

Offensive Hacking Tactical and Strategic

IT444

Assignment - Exploit Development

M K S R Gunawardhana

IT16176720

Bachelor of Science (Hons) in Information Technology

Specialized in Cyber Security

Sri Lanka Institute of Information Technology

Sri Lanka

May 2020

**Exploit for Firefox Web Browser**

The older versions of Firefox web browser below 58.0.1 version were affected by the vulnerability CVE-2018-5124

Arbitrary code execution through un-sensitized browser UI. This was reported in 29th of January 2018 by Johann Hofmann. The impact was considered as critical and the bug was found as level XSS in LightWeight theme prompts. The bug is about the frontend of web extensions such as buttons, tabs, windows and popups. The bug was fixed in Firefox 58.0.1 version.

As we have analyzed the test case for the scenario is given below.

ExtentionsUI

ShowPermissionPrompt

* Causes XSS
* Uses strings from caller
* All local calls are escaped
* If the strings come from caller
* All local calls are escaped
* If the strings come from ExtentionsUI.\_buildStrings they get
* escaped
* Call from browser-addons

ShowDefaultSearchPrompt

* Causes XSS
* Uses strings from caller
* Only one call in ExtentionUI , does not escape search engine name

ShowInstallNotification

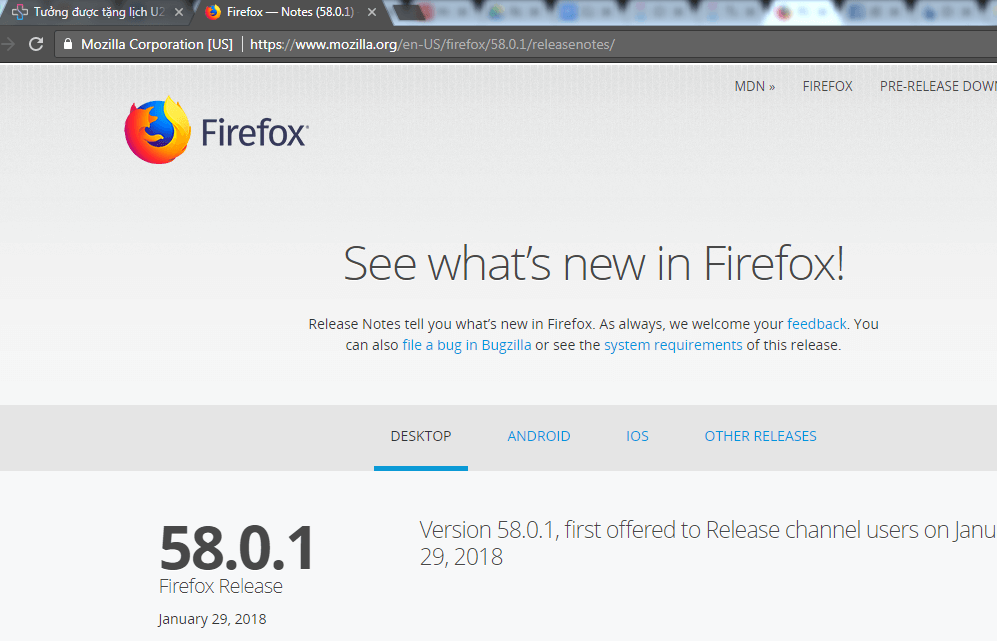
* String local to function, escaped

Extention

Format permission Strings

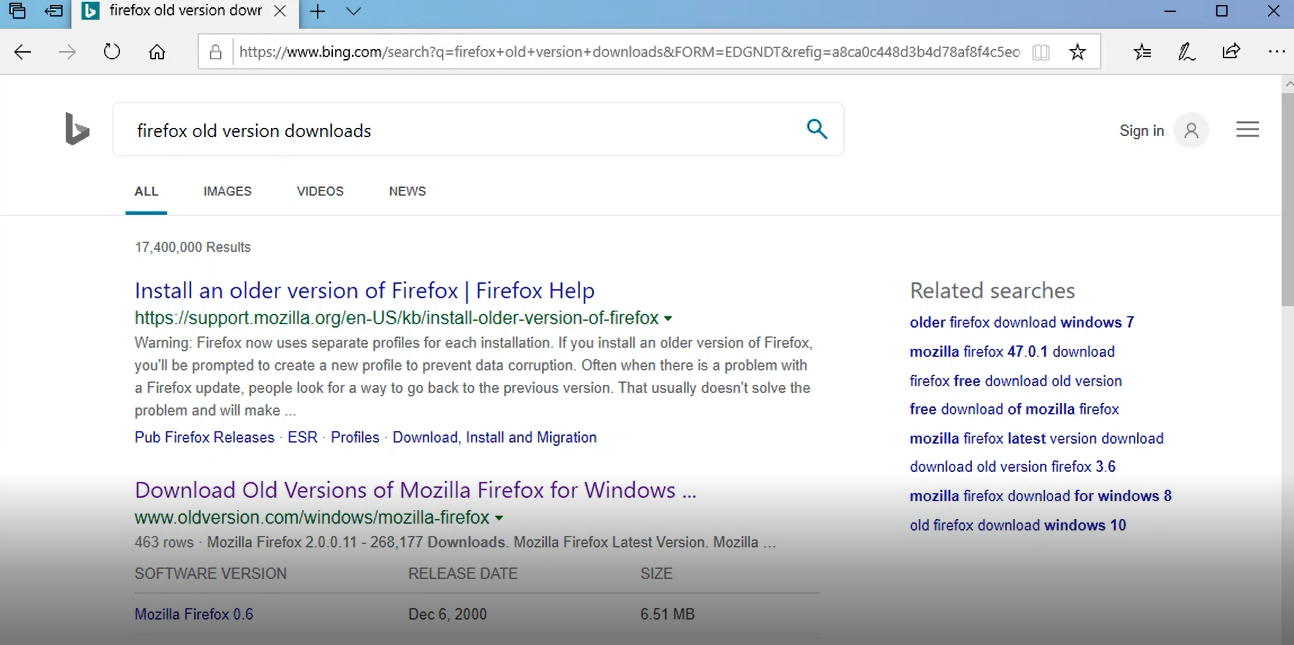
* Uses info.addonName
* This is escaped in ExtentionsUI.\_buildStrings
* This is not escaped in fennaec, but the string is sent to Java

