Photo by Krivec Ales from Pexels

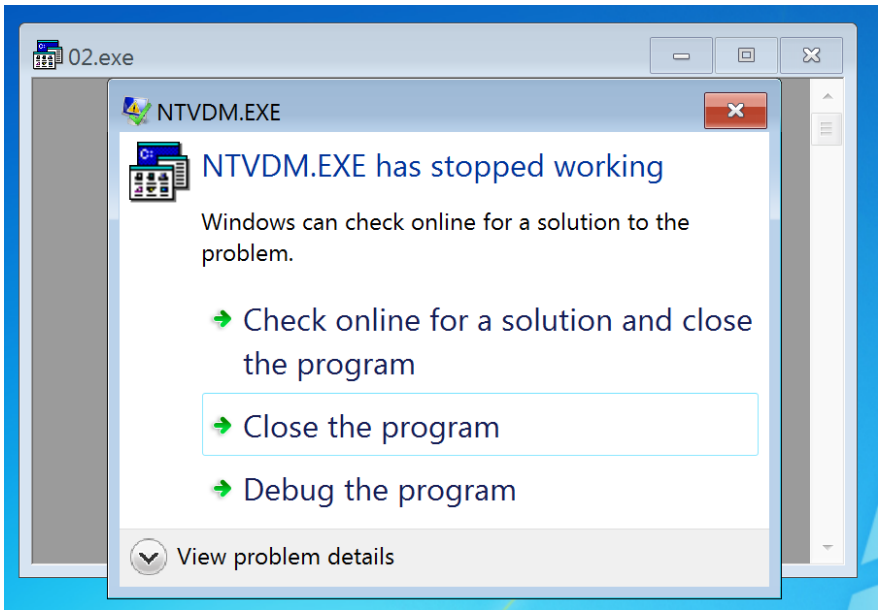
CodeEngn Basic RCE L02 Writeup

Daniel Smith
Feb 15 · 2 min read

Let’s start RCE

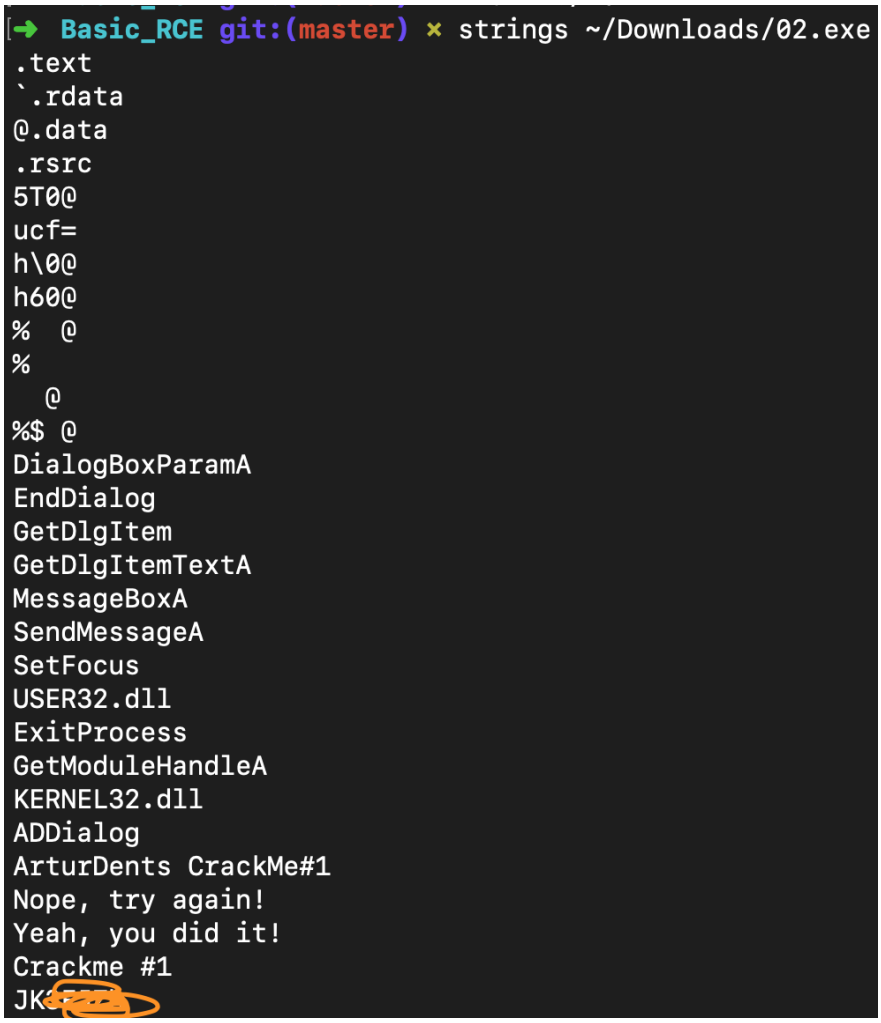
```
Filename: 02.exe
Description: 패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생
```

```
겼다. 패스워드가 무엇인지 분석하시오
Author: ArturDents
```



실행 시켜보려고 시도해 보았지만, Description 에 나와있는 대로 실행이 안된다

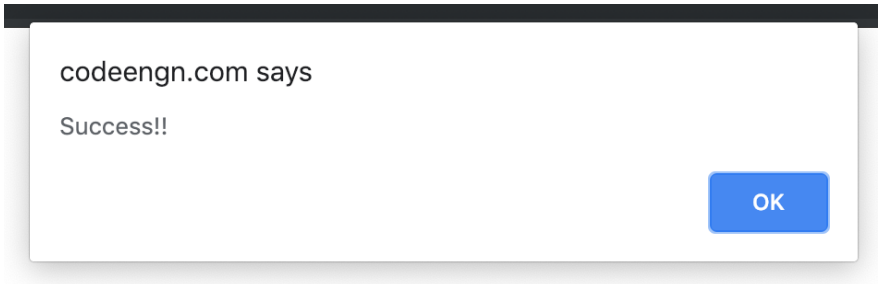
패스워드가 무엇인지 분석 해보기 위해 해당 프로그램을 strings 로 열어봤다



Key 값 유출시 CodeEngn 에서 불이익을 받을 수 있어서 가렸다

맨 아래에 보면 Nope, try again! 과 Yeah, you did it! 두개의 문자열이 있는것을 볼 수 있다

저런 문자열은 주변에 패스워드와 같이 있는 경우가 있으므로 유력한 문자열인 JK******* 문자열을 CodeEngn 에서 인증시켜 보았다



이번 문제는 파일 내부를 열어볼 수 있는지 알아보는 문제였던 것 같다