Today we are going to be talking about the power of ‘string’. Have you ever used an input tag and wanted to use the typeof javascript operation to validate its value if for example the value of the input is a string do this else do that.

Here we have this html file that has an input tag in it and a script that consoles the typeof the value of the input tag on input of a key. So in this html file the type of the input tag has been put to number so it can only accept numbers. What do you think the type of the input value would be

As you can see in the console although I am inputting numbers and receiving string as my typeof the value although the type has been set to number it gives me a string. Does anyone have any idea why html is forcing the type to be only string. Maybe these topics I am about to talk about will help

SQL injection. What is sql injection? It is a common web hacking technique used by hackers that can enable them steal information from your database or even harm the database by using a well crafted string template or from the url craft to send a different information or query to the database so its output would not be the original output which the creator of the web-app hoped it would be rather it would be an output that the hacker wants provided that the information is in the database.

Now how does this work. In querying a data base the syntax is usually like this. Where hammer is a variable which is presented in a string form. This is basically visual way of how the data is presented to the backend and from this if you are crafty enough knowing that hammer is the variable which is the input of the code then what you’d be looking to do is to craft the string in such a way that we can make it return more data or anything but to do this first the hacker needs to know what SQL language is used making the app, and that is usually done by doing bling injections. Blind injections is a way to communicate with the query but without returning a result. For example trying a sleep function if MySQL or the equivalent for each language

Now here is in this javascript code it takes information from the variable city. Now imagine if the variable city was transformed in such a way to allow us manipulate the query, basically the hacker would try to maybe add and or (2 = 2) now the query being sent to the database is no longer select from user info where city = a city its now select from user info where city = a city or 2 = 2 which is true and we know how the or operator works if one is true then it returns true so now basically the query Is select from user info where city = true and as long as a city exists it would equal to true so it would bring up all the occurrence of the city

Now a way to fix this is by checking the value of the variable you are putting in for example checking if it’s a number if not throw an error or a string which gets more complicated but then an easier way is from your client which is a js library that cleans your input for you just by adding a parameter $1 and then the parameter checks to see if the input fits else it would throw an error.

Now another thing I want to talk about is LOG 4J is a java framework used in logging information. And it is famously used by a lot of big companies. But log 4j had some vulnerabilities which can exploited. So id be showing some of the vulnerabilities and explaining

This is a simple java application that takes input from the user and then puts the input in the log and then logs it to the console. You can log your information anywhere but here it is being logged to the console.

Now log 4j allows you concatenate variable values into string doing this. Now that’s not such a bad thing but then it gives the user some power

An example is here where the user uses this code to check the current version of java running on the application and sends it to the log. Now looking at this its not so bad but it gets worse because of something called jndi.

Now jndi is The Java Naming and Directory Interface™ (JNDI) is an application programming interface (API) that provides naming and directory functionality to applications written using the Java™ programming language and it can allow you communicate with other server for example if you write jndi: ldap://a url. It would automatically connect to the url. And now information can be logged into that url or instead something from that url can be downloaded into the java program in the form of objects

For example this is a url that downloads a simple code calculator from that url and runs it on the java program now this is dangerous cause you can download something malicious to a program. Or send useful information from the program to another