

전북대 Litmus Online Judge 취약점 점검

BCGLAB 240522
IT정보공학과 박수빈

웹 취약점 분석 평가 항목

점검항목	항목 중요도	항목코드
버퍼 오버플로우	상	BO
포맷스트링	상	FS
LDAP 인젝션	상	LI
운영체제 명령 실행	상	OC
SQL 인젝션	상	SI
SSI 인젝션	상	SS
XPath 인젝션	상	XI
디렉터리 인덱싱	상	DI
정보 누출	상	IL
악성 콘텐츠	상	CS
크로스사이트 스크립팅	상	XS
약한 문자열 강도	상	BF
불충분한 인증	상	IA
취약한 패스워드 복구	상	PR
크로스사이트 리퀘스트 변조(CSRF)	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV
파일 업로드	상	FU
파일 다운로드	상	FD
관리자 페이지 노출	상	AE
경로 추적	상	PT
위치 공개	상	PL
데이터 평문 전송	상	SN
쿠키 변조	상	CC

-이용 도구

Burp suite, wireshark

정보 누출

Case 1. 임의의 계정으로 로그인을 시도하여 반환되는 에러 메시지를 통해 특정 ID의 가입 여부를 식별할 수 있는지 확인

Step 1. [ID/PW 찾기]에서 아이디에 'admin' 입력 시, 관리자 아이디라는 정보 반환

litmus.jbnu.ac.kr 내용:

관리자 아이디는 접근 불가능합니다.

확인

크로스사이트 스크립팅

Case 1. litmus board (문의하기 페이지) Stored XSS 가능

[litmus board] > [글쓰기]

Step 1. 게시글에 스크립트 구문 삽입 후 전송

삽입 구문: `<style>@keyframes x{}</style><xss style="animation-name:x" onanimationstart="alert(document.cookie)"></xss>`

:: 글수정 ::

옵션

☒ html

분류

질문

제목

내용

!

`<style>@keyframes x{}</style><xss style="animation-name:x" onanimationstart="alert(document.cookie)"></xss>`

링크 #1

링크 #2

파일첨부

파일 선택

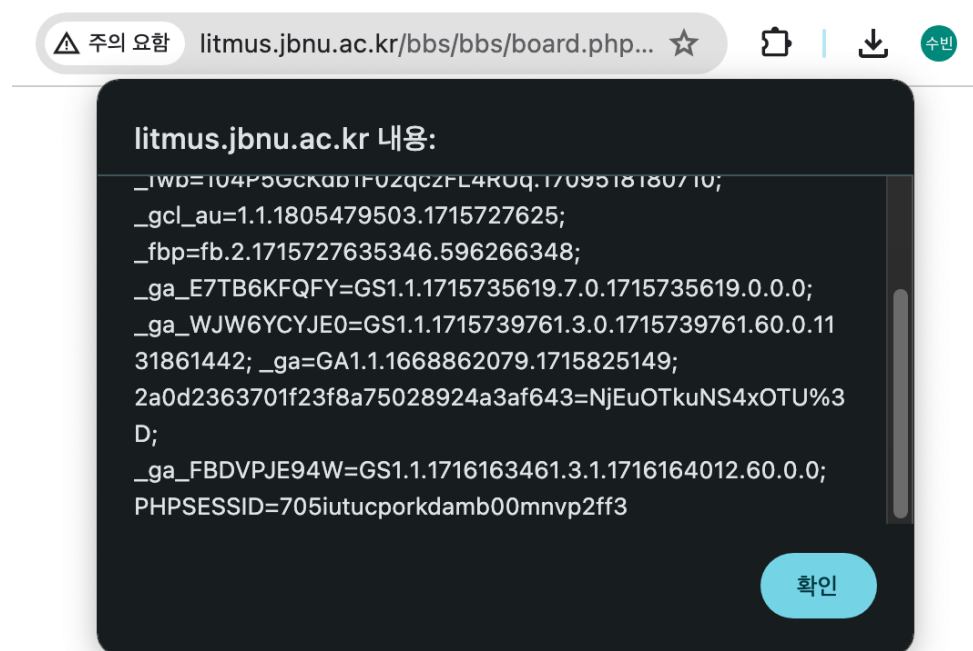
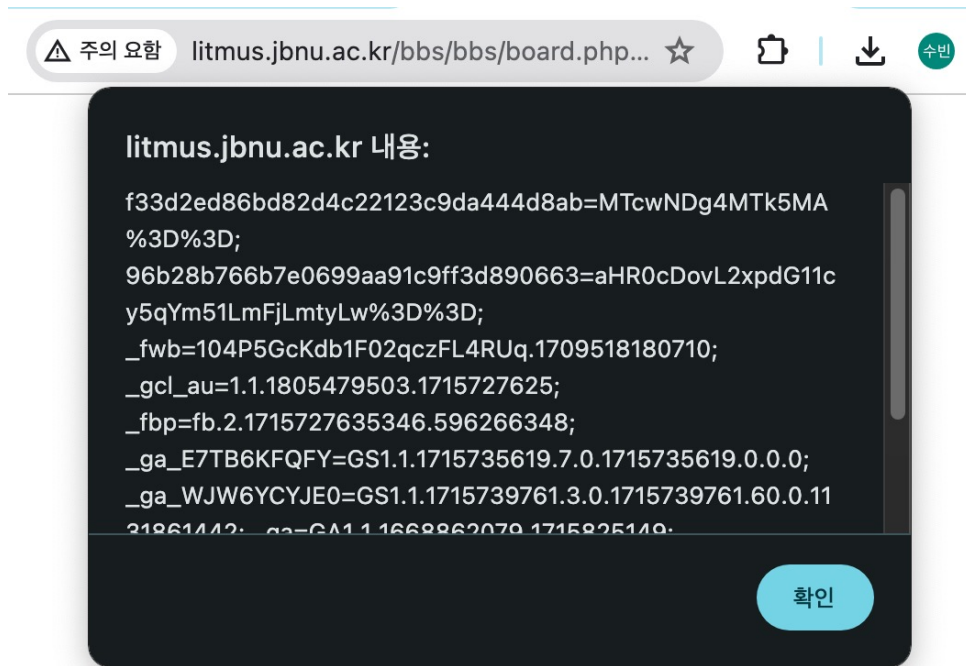
선택된 파일 없음

