LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.6**

**A.1 Aim:**

To analyze browser security and detection of threats.

**A.2 Prerequisite:**

Knowledge of web security threats.

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Install browser security tool

2. Protect Content from malware

2. Alert the User on visiting Malicious Webpages

3. Analyses of webpage threats

**A.4 Theory:**

In the recent times, most of the systems connected to Internet are getting infected with malware and some of these systems are even becoming zombies for the attacker. When user knowingly or unknowingly visits a malware website, his system gets infected. Attackers do this by exploiting vulnerabilities in web browser and it is possible to acquire control over the underlying Operating System. Once attacker compromises the user's web browser, he can instruct the browser to visit the attacker's website by using number of redirections. During the process, user's web browser downloads the malware without the intervention of the user. Once the malware is downloaded, it would be placed in the file system and responds as per the instructions of the attacker. These types of attacks mostly happen through JavaScript and malicious HTML tags.

Browser security software’s can detect and defend from such attacks made through the web browser. It blocks access to the harmful, inappropriate and dangerous websites that may contain malicious content

#### Download Links

Firefox Browser

* <https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/>

Google Chrome Browser

* <https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb>

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no portal access available)***

|  |  |
| --- | --- |
| Roll. No. N049 | Name: Tarun Tanmay |
| Class: MbaTech CE | Batch: B2 |
| Date of Experiment: 13-8-2020 | Date of Submission: 13-8-2020 |
| Grade: | |

**B.1**

**Input and Output:**

**Input:**

Provide the **details** and following

* 1. Installation screenshot
  2. Browser with tool screenshot
  3. Provide the screenshot with websites names for

-Redirections

-Encoded JavaScript

-External Domain Requests

-Trackers

1. In the recent times, most of the systems connected to the Internet are getting infected with malware and some of these systems are even becoming zombies for the attacker. When user knowingly or unknowingly visits a malware website, his system gets infected. Attackers do this by exploiting vulnerabilities in web browser and it is possible to acquire control over the underlying Operating System. Once attacker compromises the user's web browsers, he can instruct the browser to visit the attacker's website by using number of redirections. During the process, user's web browser downloads the malware without the intervention of the user. Once the malware is downloaded, it would be placed in the file system and responds as per the instructions of the attacker. These types of attacks mostly happen through JavaScript and malicious HTML tags. Browser JSGuard detects and defends from such attacks made through the web browser. It blocks access to the harmful, inappropriate and dangerous websites that may contain malicious content.
2. Features:

* Content/Heuristic based JS & HTML malware protection
* Alerts the User on visiting Malicious Web pages
* Provides detailed analysis of webpage threats
* Ease of installation / maintenance
* Suitable for both home and office usage
* Signed by Mozilla Add-on community

1. Hidden redirect allows you to quickly create subdomains that seamlessly redirect users to another URL - without changing the URL shown in the address bar. This is done using an iFrame redirect (full-screen iFrame).

A hidden redirect is useful for assigning a custom domain to another website which does not support custom domains otherwise.

1. The JavaScript code uses a publicly available JavaScript library to collect information about browser plugins. Once it has collected the information it makes a POST request to the server indicating whether the victim has Java and Adobe Acrobat Reader installed in the system. The server redirects the browser to a server that makes another redirection very likely depending on the plugins detected on the victim. The server has returned HTML code that is embedding some Flash content in the browser as well as a new iframe and encoded JavaScript content with String.fromCharCode() function.
2. With the advent of web, attackers have changed their target to web browser and its plug-ins. Some of the current day attacks such as XSS (Cross Site Scripting) and CSRF (Cross Site Request Forgery) does not require exploiting the vulnerabilities in the client‘s browser or system. In these attacks, malicious code is injected into the webpage and attacker tricks the client to visit the infected webpage for getting access to user‘s web browser. Through this Drive by Download attack is carried out. In some scenarios, Drive by Download attack is initiated from a genuine web server.
3. Cross-origin resource sharing (CORS) is a mechanism that allows restricted [resources](https://en.wikipedia.org/wiki/Web_resource) on a [web page](https://en.wikipedia.org/wiki/Web_page) to be requested from another [domain](https://en.wikipedia.org/wiki/Domain_name) outside the domain from which the first resource was served.

