TTKS0700 Data Security Testing

Lab 05. Web applications

Jarmo Nevala, 10.09.2019

Lab 05. Web applications

WEB Application testing

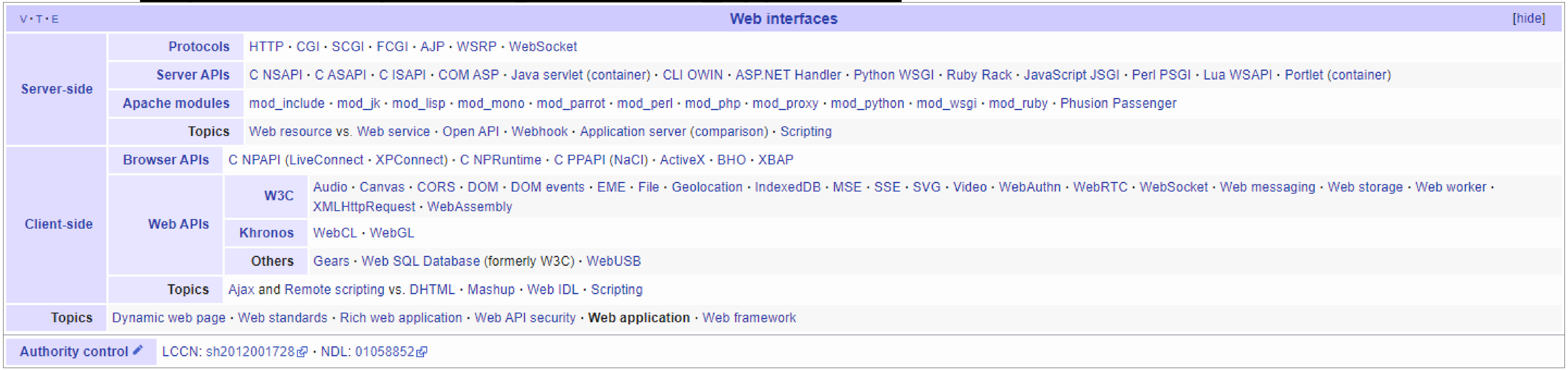
- GOAL
  - To understand basics of the WEB application testing
    - Proxies
    - Automated scanners
    - Manual testing

- In this document
  - RED color = TASK
  - BLUE color = TIP
  - Green color = Example

Lab 05. Web applications

Web applications everywhere!

- Vulnerabilities (COMMON)
    - OWASP TOP 10 (yearly list of top ten web application vulnerabilities)
- https://en.wikipedia.org/wiki/Web_application



V · T · E			Web interfaces [hide]
Server-side	Protocols		HTTP · CGI · SCGI · FCGI · AJP · WSRP · WebSocket
	Server APIs		C NSAPI · C ASAPI · C ISAPI · COM ASP · Java servlet (container) · CLI OWIN · ASP.NET Handler · Python WSGI · Ruby Rack · JavaScript JSGI · Perl PSGI · Lua WSAPI · Portlet (container)
	Apache modules		mod_include · mod_jk · mod_lisp · mod_mono · mod_parrot · mod_perl · mod_php · mod_proxy · mod_python · mod_wsgi · mod_ruby · Phusion Passenger
	Topics		Web resource vs. Web service · Open API · Webhook · Application server (comparison) · Scripting
Client-side	Browser APIs		C NPAPI (LiveConnect · XPConnect) · C NPRuntime · C PPAPI (NaCl) · ActiveX · BHO · XBAP
	Web APIs	W3C	Audio · Canvas · CORS · DOM · DOM events · EME · File · Geolocation · IndexedDB · MSE · SSE · SVG · Video · WebAuthn · WebRTC · WebSocket · Web messaging · Web storage · Web worker · XMLHttpRequest · WebAssembly
		Khronos	WebCL · WebGL
		Others	Gears · Web SQL Database (formerly W3C) · WebUSB
	Topics		Ajax and Remote scripting vs. DHTML · Mashup · Web IDL · Scripting
Topics			Dynamic web page · Web standards · Rich web application · Web API security · **Web application** · Web framework
Authority control			LCCN: sh2012001728 · NDL: 01058852

Lab 05. Web applications

Some tools…

- Proxies
  - BurbSuite (limited free version available)
  - OWASP Zed Attack Proxy
- Scanners
  - Nikto (web application vulnerability scanner)
  - Wpscan (wordpress scanner)
- Test injections & simulate attacks (exploitation)
  - SQLmap (automate SQL-injection)
- CheatSheets
  - XSS cheat sheet https://gist.github.com/kurobeats/9a613c9ab68914312cbb415134795b45
  - SQL injection cheat sheet https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection

Lab 05. Web applications

NIKTO security scanner

- Install NIKTO scanner
  - sudo apt-get update
  - sudo apt-get install nikto

Lab 05. Web applications

ZAP -proxy

- Install ZAP-proxy
  - sudo apt-get update
  - sudo apt-get install zaproxy
- Change your browser settings

Lab 05. Web applications

Task 1.

- List the possible targets (web servers) in the target environment
  - Port scans made in lab2
  - Vulnerability scans made in lab3

- SCAN web services with NIKTO scanner

- Tutorial (basic examples of NIKTO scanner) https://www.youtube.com/watch?v=GH9qn_DBzCk

Lab 05. Web applications

Task 2. – DVWA

- One target is DamnVulnerableWebApplication (DVWA), which is made to test skills and tools in legal environment
  - By default it is not vulnerable
  - Log in with default username and password (admin:password)
  - Go to DVWA security –page
  - Change security level from impossible to low, and submit changes
    - (low is good if you have zero experience)

- SCAN service again with NIKTO

- TIP1: you have to configure cookie –parameter to nikto (/etc/nikto.conf) for proper scan results
- TIP2: Use BURP –proxy OR ZAP proxy OR wireshark to capture valid cookie
- TIP3: Give proper path to NIKTO (GET path from possible vulnerable form)
- TIP4: Don’t bang your head against the wall too long!! ASK!! (teams chat, other students, email)

Lab 05. Web applications

Task 3. – SQLMap

- SCAN DVWA SQLi –site/form with SQLMAP –software

- TIP1: you have to configure cookie –parameter to SQLMAP (use sqlmap --help)
- TIP2: Use BURP –proxy OR ZAP proxy OR wireshark to capture valid cookie
- TIP3: Give proper path to SQLMAP (GET path from possible vulnerable form)
- TIP4: Don’t bang your head against the wall too long!! ASK!! (Teams chat, other students, email)

Lab 05. Web applications

Task 4.

- SELECT TASK 4.1 OR 4.2 (Same tasks - different tools)
    - Of course you can do both if you want..

Lab 05. Web applications

Task 4.1 Burbsuite -proxy

- Installed in KALI

- Configure proxy settings in BURP and WEB browser
- Use the web applications and capture
  - 1. Login
  - 2. cookie
  - 3. configuration change
  - 4. logout
- Try to intercept any request and change content

Lab 05. Web applications

Task 4.2 ZAP -proxy

- Installed in KALI

- Configure proxy settings in ZAP and WEB browser
- Use the web applications and capture
  - 1. Login
  - 2. cookie
  - 3. configuration change
  - 4. logout
- Try to intercept any request and change content

jamk.fi

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences