

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

프록시

저장

수동 프록시 설정

인터넷 또는 Wi-Fi 연결에 프록시 서버를 사용합니다. 이 설정은 VPN 연결에 적용되지 않습니다.

프록시 서버 사용

켄

주소

127.0.0.1

포트

8081

다음 항목으로 시작하는 주소를 제외하고 프록시 서버를 사용합니다.
여러 항목은 세미콜론(;)으로 구분합니다.

loopback>;127.0.0.1:16105;127.0.0.1:16106;127.0.0.1:21300

☐ 로컬(인트라넷) 주소에 프록시 서버 사용 안 함

저장

[도움말 보기](#)

[피드백 보내기](#)

Untitled Session - Fiddler

File Edit View Analyse Report Tools Help

Sites

Request Response Trap

Raw View

☒ Trap request ☐ Trap response

Continue Stop

1	GET	http://www.eclipse.org/setup/setup.jsp	200	OK	2700ms
4	GET	http://localhost:8080/openegf	200	OK	64ms
6	GET	http://localhost:8080/openegfmain.do	200	OK	1189ms
8	GET	http://localhost:8080/openegfmain.css	404	Not Found	3ms
11	GET	http://localhost:8080/openegfmain.js	200	OK	19ms
14	GET	http://localhost:8080/openegfmain.do	200	OK	11ms
15	GET	http://localhost:8080/openegfmain.css	200	OK	10ms
17	GET	http://localhost:8080/openegfmain.css	404	Not Found	9ms
19	GET	http://localhost:8080/openegfmain.js	404	Not Found	7ms
20	GET	http://localhost:8080/openegfmain.js	200	OK	615ms
22	POST	http://localhost:8080/openegfmain.do	302	Moved Temporarily	310ms
23	GET	http://localhost:8080/openegfmain.do	200	OK	60ms
25	GET	http://localhost:8080/openegfmain.css	200	OK	28ms
27	GET	http://localhost:8080/openegfmain.js	200	OK	90ms

시큐어코딩 테스트

- 인코딩
- 접근성
- SQL 인젝션
- 명령어 인젝션
- XPath 인젝션
- XSS
- CSRF
- 암호화
- 오픈리다이렉트
- 보안쿠키
- 인증
- HTTP 응답본합
- 접근 제어
- 데이터 처리
- 결수오버플로우
- TOCTOU
- 세션의 정보 노출
- 반복문 제어 부패
- 널포인트 역침조
- 범용화 위해
- 중요정보 노출

Command 인젝션

명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생합니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)를 삽입하여 전송되도록 조작해서 테스트 합니다.

작업 선택 :

--- show File1.txt ---

 실행

실행 결과

설정

홈

설정 검색

시스템

디스플레이

4K 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-AADEM

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/openegtestcommand_test.do HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Accept: */*

X-Requested-With: XMLHttpRequest

Referer: http://localhost:8080/openegtest.do?no=4

Accept-Language: ko

data=type

Raw View

Trap response

Continue Drop

9 POST http://localhost:8080/openegtestcommand_test.do

13 GET http://update.ahnlab.com/loadMain-00.jsp?prod=&ver=2&serial=9704

14 GET http://update.ahnlab.com/patchfinder.jsp?na=082&pd=04&svr=0&ser

15 GET http://su5.ahnlab.com/dlsth/cdn

19 GET http://su5.ahnlab.com/ses/04lonetouch/switch3/ahn.id

24 GET http://update.ahnlab.com/patchfinder.jsp?na=082&pd=da&svr=0&ser

25 GET http://su5.ahnlab.com/dlsth/cdn

26 POST http://spt.ahnlab.com/status

28 GET http://su5.ahnlab.com/ses/00lonetouch/switch3/ahn.id

32 GET http://www.gstatic.com/generate_204

34 POST http://localhost:8080/openegtestcommand_test.do

35 GET http://su5.ahnlab.com/ses/da/lonetouch/switch1/ahn.id

39 POST http://localhost:8080/openegtestcommand_test.do

40 POST http://localhost:8080/openegtestcommand_test.do

History Spider Alerts Output

Started Restart

Tomcat v7.0 Server at localhost [Apache Tomcat] C:\SecureCoding\work

cmd.exe /c type C:\SecureCoding\work

cmd.exe /c type C:\SecureCoding\work

cmd.exe /c type C:\SecureCoding\work

Command 인젝션

명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생합니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)를 삽입하여 전송되도록 조작해서 테스트 합니다.

