Gabriel Salcedo

IST 5930

Lab Assignment 8

XSS

* Clone repository “git clone <https://github.com/MariaGarber/XSS-Scanner.git>”
* Enter cloned folder “cd XSS-Scanner”
* Install “npm install”
* Run the application “npm start”

Server XSS occurs when untrusted user supplied data is included in an HTTP response generated by the server.

Client XSS occurs when untrusted user supplied data is used to update the DOM with an unsafe JavaScript call.

User Enumeration

* Identify an FTP Server using “nmap -p 21 X.X.X.X”
* Grab a banner “nc -nv X.X.X.X 21”
* Identify current working directory
* Identify FTP is giving access to directories for other services
* Identify files and folders user has access to.

Types of user enumeration:

* Forgotten password
* Predictable Username Formats
* RID Cycling
* OpenSSH username enumerations