# REPORT

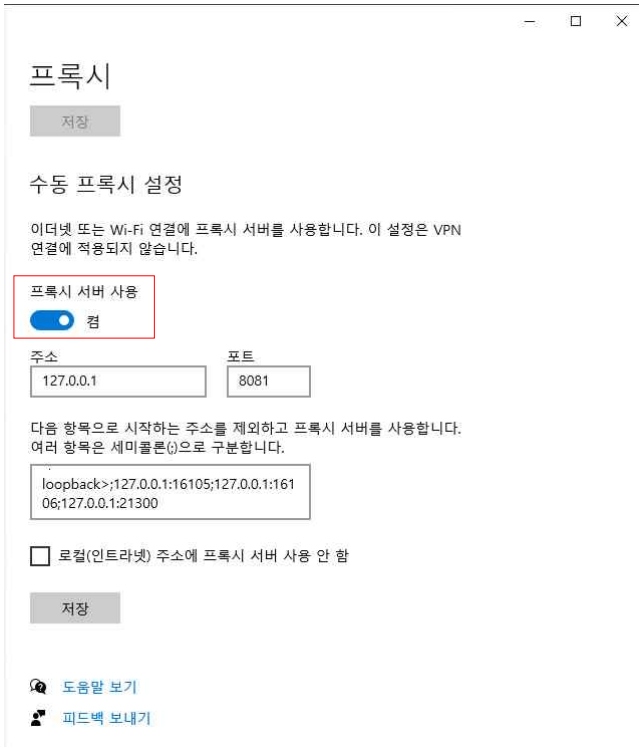

## 제 목 : 12주차 실습 보고서

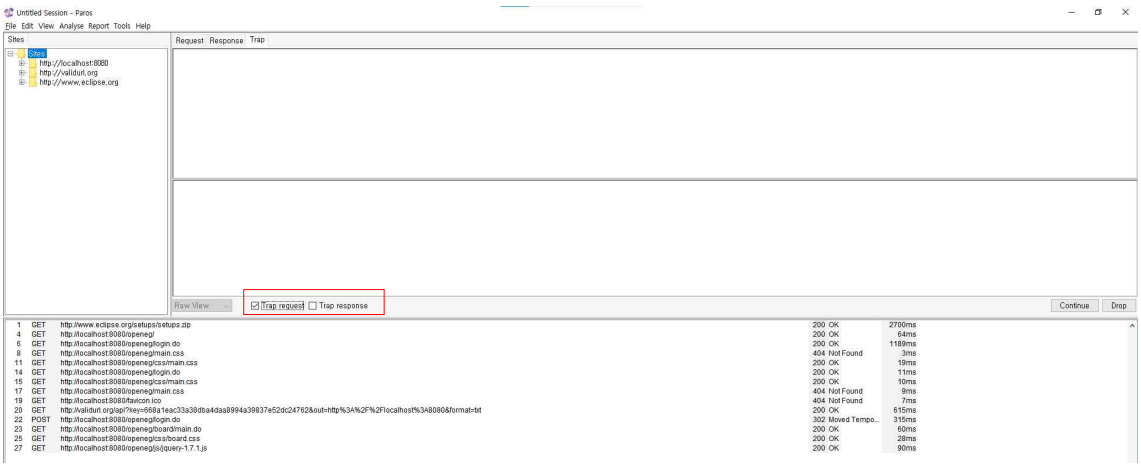
과 목 명 : 시큐어코딩
담당교수 : 우사무엘 교수님
이 름 : 조 정 민
학 번 : 32164420

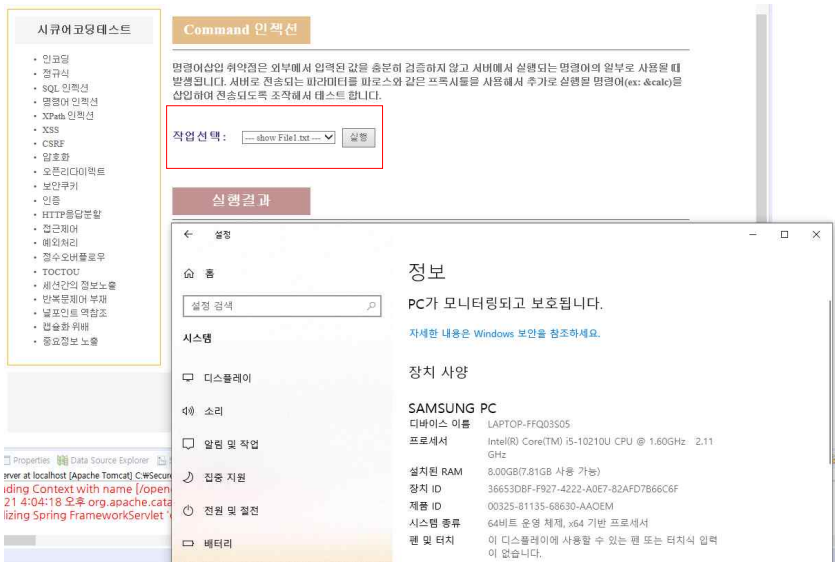
단국대학교
Dankook University

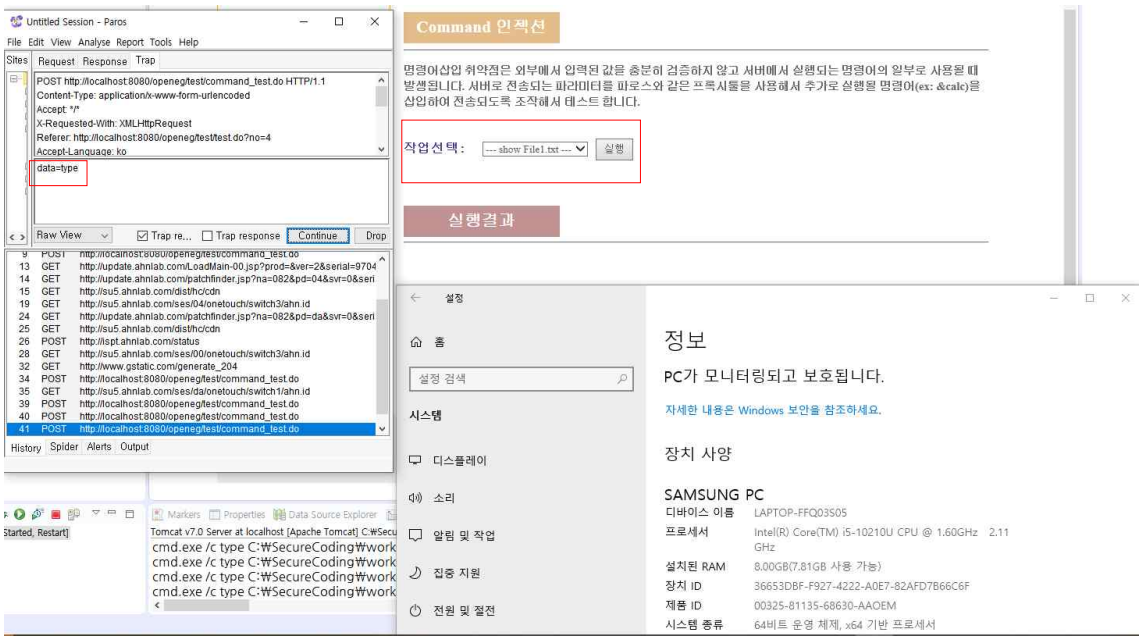
# [운영체제 명령어 삽입 공격 및 방어 실습]