**B.2 Observations and learning:**

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

1.

A screenshot of a cell phone

Description automatically generated

2.

A screenshot of a cell phone

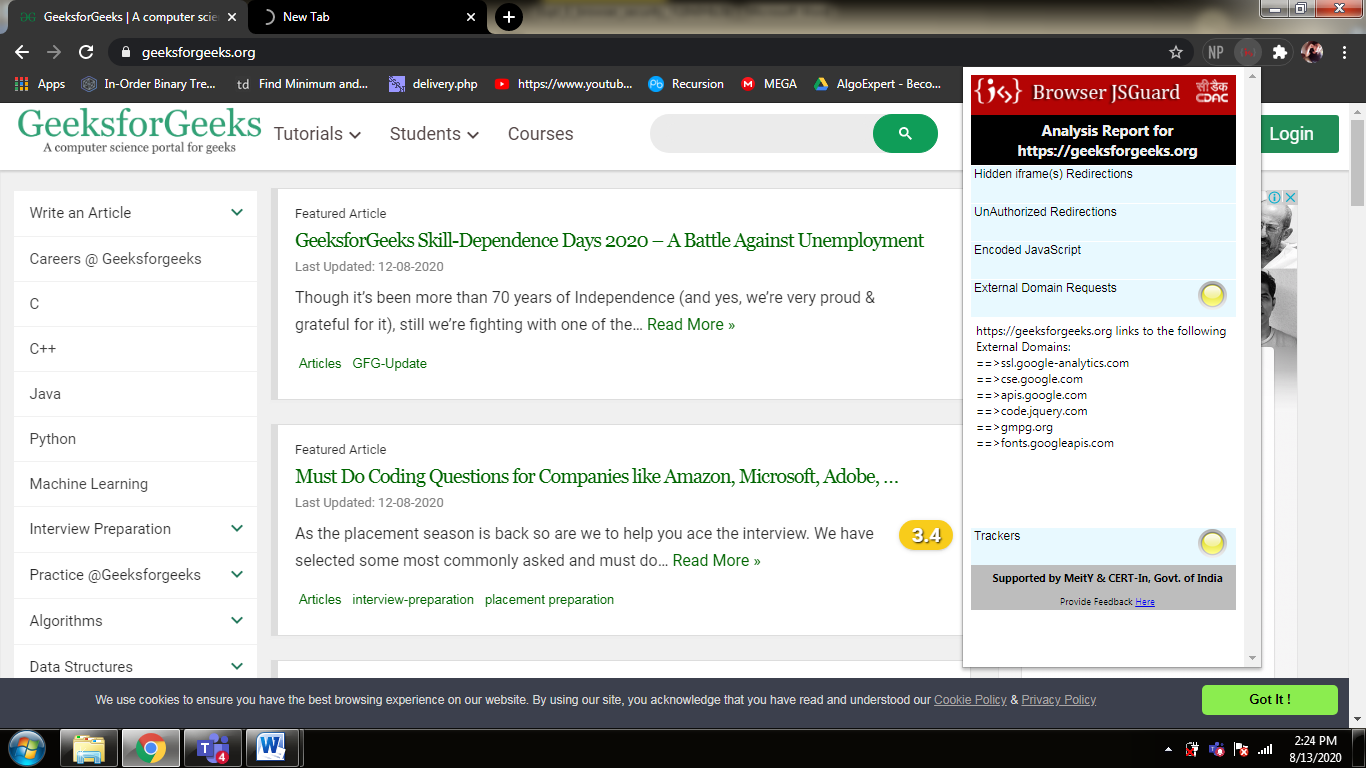
Description automatically generated

3.