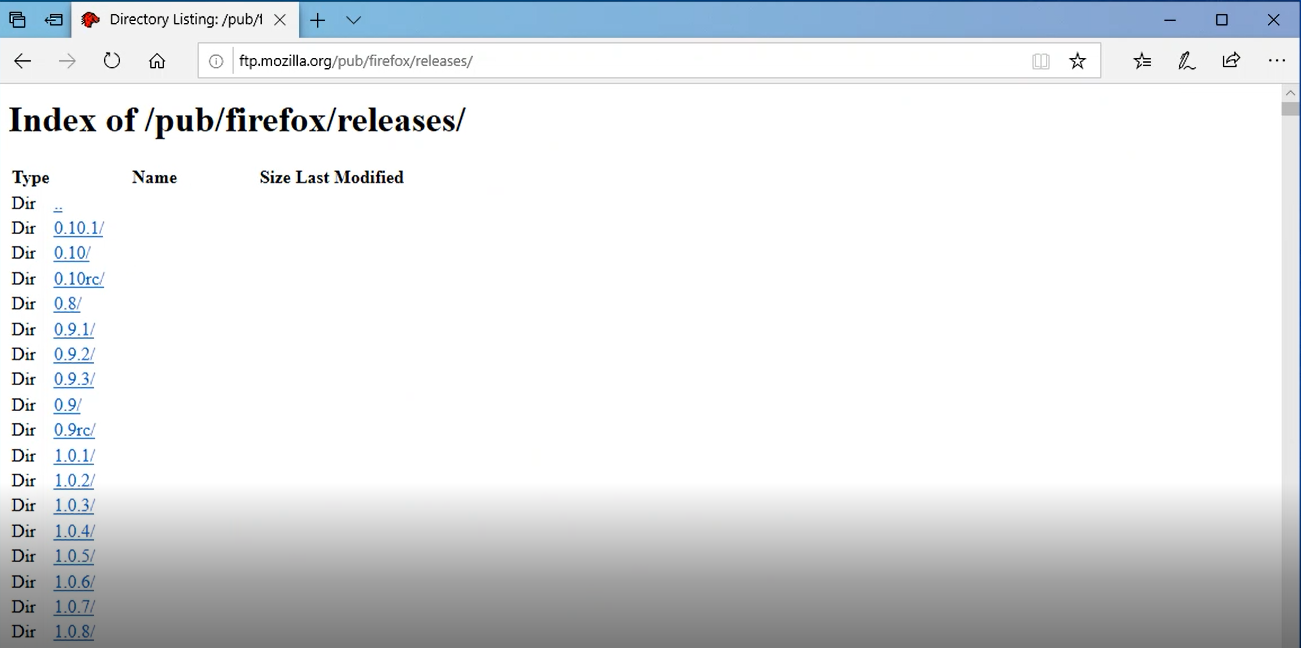
Below is an image related to the bug of CVE-2018-5124