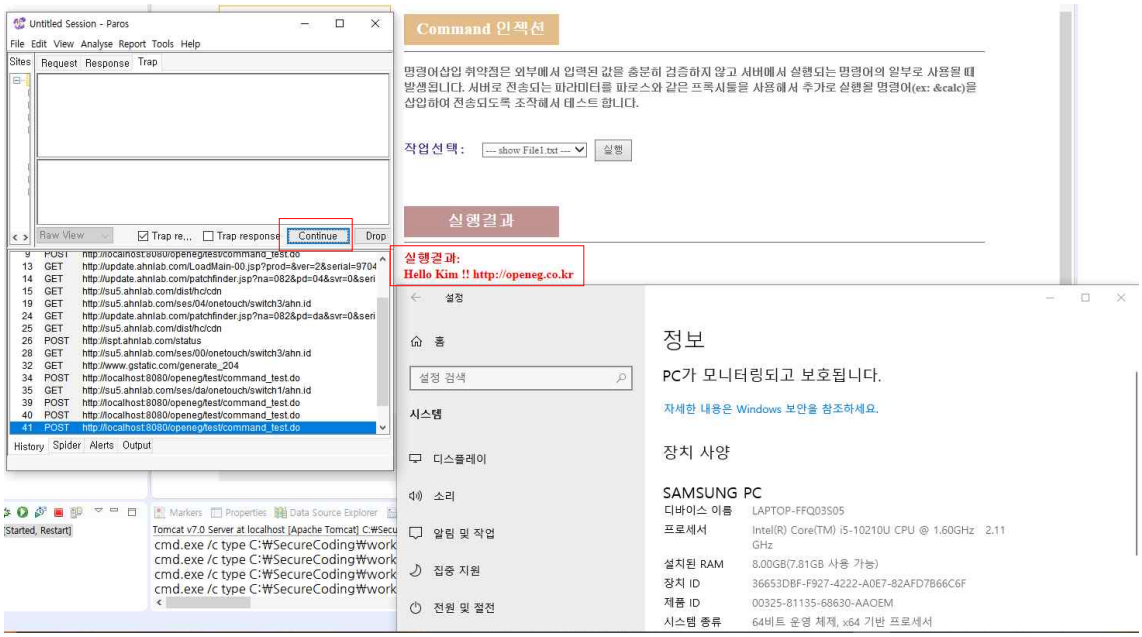
## - 공격

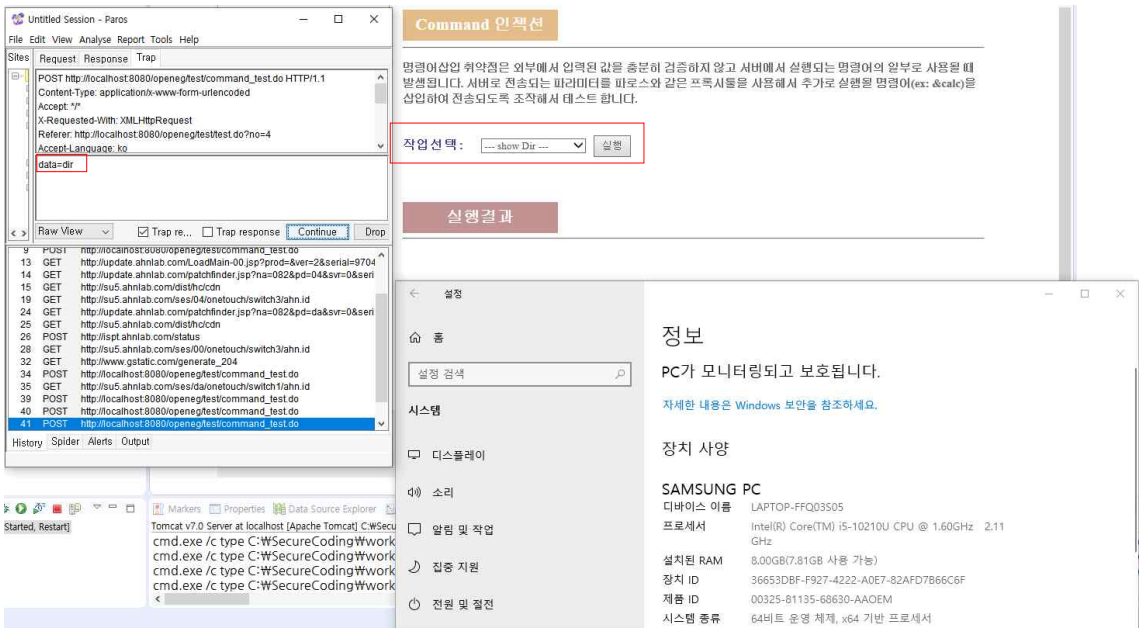


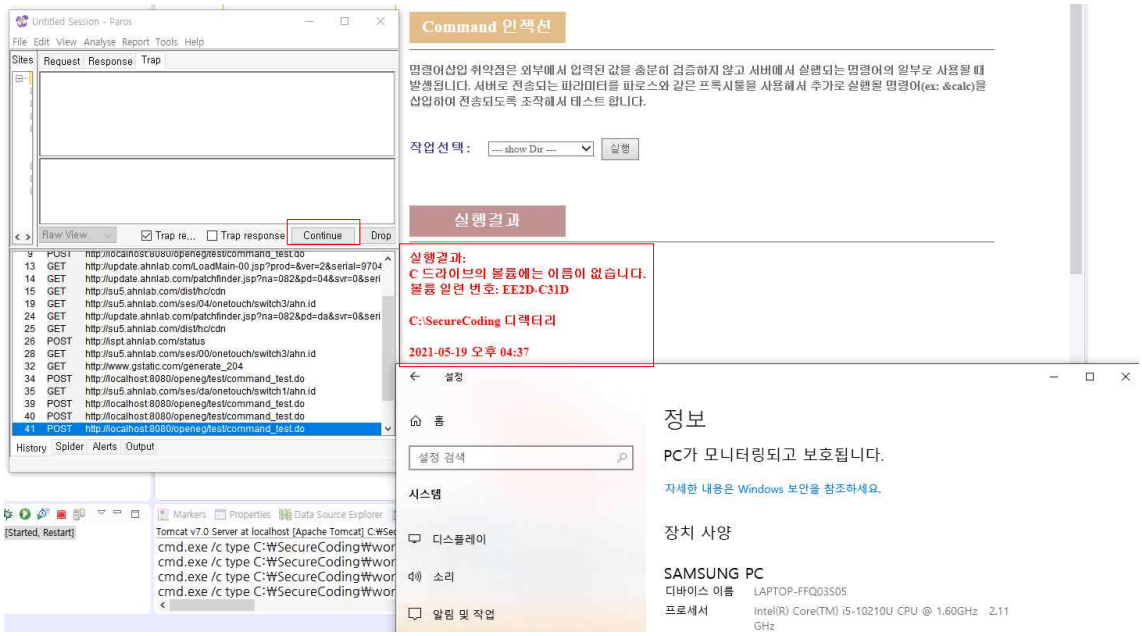




시큐어코딩테스트
• 인코딩
• 정규식
• SQL 인젝션
• 명령어 인젝션
• XPath 인젝션
• XSS
• CSRF
• 암호화
• 오픈리다이렉트
• 보안쿠키
• 인증
• HTTP응답분할
• 접근제어
• 예외처리
• 정수오버플로우
• TOCTOU
• 세션간의 정보노출
• 반복문제어 부재
• 널포인터 역참조
• 캡슐화 위배
• 중요정보 노출
Command 인젝션
명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생됩니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시툴을 사용해서 추가로 실행될 명령어(ex: &calc)을 삽입하여 전송되도록 조작해서 테스트 합니다.
작업선택 : --- show File1.txt --- 실행
실행결과
설정
홈
설정 검색
시스템
디스플레이
소리
알림 및 작업
집중 지원
전원 및 절전
배터리
정보
PC가 모니터링되고 보호됩니다.
자세한 내용은 Windows 보안을 참조하세요.
장치 사양
SAMSUNG PC
디바이스 이름 LAPTOP-FFQ03S05
프로세서 Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz
설치된 RAM 8.00GB(7.81GB 사용 가능)
장치 ID 36653DBF-F927-4222-A0E7-82AFD7B66C6F
제품 ID 00325-81135-68630-AAOEM
시스템 종류 64비트 운영 체제, x64 기반 프로세서
펜 및 터치 이 디스플레이에 사용할 수 있는 펜 또는 터치식 입력이 없습니다.

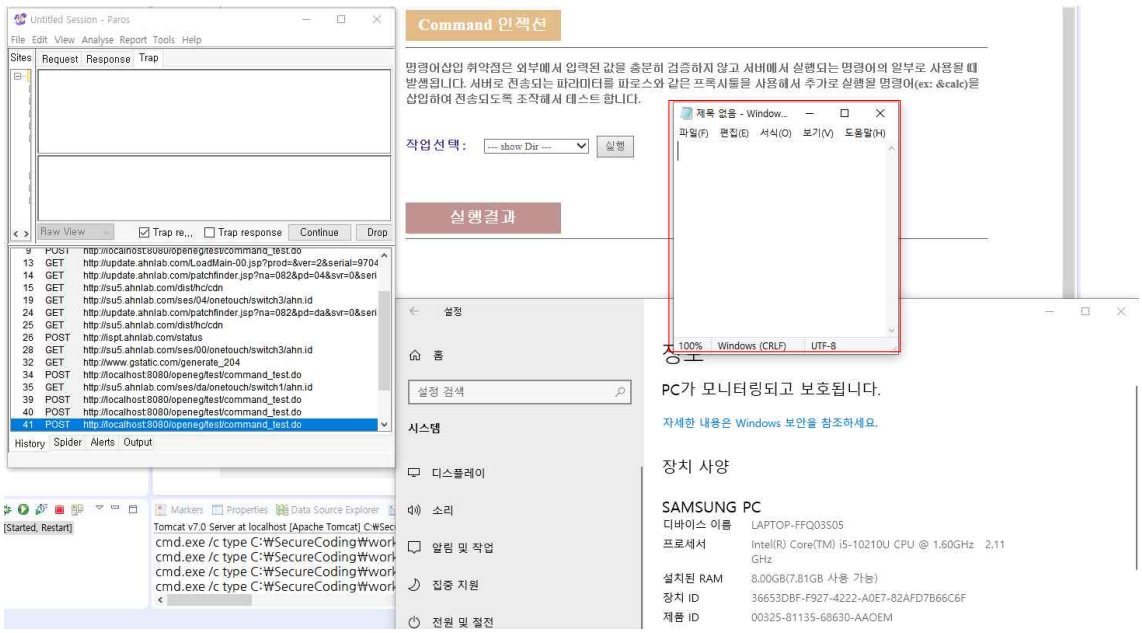

Untitled Session - Paros
File Edit View Analyse Report Tools Help
Sites
Request Response Trap
POST http://localhost:8080/openeg/test/command_test.do HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
X-Requested-With: XMLHttpRequest
Referer: http://localhost:8080/openeg/test/test.do?no=4
Accept-Language: ko
data=type
Raw View
Trap re...
Trap response
Continue
Drop
History Spider Alerts Output
Command 인젝션
명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생됩니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시툴을 사용해서 추가로 실행될 명령어(ex: &calc)을 삽입하여 전송되도록 조작해서 테스트 합니다.
작업선택 : --- show File1.txt --- 실행
실행결과
설정
홈
설정 검색
시스템
디스플레이
소리
알림 및 작업
집중 지원
전원 및 절전
정보
PC가 모니터링되고 보호됩니다.
자세한 내용은 Windows 보안을 참조하세요.
장치 사양
SAMSUNG PC
디바이스 이름 LAPTOP-FFQ03S05
프로세서 Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz
설치된 RAM 8.00GB(7.81GB 사용 가능)
장치 ID 36653DBF-F927-4222-A0E7-82AFD7B66C6F
제품 ID 00325-81135-68630-AAOEM
시스템 종류 64비트 운영 체제, x64 기반 프로세서


Untitled Session - Paros
File Edit View Analyse Report Tools Help
Sites
Request Response Trap
Raw View
Trap re...
Trap response
