Montrehack 2016-06

NorthSec 2016 - Strudel Maker by François Proulx

Intro

In the context of the “Marcus Madison Bakery”,

You were hiring as a pentesting consultant and asking to perform various tasks.

With regards to the “Strawberry Strudel Maker”,

Marcus asked you to perform a Code Review of the update manager of the system.

Challenge

http://159.203.62.171:9001/

Hint #1 - The scenario

- It’s a Code Review challenge
  - Check the HTML source
- Notice some odd comment and debug trace
  - Try going to /?support=authorized
- Notice some new block with a <form> POST
  - You can change CSS to display: block to show it
- Try uploading some file
  - Nothing happens
- Notice debug = false
  - Change to debug = true before uploading
- Notice the <pre> block with the exact name and file hash

Hint #2 - The real challenge

- MD5 Collision to the rescue !
- Huh…
  - Very few practical attacks realistic within the span of a 2 day competition
  - **NO**, we are NOT expecting you buy 500$ worth of EC2 GPGPU cluster to run some fancy tool like **HashClash**
- There are simpler, faster attacks
  - **BUT**, it requires some very “special conditions”
- Of course, this is a challenge meant to be cracked
  - So those “special conditions” are probably present
- You need one file that matches your target hash
  - Look under the rug…. Leftover static files maybe?

Hint #3 - The magic bytes!

- Look very very carefully at **every byte** in that special file
- **Remember**, Marcus asked you to do a **Code Review**
  - Oh, look there's a Command Injection vulnerability !
  - But …. You cannot use it unless….
- And AGAIN, you don't need 1000$ AWS cluster

Hint #4 - The evil cryptographer

- In that special file, there's the name of a person…
- Apparently it's the person who designed the Strudel Maker update manager cryptosystem…
  - Xiaoyun Wang
- Look up his academic work…
- Maybe he published some tools along with his work?

Hint #5 - The Ha Ha moment !

- Get the `fastcoll` tool by Marc Stevens
  - http://www.win.tue.nl/hashclash/fastcoll_v1.0.0.5-1_source.zip
- Study very carefully how it actually works...

SOLUTION!

- Get the **“GOOD”** the license_validator.py
- Get the `fastcoll` tool from Marc Stevens
  - http://www.win.tue.nl/hashclash/fastcoll_v1.0.0.5-1_source.zip
- Study the code
- Notice that you can modify it slightly to do your bidding
- Change so that you can pass the **GOOD** file path as `argv`
- If you want to modify the least amount of code, you may need to massage the file before processing it.
- Boom - **EVIL** license_validator.py
- Upload evil