Universidade do Minho

Estruturas de Segurança

Vulnerabilities Mapping

Raphael J. S. Pinheiro
pg37160@alunos.uminho.pt

Vulnerability Management

- Area of Information Security
- Management of vulnerabilities found in:
    - pentests
    - bug bounty programs
    - user contribution
    - researches

Vulnerability Management

- Various Data Source
  - Nessus
  - Qualys
  - Acunetix
  - OpenVas
  - Nmap
  - Nexpose
  - so on

Vulnerability Representation

	Nessus	Qualys
ID	10669	10340
Name	A1Stats Multiple Script Traversal Arbitrary File Access	Drummon Miles A1Stats Directory Traversal Vulnerability
Categories	infos	Remote Discovery, Patch Available, Exploit Available
Family	CGI abuses	CGI
CVE	CVE-2001-0561	CVE-2001-0561
CVSS Score	Medium / CVSS Base Score : 5.0	7.5
Bugtraq ID	2705	2705

Problem

How to map vulnerabilities from different sources?

Solution

- Compare the attributes:
    - Title
    - CVE
    - References
- Calculate the similarity