A green chameleon logo

Description automatically generated

HSTS And SSL STRIPPING

Contents

[HSTS 2](#_Toc146122915)

[SSL Stripping 3](#_Toc146122916)

[Tools Used 3](#_Toc146122917)

[Results 6](#_Toc146122918)

[Conclusion 7](#_Toc146122919)

# HSTS

HTTP Strict Transport Security (HSTS) is a web security measure that defends websites and their users from certain types of attacks, like SSL stripping and man-in-the-middle attacks. Its purpose is to make sure that a user's browser and a website always communicate to each other over a secure HTTPS channel. With HSTS, a user's web browser is told to always use HTTPS when linking to a certain website. This means that even if a user types "http://" into their browser or clicks on an HTTP link, the browser will change it to "https://" and set up a secure relationship. This keeps people from using unsecure HTTP by mistake or on purpose.

The website sends HSTS headers with a "max-age" command that tells the browser how long it should remember to use HTTPS for that site. Most of the time, this is set for a long period of time, like a year or more. Also, websites can choose to be on HSTS preload lists that are kept by the most popular browsers. Being preloaded means that HSTS is turned on by default for that site in all computers that can handle it.

To use HSTS, website admins must set up their web server to send HTTP responses with the HSTS header.

Below attached is the screenshot of Strict Transport Security enabled in MOP Website and the existing chameleon website which doesn’t implement HSTS therefore making the website vulnerable to SSL stripping and Man in the Middle attack.

A computer screen with a green lizard

Description automatically generated

A screenshot of a computer

Description automatically generated

# SSL Stripping

SSL stripping, which is also called HTTPS stripping, is a type of cyberattack that tries to break the security of HTTPS (Hypertext Transfer Protocol Secure) links. HTTPS is a protocol for sending encrypted data between a user's computer browser and a website. SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption is used to protect private information like login information, financial data, and personal information.

SSL stripping is a type of man-in-the-middle (MitM) attack in which an attacker intercepts the conversation between a user and a website, changing the secure HTTPS connection to an insecure HTTP connection. This lets the attacker listen in on the traffic and possibly steal private information, like login credentials or session cookies, which can be used to gain unauthorised access.

Since the chameleon website doesn’t implement strict transport security it was easier to downgrade the website to HTTP and perform a Man in the middle attack.

# Tools Used

* Kali
* Windows
* Bettercap
* Microsoft Edge/ Firefox/ Chrome

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The above screenshot are the usage and configuration of Bettercap.

Using the Bettercap to enable ARP spoofing, DNS spoofing on my windows machine which I chose as the target machine and downgrading the website I was able to capture the user credentials when I tried to use the login page.

Screens screenshot of a computer

Description automatically generated

Screens screenshot of a computer screen

Description automatically generated

Screens screenshot of a computer

Description automatically generated

These are the screenshots of the capture obtained when using all three different browsers.

# Results

This happened only because the HSTS wasn’t enabled on the website which made it easier to implement the attacks. If the HSTS was enabled on the website, then the web browser would have prevented the downgrade thus making the communication encrypted. Since it was using HTTP the POST requests were not encrypted and they were visible as plain text. Thus, it makes it important to implement the HSTS for the website.

A computer screen shot of a computer code

Description automatically generated

This is the screenshot of using a command line tool called curl to check whether both the websites implement Strict Transport Security or not. Here the MOP website produced the output of strict transport security whereas the chameleon website returned no output which means it doesn’t implement HSTS.

# Conclusion

While the SSL stripping attack has been carried out, it becomes clear that this method is a major threat to the security and privacy of online interactions. If an attacker changes a secure HTTPS connection to an insecure HTTP connection, they can steal private data like login credentials and personal information. This could lead to identity theft and unauthorised access to accounts. This shows how important it is to use strong security methods, like HTTP Strict Transport Security (HSTS), to make sure connections are secure and protect against attacks like these.