Lab 7 Report

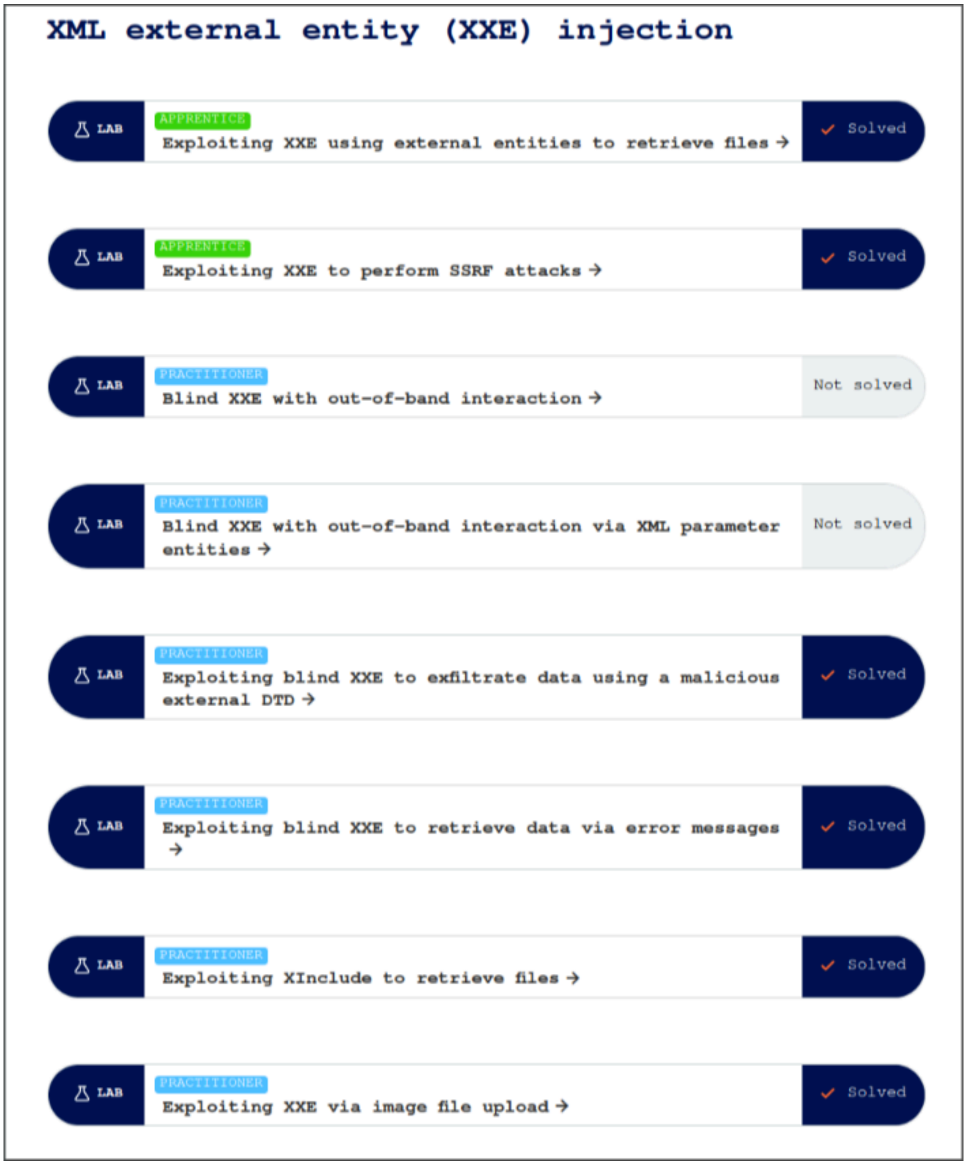
1. Name: 林靖昀   Student ID: B12902116

2. XXE: How many problems you solved? A: 6

   Show the Screenshot of your finished list

   4 basic in class (30%)

   2 advance (1 for 10%)



XML external entity (XXE) injection

LAB APPRENTICE Exploiting XXE using external entities to retrieve files → ✓ Solved

LAB APPRENTICE Exploiting XXE to perform SSRF attacks → ✓ Solved

LAB PRACTITIONER Blind XXE with out-of-band interaction → Not solved

LAB PRACTITIONER Blind XXE with out-of-band interaction via XML parameter entities → Not solved

LAB PRACTITIONER Exploiting blind XXE to exfiltrate data using a malicious external DTD → ✓ Solved

