**CIS 480 Project – Injection 5**

**Injection**

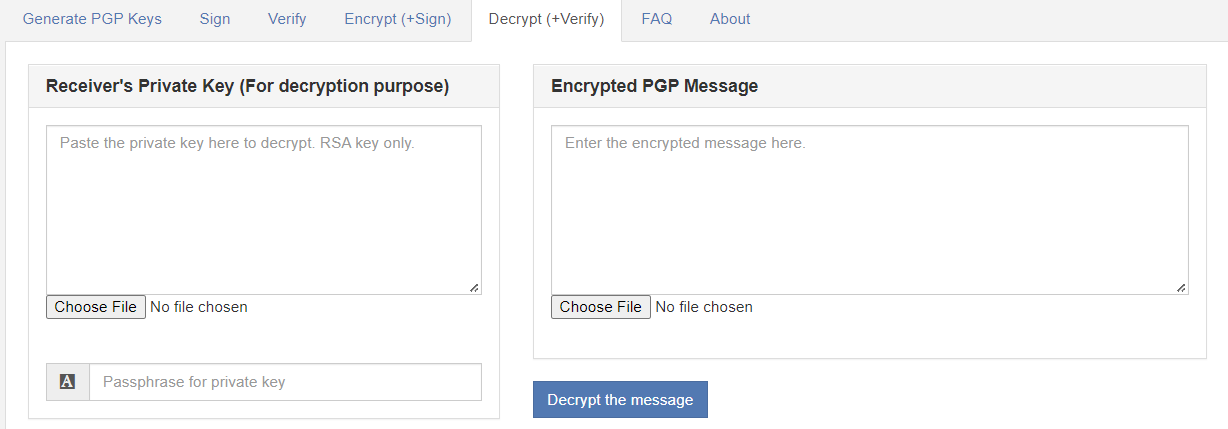
* Well done, team! It has been reported that you discovered mysterious files on the e-commerce server and transferred these to Kali successfully.
* Using the information in the files, find a treasure in the image file.
* Ignore *GoodData-e.txt* file you transferred from the e-commerce server.
* Use the following file for the instruction for Injection 5: *0x8F6568A3-pub.asc.encrypted.txt*. This file is posted on BB Injection 5. You need to download the private key as well from BB Injection 5.

**Tutorials**

* A private and public key pair was created using RSA algorithm on a site that offers generation of PGP keys ([pgptool.org](https://pgptool.org/)). The instruction for Injection 5 is encrypted with the public key and you need to use the private key to decrypt.
* What is Pretty Good Privacy (PGP)?
* <https://en.wikipedia.org/wiki/Pretty_Good_Privacy>

**Steps**

* Go to [pgptool.org](https://pgptool.org/). You will see the webpage shown below.
* Import the privake key.
* Import the encrypted message.
* Enter the passphrase: *louisville*.
* Click on **Decrypt the message**.
* Use the decrypted message for the next steps.



The treasure is hidden in the image file you transferred. You can discover the treasure using steganography.

To understand steganography, watch this video:

https://www.youtube.com/watch?v=9UZh-4Er7BQ&ab\_channel=NullByte

One of the files you transferred from the e-commerce server is a dictionary for password cracking.

* Provide a screenshot of the decrypted message on [pgptool.org](https://pgptool.org/).
* Explain the process of treasure discovery.
* Provide screenshots of the commands you used along the way.
* Show the treasure in a screenshot.