작업 선택 :

--- show File1.txt ---

 실행

실행 결과

설정

홈

설정 검색

시스템

디스플레이

4K 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-AADEM

시스템 종류 64비트 운영 체제, x64 기반 프로세서

Untitled Session - Paros

File Edit View Analyse Report Tools Help

Sites Request Response Trap

Raw View

Continue

POST http://localhost:8080/openegtest/command_test.do

History Spider Alerts Output

Started, Restart

Tomcat v7.0 Server at localhost [Apache Tomcat] C:\SecureCoding\work cmd.exe /c type C:\SecureCoding\work cmd.exe /c type C:\SecureCoding\work cmd.exe /c type C:\SecureCoding\work

Command 입력선

명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생합니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)를 삽입하여 전송되도록 조작해서 테스트 합니다.

작업선택: show File1.txt 실행

실행결과

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

설정

종

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

Continue

POST http://localhost:8080/openegtest/command_test.do HTTP/1.1

History Spider Alerts Output

Started, Restart

Tomcat v7.0 Server at localhost [Apache Tomcat] C:\SecureCoding\work cmd.exe /c type C:\SecureCoding\work cmd.exe /c type C:\SecureCoding\work cmd.exe /c type C:\SecureCoding\work

Command 입력선

명령어삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생합니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)를 삽입하여 전송되도록 조작해서 테스트 합니다.

작업선택: show Dir 실행

실행결과

설정

종

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

- 방어

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

추가 코드

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

The screenshot displays a web security tool interface with a list of HTTP requests on the left and a command execution window on the right.

Command 안쪽선

명령어산인 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생합니다. 서버로 전송되는 파라미터를 파싱하고 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)를 삽입하여 전송되도록 조작해서 테스트 합니다.

작업선택: 실행

실행결과

잘못된 요청입니다.

설정

홈

설정 검색

시스템

디스플레이

소리

알림 및 작업

접속 지원

전원 및 절전

정보

PC가 모니터링되고 보호됩니다.

자세한 내용은 Windows 보안을 참조하세요.

장치 사양

SAMSUNG PC

디바이스 이름: LAPTOP-FFQ03505

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

History Spider Alerts Output

Started, Synchronized

Tomcat v7.0 Server at localhost [Apache Tomcat] C:\Sec

정보: Server startup in 1345 ms

5월 26, 2021 4:47:12 오후 org.apache.ca

정보: Initializing Spring FrameworkServlet

데이터가 스트링인 경우(type)

데이터가 인트형인 경우(0)

데이터가 스트링인 경우 (dir)

Untitled Session - Paros

File Edit View Analyse Report Tools Help

Sites Request Response Trap

Raw View

24 GET http://update.ahnlab.com/compat/minor.jsp?ma=us&sp=qa&sv=us&sen...
25 GET http://su5.ahnlab.com/dst/hcdn
26 POST http://spt.ahnlab.com/status
28 GET http://su5.ahnlab.com/sea/00onetouch/switch3/ahn.id
32 GET http://www.gstatic.com/generate_204
34 POST http://localhost:8080/openegfest/command_test.do
35 GET http://su5.ahnlab.com/sea/daonetouch/switch1/ahn.id
39 POST http://localhost:8080/openegfest/command_test.do
40 POST http://localhost:8080/openegfest/command_test.do
41 POST http://localhost:8080/openegfest/command_test.do
42 POST http://localhost:8080/openegfest/command_test.do
43 POST http://localhost:8080/openegfest/command_test.do
44 POST http://localhost:8080/openegfest/command_test.do
45 GET http://clientservices.googleapis.com/chrome-variations/seed?osname...
48 GET http://file-service.weather.microsoft.com/ko-KR/live/preinstall/resp...

History Spider Alerts Output

Started, Synchronized

Markers Properties Data Source Explorer

Tomcat v7.0 Server at localhost [Apache Tomcat] C:\Sec...
5월 26, 2021 4:47:12 오후 org.apache.c...
정보: Initializing Spring FrameworkServlet
type C:\WSecureCoding\workspace\W...
cmd.exe /c type C:\WSecureCoding\Wwor...

Command 인젝션

명령어 삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생합니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)를 삽입하여 전송되도록 조작해서 테스트 합니다.

작업선택: show Dir 실행

실행결과

잘못된 요청입니다.

정보

PC가 모니터링되고 보호됩니다.

자세한 내용은 Windows 보안을 참조하세요.