Continue
Drop
History Spider Alerts Output
Command 인젝션
명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생됩니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)을 삽입하여 전송되도록 조작해서 테스트 합니다.
작업선택 :
--- show File1.txt ---
실행
실행결과
실행결과:
Hello Kim !! http://openeg.co.kr
Markers Properties Data Source Explorer
Started, Restart]
Tomcat v7.0 Server at localhost [Apache Tomcat] C:₩Secu
cmd.exe /c type C:₩SecureCoding₩work
cmd.exe /c type C:₩SecureCoding₩work
cmd.exe /c type C:₩SecureCoding₩work
cmd.exe /c type C:₩SecureCoding₩work
설정
홈
설정 검색
시스템
디스플레이
소리
알림 및 작업
집중 지원
전원 및 절전
정보
PC가 모니터링되고 보호됩니다.
자세한 내용은 Windows 보안을 참조하세요.
장치 사양
SAMSUNG PC
디바이스 이름 LAPTOP-FFQ03S05
프로세서 Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz
설치된 RAM 8.00GB(7.81GB 사용 가능)
장치 ID 36653DBF-F927-4222-A0E7-82AFD7B66C6F
제품 ID 00325-81135-68630-AAOEM
시스템 종류 64비트 운영 체제, x64 기반 프로세서


Untitled Session - Paros
File Edit View Analyse Report Tools Help
Sites
Request Response Trap
POST http://localhost:8080/openeg/test/command_test.do HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
X-Requested-With: XMLHttpRequest
Referer: http://localhost:8080/openeg/test/test.do?no=4
Accept-Language: ko
data=dir
Raw View
Trap re...
Trap response
Continue
Drop
History Spider Alerts Output
Command 인젝션
명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생됩니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)을 삽입하여 전송되도록 조작해서 테스트 합니다.
작업선택 :
--- show Dir ---
실행
실행결과
Markers Properties Data Source Explorer
Started, Restart]
Tomcat v7.0 Server at localhost [Apache Tomcat] C:₩Secu
cmd.exe /c type C:₩SecureCoding₩work
cmd.exe /c type C:₩SecureCoding₩work
cmd.exe /c type C:₩SecureCoding₩work
cmd.exe /c type C:₩SecureCoding₩work
설정
홈
설정 검색
시스템
디스플레이
소리
알림 및 작업
집중 지원
전원 및 절전
정보
PC가 모니터링되고 보호됩니다.
자세한 내용은 Windows 보안을 참조하세요.
장치 사양
SAMSUNG PC
디바이스 이름 LAPTOP-FFQ03S05
프로세서 Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz
설치된 RAM 8.00GB(7.81GB 사용 가능)
장치 ID 36653DBF-F927-4222-A0E7-82AFD7B66C6F
제품 ID 00325-81135-68630-AAOEM
시스템 종류 64비트 운영 체제, x64 기반 프로세서