**Response to Injection 5**

1. Team members: *list the leader and participants.*

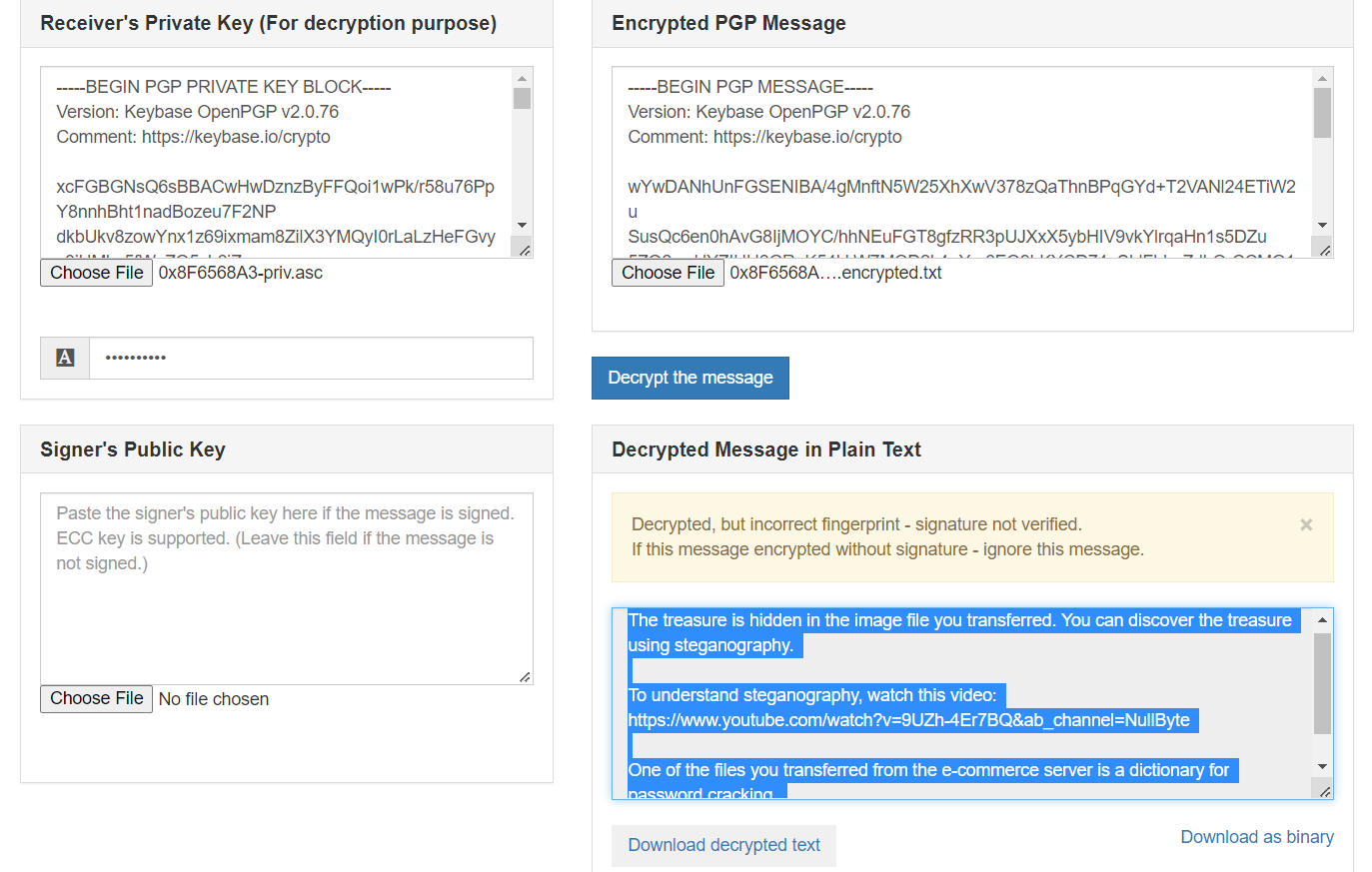
Jon McCarrick

Jacob Ornstein

Stephen Welsh

1. Address the above requirements.

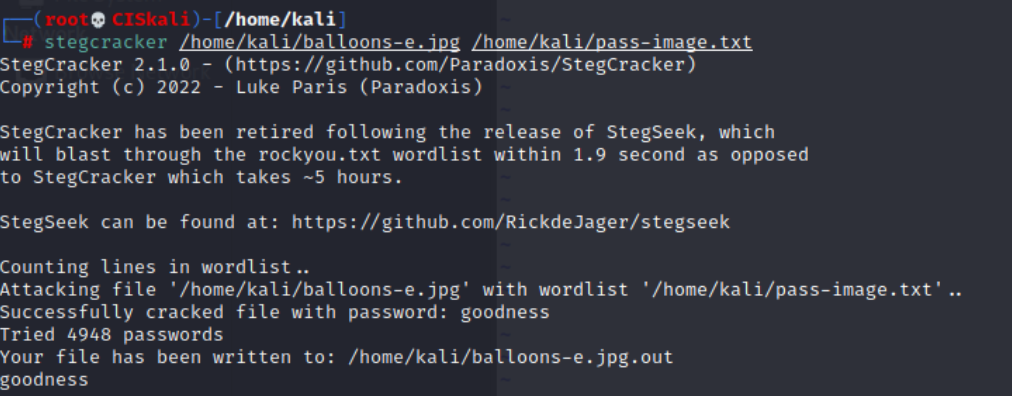
Decrypted Message



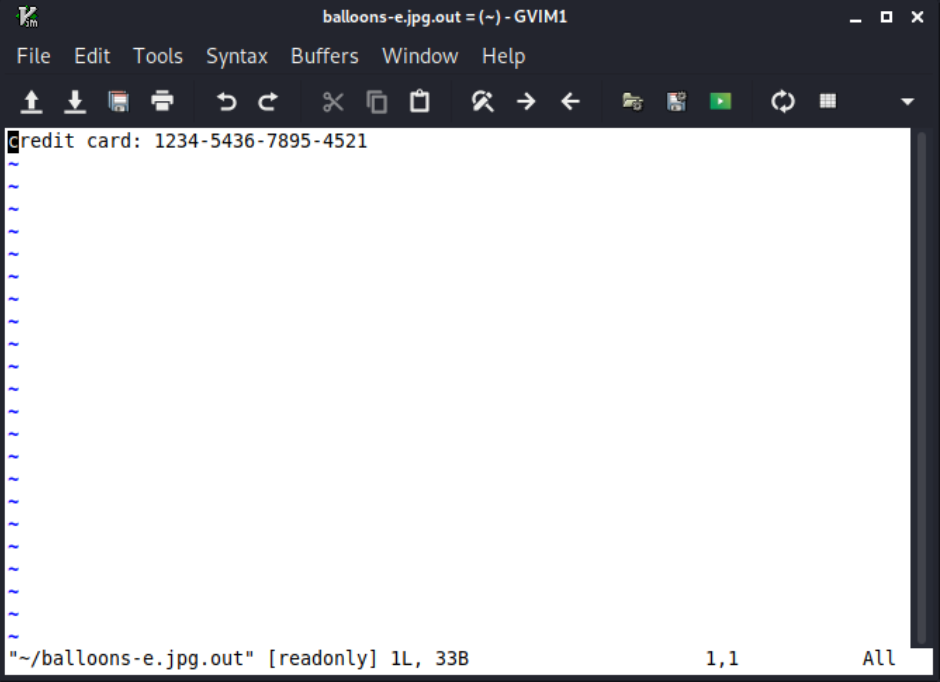
Treasure discovery process

The balloons-e.jpg has been embedded with additional information beyond the initial picture. The information was compressed, encrypted, then using a password the user created, makes slight changes to the pixels in the image to hide the information while the image looks essentially the same. To extract the treasure we had to use a tool called stegcracker. Since we knew the file was embedded but didn’t know the password, we used the password dictionary we got from the same place as the file and ran that in stegcracker which brute forced it’s way into the decryption.

Treasure discovery commands



Treasure



## Logistics

|  |  |  |
| --- | --- | --- |
| **Injections** | **Post** | **Due (midnight)** |
| Injection 1 – Introduce the team | Mon, 7th | Tue, 8th |
| Injection 2 – Scan the network | Tue, 8th | Wed, 9th |
| Injection 3 – Break into the target | Wed, 9th | Fri, 11th |
| Injection 4 – File transfer | Wed, 9th | Fri, 11th |
| Injection 5 – Treasure hunt | Thur, 10th | Sat, 12th |