演習 1

1270360:稗田隼也

12 月 29 日

1 OS コマンドインジェクションの危険性

入力として特殊文字や OS コマンド、SQL などを入力することで誤動作させて不正な行動を誘発させる攻撃であり、情報が奪われたりサーバ自体が停止させられたりする。また、仕組みは WEB の入力処理で既存する OS コマンドを入力し、OS コマンドが comand ’ 入力’ となっている場合に XSS の要領で x’;comand2; を入力することで 2 つ目のコマンドが実行される。

2 危険な記述

今回の演習では以下のコードの部分が OS インジェクションの可能性がある

Listing 1 switch

```
1  cmd ='big {} @localdns'.format(target)
2  proc = subprocess.run(cmd,shell=True,
3  stdout=PIPE, stderr=PIPE, text=True)
```

これは入力情報をそのまま Shell で利用してしまっているからで、これによって OS コマンドが実行されてしまう。

3 修正すべき点

この問題点は以下のようにシェルを利用せずにコマンドを実行できるようにすることで改善される。

Listing 2 switch

```
1  proc = subprocess.run(['big', target,
2    '@localdns'], shell=False, stdout=PIPE,
3  stderr=PIPE, text=True)
```

4　演習の感想

今回の演習で OS コマンドインジェクションがどのような場面で起こり、防御側がどのような修正をするべきかを実践的に学べた。

また、実践を通して学んだことで明確なイメージを持つことができてとても良かったです。しかし、実践のパターンが一つしかできなかったのでたくさんのバリエーションがあるといいなと思いました。また演習の際にリモートサーバーにアクセスする際に様々なアクシデントがあったので次からはスムーズにしたいと思った。