2. To hide the attack code to the victim :

In reflected Cross-site scripting (XSS) attack, a user accidentally requests malicious javascript code from the website. Once the attacker identifies XSS vulnerabilities in an application, it gives them ability to inject javascripts into the application on the client side i.e. to redirect users to malicious website. Apart from javascript, they can also include any executable active content like HTML, VBScript, Activex and other client-side languages. Unlike most attack that involves two parties **Attacker** and the **website** or the **Attacker** and the **Client**, the cross-site scripting comprises three parties—**Attacker**, **Client and a Website** with vulnerability.

The attacks are normally injection attacks into several interpreters in the web browser.

One way to hide the attack code to the victims which is visible within the URL is to use URL shorteners to hide the malicious script written by the attacker. The attacker can also post a message with a link to a seemingly harmless site, which encodes the script that attacks the user once they click the link. They can use wide range of encoding practices to conceal and obscure the malicious script. They also can avoid explicit use of the <script> tags when using javascript. The hackers can implement Double Encoding, Hex converter techniques as well to hide the malicious scripts.

The below screenshot shows concealing of the script to the victim using URL shortener called TinyURL :


Fig1: TinyURL

Now, this is how the link will look at the victim's end :

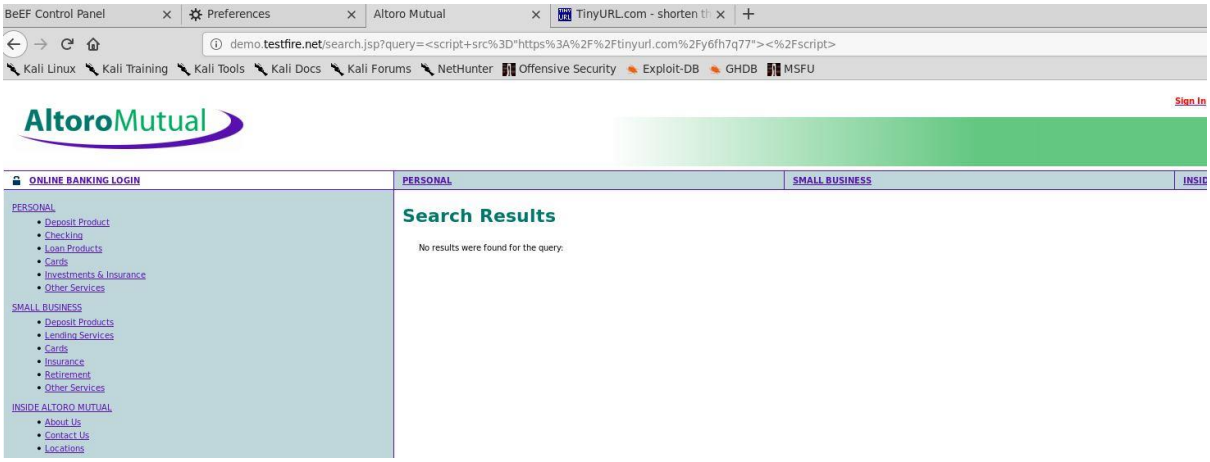


Fig 2: Concealed script at victim's end