**TEAM : ANONYMOUS**

* ***HSTS Vulnerability(HTTPS Sourcing to HTTP)***

1. **TARGET -I**

**DESCRIPTION:** HSTS Vulnerability is the vulnerability where the websites containing “https” protocols are being downgraded to unsecured “http” protocol page.

**VULNERABLE TARGET:**

**STEPS TO TEST THE HSTS VULNERABILITIES OVER THE RANDOM WEBSITES:**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Open some websites having “https” in their URL

**Step3:** Now manually remove ‘s’ letter from “https”

**Step4:** now reload the page

**Step5:** If the page URL has “http” after reloading then there is chance for HSTS Vulnerability and thus the page is down graded

**Step6:** If the page URL has “https” after reloading then there is no chance for HSTS Vulnerability.

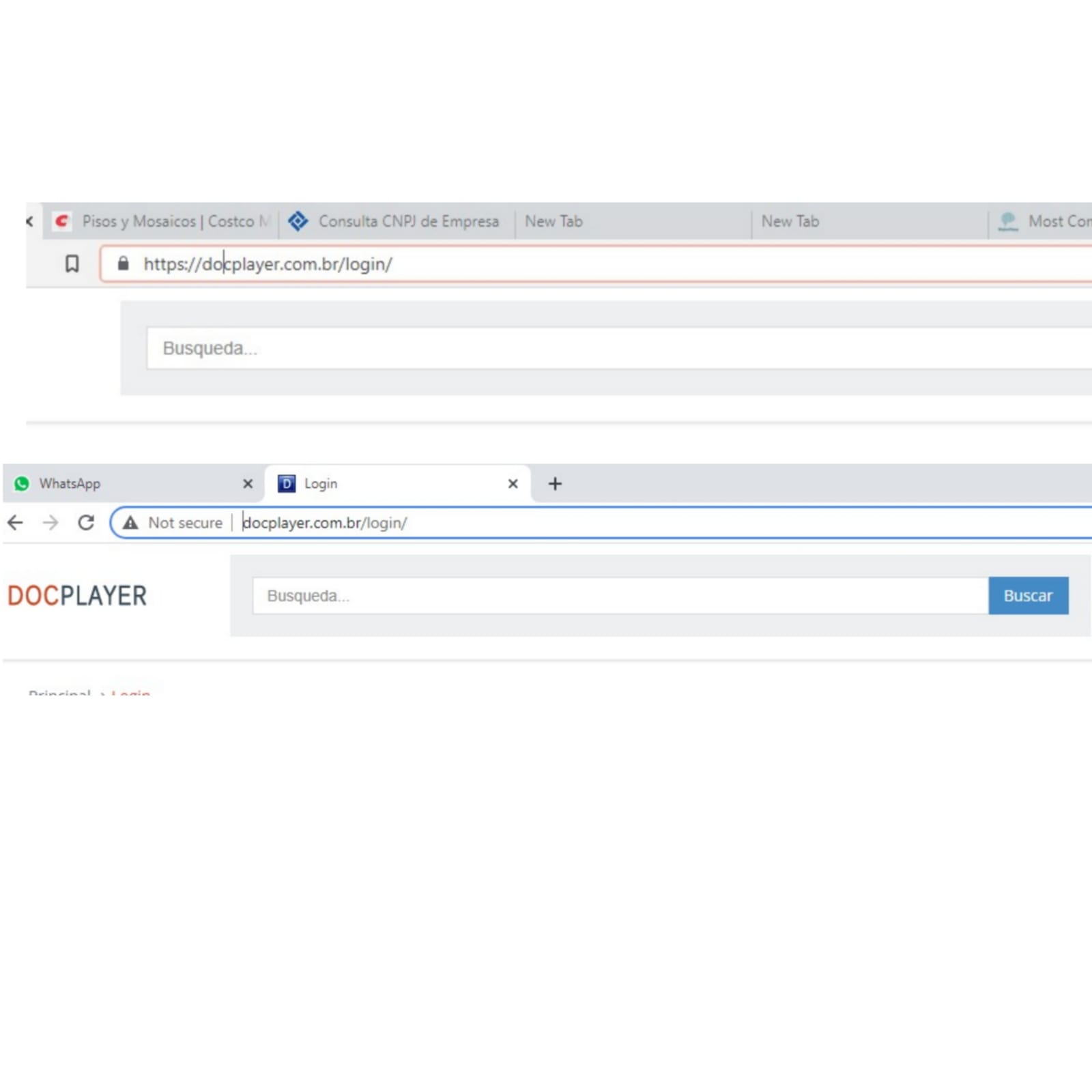
**IMPACT:**

If the HSTS vulnerability is present in any website then there can be the chances of data breaching , compromising the data and its privacy

**MITIGATION:**

In order to avoid the HSTS Vulnerability, developers of the websites should disable the actions of changing the protocols in the respective URL’s

**PROOF OF CONCEPT:**

****

1. **TARGET -II**

**DESCRIPTION:** HSTS Vulnerability is the vulnerability where the websites containing “https” protocols are being downgraded to unsecured “http” protocol page.