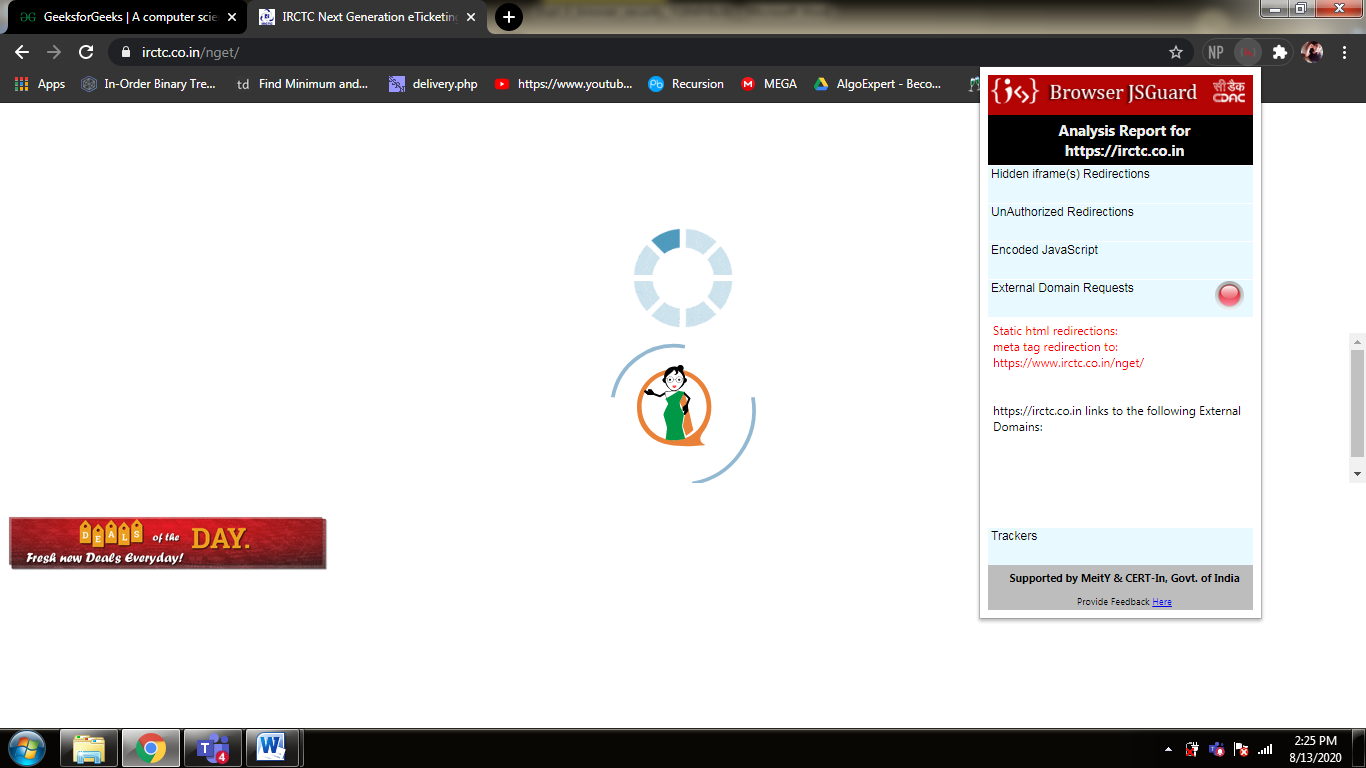
A screenshot of a cell phone