크로스사이트 스크립팅

Case 1. litmus board (문의하기 페이지) Stored XSS 가능

[litmus board] > [글쓰기]

Step 2. 이후 게시글을 확인할 때마다 저장된 스크립트 구문이 실행됨을 확인



약한 문자열 강도

Case 1. 일정 횟수(3~5회) 이상 인증 실패 시 로그인 제한 없음

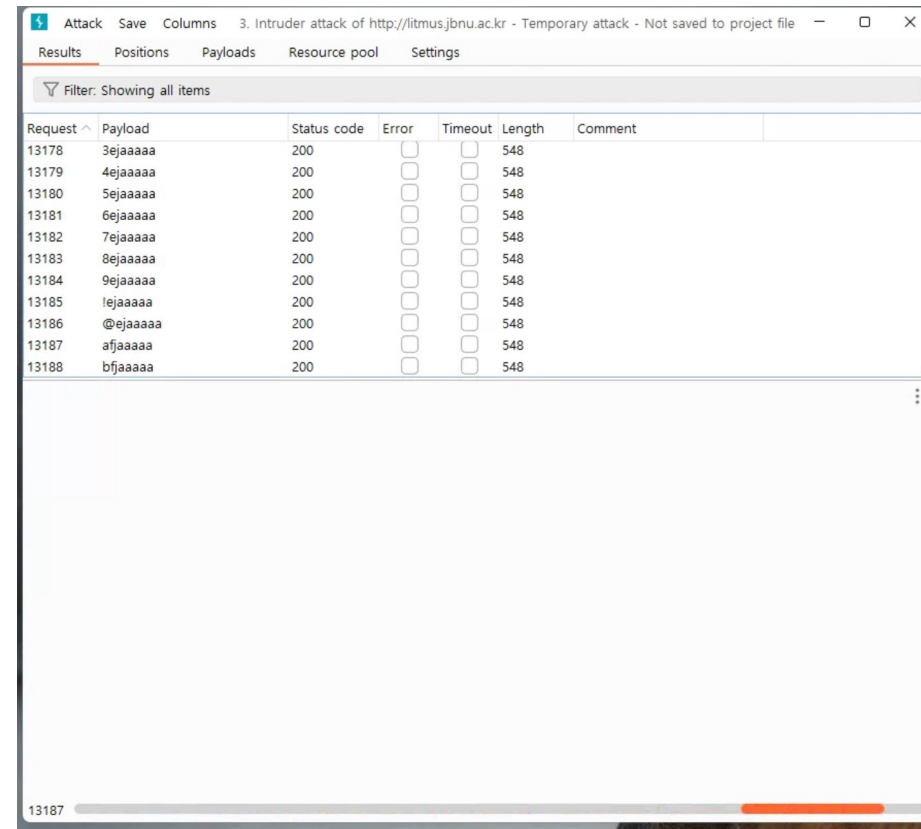
Step 1. 로그인 시 잘못된 비밀번호를 입력하여 지속적으로 로그인을 요청했음에도 제한사항 없음을 확인

litmus.jbnu.ac.kr 내용:

가입된 회원이 아니거나 비밀번호가 틀립니다.