**VULNERABLE TARGET:** https://www.ellenkicet.ac.in/

**STEPS TO TEST THE HSTS VULNERABILITIES OVER THE RANDOM WEBSITES:**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Open some websites having “https” in their URL

**Step3:** Now manually remove ‘s’ letter from “https”

**Step4:** now reload the page

**Step5:** If the page URL has “http” after reloading then there is chance for HSTS Vulnerability and thus the page is down graded

**Step6:** If the page URL has “https” after reloading then there is no chance for HSTS Vulnerability.

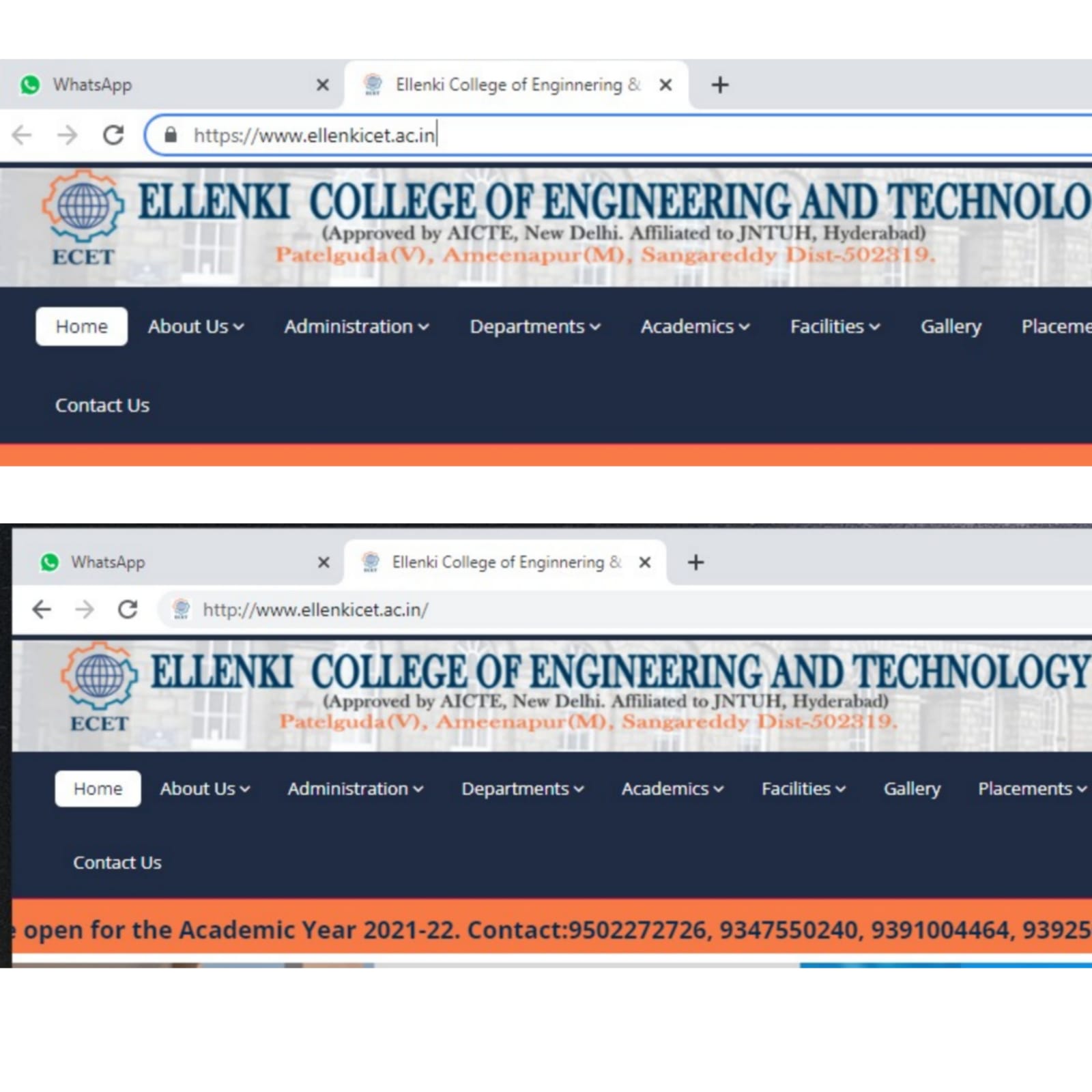
**IMPACT:**

If the HSTS vulnerability is present in any website then there can be the chances of data breaching , compromising the data and its privacy

