

# REPORT:

## 코드엔진 Basic

### RCE 06 Writeup

COLONY  
1824275 정상지

2021.05.23

Unpack을 한 후 Serial을 찾으시오. 정답인증은 OEP + Serial  
Ex) 00400000PASSWORD

## 0. 프로그램 실행

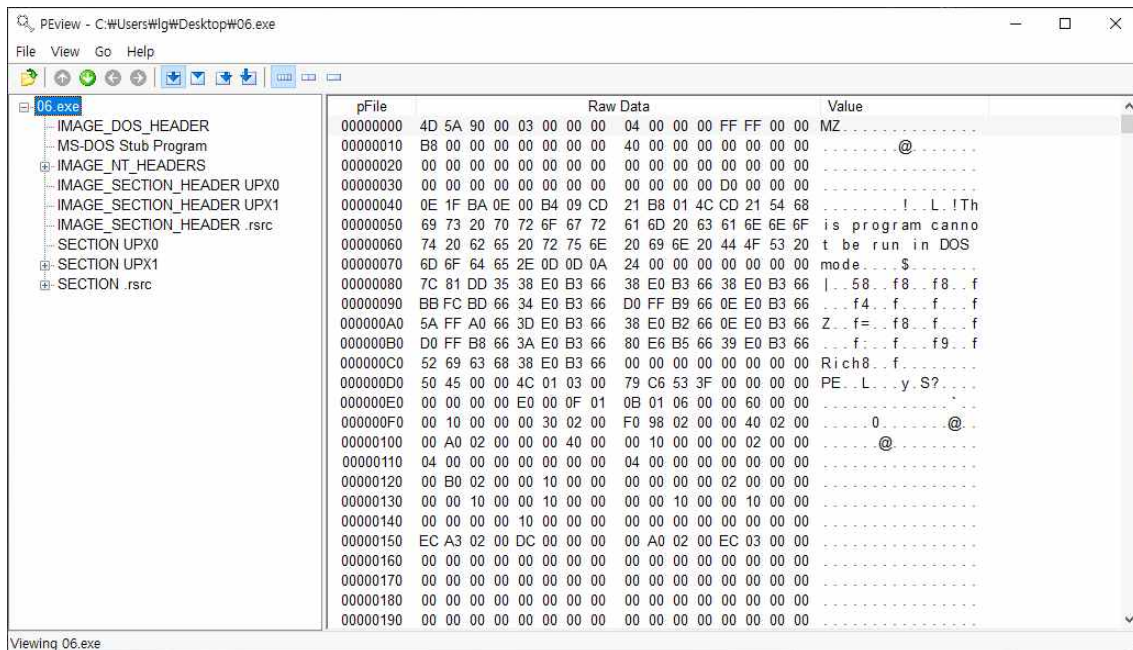


시리얼을 입력하는 창과 시리얼을 체크하는 버튼이 있다



아무 시리얼 값을 넣고 체크했을 때의 에러 출력 문구

## 1. PE view로 해당 파일 분석



UPX로 패킹되어 있는 모습을 볼 수 있다

## 2. UPX를 통해 언패킹

```

C:\Users\Wlg>cd ../
C:\Users>cd lg
C:\Users\Wlg>cd desktop
C:\Users\Wlg\Desktop>upx.exe -d hxd.exe -o hxe_unpack.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

File size      Ratio      Format      Name
-----
hxd.exe: FileNotFoundException: hxd.exe: No such file or directory
Unpacked 0 files.

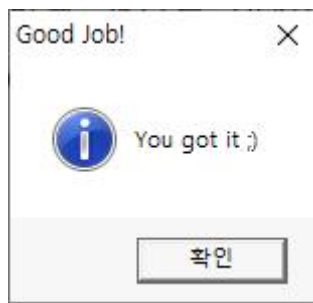
C:\Users\Wlg\Desktop>upx.exe -d 06.exe -o 06_unp.exe
Ultimate Packer for executables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

File size      Ratio      Format      Name
-----
159744 <-    26112    16.35%    win32/pe    06_unp.exe
Unpacked 1 file.
C:\Users\Wlg\Desktop>