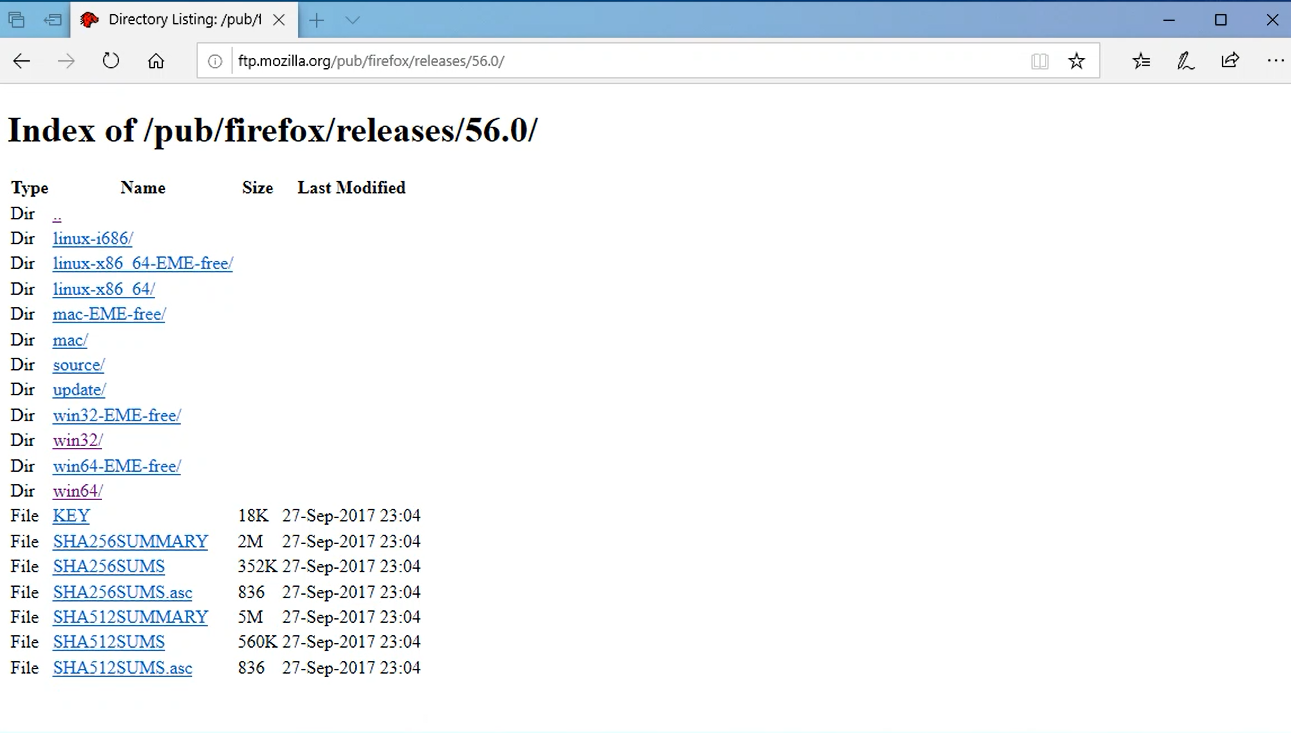


CVE-2018-5124 - Arbitrary code execution through un-sanitized browser UI

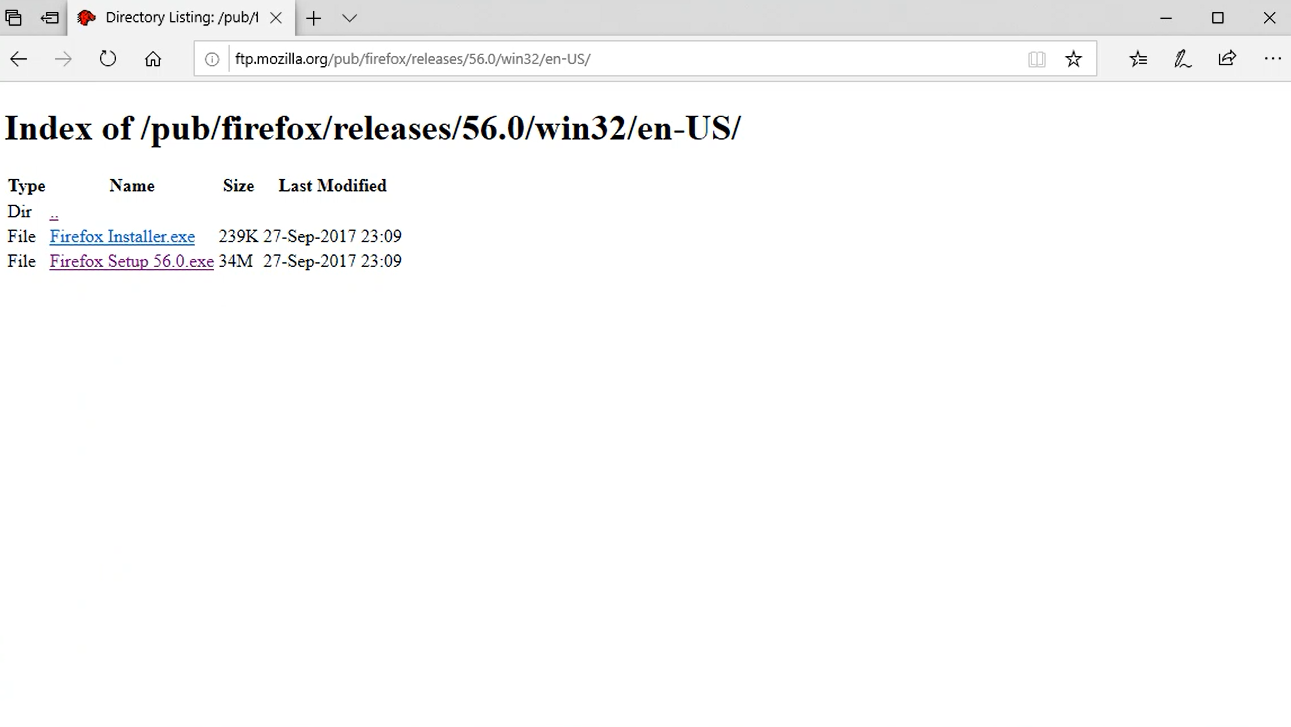
First off download a Firefox older version.