**MITIGATION:**

In order to avoid the HSTS Vulnerability, developers of the websites should disable the actions of changing the protocols in the respective URL’s

**PROOF OF CONCEPT:**

****

1. **TARGET -III**

**DESCRIPTION:** HSTS Vulnerability is the vulnerability where the websites containing “https” protocols are being downgraded to unsecured “http” protocol page.

**VULNERABLE TARGET** **:** https://4movierulz3.com/

**STEPS TO TEST THE HSTS VULNERABILITIES OVER THE RANDOM WEBSITES:**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Open some websites having “https” in their URL

**Step3:** Now manually remove ‘s’ letter from “https”

**Step4:** now reload the page

**Step5:** If the page URL has “http” after reloading then there is chance for HSTS Vulnerability and thus the page is down graded

**Step6:** If the page URL has “https” after reloading then there is no chance for HSTS Vulnerability.

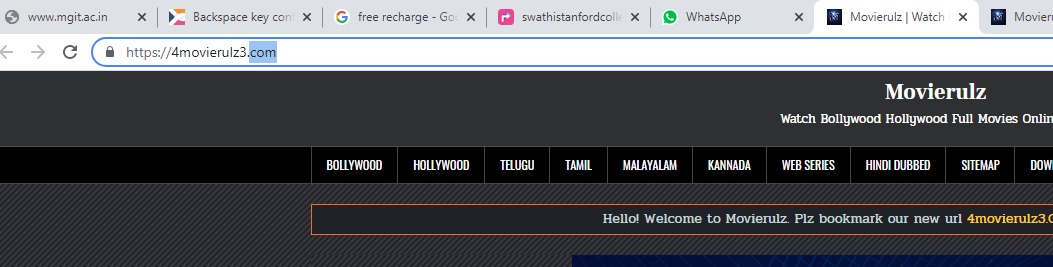
**IMPACT:**

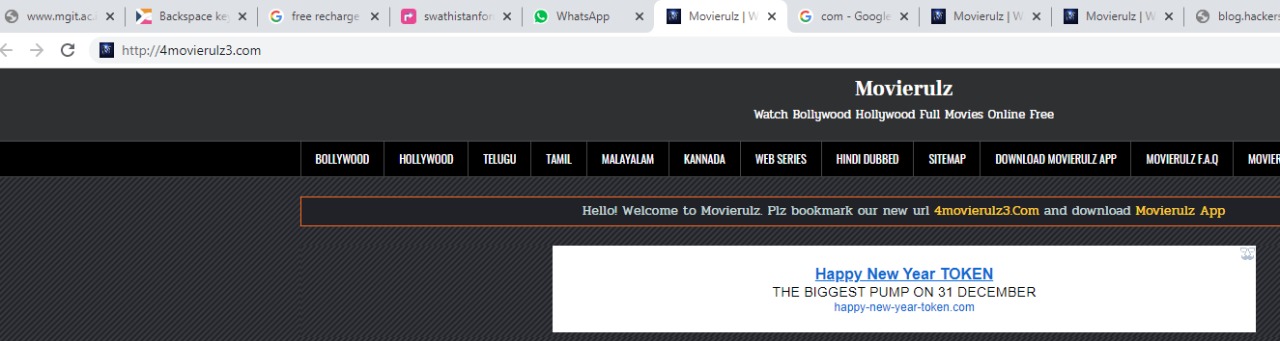
If the HSTS vulnerability is present in any website then there can be the chances of data breaching , compromising the data and its privacy

**MITIGATION:**

In order to avoid the HSTS Vulnerability, developers of the websites should disable the actions of changing the protocols in the respective URL’s

**PROOF OF CONCEPT:**





1. **TARGET -IV**

**DESCRIPTION:** HSTS Vulnerability is the vulnerability where the websites containing “https” protocols are being downgraded to unsecured “http” protocol page.

