XSSer

The Cross Site Scripting Framework

Roadmap Version:
v1.7b

Revision:
0.2

Author:
psy (epsylon@riseup.net)

Date:
11/09/2012

Resources:
https://www.owasp.org/index.php/OWASP_XSSER
http://xsser.sourceforge.net/

irc.freenode.net – channel: #xsser

Description of Roadmap:

This roadmap tries to help developers to understand which are the next steps to launch a new release of 'XSSer' (v1.7b).

Below is shown a structure of phases and milestones code areas.

Milestones:

- *Phase 1: Core:*

    <u>Bugfixing</u>:
    - False positives
    - Fix "swarm" results
    - Fix 'maximize' screen (bug reported)
    - Add auto-update revision
    - Fix multithreading (review)
    - Research 'glibc' corruption
    - [...]

    <u>Add crawlering</u> for POST+GET (auto test 'whole' page forms)

    <u>Update XSS payloads</u> (vectors.py / DOM.py / DCP.py / etc...)

    <u>Advance Statistics results</u> (show more detailed outputs)

    <u>Advance Exporting methods</u> (create 'whitehat' reports (xml/json))

    <u>Advance "WebSockets"</u> technology on XSSer 'fortune' option

    <u>Update Interface (GTK+)</u>

- *Phase 2: New features:*

    ○ Add '<u>code pre-check' option</u>: Users can set which code will return **target's** website, to try to evade false positive results.

    ○ Add '<u>CSSer' option</u>: Payloads for CSS injections.

    ○ <u>Research/Search anti-IDS/NIDS/IPS...</u> codes to evade XSS filters.

    ○ BurpXSSer: Create a Burp plugin (with Jython libs)

    ○ ZAPXSSer: Create a ZAP plugin (with Jython libs)

<u>EndRoad:</u> <u>01 / 05 / 2013</u> - (last code revision)