패스워드는 대소문자를 구분합니다.

확인



The screenshot shows the 'Results' tab of the Litmus Intruder tool. The title bar indicates the target is 'http://litmus.jbnu.ac.kr'. The interface includes tabs for 'Results', 'Positions', 'Payloads', 'Resource pool', and 'Settings'. A filter bar shows 'Showing all items'. Below is a table with columns: Request, Payload, Status code, Error, Timeout, Length, and Comment. The table lists 11 requests (13178 to 13188) with payloads ranging from '3ejaaaaa' to 'bfjaaaaa'. All requests have a status code of 200, no errors, and a length of 548. A scrollbar at the bottom indicates the list continues.

Request	Payload	Status code	Error	Timeout	Length	Comment
13178	3ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13179	4ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13180	5ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13181	6ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13182	7ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13183	8ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13184	9ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13185	!ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13186	@ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13187	afjaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13188	bfjaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	

약한 문자열 강도

Case 2. 패스워드에 대한 규정 취약

[정보수정] -> [패스워드]

Step 1. 3글자 이상이면 패스워드 규정을 만족하며 패스워드 수정 시 전에 사용했던 패스워드 재사용이 가능하므로 다음 규정에 미달

1) 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

(1) 영문 대문자(26개)

(2) 영문 소문자(26개)

(3) 숫자(10개)

(4) 특수문자(32개)

2) 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고

3) 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

4) 최근 사용되었던 패스워드 재사용 금지

litmus.jbnu.ac.kr 내용:

패스워드를 3글자 이상 입력하십시오.

확인

취약한 패스워드 복구

Case 1. 패스워드 찾기 시 재설정된 패스워드를 인증된 사용자 메일이나 SNS로 전송하지 않고 웹 사이트 화면에 바로 출력함

[ID/PW 찾기]

Step 1. 회원아이디(혹은 이름, E-mail), 패스워드 분실시 답변을 입력

주의 요함

litmus.jbnu.ac.kr/bbs/bbs/password_forget.php

+ 회원아이디/패스워드 찾기

/ STEP 01

회원아이디를 입력해 주세요.

회원아이디

회원아이디를 잊으셨나요?

이름

E-mail

다음

창닫기

+ 회원아이디/패스워드 찾기

/ STEP 02

회원아이디 22222222

패스워드 분실시 질문
and 1=1

패스워드 분실시 답변

5368c99c8be5368c99cc8t 자동등록방지 코드를 입력하세요.

다음

창닫기

취약한 패스워드 복구

Case 1. 패스워드 찾기 시 재설정된 패스워드를 인증된 사용자 메일이나 SNS로 전송하지 않고 웹 사이트 화면에 바로 출력함

[ID/PW 찾기]

Step 2. 웹 페이지에 새로운 패스워드가 출력됨을 확인

+ 회원아이디/패스워드 찾기 결과

• 회원아이디 **222222222**

• 부여된 패스워드 **e4024**

새로 부여된 패스워드는 로그인 후 변경해 주십시오.

불충분한 세션 만료

Case 1. 로그인 후 재접속 시 세션 유지

[로그인]

Step 1. 로그인으로 세션을 발급받은 후 리트머스 창을 닫고 재접속 시 세션이 유지됨

Case 2. 로그인 후 일정 시간이 지난 후에 재전송 시 세션 유지

[로그인]