**VULNERABLE TARGET** **:** http://www.hcmadras.tn.nic.in/

**STEPS TO TEST THE HSTS VULNERABILITIES OVER THE RANDOM WEBSITES:**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Open some websites having “https” in their URL

**Step3:** Now manually remove ‘s’ letter from “https”

**Step4:** now reload the page

**Step5:** If the page URL has “http” after reloading then there is chance for HSTS Vulnerability and thus the page is down graded

**Step6:** If the page URL has “https” after reloading then there is no chance for HSTS Vulnerability.

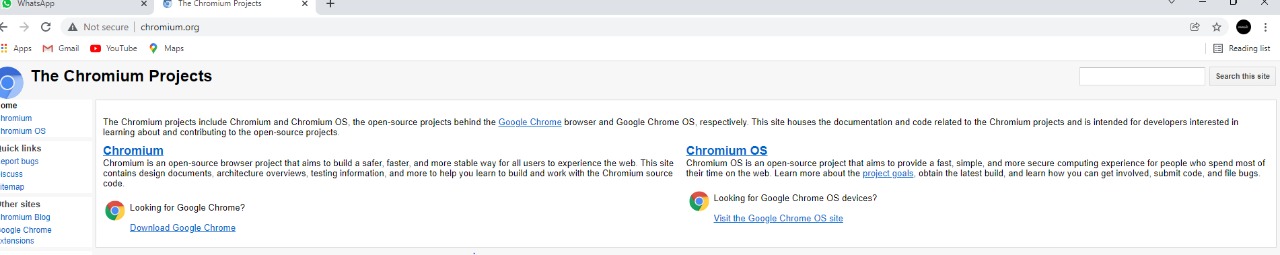
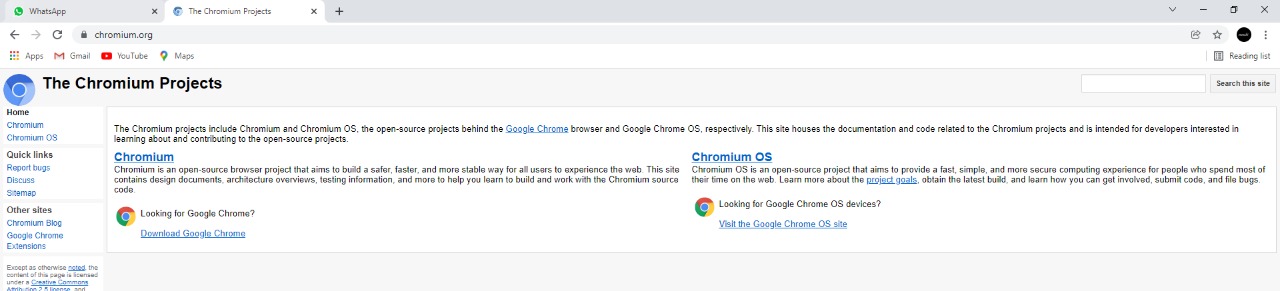
**IMPACT:**

If the HSTS vulnerability is present in any website then there can be the chances of data breaching , compromising the data and its privacy

**MITIGATION:**

In order to avoid the HSTS Vulnerability, developers of the websites should disable the actions of changing the protocols in the respective URL’s

**PROOF OF CONCEPT:**



1. **TARGET -V**

**DESCRIPTION:** HSTS Vulnerability is the vulnerability where the websites containing “https” protocols are being downgraded to unsecured “http” protocol page.

**VULNERABLE TARGET** **:**

**STEPS TO TEST THE HSTS VULNERABILITIES OVER THE RANDOM WEBSITES:**

**Step1:** Open any browser of your choice(google, firefox, opera…etc)

**Step2:** Open some websites having “https” in their URL

**Step3:** Now manually remove ‘s’ letter from “https”

**Step4:** now reload the page

**Step5:** If the page URL has “http” after reloading then there is chance for HSTS Vulnerability and thus the page is down graded

**Step6:** If the page URL has “https” after reloading then there is no chance for HSTS Vulnerability.

**IMPACT:**

If the HSTS vulnerability is present in any website then there can be the chances of data breaching , compromising the data and its privacy

**MITIGATION:**

In order to avoid the HSTS Vulnerability, developers of the websites should disable the actions of changing the protocols in the respective URL’s

**PROOF OF CONCEPT:**

**THANK YOU**

**BY :**

**M.VUJWALA (CSE BTECH-II)**

**B.SAI TEJA (CSE-CS BTECH-I)**

**A.VAMSHI (CSE-CS BTECH-I)**

**SRI NIKHIL.C (CSE-CS BTECH-I)**