HTU

جامعة الحسين التقنية

Al Hussein Technical University

NAME/ID : ABDELKAREEM YOUSEF MAMDOH SOUBAR/19110022
SUBJECT : SECURITY LAB
ASSIGNMENT INCLUDES : SECURITY LAB (PART 3)
DEAD LINE : 9/1/2022

Identification

Risks we have at geeks for geeks website are :

- CGI Generic XML Injection
- HSTS Missing From HTTPS Server (RFC 6797)

what is CGI Generic XML Injection:
it means that the hacker can access the website back end data base through the HTMl on the browser by changing the code of the website and how it deals and sends data to the main server.

What is HSTS Missing From HTTPS Server (RFC 6797):
it means that it allowed other than HTTPS traffic on the website which means that the connect that the web site is having became in secure for not fully using HTTPS.

Analysis

CGI Generic XML Injection
this problem is very big problem because this enables the hackers to inject your server with information that you don't need which can result in them changing the content in the database through changing the XML inside the website, it can also enable criminal to access account the do not belong to them and edit them or change things in the data that can lead your website to crash or spread viruses and it can also enable them to create accounts without having any authorization which can result in them accessing your website/system at any time they want.

HSTS Missing From HTTPS Server (RFC 6797)
the problem is that the server is not enforcing the HTST and yes it is optional when building a website to have HTST forced or not but forcing it will eliminate the element of striping data from the user by that it means low end hacker will be able to do a simple man in the middle attack and read the credential of the website and take your use and modify your cookie (not secured connection) to the website.

Solution

CGI Generic XML Injection
First of all this error can be a false positive because we are using XML and it can be figured out be checking the website PHP if it uses ‘strip_tag()’ to sanitize user input if its not sanitized it means your not in a falsie positive situation its real, go modify the PHP script to suit this problem/risk and re run the nessus vulnerability test just to be sure that its good and fixed.

HSTS Missing From HTTPS Server (RFC 6797)

in this problem you will need to do a simple thing which to reconfigure the remote web server to use HSTS so the connection would be encrypted and secure.