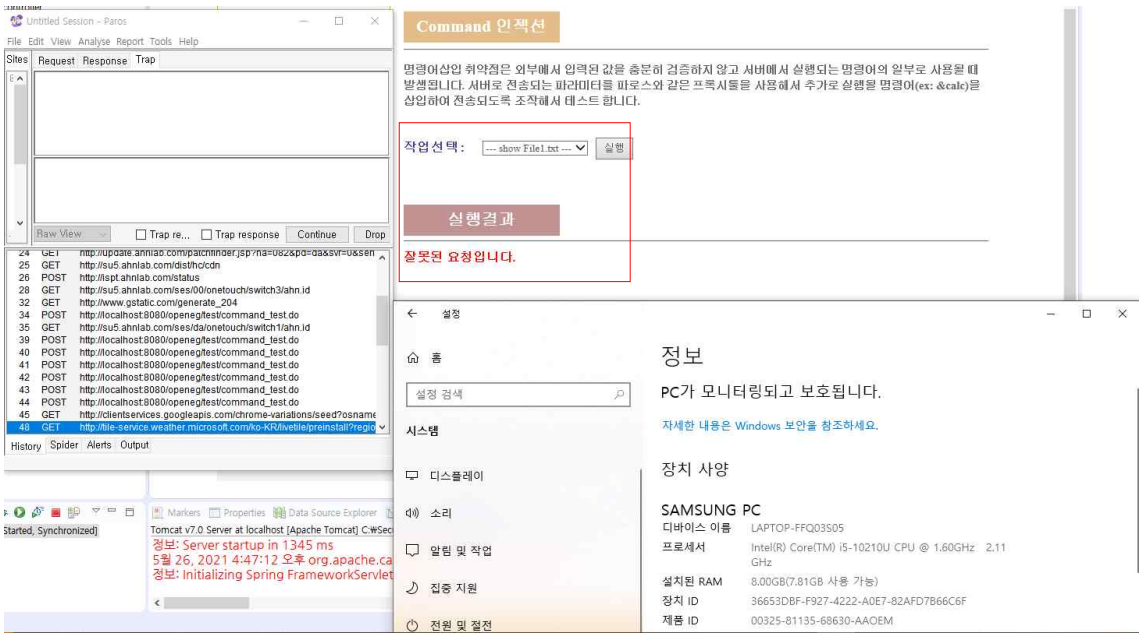

## data에 notepad를 넘겼을 때,



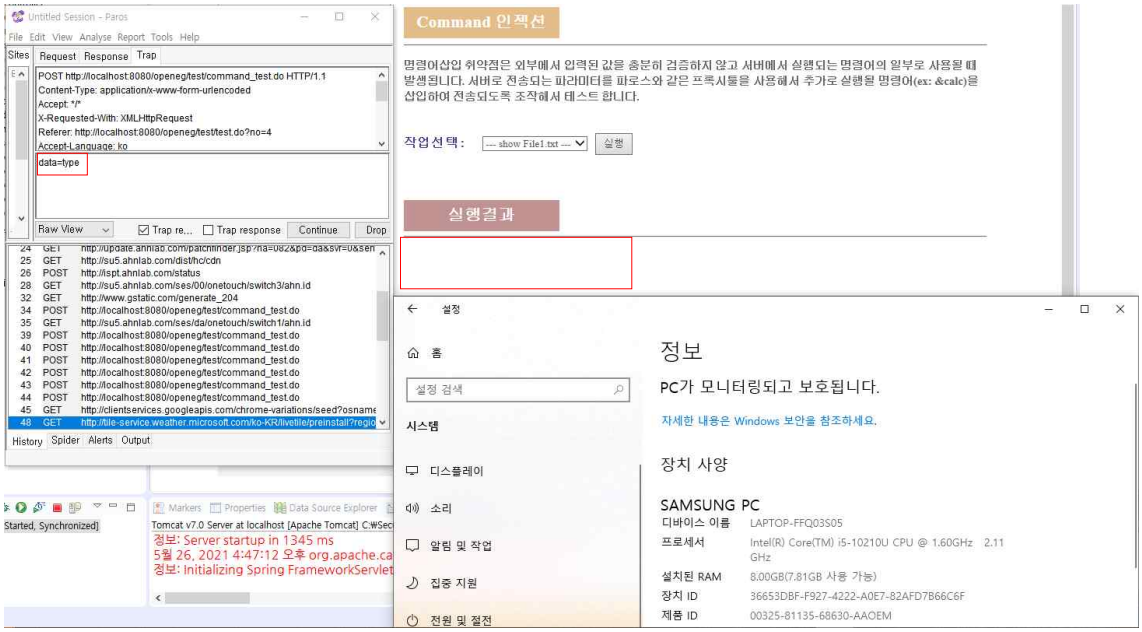
- 방어

<openeg-Java Resources-src-kr.co.openeg.lab.test.controller-TestController.java>
추가 코드

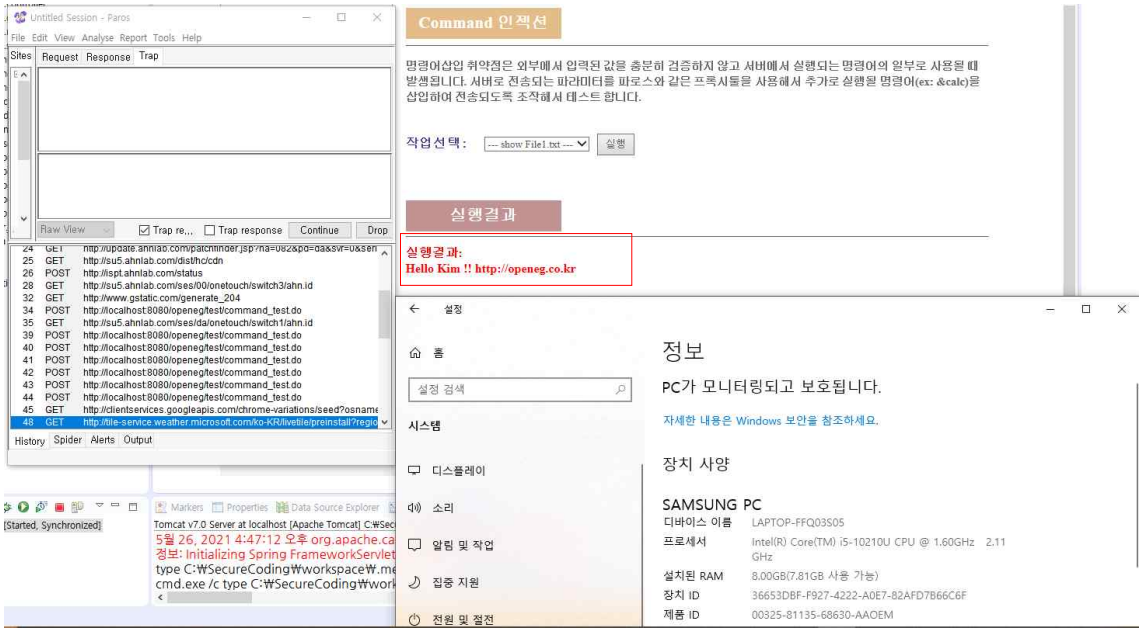
```
String[] allowCommand = {"type", "dir"};
int index = TestUtil.getInt(data);
if(index < 0 || index > 1) {
   buffer.append("잘못된 요청입니다.");
   return buffer.toString();
}
else {
   data = allowCommand[index];
}
```



