**Problem**

Beaker before 1.6.4, when using PyCrypto to encrypt sessions, uses **AES in ECB cipher mode**, which might allow remote attackers to obtain portions of sensitive session data via unspecified vectors.

<https://github.com/bbangert/beaker/commit/91becae76101cf87ce8cbfabe3af2622fc328fe5>

**pycrypto.py**

def aesEncrypt(data, key):

cipher = **AES.new(key)**

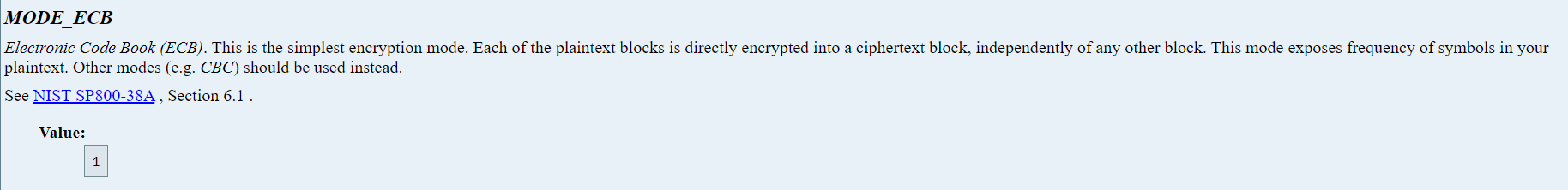
data = data + (" " \* (16 - (len(data) % 16)))

return cipher.encrypt(data)

def aesDecrypt(data, key):

cipher = **AES.new(key)**

return cipher.decrypt(data).rstrip()



**Fix**

**pycrypto.py**

from Crypto.Util import Counter

def aesEncrypt(data, key):

**cipher = AES.new(key, AES.MODE\_CTR,**

**counter=Counter.new(128, initial\_value=0))**

return cipher.encrypt(data)

def aesDecrypt(data, key):

**cipher = AES.new(key, AES.MODE\_CTR,**

**counter=Counter.new(128, initial\_value=0))**

return cipher.decrypt(data)

A picture containing application

Description automatically generated