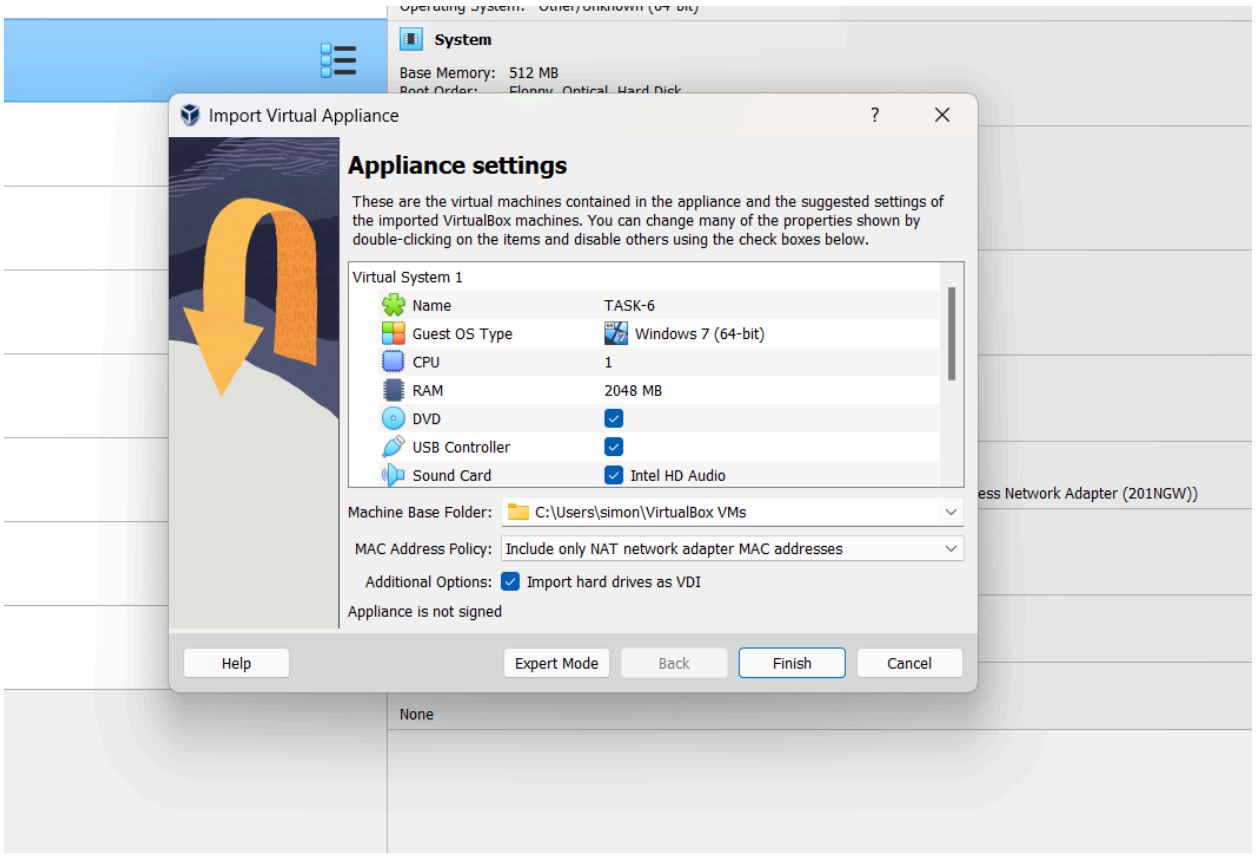
Step 2 : The message is in the encrypted format we need to decrypt message using tools like cyberchef and use Base58 for decryption



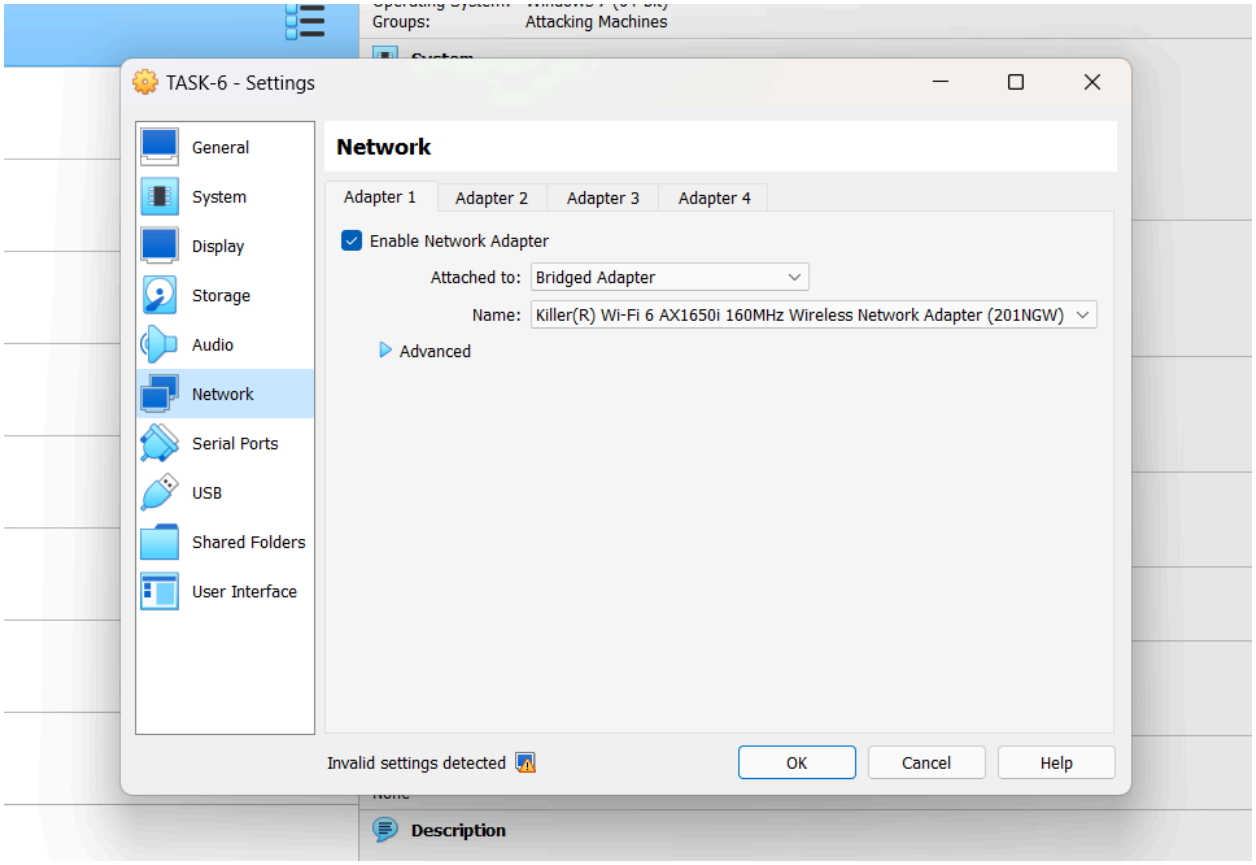
Step 3 : When decrypted we will get a link to download, open that link in browser and click on download the OVA



