|  |  |
| --- | --- |
| C1: New penetration testing tools | |
|  | title |
| 1 | Diagnostic model of vulnerability based on penetration testing |
| 2 | A Web Second-Order Vulnerabilities Detection Method |
| 3 | Development of an Architecture for a Cyber-Physical Emulation Test Range for Network Security Testing |
| 4 | An Improved Attack Path Discovery Algorithm Through Compact Graph Planning |
| 5 | Web Application Security: Threats, Countermeasures, and Pitfalls |
| 6 | Simulation platform for cyber-security and vulnerability analysis of critical infrastructures |
| 7 | Designing vulnerability testing tools for web services: approach, components, and tools |

SUB CLUSTERS

|  |  |
| --- | --- |
| C1: New penetration testing tools | |
| 1 | Web scanners |
| 2 | Other tools |

|  |  |
| --- | --- |
| C2: New penetration testing methods | |
| 1 | AI enhanced pentesting |
| 2 | Other methods |

|  |  |
| --- | --- |
| C3: penetration testing something | |
| 1 | Certain area |
| 2 | Certain technology |
| 3 | Certain tool |
| 4 | Certain thing |
| 5 | Certain place |
| 6 | Pentesting something new, not pentested before |
| 7 | Certain devices |

|  |  |
| --- | --- |
| C4: Informative research about penetration testing | |
| 1 | General information |
| 2 | Information about specific attacks |

|  |  |
| --- | --- |
| C5: Evaluation of penetration testing results or methods | |
| 1 | Evaluating specific attacks |
| 2 | Evaluating specific pentest methods |
| 3 | Evaluating specific defenses |