Stored XSS Fuzzer

Beta 1

Written by 秋风落木

A Secondary Element Specie in China

liyawei.cn

chiruom@live.com

https://github.com/chiruom/

Introduction

This tool can give you a hand if you want to discover stored XSS in your Web Application.

However,This tool is a beta edition now, So some bugs may be found when use it,You can edit the python code by yourself or connect author by *root@liyawei.cn* as well as in *Github.com* . Thanks for your support , if you can give me useful advice,I will very happy!

Theory

This tool include a proxy to record the input and output points of user`s data when you browse your Web Application,and After your browsing,This tool will Resend the HTTP Request of the input point and output point many times,as the same time cheak the output ponits.The Tool will classify the Output points based the specific location (html,JavaScript,Css,eg)of data too.This process is a Fuzzing Test .

Usega

1. Open the *Record.py* .Set your browser proxy to 127.0.0.1:8083(you can change this in *Record.py*)
2. Browse your Web Application as far as your can,Input the string *<chiruomorg>* in every input points.Becaues the tool is base on the resending HTTP request , You should pay attention to do operation which can be Resent as you can .(For example,If your Web Application has a

"Blog" function,You should Use "Edit Blog" input the string *<chiruomorg>* install of "White New Blog"function)

3. You can see input point HTTP Request in *Srcreq.txt* after run *Srcreq.py* . Same method,you can do it uder idct *./_Record/* to see output point HPPT request.
4. After your browsing , Close *Record.py* and run *Test.py* .wait some miniters,The Report will be wrote in *Repot.html* .
5. Use *Clear.py to*clear the record and trace.

Expansion

All the XSS Fuzz Vectors are in dict *./_XSS/* ,XSS Vectors are classifide in **.txt* by the specific location of output point.

File	Location of output point
xss_html	Between html label, out of <>
xss_in_html	In html label,html attribute eg.
xss_html_js	In javascript which is inset in html code
xss_js	In Script label of *.js file
xss_css	In css
xss_json	Transmited in json

You can edit those txt files by your means.