Step 4 : Import the OVA into virtual box, just double click on the OVA file which we downloaded, if might ask permission just click on agree and finish



Step 5 : Check the network setting and change the network setting to bridge adapter because the Kali linux machine is in bridge adapter



B) Gaining Access

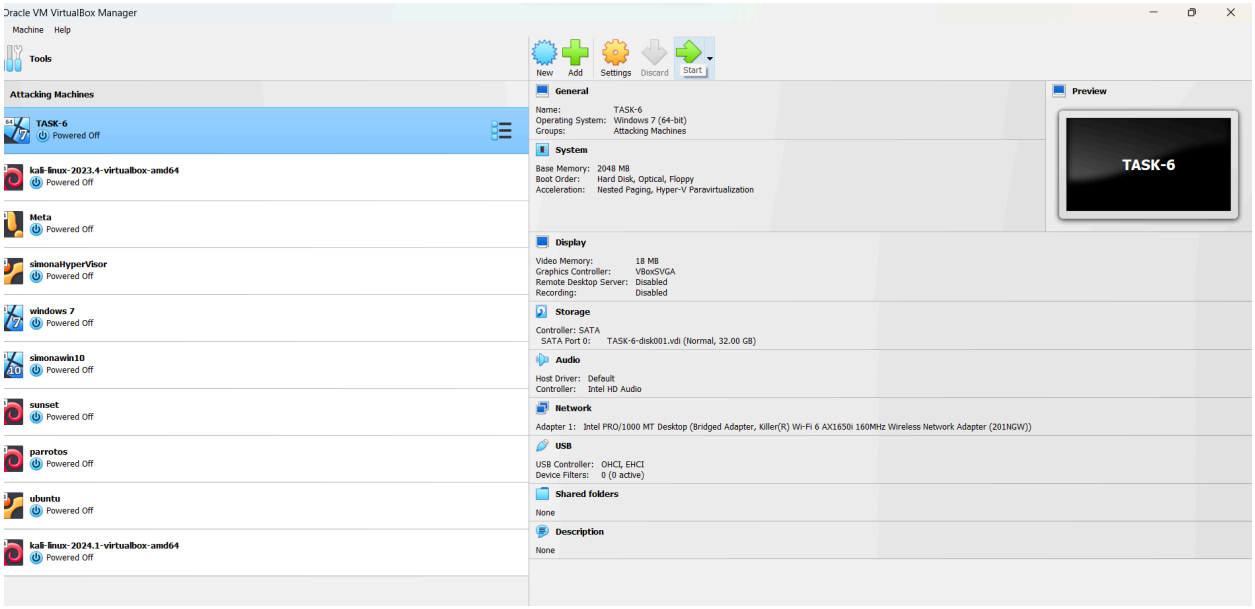
Method -1

Crack the system password

Using OPH-Crack Tool

Check the machine, if it consists of any files.

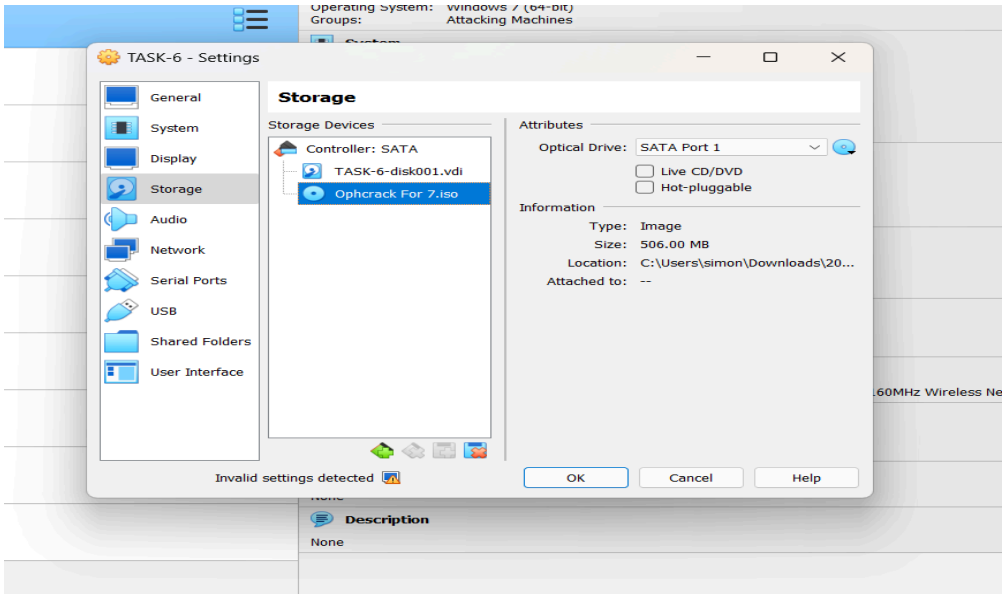
Step 1 : Go to the Virtual Machine and open the Task6 OS