장치 사양

SAMSUNG PC

디바이스 이름 LAPTOP-FFQ03505

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

데이터가 인트형인 경우 (1)

Untitled Session - Paros

File Edit View Analyse Report Tools Help

Sites Request Response Trap

Raw View

24 GET http://update.ahnlab.com/compat/minor.jsp?ma=us&sp=qa&sv=us&sen...
25 GET http://su5.ahnlab.com/dst/hcdn
26 POST http://spt.ahnlab.com/status
28 GET http://su5.ahnlab.com/sea/00onetouch/switch3/ahn.id
32 GET http://www.gstatic.com/generate_204
34 POST http://localhost:8080/openegfest/command_test.do
35 GET http://su5.ahnlab.com/sea/daonetouch/switch1/ahn.id
39 POST http://localhost:8080/openegfest/command_test.do
40 POST http://localhost:8080/openegfest/command_test.do
41 POST http://localhost:8080/openegfest/command_test.do
42 POST http://localhost:8080/openegfest/command_test.do
43 POST http://localhost:8080/openegfest/command_test.do
44 POST http://localhost:8080/openegfest/command_test.do
45 GET http://clientservices.googleapis.com/chrome-variations/seed?osname...
48 GET http://file-service.weather.microsoft.com/ko-KR/live/preinstall/resp...

History Spider Alerts Output

Started, Synchronized

Markers Properties Data Source Explorer

Tomcat v7.0 Server at localhost [Apache Tomcat] C:\Sec...
5월 26, 2021 4:47:12 오후 org.apache.c...
정보: Initializing Spring FrameworkServlet
type C:\WSecureCoding\workspace\W...
cmd.exe /c type C:\WSecureCoding\Wwor...

Command 인젝션

명령어 삽입 취약점은 외부에서 입력된 값을 충분히 검증하지 않고 서버에서 실행되는 명령어의 일부로 사용될 때 발생합니다. 서버로 전송되는 파라미터를 파로스와 같은 프록시들을 사용해서 추가로 실행될 명령어(ex: &calc)를 삽입하여 전송되도록 조작해서 테스트 합니다.

작업선택: show Dir 실행

실행결과

실행결과:
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: EE2D-C31D

정보

PC가 모니터링되고 보호됩니다.

자세한 내용은 Windows 보안을 참조하세요.

장치 사양

SAMSUNG PC

디바이스 이름 LAPTOP-FFQ03505

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

[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

The image shows two screenshots of a web application security tool, likely Burp Suite, demonstrating an XPath injection attack. The left sidebar contains a list of vulnerabilities, including 'XPath injection'. The main area is titled 'XPath 인젝션' (XPath Injection) and contains a description of the attack: '외부입력값이 XML문서를 조회하기위한 XPATH 쿼리에 사용되는 경우, 공격자는 '[@ 와 같은 문자를 이용하여 XPATH를 조작하여 원하는 정보를 탈취할 수 있습니다.' (When an external input value is used in an XPATH query to retrieve XML documents, an attacker can steal desired information by manipulating the XPATH using characters like '[' and '@').

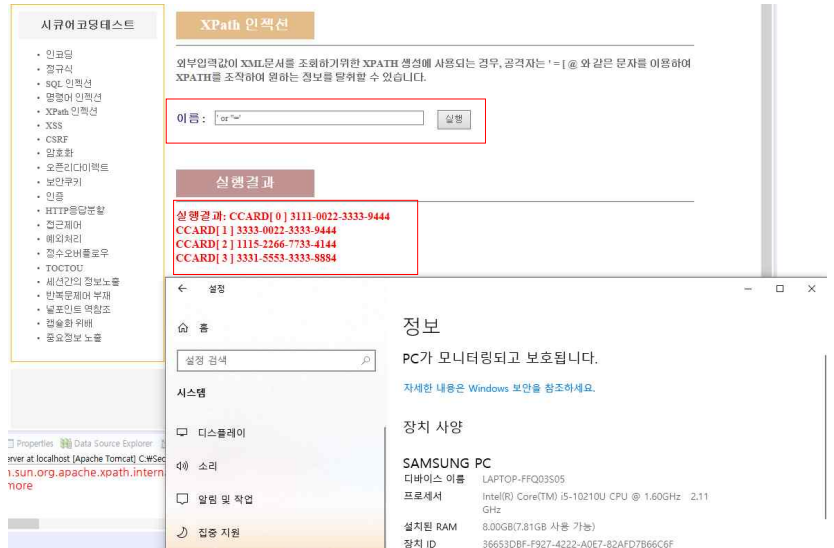
The first screenshot shows the '이름' (Name) field with an empty input and a '실행' (Execute) button. The second screenshot shows the '이름' field with the input '홍길동' (Hong Gildong) and the '실행' button. Below the '실행' button, the '실행결과' (Execution Result) is displayed, showing a list of phone numbers: 'CCARD[0] 3333-0022-3333-9444'.