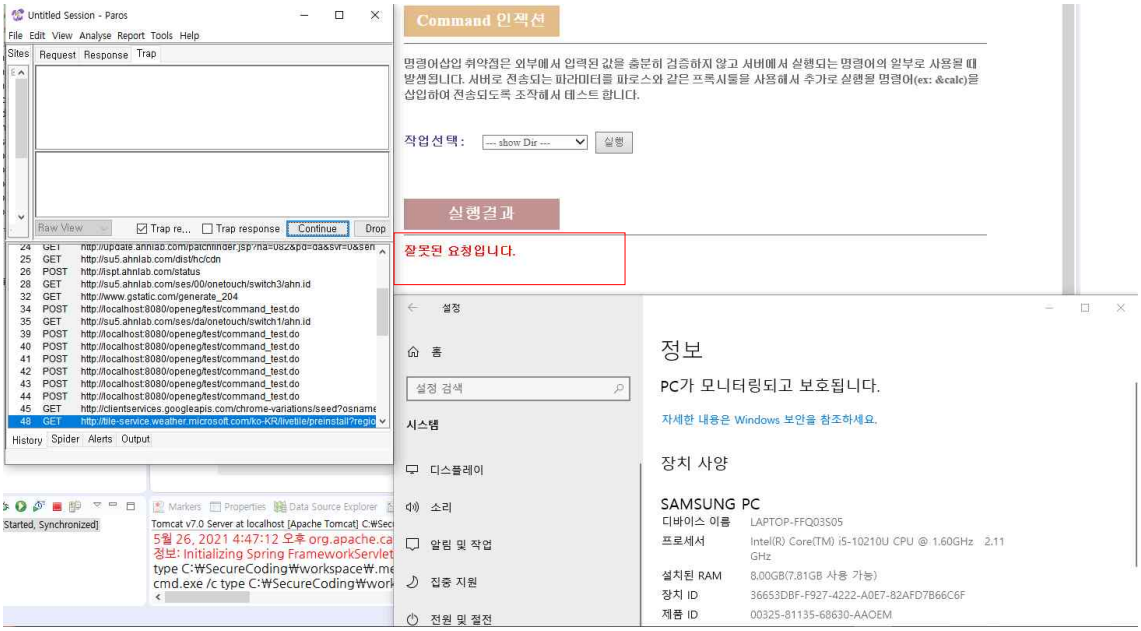
## 데이터가 스트링인 경우(type)



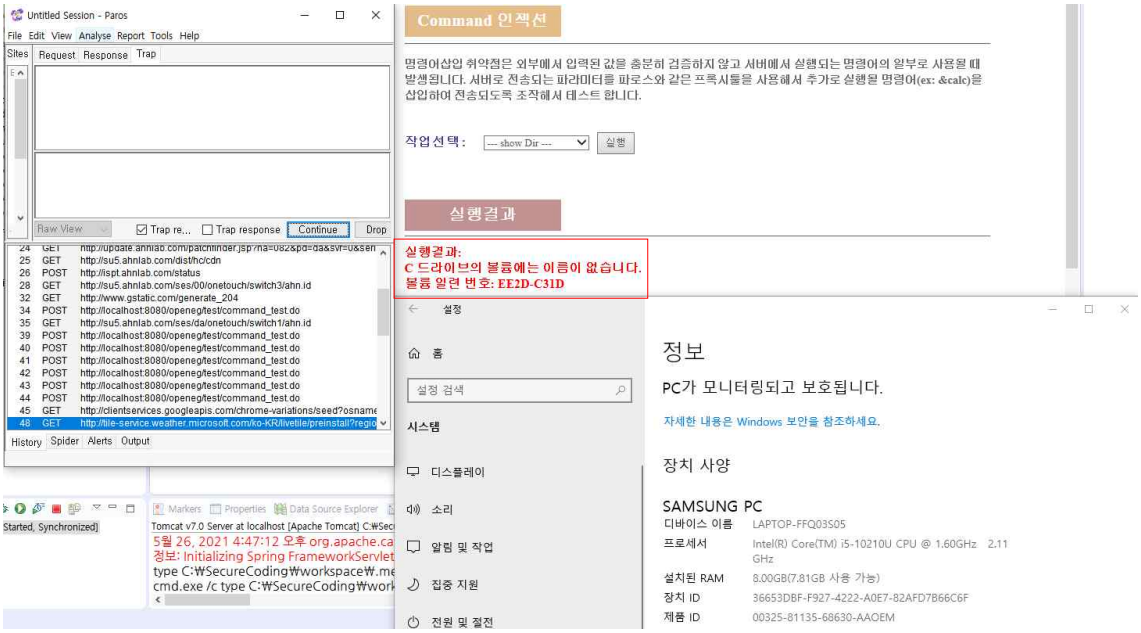

## 데이터가 인트형인 경우(0)



## 데이터가 스트링인 경우 (dir)




## 데이터가 인트형인 경우 (1)

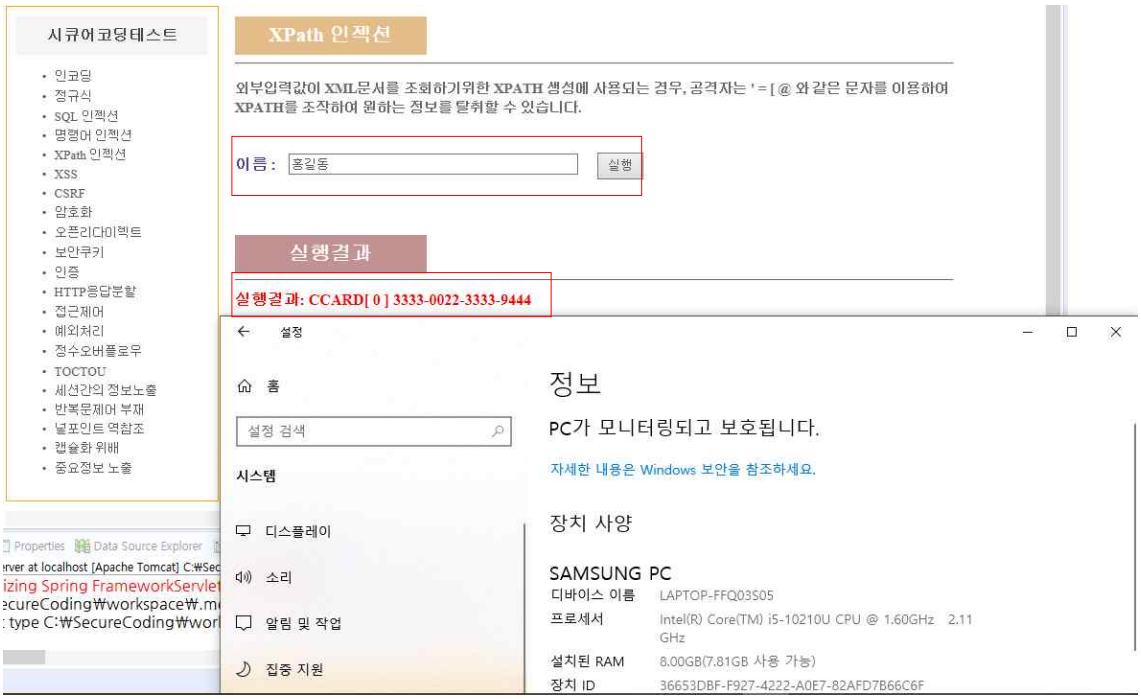


## [Xpath 삽입 공격 및 방어 실습]

Xpath(XML Path Language): XML 문서에 저장된 데이터를 애플리케이션에서 검색하거나 일기 위해 사용하는 표현 방식

Xpath 삽입 취약점 발생 원인: 사용자 입력을 받은, 입력 값에 대한 검증 없이, 동적으로 XPath 쿼리를 생성하면 공격자가 해당 쿼리 문의 의미를 수정할 수 있음