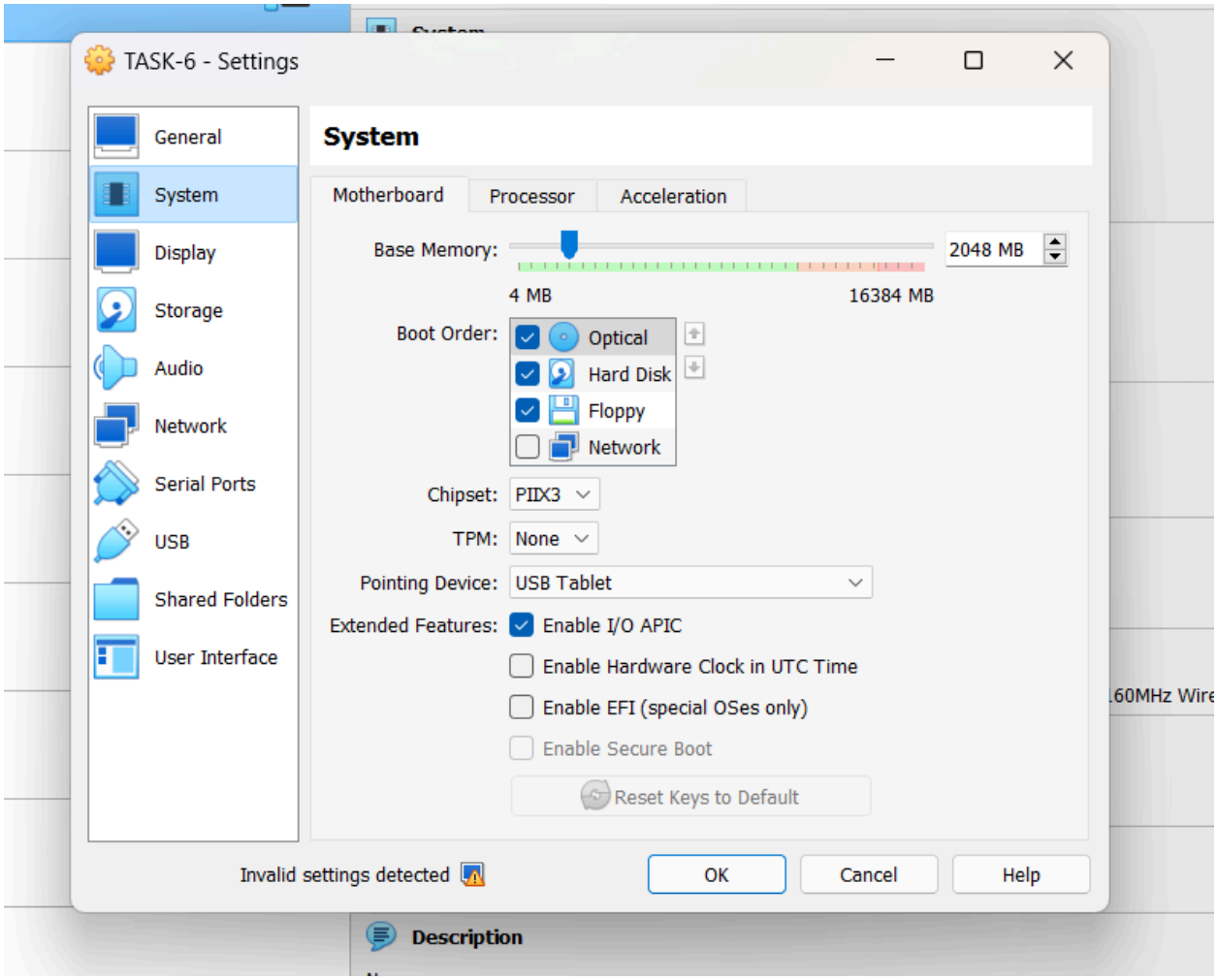
Step 2 : Once we open the machine we need to put the password, but since we are unaware about the password we need to crack the password using ophcrack

