Conquest Web Application Exploit Tool

Daniel Zhang, Abhi Rathod, Tanner Harper, Asad Mahdi

Overview

- Automates SQL/XSS attack when provided with target domain:
  - Reconnaissance
  - Vulnerability Checking
    - Exploitation
- Authorized Mode
- Python 3.6
  - Requests
  - BeautifulSoup

Modules: Recon

- Gathers all live web pages from the target url
  - Crawler - Follows HTML links recursively
  - Forced Browse - Uses popular files and directories list to access pages not referenced by an application
- Authenticated mode
  - Will attempt to authenticate given credentials and crawl for pages only accessible once logged in

Modules: Vulnerability Checking

- Probe live pages
- Parses HTML - Inserts multiple XSS and SQL strings into input fields and POSTS
- Exhibited vulnerabilities marked for further exploitation

Modules: Exploitation

- User given options to exploit vulnerable pages
- XSS
  - iframe
  - Redirect
  - Cookie theft
- SQL
  - Authorization bypass
  - Table enumeration

Improvements

- Expand SQL coverage beyond SQLite
- Add breadth
  - Command injection
  - CSRF
  - RFI/LFI
- Add depth
  - More XSS (stored/reflected)
  - More SQL payloads