- **공격**

## 분석 작업





## 분석작업 – 항상 참인 결과 (‘ or “=’)


**위 입력 값과 같은 입력이 들어왔을 때의 검증, 필터링 작업이 없음이 확인 됨**

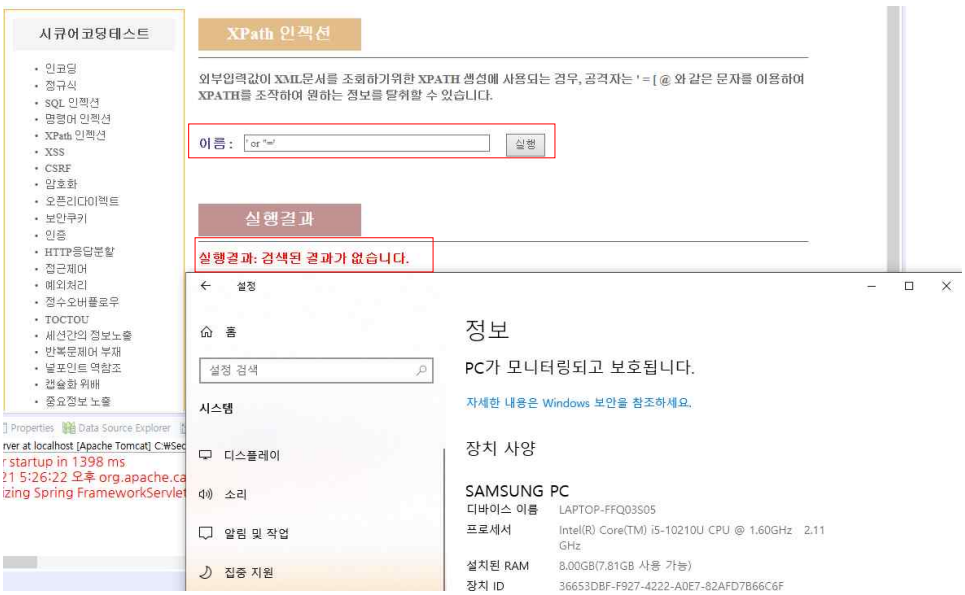
- **방어**

**추가/수정 코드**

**<openeg-Java Resources-src-kr.co.openeg.lab.test.util-TestUtil.java>**

```
public String XPathFilter(String input) {
    return input.replaceAll("['₩₩[]", "");
}
```

```
System.out.println("ccard 출력");
//String expression = "/addresses/address[@name='"+name+"']/ccard";
String expression = "/addresses/address[@name='"+XPathFilter(name)+"']/ccard";
```


이전에 항상 참인 결과를 불러오는 **문자열(' or "=')**이 방어됨을 확인

## [XSS 공격 및 방어 실습]

XXS 취약점: 외부 입력 값이 충분한 검증 없이 동적으로 생성되는 응답 페이지에 사용되는 경우

Reflective XSS : 공격자가 악성 스크림트가 포함된 URL을 클라이언트에 노출
 -> 클릭 유도, 악성 행위 수행

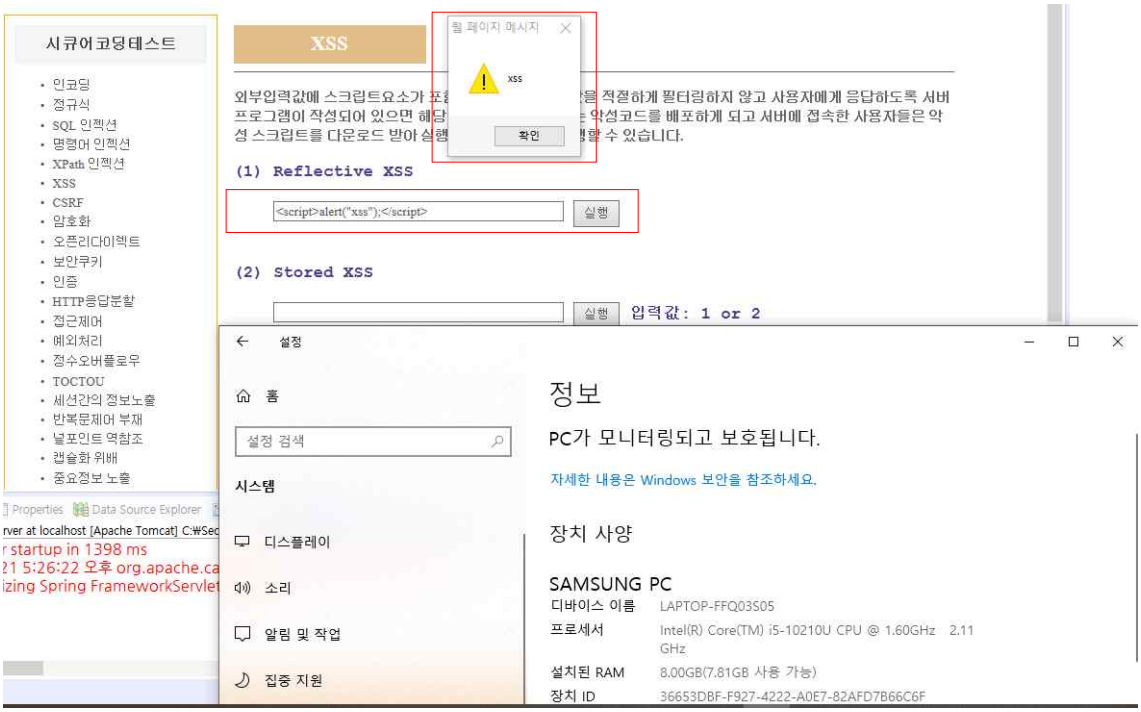
Stored XSS : 악성 스크립트를 데이터베이스에 저장
 -> 모든 사용자들이 해당 스크립트를 실행, 악성 행위 수행