```

### 3. 언패킹한 파일을 x32dbg로 디버깅

Address	Disassembly	Comment
00401360	push ebp	
00401361	mov ebp,esp	
00401363	push 0	
00401365	push 0	
00401366	push 0	
00401367	push 0	
00401368	push 0	
00401369	push 0	
0040136A	push 0	
0040136B	push 0	
0040136C	push 0	
0040136D	push 0	
0040136E	push 0	
0040136F	push 0	
00401370	push 0	
00401371	push 0	
00401372	push 0	
00401373	push 0	
00401374	push 0	
00401375	push 0	
00401376	push 0	
00401377	push 0	
00401378	push 0	
00401379	push 0	
0040137A	push 0	
0040137B	push 0	
0040137C	push 0	
0040137D	push 0	
0040137E	push 0	
0040137F	push 0	
00401380	push 0	
00401381	push 0	
00401382	push 0	
00401383	push 0	
00401384	push 0	
00401385	push 0	
00401386	push 0	
00401387	push 0	
00401388	push 0	
00401389	push 0	
0040138A	push 0	
0040138B	push 0	
0040138C	push 0	
0040138D	push 0	
0040138E	push 0	
0040138F	push 0	
00401390	push 0	
00401391	push 0	
00401392	push 0	
00401393	push 0	
00401394	push 0	
00401395	push 0	
00401396	push 0	
00401397	push 0	
00401398	push 0	
00401399	push 0	
0040139A	push 0	
0040139B	push 0	
0040139C	push 0	
0040139D	push 0	
0040139E	push 0	
0040139F	push 0	
004013A0	push 0	
004013A1	push 0	
004013A2	push 0	
004013A3	push 0	
004013A4	push 0	
004013A5	push 0	
004013A6	push 0	
004013A7	push 0	
004013A8	push 0	
004013A9	push 0	
004013AA	push 0	
004013AB	push 0	
004013AC	push 0	
004013AD	push 0	
004013AE	push 0	
004013AF	push 0	
004013B0	push 0	
004013B1	push 0	
004013B2	push 0	
004013B3	push 0	
004013B4	push 0	
004013B5	push 0	
004013B6	push 0	
004013B7	push 0	
004013B8	push 0	
004013B9	push 0	
004013BA	push 0	
004013BB	push 0	
004013BC	push 0	
004013BD	push 0	
004013BE	push 0	
004013BF	push 0	
004013C0	push 0	
004013C1	push 0	
004013C2	push 0	
004013C3	push 0	
004013C4	push 0	
004013C5	push 0	
004013C6	push 0	
004013C7	push 0	
004013C8	push 0	
004013C9	push 0	
004013CA	push 0	
004013CB	push 0	
004013CC	push 0	
004013CD	push 0	
004013CE	push 0	
004013CF	push 0	
004013D0	push 0	
004013D1	push 0	
004013D2	push 0	
004013D3	push 0	
004013D4	push 0	
004013D5	push 0	
004013D6	push 0	
004013D7	push 0	
004013D8	push 0	
004013D9	push 0	
004013DA	push 0	
004013DB	push 0	
004013DC	push 0	
004013DD	push 0	
004013DE	push 0	
004013DF	push 0	
004013E0	push 0	
004013E1	push 0	
004013E2	push 0	
004013E3	push 0	
004013E4	push 0	
004013E5	push 0	
004013E6	push 0	
004013E7	push 0	
004013E8	push 0	
004013E9	push 0	
004013EA	push 0	
004013EB	push 0	
004013EC	push 0	
004013ED	push 0	
004013EE	push 0	
004013EF	push 0	
004013F0	push 0	
004013F1	push 0	
004013F2	push 0	
004013F3	push 0	
004013F4	push 0	
004013F5	push 0	
004013F6	push 0	
004013F7	push 0	
004013F8	push 0	
004013F9	push 0	
004013FA	push 0	
004013FB	push 0	
004013FC	push 0	
004013FD	push 0	
004013FE	push 0	
004013FF	push 0	
00401400	push 0	
00401401	push 0	
00401402	push 0	
00401403	push 0	
00401404	push 0	
00401405	push 0	
00401406	push 0	
00401407	push 0	
00401408	push 0	
00401409	push 0	
0040140A	push 0	
0040140B	push 0	
0040140C	push 0	
0040140D	push 0	
0040140E	push 0	
0040140F	push 0	
00401410	push 0	
00401411	push 0	
00401412	push 0	
00401413	push 0	
00401414	push 0	
00401415	push 0	
00401416	push 0	
00401417	push 0	
00401418	push 0	
00401419	push 0	
0040141A	push 0	
0040141B	push 0	
0040141C	push 0	
0040141D	push 0	
0040141E	push 0	
0040141F	push 0	
00401420	push 0	
00401421	push 0	
00401422	push 0	
00401423	push 0	
00401424	push 0	
00401425	push 0	
00401426	push 0	
00401427	push 0	