Step 3 : Shutdown this machine

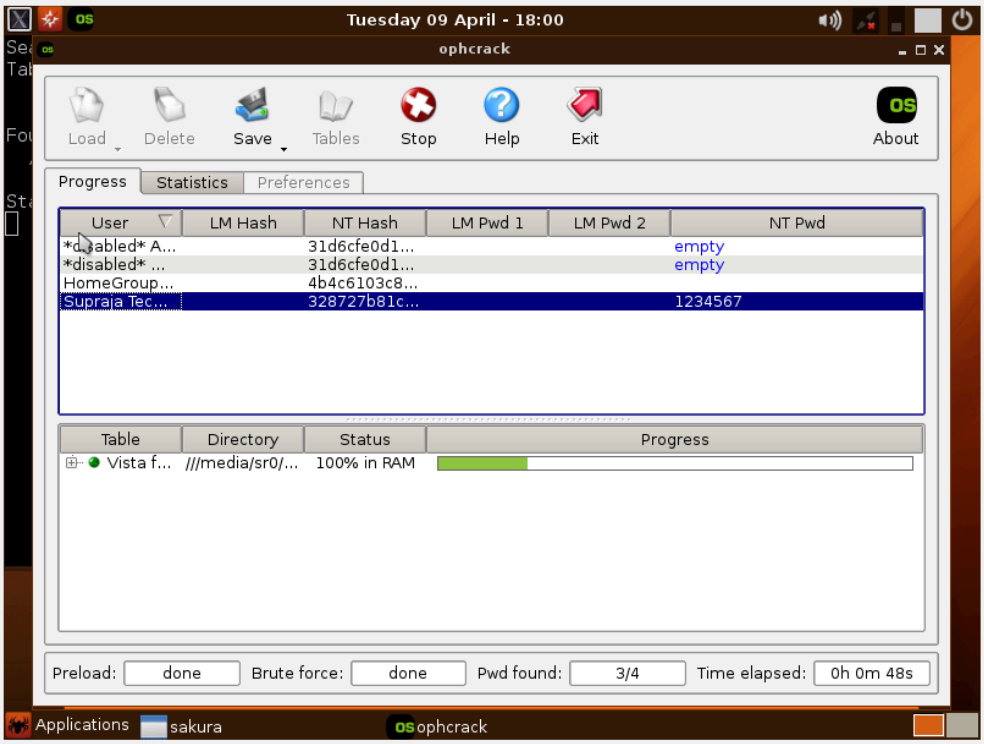
Step 4 : Go to the Virtual Machine and open settings and go to the storage tab, in the storage tab click on the empty and select the disk icon and put the OPH crack disk file in that



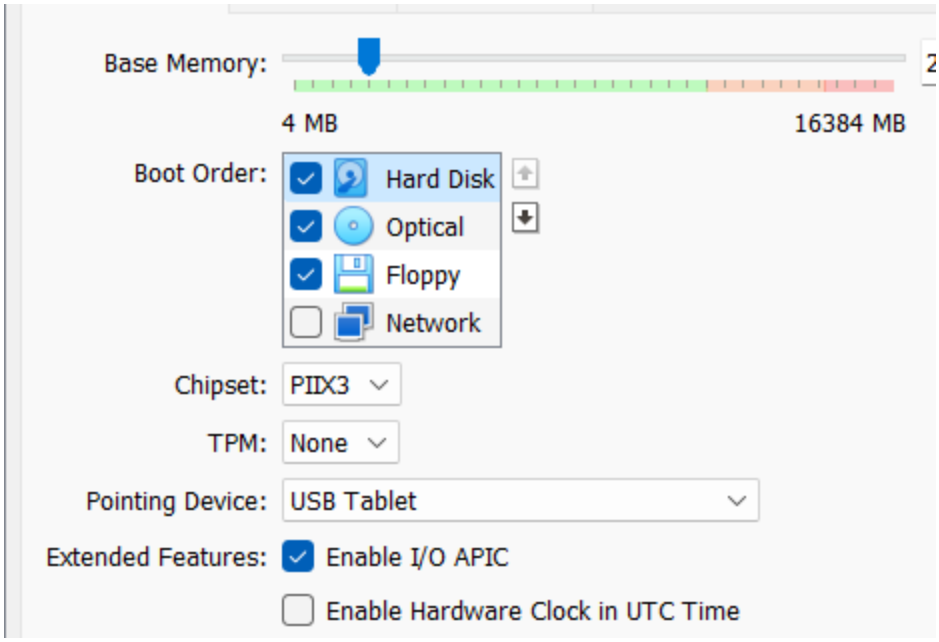
Step 5 : Then go to the system tab and select the optical file and click on upwards arrow and take the hard disk file down



Step 6 : Start the machine again, when you start the machine the oph tool will get open and in that we can see all the passwords



Step 7 : Then again shut down the machine, go to the storage tab remove the disk file and in the system tab again change the order to hard disk



Step 8 : Now we can start the machine and we have successfully cracked the password of the task6 ova file

C) Analysing the Checksums

Check the files in the system

Calculate the Checksums for it

Try to Identify the hidden data inside the Tampered document

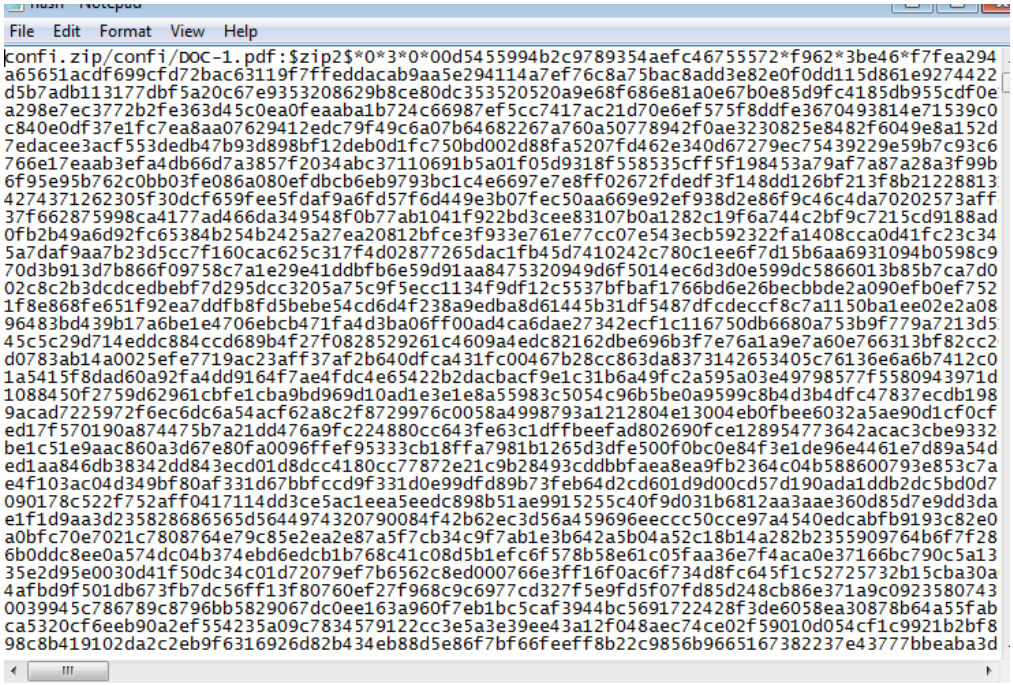
Identify the FLAG {*******}

Step 1: Open the Documents folder in the given machine

Step 2 : In the Documents folder we have confidential folder , open that confidential folder and extract it