XSS 취약점의 발생 원인 : 사용자의 입력값과 데이터베이스를 검색한 결과값을 검증하지 않고 응답의 일부로 사용하기 때문

### - 공격

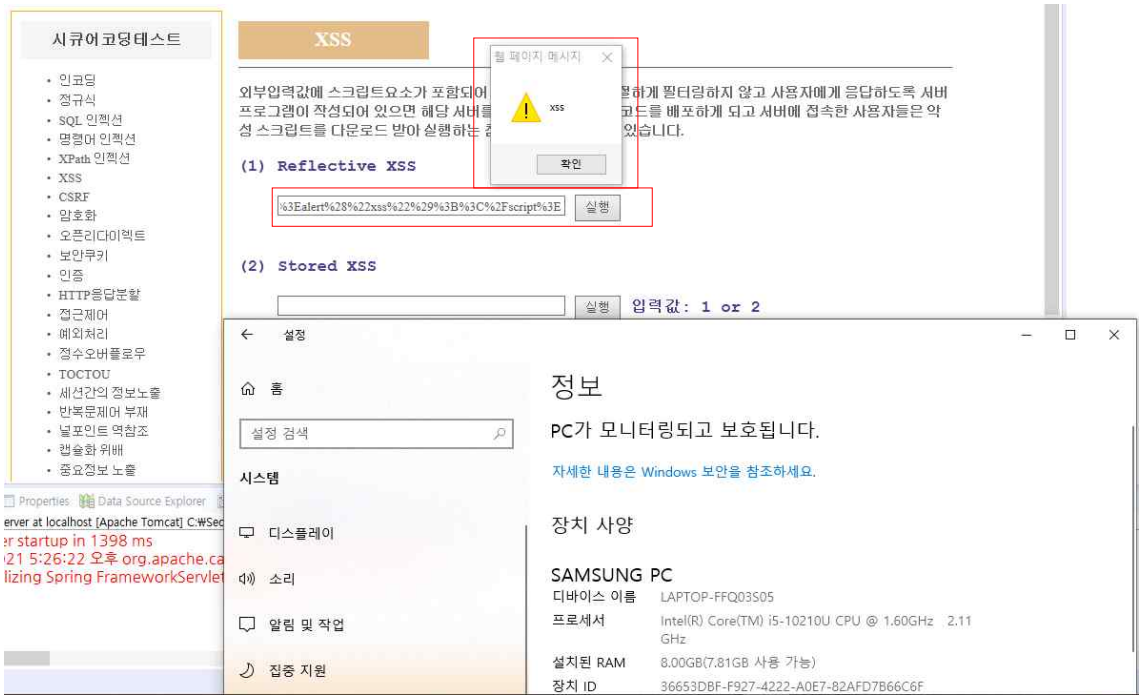
**경고창을 띄울 수 있는 스크립트 입력 값으로 사용하기**

**input : <script>alert("xss");</script>**



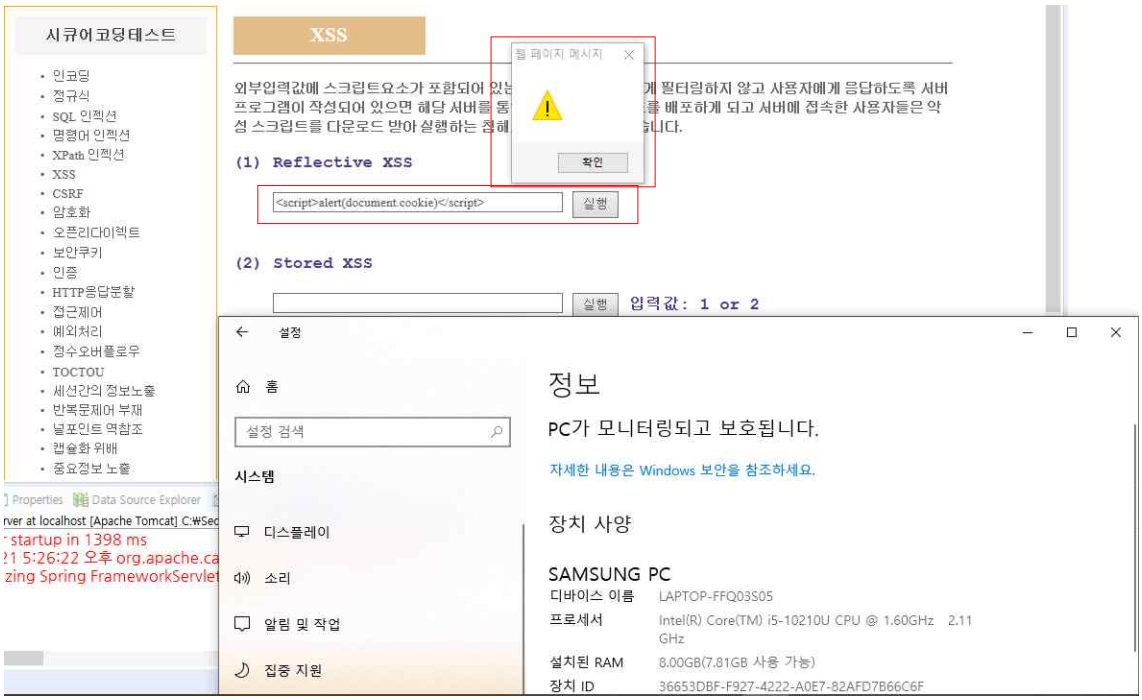
**URL 인코딩 값 이용하여 경고창 띄우기**

**input : %3Cscript%3Ealert%28%22xss%22%29%3B%3C%2Fscript%3E**




**경고창 팝업 이용하여 쿠키 값 확인하기 – http only 속성 미해제**

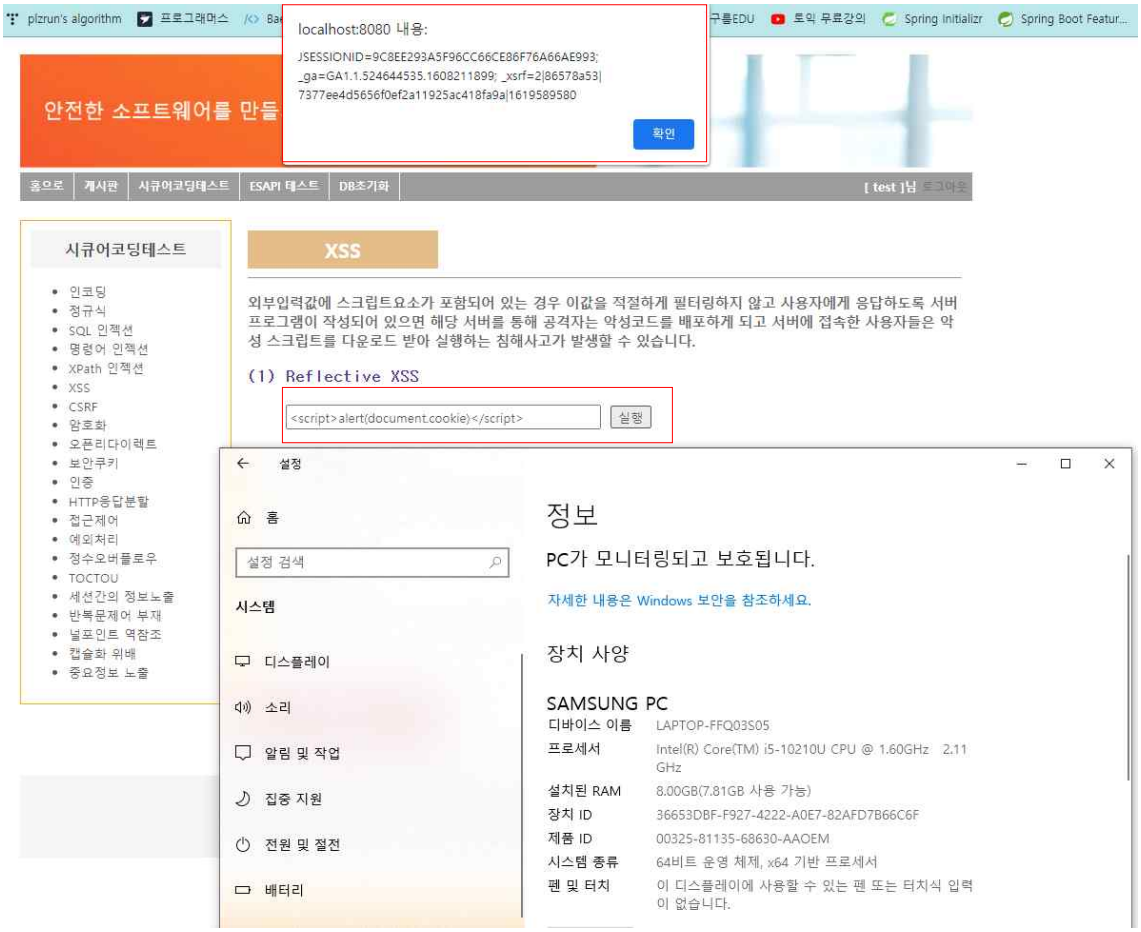
**input : <script>alert(document.cookie)</script>**