LAB PRACTITIONER Exploiting blind XXE to retrieve data via error messages → ✓ Solved

LAB PRACTITIONER Exploiting XInclude to retrieve files → ✓ Solved

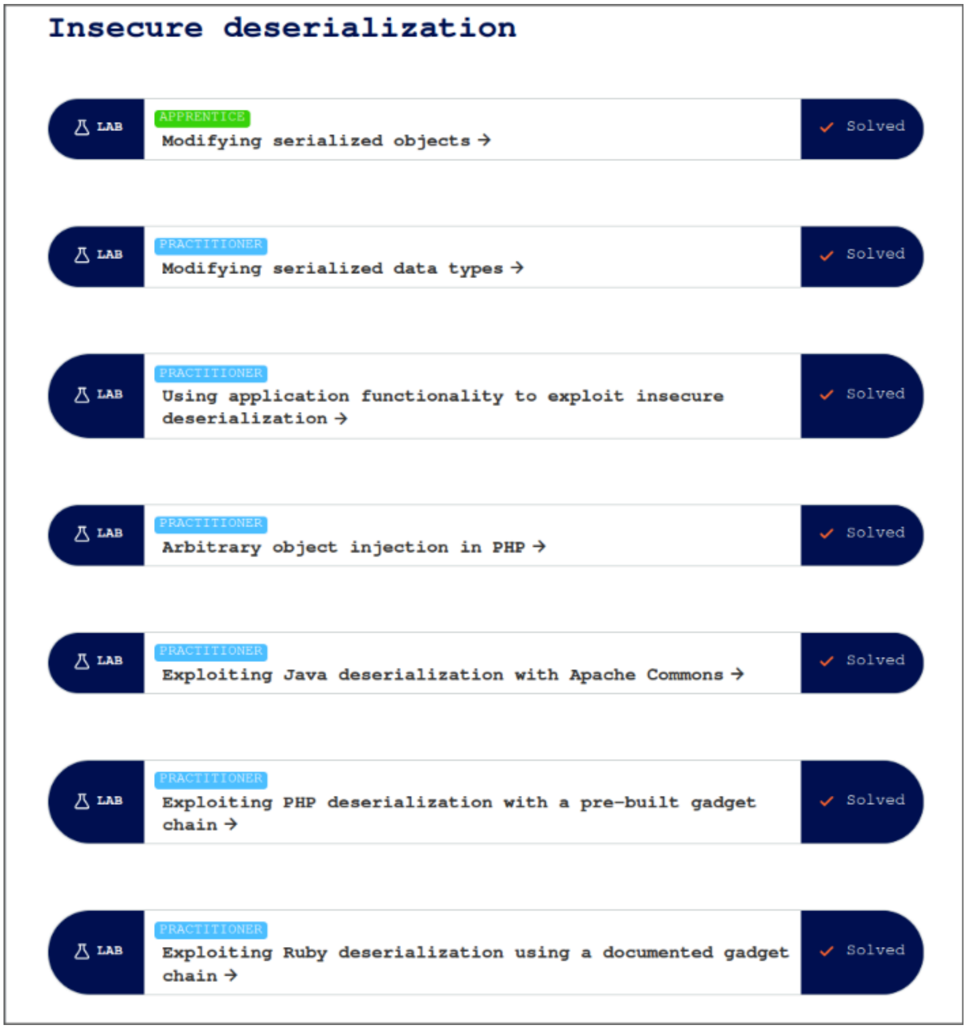
LAB PRACTITIONER Exploiting XXE via image file upload → ✓ Solved

3. Insecure Deserialization: How many problems you solved? A: 7

   Show the Screenshot of your finished list

   4 basic in class (30%)

   3 advance (1 for 6.6%)



Insecure deserialization

LAB APPRENTICE Modifying serialized objects → ✓ Solved

LAB PRACTITIONER Modifying serialized data types → ✓ Solved

LAB PRACTITIONER Using application functionality to exploit insecure deserialization → ✓ Solved

LAB PRACTITIONER Arbitrary object injection in PHP → ✓ Solved

LAB PRACTITIONER Exploiting Java deserialization with Apache Commons → ✓ Solved

LAB PRACTITIONER Exploiting PHP deserialization with a pre-built gadget chain → ✓ Solved

LAB PRACTITIONER Exploiting Ruby deserialization using a documented gadget chain → ✓ Solved

4. 你預計會得幾分? 100