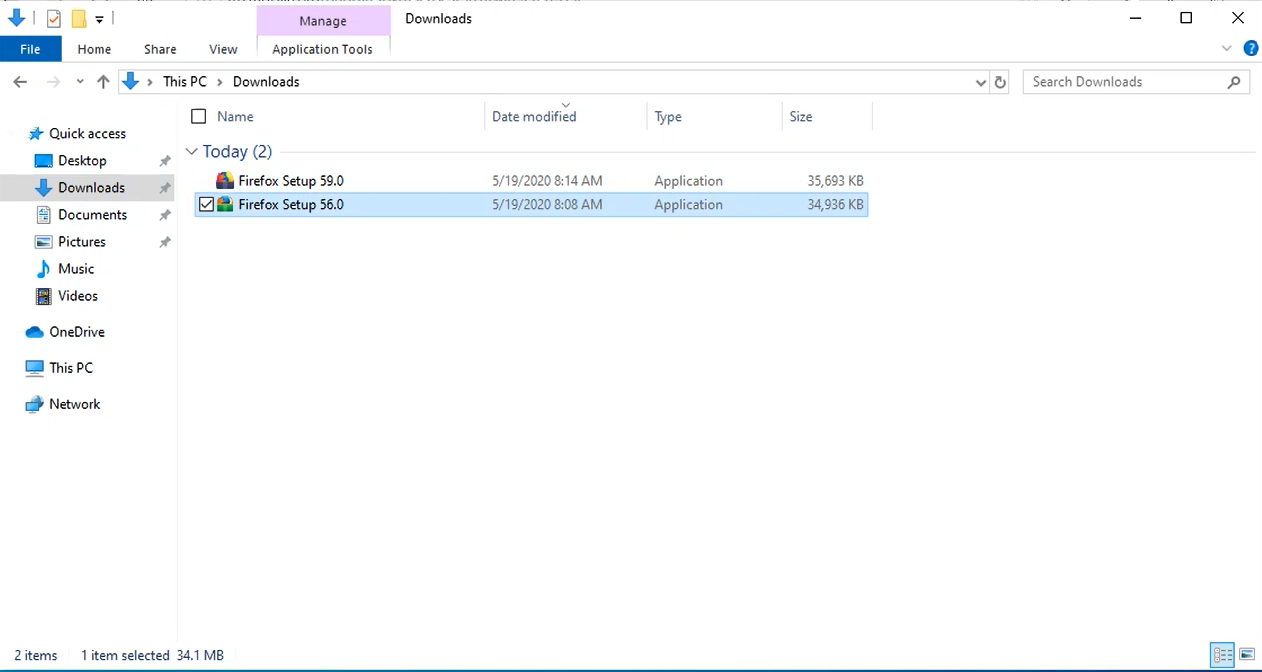




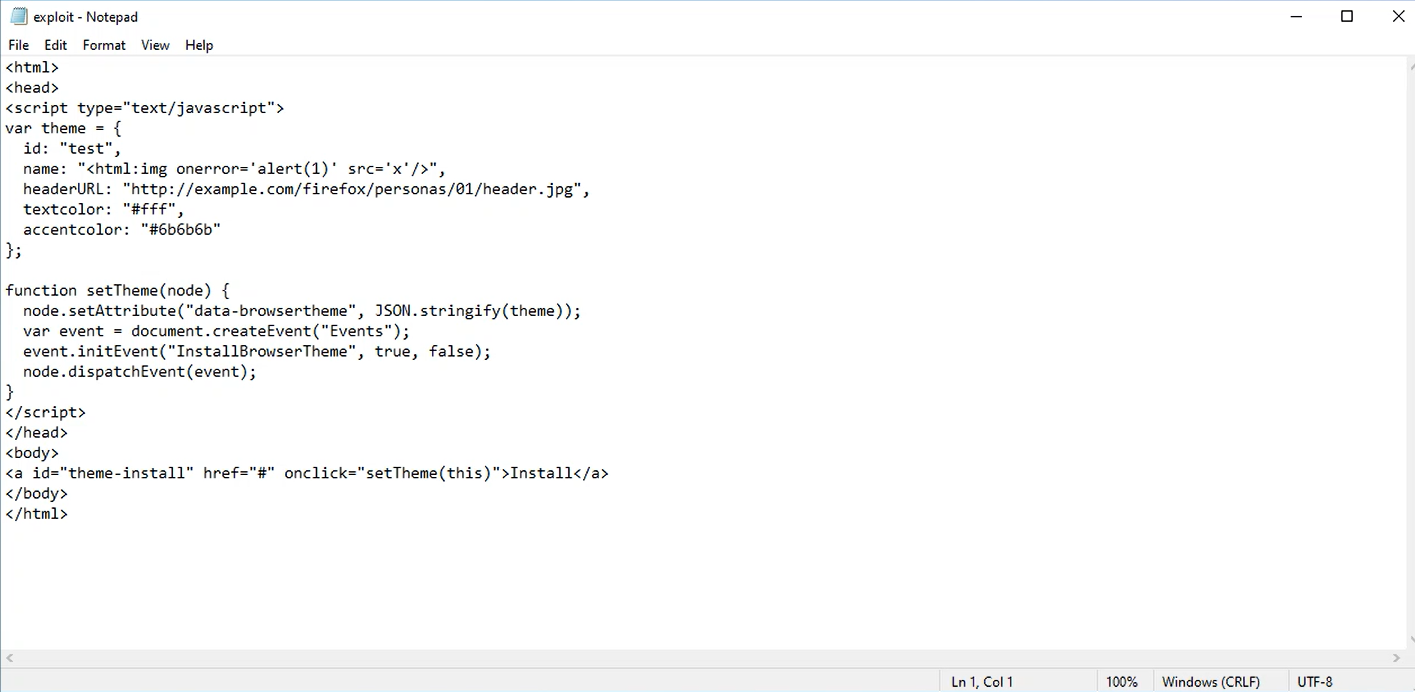
Since the version of Windows I use is 32 bit, downloading a 32 bit version of Firefox