The right sidebar displays system information for the target device, identified as a SAMSUNG PC. The information includes the device name (LAPTOP-FFQ03S05), processor (Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz), installed RAM (8.00GB), and various IDs (장치 ID, 제품 ID).

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";

The screenshot shows the OpenEG web application interface. On the left is a sidebar menu with various security testing categories. The main content area is titled 'XPath 인젝션' (XPath Injection). It contains a description of the attack and a form with a label '이름:' (Name:) and a text input field containing '홍길동' (Hong Gildong). Below the form, the '실행결과' (Execution Result) section displays '실행결과: CCARD[0] 3333-0022-3333-9444'. The bottom part of the screen shows a Windows taskbar and a system information window for a Samsung PC.

This screenshot shows the same OpenEG web application interface as the previous one, but with a different input. The '이름:' (Name:) input field now contains ' or '='. The '실행결과' (Execution Result) section displays '실행결과: 검색된 결과가 없습니다.' (Execution Result: No search results found). The rest of the interface, including the sidebar and system information window, remains the same.

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

[XSS 공격 및 방어 실습]

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

Reflective XSS : 공격자가 악성 스크립트가 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>`

The screenshot shows a web application interface for XSS testing. On the left, there's a sidebar with a list of security tests including '시큐어코딩테스트' (Secure Coding Test) and various attack types like '인코딩', '정규식', 'SQL 인젝션', etc. The main content area is titled 'XSS' and contains two sections: '(1) Reflective XSS' and '(2) Stored XSS'. In the 'Reflective XSS' section, there's an input field containing the payload `<script>alert("xss");</script>` and a '실행' (Execute) button. A yellow warning dialog box with a triangle icon and the text 'XSS' is overlaid on the page. At the bottom, a Windows taskbar is visible with a terminal window open, showing the command 'C:\Windows\system32\cmd.exe' and the output 'C:\Windows\system32\cmd.exe'.

URL 인코딩 값 이용하여 경고창 띄우기

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

The screenshot shows a web application security tool interface. On the left, a sidebar lists various attack types including '시큐어코딩테스트' (Security Coding Test) and '인코딩' (Encoding). The main panel is titled 'XSS' and contains sections for '(1) Reflective XSS' and '(2) Stored XSS'. A warning message box is overlaid on the 'Reflective XSS' section, displaying the alert message: 'alert(%28%22xss%22%29%3B%3C%2Fscript%3E)'. The system information window on the right shows details for a 'SAMSUNG PC' with a 'LAPTOP-FFQ03S05' device name, an 'Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz' processor, and '8.00GB(7.81GB 사용 가능)' RAM.

경고창 팝업 이용하여 쿠키 값 확인하기 - http only 속성 미해제

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

The screenshot shows the same web application security tool interface as the previous one. The sidebar and main panel are identical. However, the warning message box is not present, indicating that the alert function failed to execute. The system information window on the right remains the same, showing details for the 'SAMSUNG PC'.

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>`

The screenshot shows a web application interface. At the top, there's a navigation bar with links like 'plzrun's algorithm', '프로그래머스', and 'Spring Initializr'. Below this, a red box highlights the browser console output, which shows the alert message: 'localhost:8080 내용: JSESSIONID=9C8EE293A5F96CC66CE86F76A66AE993; _ga=GA1.1.524644535.1608211899; _xsr=2[86578a53] 7377ee4d5656f0ef2a11925ac418fa9a|1619589580'. Below the console output, there's a blue button labeled '확인'. The main content area has a title '안전한 소프트웨어를 만들' and a sidebar menu with various security topics like '인코딩', '정규식', 'SQL 인젝션', etc. The bottom part of the image shows a Windows Settings window with the '정보' (Information) tab selected, displaying system details for a Samsung PC.

localhost:8080 내용:

```
JSESSIONID=9C8EE293A5F96CC66CE86F76A66AE993;
_ga=GA1.1.524644535.1608211899; _xsr=2[86578a53]
7377ee4d5656f0ef2a11925ac418fa9a|1619589580
```