Step 3: While extracting, it will ask for passwords to open that file

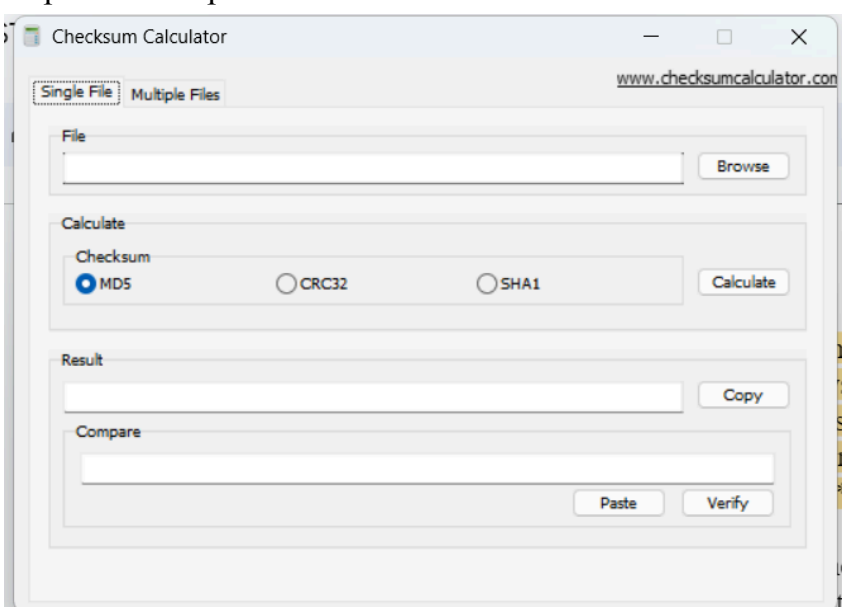
Step 4: We can get the password by using the tool JohntheRipper



