Getting started with WebGoat & WebScarab

Erwin Geirnaert
Partner & Co-founder – ZION SECURITY
Erwin.geirnaert@zionsecurity.com
www.linkedin.com/in/erwingeirnaert

OWASP Day
Belgium

6 Sep 2007

The OWASP Foundation
http://www.owasp.org/

Agenda

- Configure WebScarab as a local proxy
- Intercept HTTP requests and responses
- Modify HTTP requests to solve the lesson "Hidden field manipulation"
- Modify HTTP responses to solve the lesson "Bypass client-side Javascript validation"
- Use the session analysis tab in WebScarab
- Use the web services tab in WebScarab
- Use WebScarab to analyze Ajax XML messages

Configure WebScarab as a local proxy

- Extract WebGoat
- Start WebGoat with webgoat.bat
- Start WebScarab
  - Double-click the JAR should work
    - Otherwise create a .bat file that executes java.exe –jar 'filename'
    - A Java executable is included with WebGoat
- Configure your browser to use as proxy localhost on port 8008

Intercept HTTP requests and responses

- Open http://localhost/WebGoat/attack
- Login with guest – guest
- Do you see a pop-up window in WebScarab?
- You can select "Intercept request" and "Intercept response" in the pop-up window or in WebScarab via "Proxy" – "Manual edit"

Modify HTTP requests to solve the lesson "Hidden field manipulation"

- Go to the "Hidden field manipulation" lesson in "Unvalidated parameters"
- Read the lesson plan ☺
- Intercept the request
- Change the hidden field

Modify HTTP responses to solve the lesson "Bypass client-side Javascript validation"

- Go to the lesson "Bypass client-side Javascript validation"
- Read the lesson plan ☺
- Intercept the response
- Remove the Javascript validation
- Submit unvalid data

Use the session analysis tab in WebScarab

- Go to the lesson "How to hijack a session"
- Read the lesson plan ☺
- Let the request pass
- Go to the tab "Session analysis"
- Get 100 cookie values
- Examine the difference using the analysis options

Use the web services tab in WebScarab

- Go to the web services lesson in WebGoat
- Read the lesson plan ☺
- Click on the link for the WSDL file
- Go to the tab "web services" in WebScarab
- Select the WSDL from the drop-down box
- Execute a web service request

Use WebScarab to analyze Ajax XML messages

- Go to the Ajax security lessons in WebGoat
- Read the lesson plans ☺
- Try to solve the lessons by examining the XML messages in WebScarab

Coming soon

- New lessons in WebGoat
- New version of WebScarab NG
- WebGoat Solution Guide