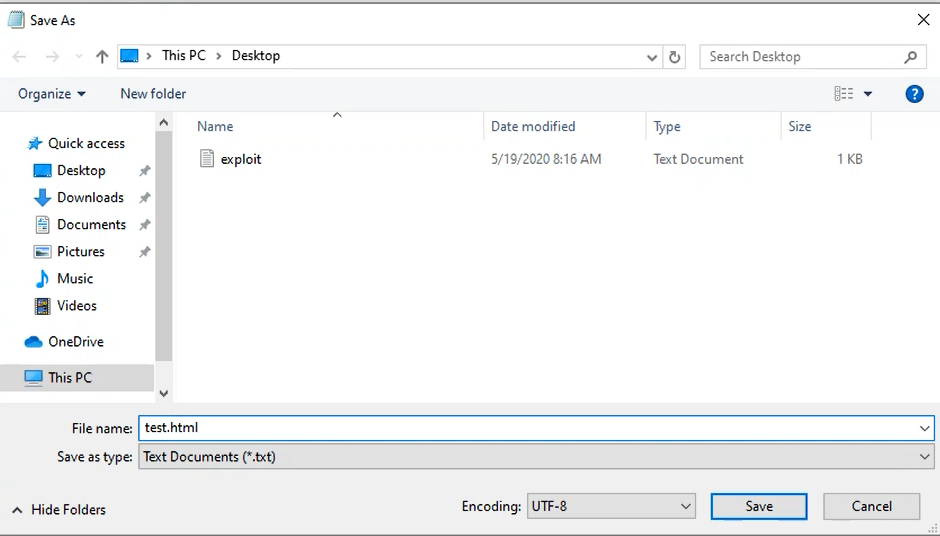
Setting up Firefox 56.0



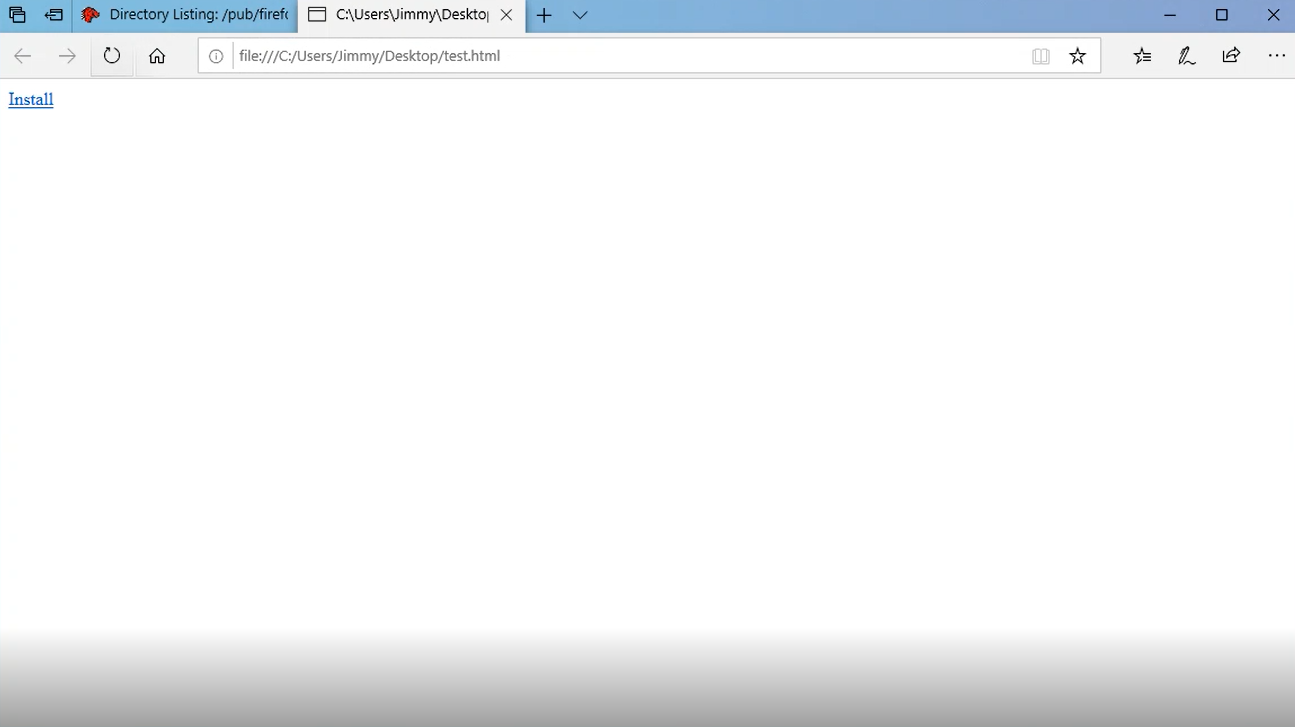
After installing Firefox 56.0, with using the exploit code, exploitation is carried out.



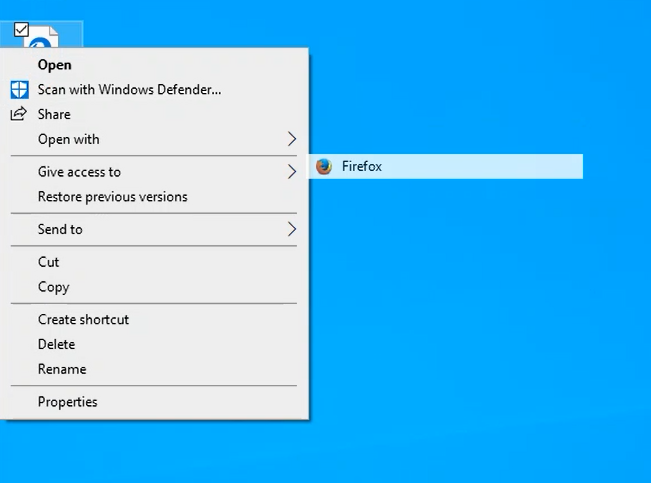
Converting the .txt file to an html file in order to run the code.

