Flipped Classroom Session 4: Software Security

CS-E3130 Information Security, 21.09.2023

1. SQL Injection

Consider the following database table

```
CREATE TABLE Documents (
   title TEXT,
   owner TEXT
);

INSERT INTO Documents VALUES ('t1', 'u1');
INSERT INTO Documents VALUES ('t2', 'u2');
```

and SQL query:

```
SELECT
  title
FROM Documents
WHERE
  Documents.owner = <name>
```

Suppose that the above query is executed using

```
$result = $connection->execute(
  "SELECT title from Documents WHERE Documents.owner = '" + $username + ');
```

1. Why is the above code insecure?
2. Suggest a value for $username that allows the user to see the titles of all documents in the system.

2. Buffer overruns

Consider the following piece of code

```
void vulnerable() {
  char str[8];
  gets(&str);
}
```

1. Draw a diagram showing what is stored in the function's stack, and where.
2. This function contains a buffer overrun vulnerability. Explain how an attacker would exploit it.
3. Suppose you want the function to return to address 0x01020304. What input should the attacker provide, assuming the stack layout above and a big-endian system? Indicate which parts of the input matter in order to change the return address.