jamk.fi

Web application security

Week3

Timo Lehosvuo, M3426
TTV18S1

Harjoitustyö
Web application security, Heikki Salo, Joni Ahonen
8.3.2021
Tekniikan ala

Reflection

OWASP Top 10 2017

- Injection
  - This one is familiar from earlier studies and from last week assignment
- Broken Authentication
  - Somewhat familiar have very little experience
- Sensitive Data Exposure
  - I have exposed this vulnerability in other labs
- XML External Entities (XXE)
  - Have read this but no practical experience
- Broken Access Control
  - I have exploited this vulnerability in other labs
- Security Misconfiguration
  - Must be the most common topic in vulnerabilities in cybersecurity studies so I am familiar with this topic
- Cross-Site Scripting (XSS)
  - Familiar, some practical experience
- Insecure Deserialization
  - Never heard of this one
- Using Components with Known Vulnerabilities
  - Quite familiar topic in cyber security, but no practical experience
- Insufficient Logging & Monitoring
  - Familiar topic, some experience of logging using pfsense

Real bugs

1. Injection (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27314)
2. Cross-site Scripting (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3395)
3. XML External Entities (XXE) (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27184)
4. Broken Authentication (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3977)
5. Broken Access Control (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12776)
6. Insecure Deserialization (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4888)

Reading Report

Vulnerabilities, weaknesses and risk

Vulnerabilities consist of weaknesses (one or more) that occur under a certain condition and makes the software behave unintendingly but not every weakness is a vulnerability. Weaknesses are more of a precursor for vulnerabilities. Also, the conditions may not exist for the exploitation of the weakness even though the weakness itself exists. Risk instead consist of both since it consists of likelihood and impact. Likelihood of an attack is increased by the amount of weaknesses and vulnerabilities and also threat agents and attack vector have a big part. The more weaknesses a system have the more vulnerabilities it has and the more vulnerabilities it has the greater likelihood of an attack it has and thus it is at greater risk.

Reflection

Viewing CWE items

1. I was surprised that how many categories there were to choose from
2. The size and how thorough the list were (clicking e.g. software development takes you to page that has 100 more links and so on)
3. Did not know that you can download the lists
4. Archive surprised me that you can go way back to version 1.0 and compare the changes