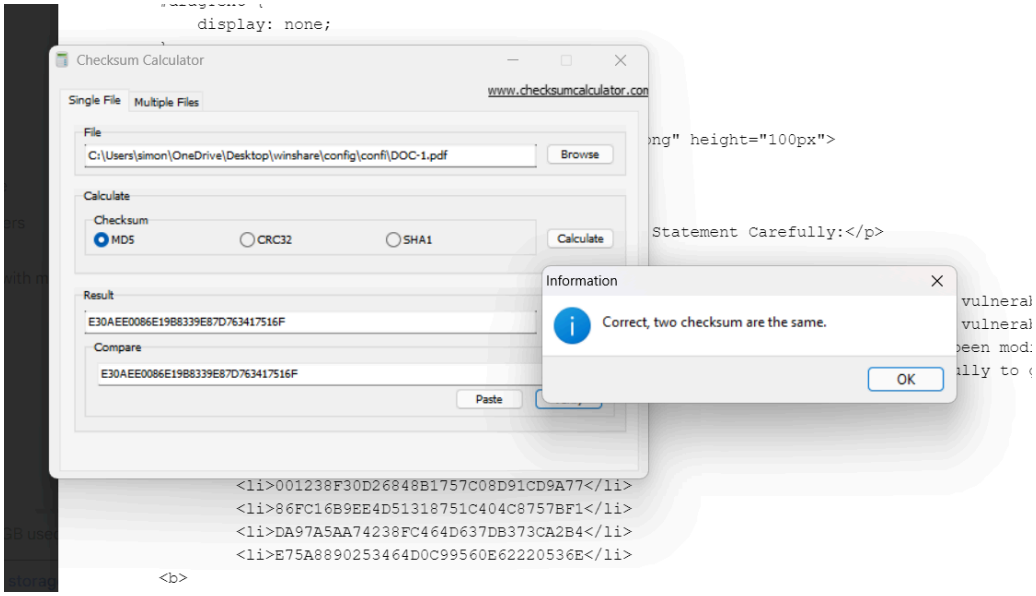
```
File  Edit  Format  View  Help
confi.zip/confi/DOC-1.pdf:$zip2$*0*3*0*00d5455994b2c9789354aefc46755572*f962*3be46*f7fea294
a65651acdf699cfd72bac63119f7ffeddacab9aa5e294114a7ef76c8a75bac8add3e82e0f0dd115d861e9274422
d5b7adb113177dbf5a20c67e9353208629b8ce80dc353520520a9e68f686e81a0e67b0e85d9fc4185db955cdf0e
a298e7ec3772b2fe363d45c0ea0feaaba1b724c66987ef5cc7417ac21d70e6ef575f8ddfe3670493814e71539c0
c840e0df37e1fc7ea8aa07629412edc79f49c6a07b64682267a760a50778942f0ae3230825e8482f6049e8a152d
7edacee3acf553dedb47b93d898bf12deb0d1fc750bd002d88fa5207fd462e340d67279ec75439229e59b7c93c6
766e17eaab3efa4db66d7a3857f2034abc37110691b5a01f05d9318f558535cff5f198453a79af7a87a28a3f99b
6f95e95b762c0bb03fe086a080efdbcb6eb9793bc1c4e6697e7e8ff02672fdedf3f148dd126bf213f8b21228813
4274371262305f30dcf659fee5fdaf9a6fd57f6d449e3b07fec50aa669e92ef938d2e86f9c46c4da70202573aff
37f662875998ca4177ad466da349548f0b77ab1041f922bd3cee83107b0a1282c19f6a744c2bf9c7215cd9188ad
0fb2b49a6d92fc65384b254b2425a27ea20812bfce3f933e761e77cc07e543ecb592322fa1408cca0d41fc23c34
5a7daf9aa7b23d5cc7f160cac625c317f4d02877265dac1fb45d7410242c780c1ee6f7d15b6aa6931094b0598c9
70d3b913d7b866f09758c7a1e29e41ddbfb6e59d91aa8475320949d6f5014ec6d3d0e599dc5866013b85b7ca7d0
02c8c2b3dcdcedbebf7d295dcc3205a75c9f5ecc1134f9df12c5537bfbaf1766bd6e26becbbde2a090efb0ef752
1f8e868fe651f92ea7ddfb8fd5bebe54cd6d4f238a9edba8d61445b31df5487dfcdeccf8c7a1150ba1ee02e2a08
96483bd439b17a6be1e4706ebcb471fa4d3ba06ff00ad4ca6dae27342ecf1c116750db6680a753b9f779a7213d5
45c5c29d714eddc884ccd689b4f27f0828529261c4609a4edc82162dbe696b3f7e76a1a9e7a60e766313bf82cc2
d0783ab14a0025efe7719ac23aff37af2b640dfca431fc00467b28cc863da8373142653405c76136e6a6b7412c0
1a5415f8dad60a92fa4dd9164f7ae4fdc4e65422b2dacbacf9e1c31b6a49fc2a595a03e49798577f5580943971d
1088450f2759d62961cbfe1cba9bd969d10ad1e3e1e8a55983c5054c96b5be0a9599c8b4d3b4dfc47837ecdb198
9acad7225972f6ec6dc6a54acf62a8c2f8729976c0058a4998793a1212804e13004eb0fbee6032a5ae90d1cf0cf
ed17f570190a874475b7a21dd476a9fc224880cc643fe63c1dffbeefad802690fce128954773642acac3cbe9332
be1c51e9aac860a3d67e80fa0096ffef95333cb18ffa7981b1265d3dfe500f0bc0e84f3e1de96e4461e7d89a54d
ed1aa846db38342dd843ecd01d8dcc4180cc77872e21c9b28493cddbbfaea8ea9fb2364c04b588600793e853c7a
e4f103ac04d349bf80af331d67bbfccd9f331d0e99dfd89b73feb64d2cd601d9d00cd57d190ada1ddb2dc5bd0d7
090178c522f752aff0417114dd3ce5ac1eea5eedc898b51ae9915255c40f9d031b6812aa3aae360d85d7e9dd3da
e1f1d9aa3d235828686565d5644974320790084f42b62ec3d56a459696eeccc50cce97a4540edcabfb9193c82e0
a0bfc70e7021c7808764e79c85e2ea2e87a5f7cb34c9f7ab1e3b642a5b04a52c18b14a282b2355909764b6f7f28
6b0ddc8ee0a574dc04b374ebd6edcb1b768c41c08d5b1efc6f578b58e61c05faa36e7f4aca0e37166bc790c5a13
35e2d95e0030d41f50dc34c01d72079ef7b6562c8ed000766e3ff16f0ac6f734d8fc645f1c52725732b15cba30a
4afbd9f501db673fb7dc56ff13f80760ef27f968c9c6977cd327f5e9fd5f07fd85d248cb86e371a9c0923580743
0039945c786789c8796bb5829067dc0ee163a960f7eb1bc5caf3944bc5691722428f3de6058ea30878b64a55fab
ca5320cf6eeb90a2ef554235a09c7834579122cc3e5a3e39ee43a12f048aec74ce02f59010d054cf1c9921b2bf8
98c8b419102da2c2eb9f6316926d82b434eb88d5e86f7bf66feeff8b22c9856b9665167382237e43777bbeaba3d
```

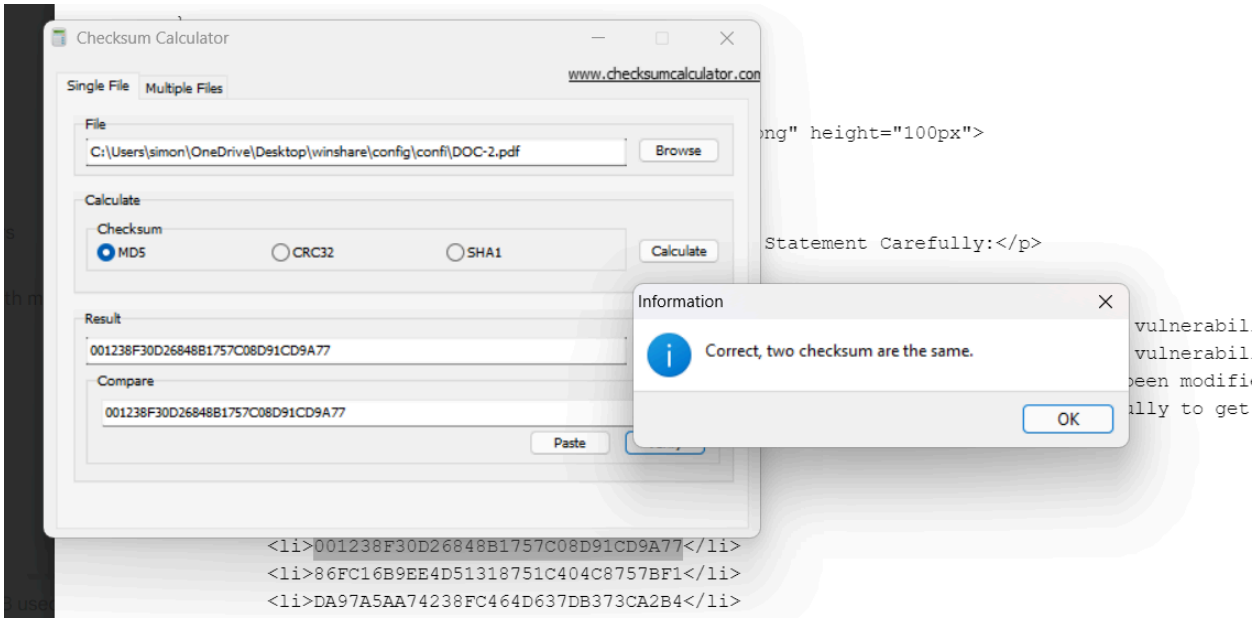
Step 5 : Once we have the passwords , we can open the documents