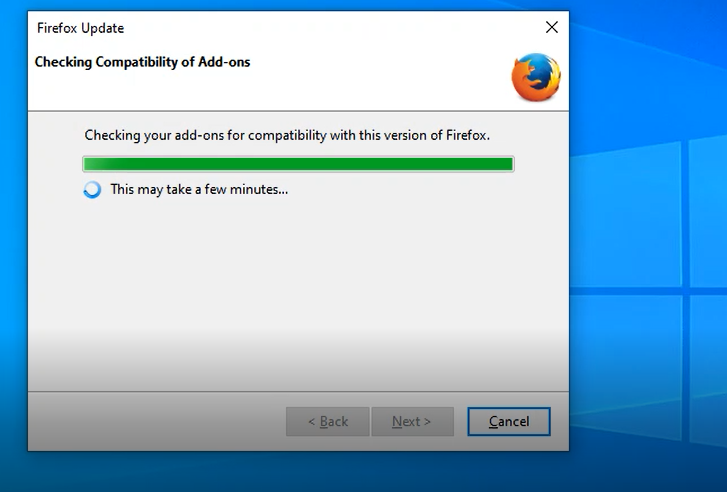


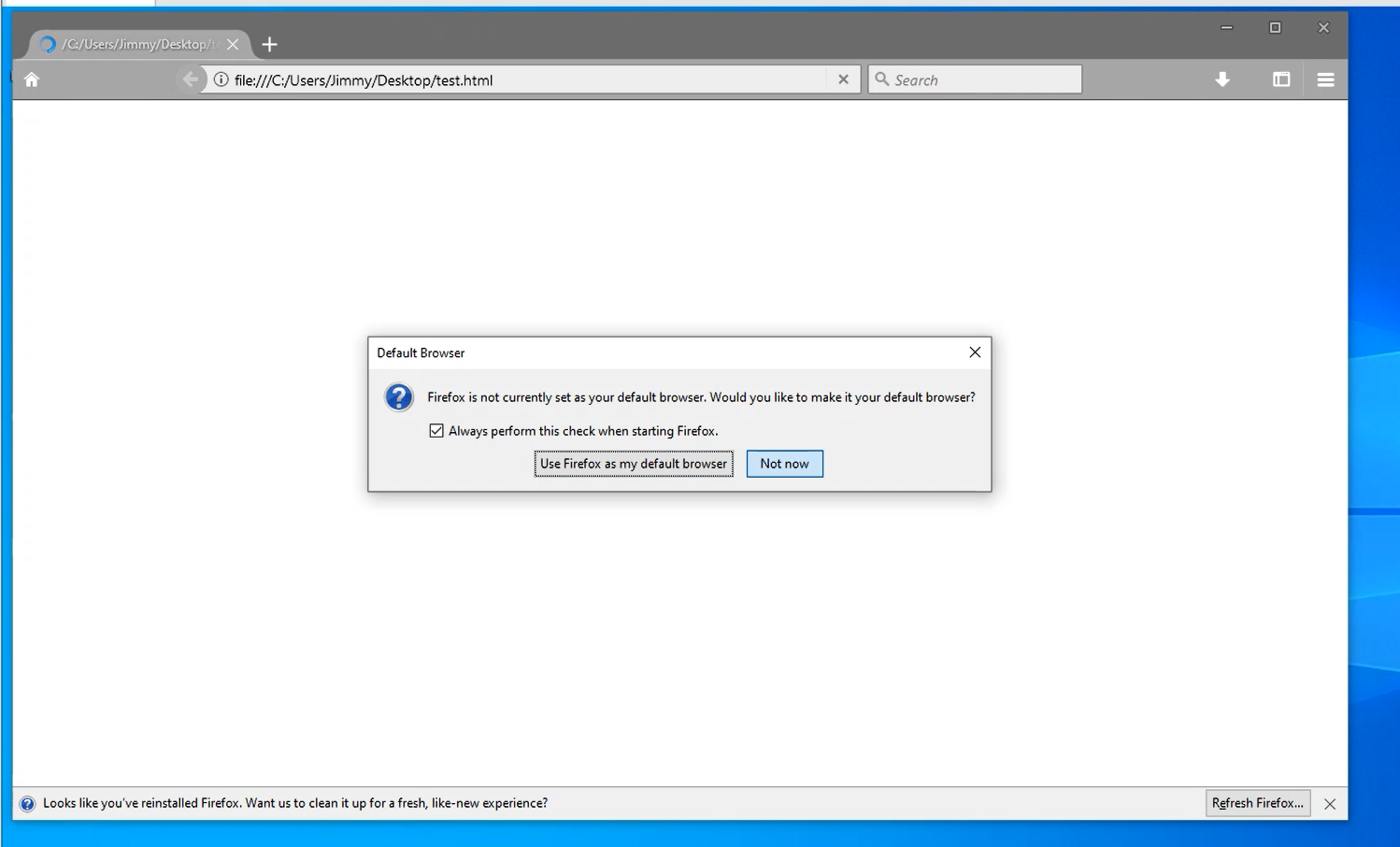
The exploit code does not affect to the Windows Explorer as it can be seen on the below screen shot.



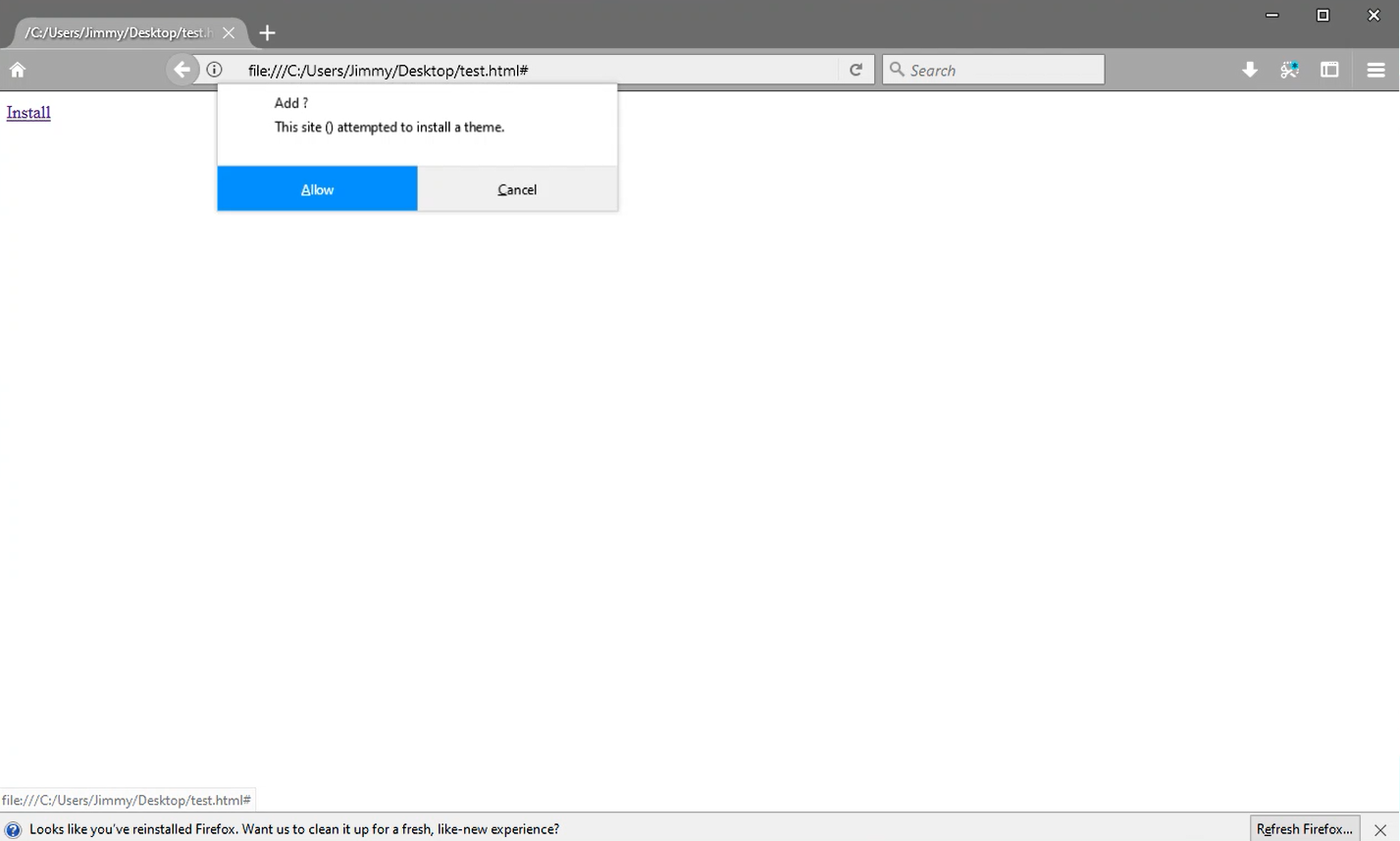
However when the exploit code is run via the Firefox 56.0, it installs as an addon.