00401428	push 0	
00401429	push 0	
0040142A	push 0	
0040142B	push 0	
0040142C	push 0	
0040142D	push 0	
0040142E	push 0	
0040142F	push 0	
00401430	push 0	
00401431	push 0	
00401432	push 0	
00401433	push 0	
00401434	push 0	
00401435	push 0	
00401436	push 0	
00401437	push 0	
00401438	push 0	
00401439	push 0	
0040143A	push 0	
0040143B	push 0	
0040143C	push 0	
0040143D	push 0	
0040143E	push 0	
0040143F	push 0	
00401440	push 0	
00401441	push 0	
00401442	push 0	
00401443	push 0	
00401444	push 0	
00401445	push 0	
00401446	push 0	
00401447	push 0	
00401448	push 0	
00401449	push 0	
0040144A	push 0	
0040144B	push 0	
0040144C	push 0	
0040144D	push 0	
0040144E	push 0	
0040144F	push 0	
00401450	push 0	
00401451	push 0	
00401452	push 0	
00401453	push 0	
00401454	push 0	
00401455	push 0	
00401456	push 0	
00401457	push 0	
00401458	push 0	
00401459	push 0	
0040145A	push 0	
0040145B	push 0	
0040145C	push 0	
0040145D	push 0	
0040145E	push 0	
0040145F	push 0	
00401460	push 0	
00401461	push 0	
00401462	push 0	
00401463	push 0	
00401464	push 0	
00401465	push 0	
00401466	push 0	
00401467	push 0	
00401468	push 0	
00401469	push 0	
0040146A	push 0	
0040146B	push 0	
0040146C	push 0	
0040146D	push 0	
0040146E	push 0	
0040146F	push 0	
00401470	push 0	
00401471	push 0	
00401472	push 0	
00401473	push 0	
00401474	push 0	
00401475	push 0	
00401476	push 0	
00401477	push 0	
00401478	push 0	
00401479	push 0	
0040147A	push 0	
0040147B	push 0	
0040147C	push 0	
0040147D	push 0	
0040147E	push 0	
0040147F	push 0	
00401480	push 0	
00401481	push 0	
00401482	push 0	
00401483	push 0	
00401484	push 0	
00401485	push 0	
00401486	push 0	
00401487	push 0	
00401488	push 0	
00401489	push 0	
0040148A	push 0	
0040148B	push 0	
0040148C	push 0	
0040148D	push 0	
0040148E	push 0	
0040148F	push 0	
00401490	push 0	
00401491	push 0	
00401492	push 0	
00401493	push 0	
00401494	push 0	
00401495	push 0	
00401496	push 0	
00401497	push 0	
00401498	push 0	
00401499	push 0	
0040149A	push 0	
0040149B	push 0	
0040149C	push 0	
0040149D	push 0	
0040149E	push 0	
0040149F	push 0	
004014A0	push 0	
004014A1	push 0	
004014A2	push 0	
004014A3	push 0	
004014A4	push 0	
004014A5	push 0	
004014A6	push 0	
004014A7	push 0	
004014A8	push 0	
004014A9	push 0	
004014AA	push 0	
004014AB	push 0	
004014AC	push 0	
004014AD	push 0	
004014AE	push 0	
004014AF	push 0	
004014B0	push 0	
004014B1	push 0	
004014B2	push 0	
004014B3	push 0	
004014B4	push 0	
004014B5	push 0	
004014B6	push 0	
004014B7	push 0	
004014B8	push 0	
004014B9	push 0	
004014BA	push 0	
004014BB	push 0	
004014BC	push 0	
004014BD	push 0	
004014BE	push 0	
004014BF	push 0	
004014C0	push 0	
004014C1	push 0	
004014C2	push 0	
004014C3	push 0	
004014C4	push 0	
004014C5	push 0	
004014C6	push 0	
004014C7	push 0	
004014C8	push 0	
004014C9	push 0	
004014CA	push 0	
004014CB	push 0	
004014CC	push 0	
004014CD	push 0	
004014CE	push 0	
004014CF	push 0	
004014D0	push 0	
004014D1	push 0	
004014D2	push 0	
004014D3	push 0	
004014D4	push 0	
004014D5	push 0	
004014D6	push 0	
004014D7	push 0	
004014D8	push 0	
004014D9	push 0	
004014DA	push 0	
004014DB	push 0	
004014DC	push 0	
004014DD	push 0	
004014DE	push 0	
004014DF	push 0	
004014E0	push 0	
004014E1	push 0	
004014E2	push 0	
004014E3	push 0	
004014E4	push 0	
004014E5	push 0	
004014E6	push 0	
004014E7	push 0	
004014E8	push 0	
004014E9	push 0	
004014EA	push 0	
004014EB	push 0	
004014EC	push 0	
004014ED	push 0	
004014EE	push 0	



따라서 정답은 처음 엔트리 포인트인 00401360 + AD46DFS547이다