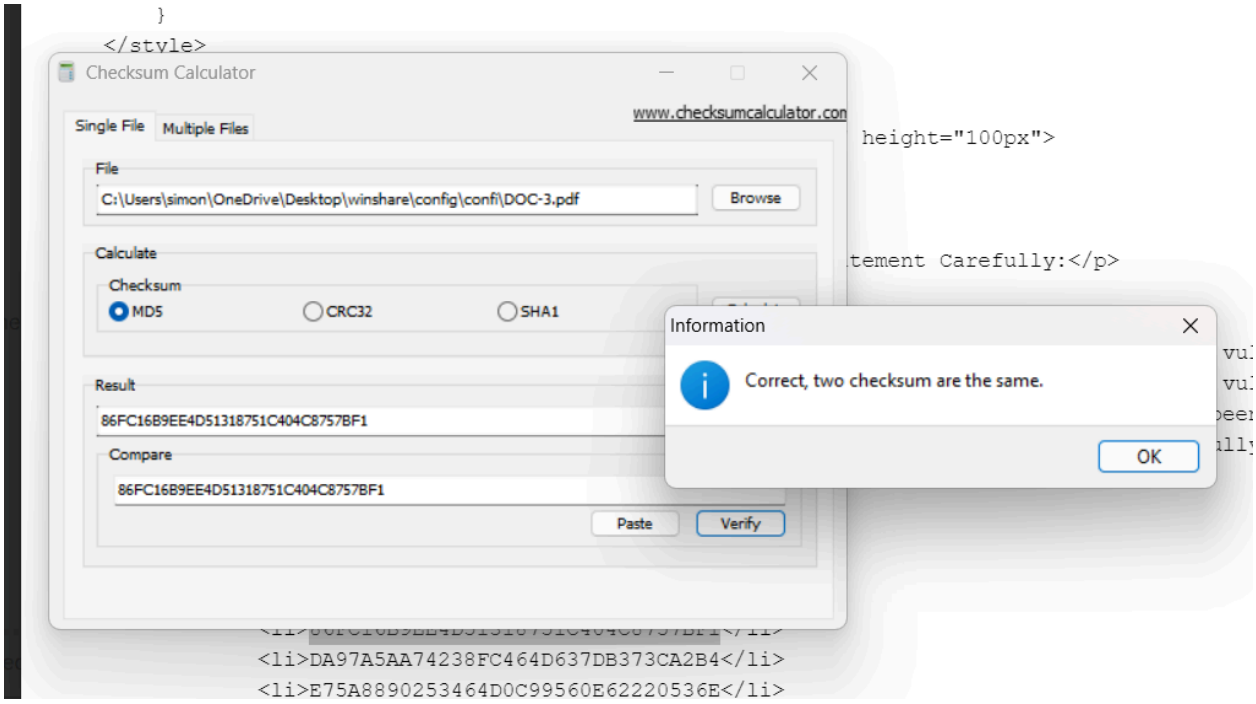
Step 6 : Now open the checksum calculator

