**INJECTING JAVASCRIPT CODE**

**IN BETTERCAP**

**We can:**

**- Inject Javascript code in loaded pages**

**- Code gets executed by the target browser**

**This can be used to:**

**- Replace links**

**- Replace images**

**- Insert html elements**

**- Hook target browser to exploitation frameworks**

**- and much more!**

**For now we will inject simple JS code and build it up later**

To inject JS code into the target browser we must have a JS code on our Kali

**So we will open a text editor and we are going to write a very very simple JS code:**

alert('javascript test');

**This will display an alert message saying javascript code**

Since we are going to try to inject this code into all pages, every time we load a webpage, we should see a message saying javascript test

**So lets save the file in root and name it alert.js**

**The next step is to go to our HSTS hijack plugin which is in:**

**/usr/share/bettercap/caplets/hstshijack**

Here we have the **hstshijack.cap** file which is the configuration file for the whole plugin so we are going to **right click it and open it with our text editor**

**In there what we want to modify is the payloads**

**We can already see it is injecting a JS code file called keylogger.js but we also want to inject our own code**

**So we add a comma at the end of the keylogger.js and we are going to add a star( \* ) followed by a colon( : )**

**We added this star to say that we want to inject our script into any page that the target loads**

If you want to inject your code into specific domains, then you can remove the star and list the domains that you want to inject this code in on the place of the star ( \* )

**But we want to inject this into all pages so we put the star ( \* ) and after the colon ( : ), we are going to put the location of the JS file that we want to inject into the browser so we put:**

oafjaofahfa/keylogger.js,\*:/root/alert.js

Lets save it with Ctrl + S and quit it Ctrl + Q and we are ready to go

**We go to our terminal, run BetterCAP using the same command we have been using**

**What we want to do now is run our HSTS hijack plugin:**

hstshijack/hstshijack

We can see in hstshijack.payloads that the payloads are running the default and our own JS payload

So now anytime our targets loads any web page, the whatever code we put in the alert.js should be injected in the loaded page and it should get executed

**The result of that should show us a simple message saying javascript test, that means our injection was success**