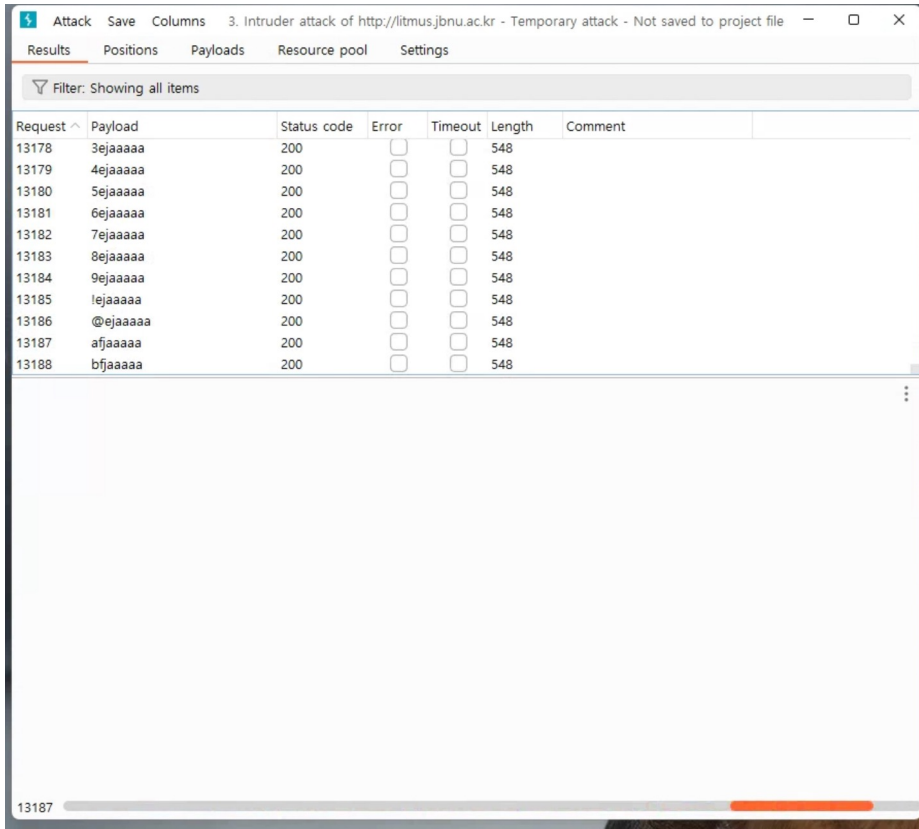
Step 1. 로그인으로 세션을 발급받은 후 2시간 후 재전송 시에도 세션이 유지되는 것을 확인

자동화 공격

Case 1. 로그인

[로그인]

Step 1. 자동화 도구로 반복적으로 로그인을 시도해도 통제가 이루어지지 않음



Attack Save Columns 3. Intruder attack of http://litmus.jbnu.ac.kr - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
13178	3ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13179	4ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13180	5ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13181	6ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13182	7ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13183	8ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13184	9ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13185	!ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13186	@ejaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13187	afjaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	
13188	bfjaaaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	548	

13187

자동화 공격

Case 2. 시험 참여

[시험목록] > [시험코드 변경]

Step 1. 자동화 도구로 반복적으로 시험 코드 입력을 시도

시험 정보	
시험코드	잘못된 시험코드이거나 시험시간이 아님
시험제목	잘못된 시험코드이거나 시험시간이 아님
교수님	잘못된 시험코드이거나 시험시간이 아님
시작시간	잘못된 시험코드이거나 시험시간이 아님
종료시간	잘못된 시험코드이거나 시험시간이 아님

시험코드를 변경하고자 할 경우에만 이용하세요!!
교수님께서 알려주시는 시험코드를 입력하세요.

시험코드 변경:

실시간 순위 보기

문제 목록			
문제 번호	제 목	결 과	제출하기

제출 목록					
제출 번호	문제 번호	제 목	결 과	소스보기	제출시간

자동화 공격

Case 1. 시험 참여

[시험목록] > [시험코드 변경]

Step 2. 시험에 참가하여 해당 시험 문제 목록과 실시간 순위를 확인

시험 정보

시험코드	240516KH
시험제목	[자료구조34분반] 숙제. 이진탐색트리(BST)
교수님	이경순
시작시간	2024-05-16 18:00:00
종료시간	2024-05-26 23:59:00

시험코드를 변경하고자 할 경우에만 이용하세요!!
교수님께서 알려주시는 시험코드를 입력하세요.