공격 실패가 아닌, 보안 옵션이 클라이언트 PC에 설정되어 있는 것

**경고창 팝업 이용하여 쿠키 값 확인하기 – http only 속성 해제**

**input : <script>alert(document.cookie)</script>**



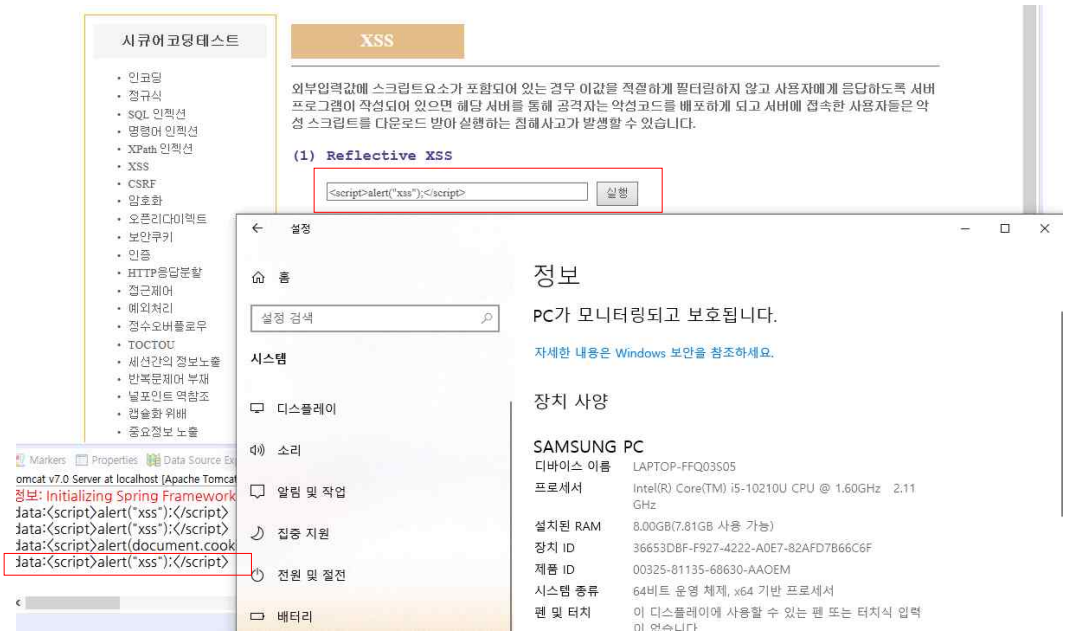
- 방어

**<openeg-Java Resources-src-kr.co.openeg.lab.test.controller-TestController.java>**

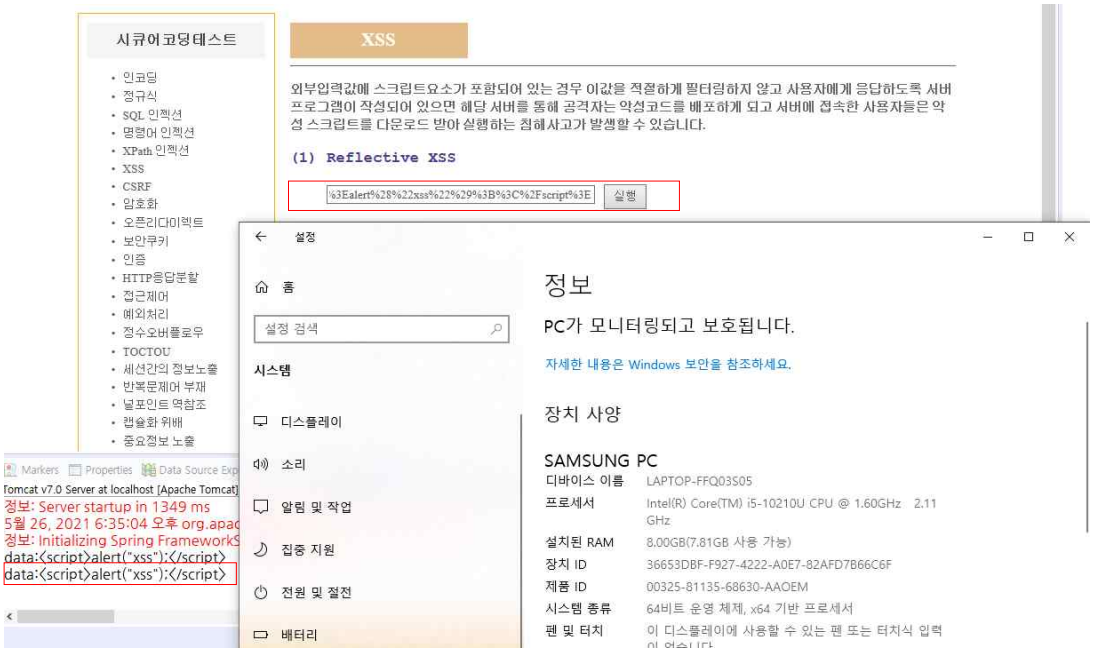
```
22 import kr.co.openeg.lab.member.model.MemberModel;
23 import kr.co.openeg.lab.member.service.MemberService;
24 import kr.co.openeg.lab.test.util.Customer;
25 import kr.co.openeg.lab.test.util.CustomerService;
26 import kr.co.openeg.lab.test.util.DBinit;
27 import kr.co.openeg.lab.test.util.Role;
28 import kr.co.openeg.lab.test.util.TestUtil;
29 import com.nhncorp.lucy.security.xss.XssFilter;
```

```
// Reflective XSS 테스트
@RequestMapping(value="/test/xss_test.do", method = RequestMethod.POST)
@ResponseBody
public String testXss(HttpServletRequest request) {
   StringBuffer buffer=new StringBuffer();
   String data=request.getParameter("data");
   try
   {
      data = URLDecoder.decode(data, "UTF-8");
      System.out.println("data:" +data);
   }
   catch(IOException e)
   {
      System.out.println(e);
   }

   XssFilter filter = XssFilter.getInstance("lucy-xss-superset.xml");
   buffer.append(filter.doFilter(data));
   return buffer.toString();

   //buffer.append(data);
   //return buffer.toString();
}
```

**input : <script>alert("xss");</script>**



**input : %3Cscript%3Ealert%28%22xss%22%29%3B%3C%2Fscript%3E**




**input : <script>alert(document.cookie)</script>**