10.14. □□□□□□□□(10.14. Code Injection and Input Validation)

10.14. □□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□--□□□□"state"□"redirect_uri"□□□□□

10.14. Code Injection and Input Validation

```
   A code injection attack occurs when an input or otherwise external  variable is used by an
application unsanitized and causes  modification to the application logic.  This may allow an
attacker to
   gain access to the application device or its data, cause denial of  service, or introduce a
wide range of malicious side-effects.
   The authorization server and client MUST sanitize (and validate when  possible) any value
received -- in particular, the value of the   "state" and "redirect_uri" parameters.
```

Revision #1
Created Wed, Mar 25, 2020 11:27 PM by □□□
Updated Wed, Mar 25, 2020 11:28 PM by □□□