Illumination

Capture the Flag Challenge.

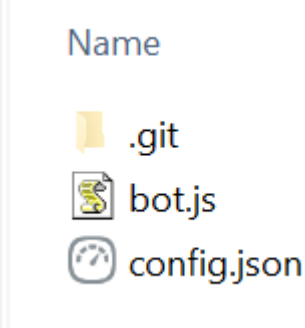
Link: Challenge can be found here.

Overview:

In this challenge we need to extract the flag from GitHub repository, exploiting human errors when dealing with GitHub commits and branches.

Method:

When opening this challenge we are presented with NodeJS bot file, config.json and .git directory



Of course the .git directory is on 'hidden' node and hidden items view should be enabled in order for the directory to be presented.

The bot.js doesn't reveals anything of significance,

However when opening the config.json:

```
{

    "token": "Replace me with token when in use! Security Risk!",
    "prefix": "~",
    "lightNum": "1337",
    "username": "UmVkIEhlcnJpbmcsIHJlYWQgdGhlIEpTIGNhcmVmdWxseQ==",
    "host": "127.0.0.1"

}
```

We see the token value is some censor on the token itself, indicating the token might be the flag and its value was modified in order to prevent the flag being exposed.

Now – we are presented with the .git file, which means we can use it to gain access to previous commits.

So I opened the git bash window, and entered ‘git log’ to get information about the commits:

```
Amit@LAPTOP-VPK63JOS MINGW64 ~/Downloads/Illumination/Illumination.JS (master)
$ git log
commit edc5aabf933f6bb161ceca6cf7d0d2160ce333ec (HEAD -> master)
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 14:16:43 2019 +0100

    Added some whitespace for readability!

commit 47241a47f62ada864ec74bd6dedc4d33f4374699
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 12:00:54 2019 +0100

    Thanks to contributors, I removed the unique token as it was a security risk. Thanks for reporting responsibly!

commit ddc606f8fa05c363ea4de20f31834e97dd527381
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 09:14:04 2019 +0100

    Added some more comments for the lovely contributors! Thanks for helping out!

commit 335d6cfe3cdc25b89cae81c50ffb957b86bf5a4a
Author: SherlockSec <dan@lights.htb>
Date:   Thu May 30 22:16:02 2019 +0100

    Moving to Git, first time using it. First Commit!

Amit@LAPTOP-VPK63JOS MINGW64 ~/Downloads/Illumination/Illumination.JS (master)
$
```

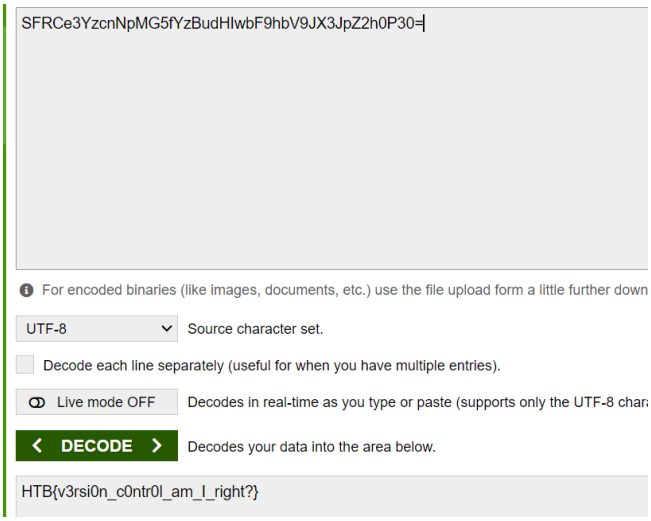
It can be observed that there is a commit was the unique token was removed due to being security risk.

Lets take a look at the commit which the unique token was cencored:

```
Amit@LAPTOP-VPK63JOS MINGW64 ~/Downloads/Illumination/Illumination.JS (master)
$ git show  47241a47f62ada864ec74bd6dedc4d33f4374699
commit 47241a47f62ada864ec74bd6dedc4d33f4374699
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 12:00:54 2019 +0100

    Thanks to contributors, I removed the unique token as it was a security risk. Thanks for reporting responsibly!

diff --git a/config.json b/config.json
index 316dc21..6735aa6 100644
--- a/config.json
+++ b/config.json
@@ -1,6 +1,6 @@
 {
-       "token": "SFRCe3YzcnNpMG5fYzBudHIwbF9hbV9JX3JpZ2h0P30=",
+       "token": "Replace me with token when in use! Security Risk!",
        "prefix": "~",
        "lightNum": "1337",
        "username": "UmVkIEhlcnJpbmcsIHJlYWQgdGhlIEpTIGNhcmVmdWxseQ==",

Amit@LAPTOP-VPK63JOS MINGW64 ~/Downloads/Illumination/Illumination.JS (master)
```

We can see the removed token value.

It can be observed that it is base64 encoded – lets decode it:



We got the flag!

Conclusions: The challenge value is to instill the importance of GitHub commits inspection in order to look for sensitive data.

In this challenge it was done manually on single digit number of repositories.

However in actual real-world GitHub repository it might take inspection of dozens, even hundreds of repositories – so an automation tool might be required in order to properly investigating GitHub repositories.