과목명	시큐어코딩
담당교수	우사무엘 교수님
학과	소프트웨어학과
학번	32153180
이름	이상민
제출일자	2020.05.29

1. 원래 코드

```
//Command 인젝션
@RequestMapping(value="/test/command_test.do", method = RequestMethod.POST)
@ResponseBody
public String testCommandInjection(HttpServletRequest request, HttpSession session){
   StringBuffer buffer=new StringBuffer();
   String data=request.getParameter("data");

   /*
   String[] allowCommand= {"type", "dir"};

   int index=TestUtil.getInt(data);

   if( index<0 || index>1 ) {
      buffer.append("잘못된 요청입니다.");
      return buffer.toString();
   }
   else {
      data=allowCommand[index];
   }
   */

   if ( data != null  && data.equals("type")) {
         data=data+" "+
               request.getSession().getServletContext().getRealPath("/")+
               "file1.txt";
         System.out.println(data);
   }
```

Command 인젝션

작업선택 : --- show File1.txt --- 실행

실행결과

data=type

Command 인젝션

작업선택 : --- show File1.txt --- 실행

실행결과

실행결과:
Hello Kim !! http://openeg.co.kr

Command 인젝션

작업선택 : --- show Dir --- 실행

실행결과

data=dir

Command 인젝션

작업선택 : --- show Dir --- 실행

실행결과

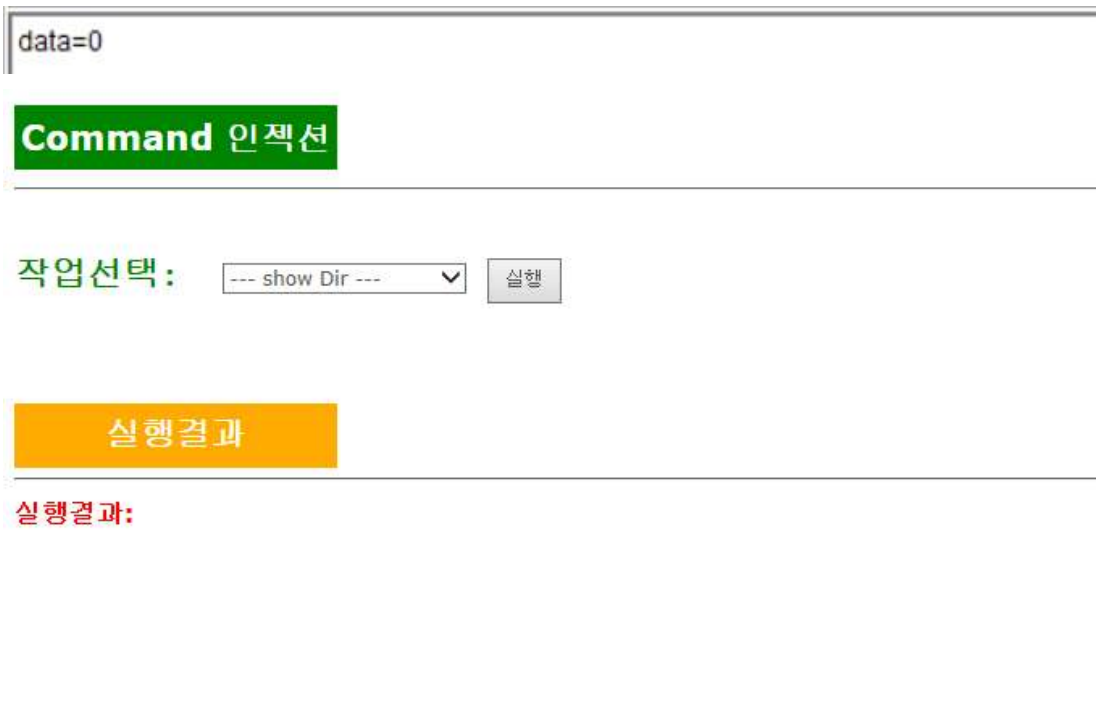
실행결과:
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: 5AB3-03A7

C:\Windows\system32 디렉터리

2020-05-25 오후 03:31

.
2020-05-25 오후 03:31

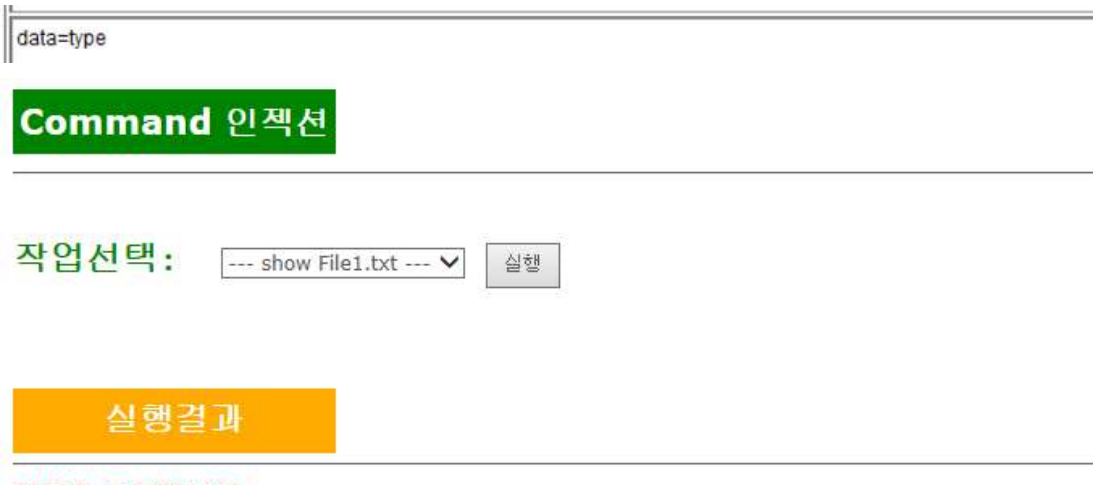

data=notepad
Command 인젝션
작업선택 :
--- show Dir ---
실행결과
제목 없음 - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)


data=0
Command 인젝션
작업선택 :
--- show Dir ---
실행
실행결과
실행결과:

2. 수정한 코드

```
//Command 인젝션
@RequestMapping(value="/test/command_test.do", method = RequestMethod.POST)
@ResponseBody
public String testCommandInjection(HttpServletRequest request, HttpSession session){
   StringBuffer buffer=new StringBuffer();
   String data=request.getParameter("data");


   String[] allowCommand= {"type", "dir"};

   int index=TestUtil.getInt(data);

   if( index<0 || index>1 ) {
      buffer.append("잘못된 요청입니다.");
      return buffer.toString();
   }
   else {
      data=allowCommand[index];
   }


   if ( data != null  && data.equals("type")) {
         data=data+" "+
               request.getSession().getServletContext().getRealPath("/")+
               "file1.txt";
         System.out.println(data);
   }
```


Command 인젝션
작업선택 :
--- show File1.txt ---
실행
실행결과


data=type
Command 인젝션
작업선택 :
--- show File1.txt ---
실행
실행결과
잘못된 요청입니다.


Command 인젝션
작업선택 :
--- show Dir ---
실행
실행결과
data=dir
Command 인젝션
작업선택 :
--- show File1.txt ---
실행
실행결과
잘못된 요청입니다.

data=notepad

Command 인젝션

작업선택 : --- show Dir --- 실행

실행결과

잘못된 요청입니다.

data=0

Command 인젝션

작업선택 : --- show Dir --- 실행

실행결과

실행결과:
Hello Kim !! http://openeg.co.kr