Description automatically generated

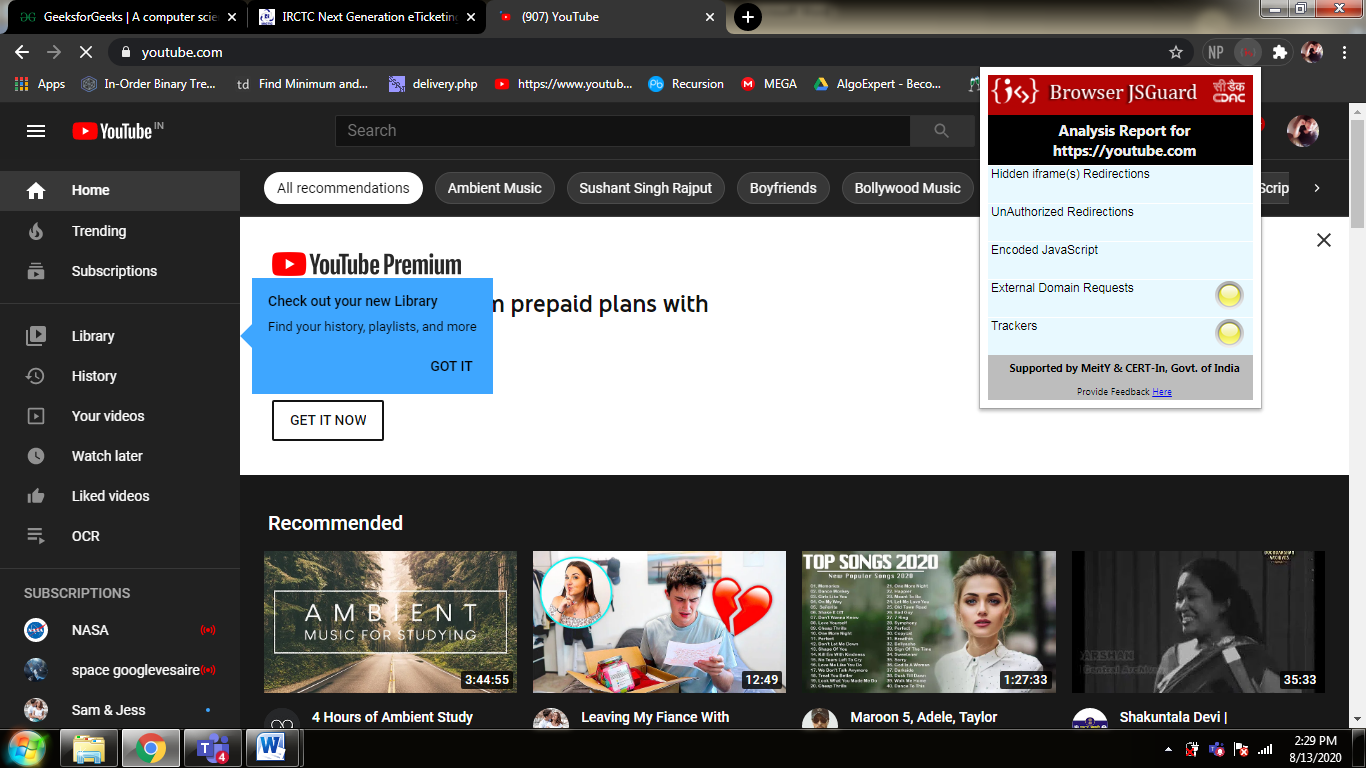
4.