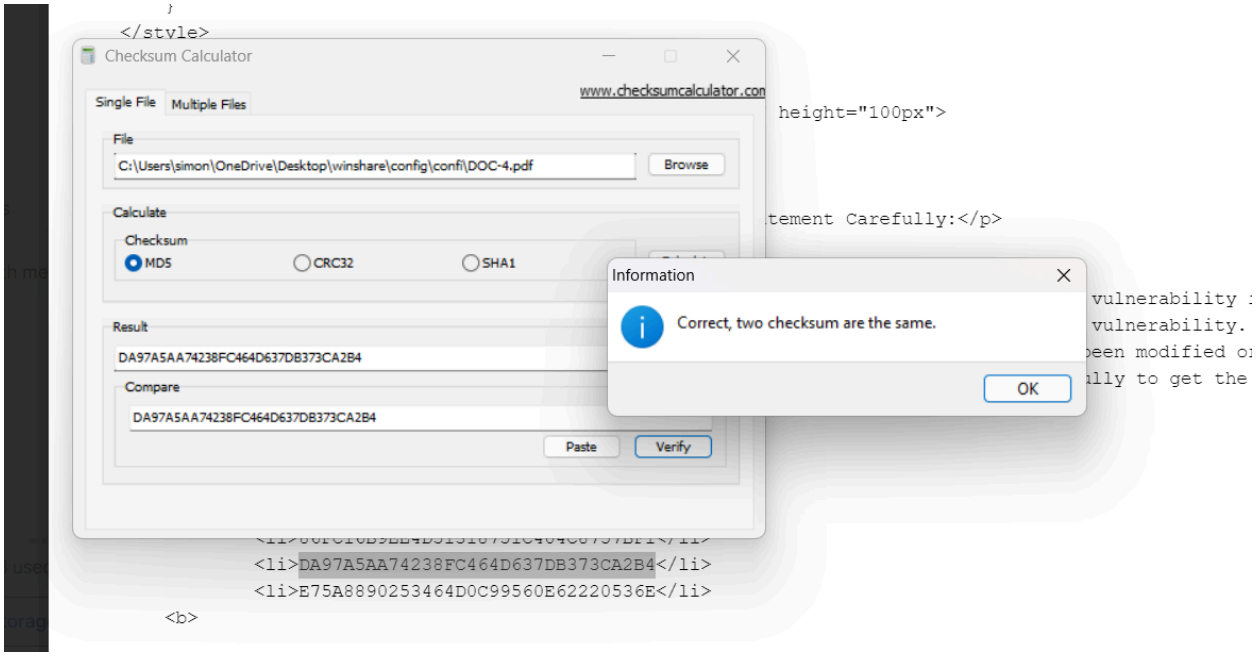


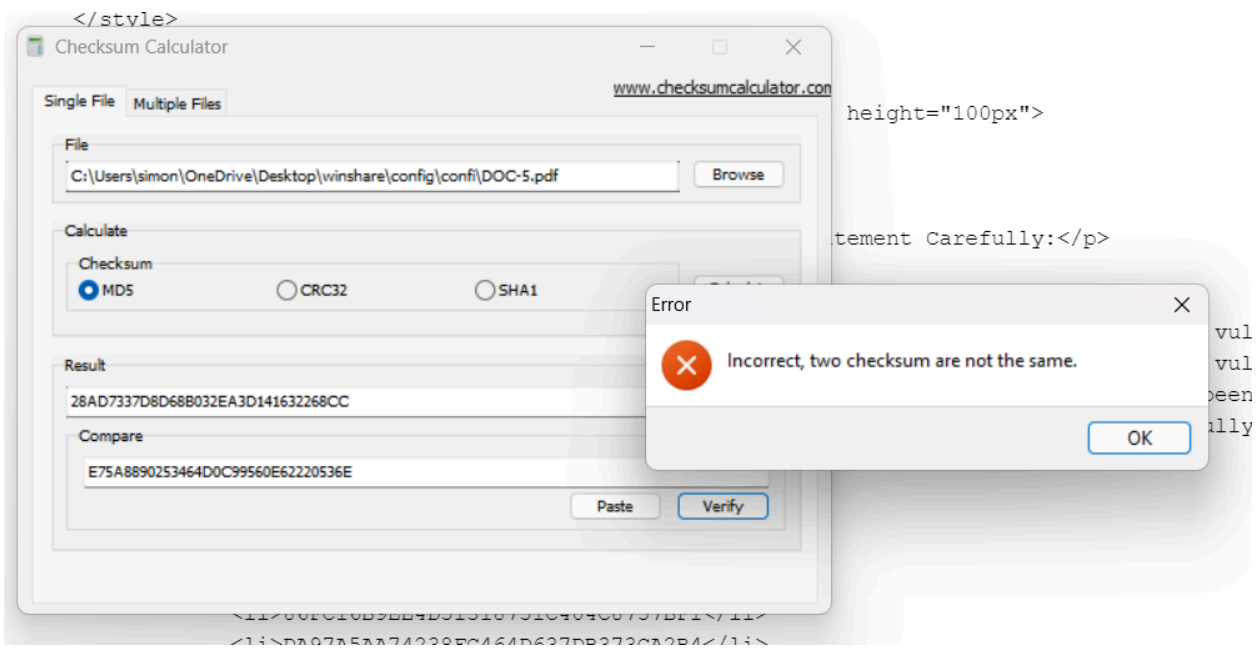
Step 7 : Browser the documents and calculate the hash value , then go to the readme file give and copy the given hash values and put it compare and verify those, we will get the result where the file is tampered or no


display: none;
Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-1.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Calculate
Result
E30AEE0086E19B8339E87D763417516F
Compare
E30AEE0086E19B8339E87D763417516F
Paste
Information
Correct, two checksum are the same.
OK
ng" height="100px">
Statement Carefully:</p>
001238F30D26848B1757C08D91CD9A77
86FC16B9EE4D51318751C404C8757BF1
DA97A5AA74238FC464D637DB373CA2B4
E75A8890253464D0C99560E62220536E
<b>


Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-2.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Calculate
Result
001238F30D26848B1757C08D91CD9A77
Compare
001238F30D26848B1757C08D91CD9A77
Paste
Information
Correct, two checksum are the same.
OK
001238F30D26848B1757C08D91CD9A77
86FC16B9EE4D51318751C404C8757BF1
DA97A5AA74238FC464D637DB373CA2B4


}
</style>
Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-3.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Result
86FC16B9EE4D51318751C404C8757BF1
Compare
86FC16B9EE4D51318751C404C8757BF1
Paste
Verify
Information
Correct, two checksum are the same.
OK
DA97A5AA74238FC464D637DB373CA2B4
E75A8890253464D0C99560E62220536E


Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-4.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Result
DA97A5AA74238FC464D637DB373CA2B4
Compare
DA97A5AA74238FC464D637DB373CA2B4
Paste
Verify
Information
Correct, two checksum are the same.
OK
</style>
height="100px">
tement Carefully:</p>
vulnerability
vulnerability.
been modified
lly to get the
DA97A5AA74238FC464D637DB373CA2B4
E75A8890253464D0C99560E62220536E
<b>


Checksum Calculator
www.checksumcalculator.com
Single File
Multiple Files
File
C:\Users\simon\OneDrive\Desktop\winshare\config\confi\DOC-5.pdf
Browse
Calculate
Checksum
MD5
CRC32
SHA1
Result
28AD7337D8D68B032EA3D141632268CC
Compare
E75A8890253464D0C99560E62220536E
Paste
Verify
Error
Incorrect, two checksum are not the same.
OK
</style>
height="100px">
tement Carefully:</p>