

A3

(A3) Sensitive Data Exposure >

Insecure Login

임의의 id, password 입력 후 확인

The screenshot displays a web application security tool interface. On the left, a sidebar lists various vulnerability categories with expandable arrows:

- (A3) Sensitive Data Exposure >
- Insecure Login**
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8:2013) Request Forgeries >

At the top of the main content area, there are navigation buttons: a back arrow, a button labeled '1', and a button labeled '2'.

The main content area features the heading "Let's try" followed by the instruction: "Click the 'log in' button to send a request containing login credentials of any user." Below this, a light gray box contains a "Log in" button. At the bottom of this box, there is a form with two input fields and a "Submit" button. The first input field contains the text "webgoat", and the second input field contains six dots ".....".

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoder

InterceptHTTP historyWebSockets historyMatch and replaceProxy settings

Intercept on

Forward

Drop all

Time	Type	Direction	Method	URL
23:24:55 17 ...	HTTP	→ Request	POST	http://localhost:8080/WebGoat/insecureLogin/task
23:24:56 17 ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonmenu
23:24:56 17 ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonoverv
23:25:01 17 ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonmenu
23:25:01 17 ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonoverv
23:25:06 17 ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonmenu

Request

PrettyRawHex

5

Accept-Language: en-US,en;q=0.9

6

sec-ch-ua: "Chromium";v="139", "Not;A=Brand";v="99"

7

sec-ch-ua-mobile: ?0

8

X-Requested-With: XMLHttpRequest

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,

10

Accept: */*

11

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

12

Origin: http://localhost:8080

13

Sec-Fetch-Site: same-origin

14

Sec-Fetch-Mode: cors

15

Sec-Fetch-Dest: empty

16

Referer: http://localhost:8080/WebGoat/start.mvc

17

Accept-Encoding: gzip, deflate, br

18

Cookie: JSESSIONID=y1hQ2E8WFn0hpzmNX3SvuG-TkcptTU6yFSsLKmDY

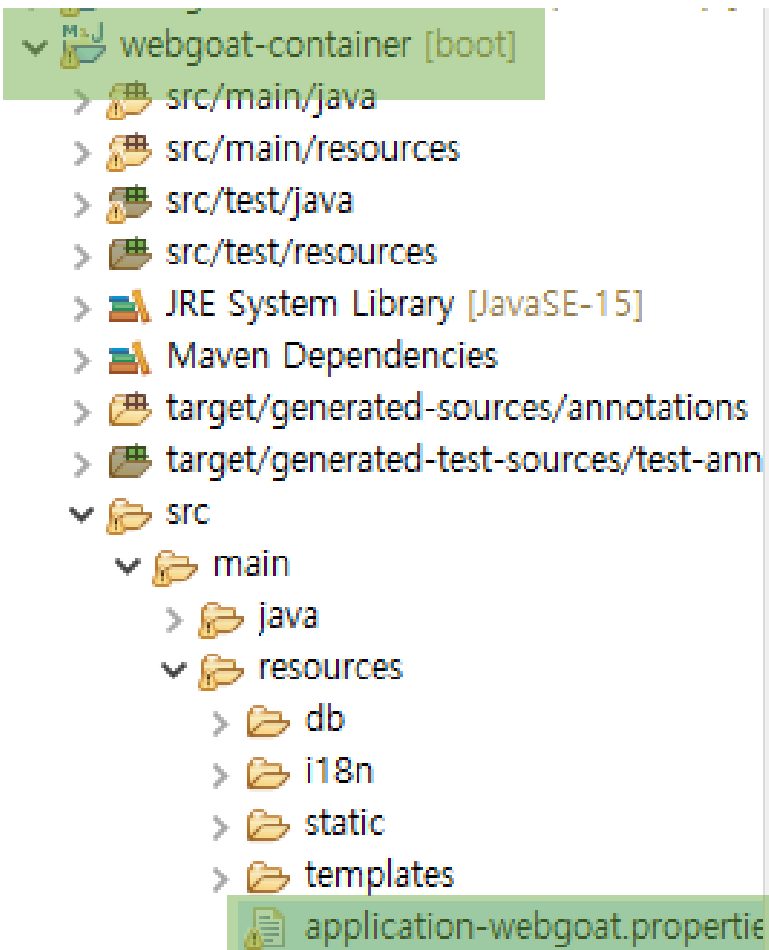
19

Connection: keep-alive

20

username=webgoat&password=123456

21



```
5 #server.port=${WEBGOAT_PORT:8080}  
6 server.port=${WEBGOAT_PORT:8443}
```

```
14 #server.ssl.enabled=${WEBGOAT_SSLENABLED:false}  
15 server.ssl.enabled=${WEBGOAT_SSLENABLED:true}
```



연결이 비공개로 설정되어 있지 않습니다.

공격자가 **localhost**에서 사용자의 정보를 도용하려고 시도할 수 있습니다(예: 비밀번호, 메시지, 신용카드 정보). [이 경고에 대해 자세히 알아보기](#)

NET::ERR_CERT_AUTHORITY_INVALID

💡 [항상된 보호 모드를 사용 설정](#)하여 Chrome의 가장 강력한 보안을 활용하세요.

세부정보 숨기기

안전한 페이지로 돌아가기

이 서버가 **localhost**임을 입증할 수 없으며 컴퓨터의 운영체제에서 신뢰하는 보안 인증서가 아닙니다. 서버를 잘못 설정했거나 불법 사용자가 연결을 가로채고 있기 때문일 수 있습니다.

localhost(안전하지 않음)(으)로 이동

자체 인증서 설치

```
keytool -genkeypair -alias webgoat-server -keyalg RSA -keysize 2048 -validity 365 -keystore webgoat.jks -  
storepass changeit -keypass angeit -dname "CN=WebGoat, OU=Dev, O=Example Corp, L=Seoul, S=Seoul, C=KR"
```

```
keytool -list -keystore webgoat.jks -storepass changeit : 별명리스트 보기
```

```
keytool -delete -alias webgoat-server -keystore webgoat.jks -storepass changeit : 사용하지 않는 별명삭제
```

```
keytool -exportcert -alias webgoat-server -keystore webgoat.jks -storepass changeit -rfc -file webgoat-root.crt
```

```
keytool -importkeystore -srckeystore webgoat.jks -destkeystore webgoat.p12 -srcstoretype JKS -deststoretype  
PKCS12 -srcstorepass changeit -deststorepass changeit -srcalias webgoat-server -srckeypass angeit -  
destkeypass changeit
```

```
cd target
```

```
java -jar -Dserver.port=8443 -Dserver.ssl.key-store=webgoat.jks -Dserver.ssl.key-store-password=changeit -  
Dserver.ssl.key-alias=webgoat-server -Dserver.ssl.key-password=angeit webgoat.jar
```