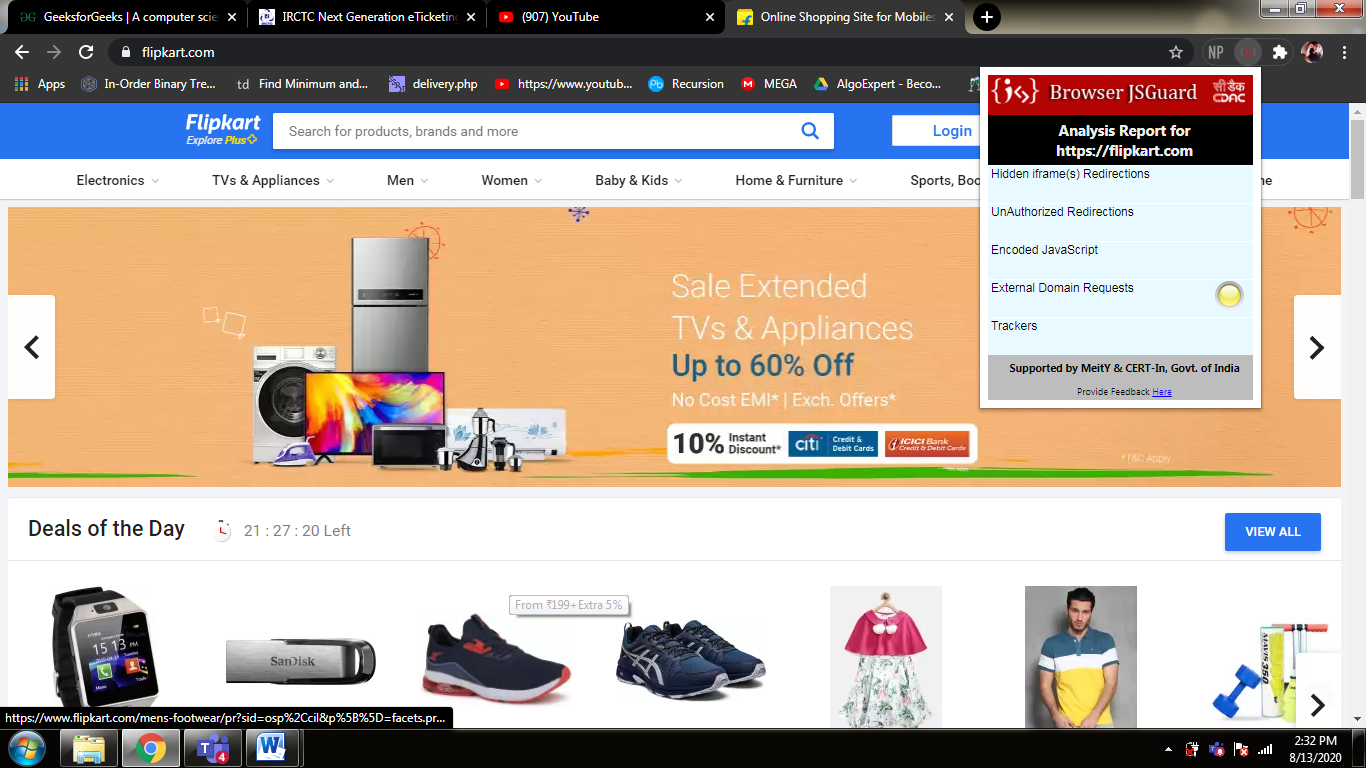
5.



6.



7.



**B.3 Conclusion:**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.2)***

JS Guard resides as part of the client web browser and detects the malicious web pages. In addition to the detection, JS Guard extension provides the flexibility to user for viewing the detailed analysis report of the webpage. Furthermore this extension gives an option for user to decide whether to continue browsing the webpage or not.

**B.4 Question of curiosities:**

1. **List the threats in internet surfing**

* **Malicious websites**  
  Kaspersky identifies these websites by using cloud-based heuristic detection methods. Most malicious URL detections are for websites that contain exploits.
* **Malicious scripts**  
  Hackers inject malicious scripts into the code of legitimate websites that have had their security compromised. Such scripts are used to perform drive-by attacks – in which visitors to the website are unknowingly redirected to malicious online resources.
* **Scripts and executable PE files**  
  Generally, these either:
  + Download and launch other malicious software programs
  + Carry a payload that steals data from [online banking](https://usa.kaspersky.com/resource-center/threats/online-banking-theft) and social network accounts, or steals login and user account details for other services
* **Trojan-Downloaders**  
  These [Trojan viruses](https://usa.kaspersky.com/resource-center/threats/trojans) deliver various malicious programs to users’ computers.
* **Exploits and exploit packs**  
  Exploits target vulnerabilities and try to evade the attention of Internet security software.
* **Adware programs**  
  Often, [adware](https://usa.kaspersky.com/resource-center/threats/adware) will simultaneously install when a user starts to download a freeware or shareware program.

1. **How website can track users?**

Every user has a unique IP address that identifies them. By using IP addresses, websites can track what each user does on their site and what pages they visit. Our IP address can be used to determine our location and is the primary piece of data that will be used to track us.

1. **What precautionary measures should be adopted by internet users?**

## Keep Personal Information Professional and Limited

## Keep Your Privacy Settings On

## Practice Safe Browsing

## Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection

## Be Careful What You Download

## Choose Strong Passwords

## Make Online Purchases From Secure Sites

## Be Careful What You Post

## Be Careful Who You Meet Online

## Keep Your Antivirus Program Up To Date

* Keep social networks secure