情報ネットワーク応用 演習 1 - レポート課題

森田 蓮

2024 年 12 月 24 日

1　OS コマンドインジェクションの危険性と対策

OS コマンドインジェクションは, 外部からの入力を OS コマンドに渡すときに開発者が予期しない不正な入力を OS が実行してしまうという脆弱性である．今回の演習の例で言えばサーバーの Python で書かれたソースコードでユーザーからの入力をそのまま dig コマンドに渡して Shell を利用して実行していることが OS コマンドインジェクションを引き起こす原因となることがわかる．

また，講義の話では C 言語で書くサーバーのコードには関数 get() を利用すること制限なしで文字列を受け取る．この関数 get() も OS コマンドインジェクションを引き起こす危険な記述である．

これらの対策として Shell を利用せずにコマンドを実行するように修正を加えることや，受け取る文字列に制限を加え OS コマンドで特別な意味を持つ文字を使えないようにする方法がある．

2　感想

今回の第 1 回演習では自分が講義を聞いただけでは実際にどんな動きをするのかわからなかったことが実際に手を動かして見ることで納得できることが多かった．今回の演習はトラブルがあり自分が納得するまで攻撃を考えてすることができなかったことが残念だった．TA さんがトラブルを直している姿がとてもお手本となる大学院生と思った．私も専門的なことを身に着けてたいなとモチベーションになりとてもいい機会であったと思う．より勉強をして今回 Doker に対する理解が足りていないのでもっと深めたいと思う．