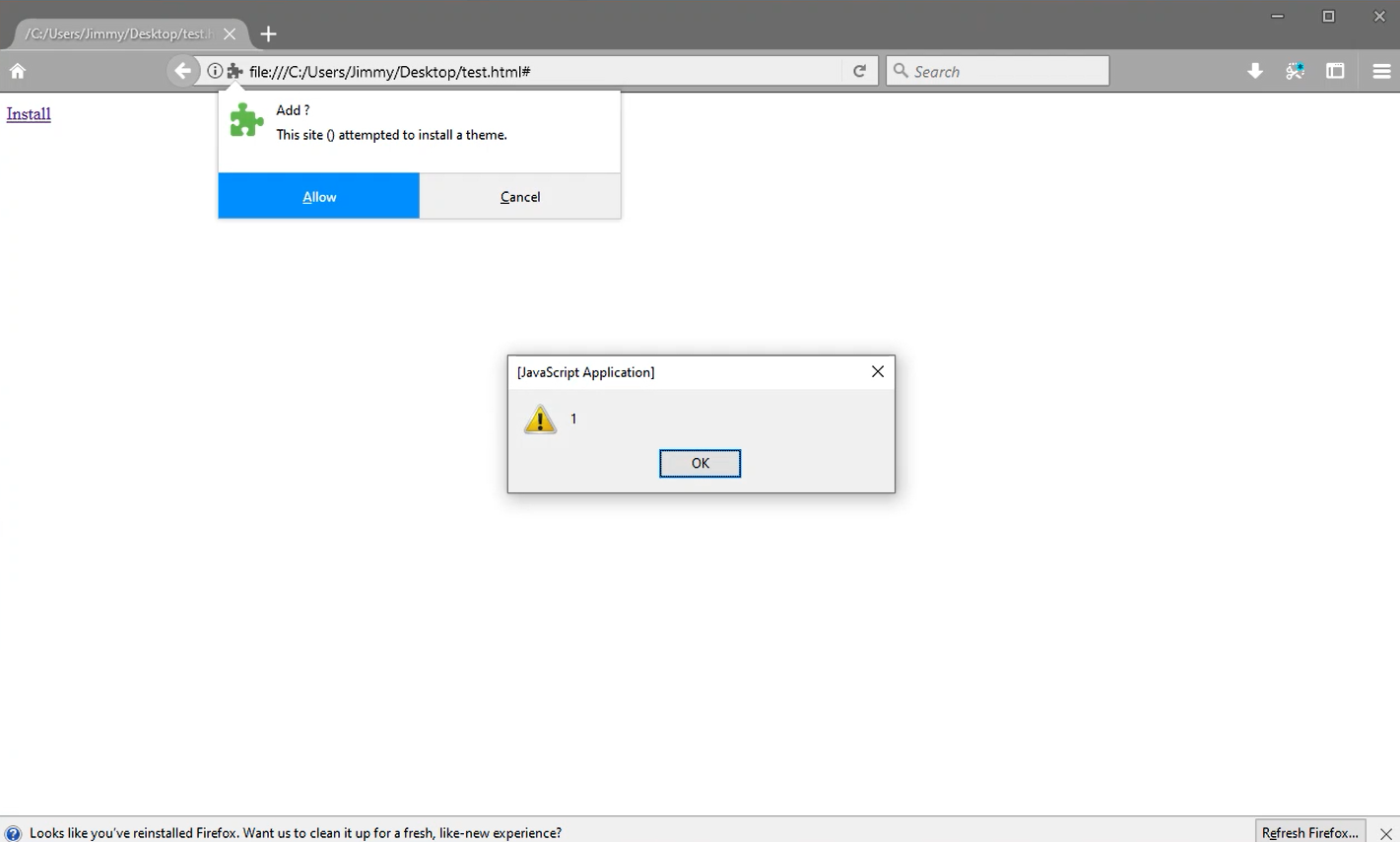




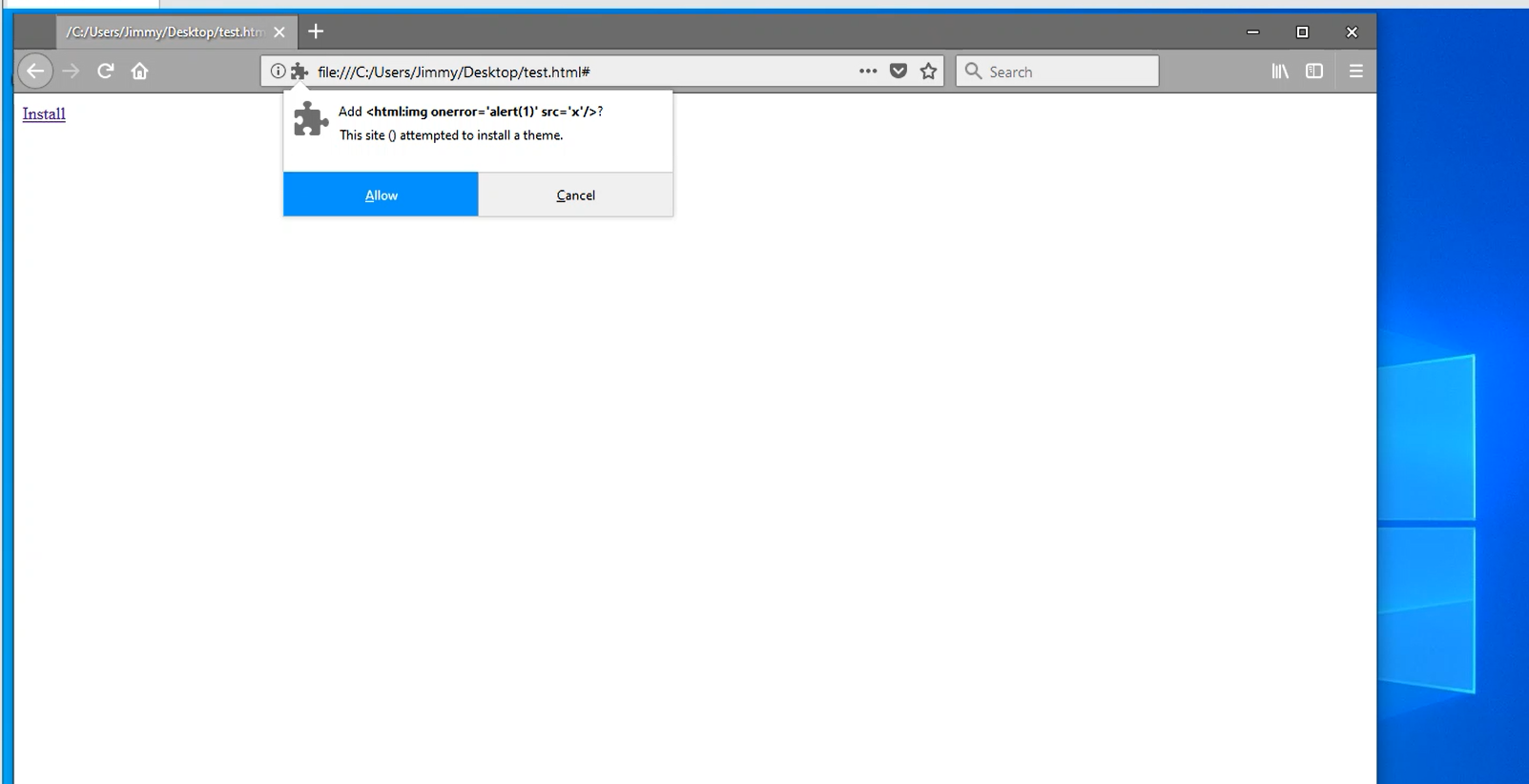


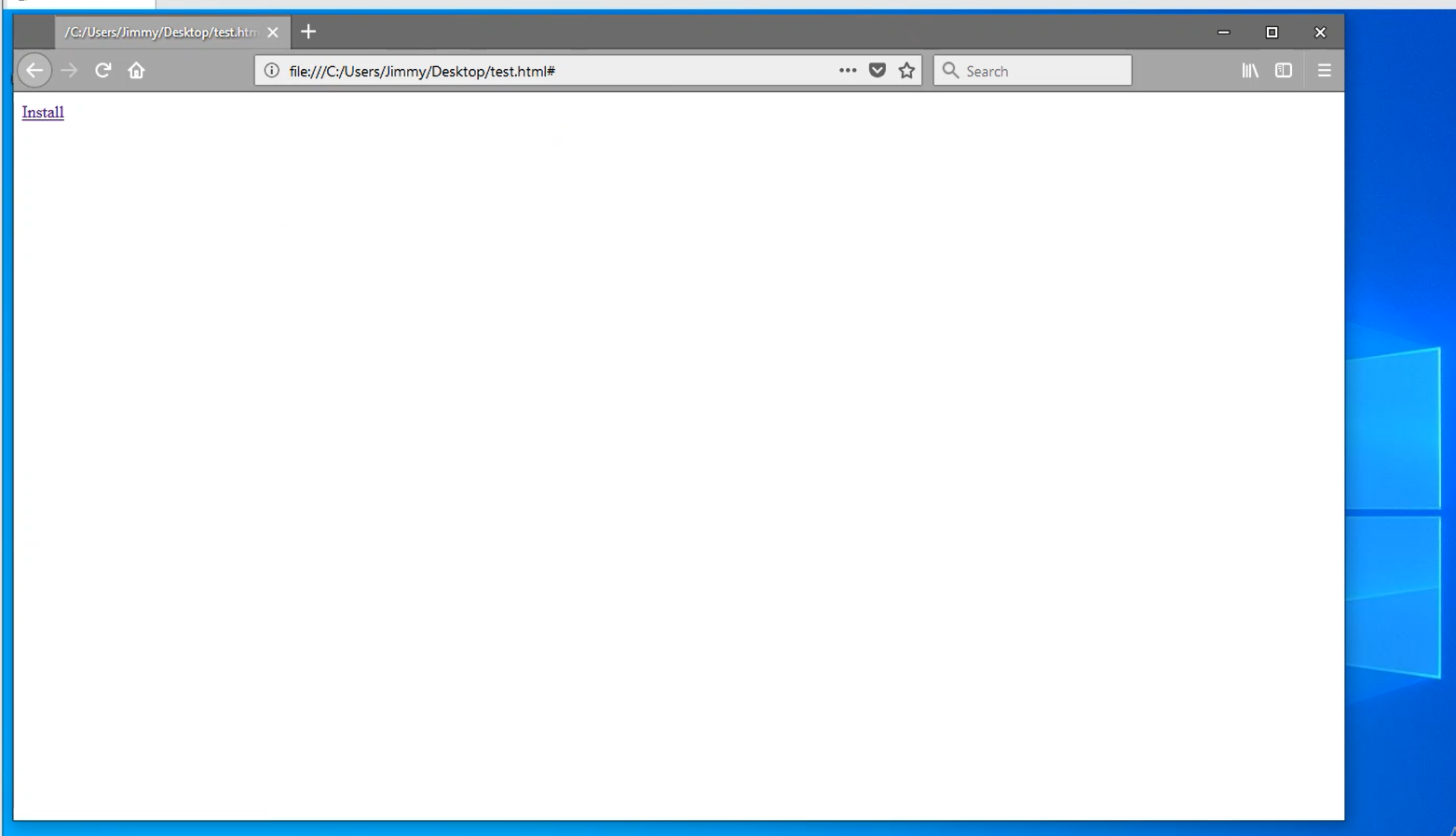
When the ‘Install’ link is clicked on, exploit successfully executes.





Even though, the exploit code does not work for Firefox versions above 59.0





References

[1] <https://bugzilla.mozilla.org/show_bug.cgi?id=1432778>

[2] <https://bugzilla.mozilla.org/attachment.cgi?id=8945069&action=edit>

[3] <https://nvd.nist.gov/vuln/detail/CVE-2018-5124>