확인

안전한 소프트웨어를 만들

홈으로 | 게시판 | 시큐어코딩테스트 | ESAPI 테스트 | DB초기화

[test]님 로그인

시큐어코딩테스트

- 인코딩
- 정규식
- SQL 인젝션
- 명령어 인젝션
- XPath 인젝션
- XSS
- CSRF
- 암호화
- 오픈리다이렉트
- 보안쿠키
- 인증
- HTTP응답분할
- 접근제어
- 예외처리
- 정수오버플로우
- TOCTOU
- 세션간의 정보누출
- 반복문제어 부재
- 널포인트 역참조
- 캐슬화 위배
- 중요정보 노출

XSS

외부입력값에 스크립트요소가 포함되어 있는 경우 이값을 적절하게 필터링하지 않고 사용자에게 응답하도록 서버 프로그램이 작성되어 있으면 해당 서버를 통해 공격자는 악성코드를 배포하게 되고 서버에 접속한 사용자들은 악성 스크립트를 다운로드 받아 실행하는 침해사고가 발생할 수 있습니다.

(1) Reflective XSS

`<script>alert(document.cookie)</script>` 실행

설치

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.

- 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>

The screenshot shows a web application security tool interface. On the left, there's a sidebar with a list of attack types: 시큐어코딩테스트, 인코딩, 정규식, SQL 인젝션, 명령어 인젝션, XPath 인젝션, XSS, CSRF, 암호화, 오픈리다이렉트, 보안쿠키, 인증, HTTP 응답분할, 접근제어, 예외처리, 경수오버플로우, TOCTOU, 세션간의 정보노출, 반복문제어 부재, 널포인트 역참조, 캡슐화 위배, 중요정보 노출. The main area is titled 'XSS' and contains a description of Reflective XSS. Below the description, there's a text input field containing the payload '<script>alert("xss");</script>' and a '실행' (Execute) button. Below this, there's a '설정' (Settings) window showing system information: 정보 (Information), PC가 모니터링되고 보호됩니다. (PC is being monitored and protected.), 자세한 내용은 Windows 보안을 참조하세요. (For more details, refer to Windows security.), 장치 사양 (Device specifications), SAMSUNG PC, 디바이스 이름 (Device name): LAPTOP-FFQ03505, 프로세서 (Processor): Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz, 설치된 RAM (Installed RAM): 8.00GB(7.81GB 사용 가능) (8.00GB(7.81GB available)), 장치 ID (Device ID): 36653DBF-F927-4222-A0E7-82AFD7B66C6F, 제품 ID (Product ID): 00325-81135-68630-AAOEM, 시스템 종류 (System type): 64비트 운영 체제, x64 기반 프로세서 (64-bit operating system, x64-based processor), 펜 및 터치 (Pen and touch): 이 디스플레이에 사용할 수 있는 펜 또는 터치식 입력이 없습니다. (No pen or touch input is available for this display.).

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

시큐어코딩테스트

- 인코딩
- 정규식
- SQL 인젝션
- 명령어 인젝션
- XPath 인젝션
- XSS
- CSRF
- 암호화
- 오픈리다이렉트
- 보안쿠키
- 인증
- HTTP응답분할
- 접근제어
- 배외처리
- 정수오버플로우
- TOCTOU
- 세션간의 정보노출
- 반복문제어 부재
- 널포인트 역참조
- 캐슬화 위배
- 중요정보 노출

XSS

외부입력값에 스크립트요소가 포함되어 있는 경우 이값을 적절하게 필터링하지 않고 사용자에게 응답하도록 서버 프로그램이 작성되어 있으면 해당 서버를 통해 공격자는 악성코드를 배포하게 되고 서버에 접속한 사용자는 악성 스크립트를 다운로드 받아 실행하는 침해사고가 발생할 수 있습니다.

(1) Reflective XSS

실행

설정

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.

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

시큐어코딩테스트

- 인코딩
- 정규식
- SQL 인젝션
- 명령어 인젝션
- XPath 인젝션
- XSS
- CSRF
- 암호화
- 오픈리다이렉트
- 보안쿠키
- 인증
- HTTP응답분할
- 접근제어
- 배외처리
- 정수오버플로우
- TOCTOU
- 세션간의 정보노출
- 반복문제어 부재
- 널포인트 역참조
- 캐슬화 위배
- 중요정보 노출

XSS

외부입력값에 스크립트요소가 포함되어 있는 경우 이값을 적절하게 필터링하지 않고 사용자에게 응답하도록 서버 프로그램이 작성되어 있으면 해당 서버를 통해 공격자는 악성코드를 배포하게 되고 서버에 접속한 사용자는 악성 스크립트를 다운로드 받아 실행하는 침해사고가 발생할 수 있습니다.

(1) Reflective XSS

실행

설정

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.