Ethical hacking and Penetration Testing

Web application attacks. Automatic tools

Author: Kutlymurat Mambetniyazov (@manfromkz)

Identifying the goals of lesson

- Understanding basic terms
- Reviewing and practicing vulnerability assessment tools

SAST vs DAST

- SAST and DAST are application security testing methodologies used to find security vulnerabilities that can make an application susceptible to attack.

- **Static application security testing (SAST)** is a white box method of testing. It examines the code to find software flaws and weaknesses.

- **Dynamic application security testing (DAST)** is a black box testing method that examines an application as it’s running to find vulnerabilities that an attacker could exploit.

SAST tools

- List of SAST tools
  - https://owasp.org/www-community/Source_Code_Analysis_Tools

- We will consider:
  - SonarQube
  - Graudit

Graudit

- https://github.com/wireghoul/graudit/
- Open Source
- Supports multiple languages, based on signatures. Signatures can be added manually.

SonarQube

- Official site - https://www.sonarqube.org/
- As virtual machine - https://bitnami.com/stack/sonarqube

- Supported languages: Java, C#, JavaScript, TypeScript, CloudFormation, Terraform, Kotlin, Ruby, Go, Scala, Flex, Python, PHP, HTML, CSS, XML and VB.NET

DAST tools

- List of DAST tools:
  - https://owasp.org/www-community/Vulnerability_Scanning_Tools

- We will consider:
  - OWASP ZAP
  - OpenVAS by Greenbone
  - Nikto

OWASP ZAP

- Official site - https://www.zaproxy.org/

- Free and open source

OpenVAS by Greenbone

- New name is GSM (Greenbone Security Manager)

- Link to download - https://www.greenbone.net/en/testnow/

Nikto

- https://www.kali.org/tools/nikto/

- Nikto is a pluggable web server and CGI scanner written in Perl, using rfp’s LibWhisker to perform fast security or informational checks.

Other tools

- Bruteforce hidden files/directories – dirsearch, dirb, dirbuster, wfuzz, ffuf
- Bruteforce web forms – Hydra, Burp Suite Intruder
- Bruteforce subdomains – sublist3r, subfuz
- Scan specific CMS – joomscan (Joomla CMS), wpscan (Wordpress), drupalgeddon2 (Drupal)
- SQL injection exploiting – sqlmap
- SSTI exploiting – tplmap
- Client-side attacks - BeEF

Cheat Sheets

- https://pentestmonkey.net/cheat-sheet
- https://github.com/coreb1t/awesome-pentest-cheat-sheets
- https://book.hacktricks.xyz/

Any questions?

Homework for the next lesson

- Try to scan Metasploitable host using OpenVAS by Greenbone
- Scan DVWA of Metasploitable using OWASP ZAP
- Exploit DVWA SQL injection using SQLmap

Feedback: did we achieved the goals of our lesson?

- Discussion 5-10 minutes

Useful links

- https://www.synopsys.com/blogs/software-security/sast-vs-dast-difference/
- https://www.kali.org/tools/nikto/
- https://github.com/wireghoul/graudit/
- https://owasp.org/www-community/Source_Code_Analysis_Tools
- https://owasp.org/www-community/Vulnerability_Scanning_Tools
- https://github.com/digininja/DVWA