시험코드 변경:

실시간 순위 보기

문제 목록

문제 번호	제 목	결 과	제출하기
A	[자료구조] 이진 탐색 트리 - 균형 잡힌 트리		제출하기
B	[자료구조] 이진 탐색 트리 - 합 경로 세기		제출하기
C	[자료구조] 이진 탐색 트리 - 한영/영한 사전 검색		제출하기

제출 목록

제출 번호	문제 번호	제 목	결 과	소스보기	제출시간
-------	-------	-----	-----	------	------

Request ^	Payload	Status	Error	Timeout	Length	Comment
186	DH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
187	EH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
188	FH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
189	GH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
190	HH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
191	IH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
192	JH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
193	KH	200	<input type="checkbox"/>	<input type="checkbox"/>	818	
194	LH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
195	NH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
196	MH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	
197	OH	200	<input type="checkbox"/>	<input type="checkbox"/>	1028	

파일 업로드

Case 1. litmus board (문의하기 페이지) 에 Server-Side Script 파일 업로드 가능

[litmus board] > [글쓰기]

Step 1. litmus board (문의하기 페이지) 게시글에 Server-Side Script 파일 업로드 시도

업로드한 웹셸 파일: shelltest.php, shell.asp, test.jsp

:: 글수정 ::

옵 섌

☐ html

분 류

기타 ▼

제 목

t

▲ ▢ ▼

> 솔루션을 게재하지 않습니다.

내용

링크 #1

링크 #2

파일첨부

파일 선택

shelltest.php

☐ shelltest.php(39byte) 파일 삭제

파일첨부



파일 선택 shell.asp

파일첨부



파일 선택 test.jsp

파일 업로드

Case 1. litmus board (문의하기 페이지) 에 Server-Side Script 파일 업로드 가능
[litmus board] > [글쓰기]

Step 2. Server-Side Script 파일 업로드가 성공함을 확인
업로드한 웹쉘 파일: shelltest.php, shell.asp, test.jsp

[질문] 4

글쓴이 : 박수빈 (14.♡.50.133)

 shell.asp (230byte) [1] DATE : 20

> 솔루션을 게재하지 않습니다.

[질문] 4

글쓴이 : 박수빈 (14.♡.50.133)

 test.jsp (34byte) [0] DATE : 202

> 솔루션을 게재하지 않습니다.

 작성일 : 24-04-18 15:46

[기타] t

글쓴이 : 박수빈 (61.♡.5.158)

 shelltest.php (39byte) [0] DATE : 2024-04-18 15:46:28

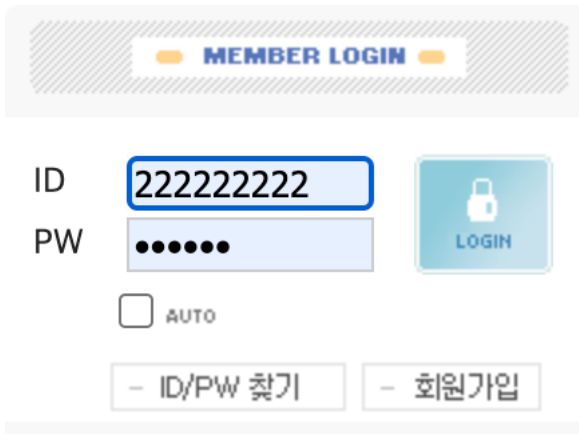
> 솔루션을 게재하지 않습니다.

데이터 평문 전송

Case 1. 로그인 시 데이터 암호화가 이루어지지 않음

[로그인]

Step 1. 중요정보(패스워드)를 송수신하는 페이지 존재 확인



Step 2. 통신 시 패스워드에 대한 암호화가 이루어지지 않음

0430	25 32 35 32 46 77 65 62	25 32 35 32 46 26 6d 62	%252Fweb %252F&mb
0440	5f 69 64 3d 32 32 32 32	32 32 32 32 32 26 6d 62	_id=2222 22222&mb
0450	5f 70 61 73 73 77 6f 72	64 3d 6c 69 74 6d 75 73	_password=litmus
0460	26 78 3d 31 39 26 79 3d	33 36	&x=19&y= 36

[정보수정] > [패스워드]

회원아이디

22222222

패스워드

▶ 확인

외부로부터 회원님의 정보를 안전하게 보호하기 위해
패스워드를 확인하셔야 합니다.

```
0450 0d 0a 6d 62 5f 69 64 3d 32 32 32 32 32 32 32 32 ..mb_id= 22222222
0460 32 26 77 3d 75 26 6d 62 5f 70 61 73 73 77 6f 72 2&w=u&mb _passwor
0470 64 3d 6c 69 74 6d 75 73 d=litmus
```

데이터 평문 전송

Case 3. 비밀번호 변경 시 평문 통신함을 확인

[로그인]

[정보수정] > [패스워드] > [패스워드], [패스워드 확인]

Step 1. 중요정보(패스워드)를 변경하는 페이지 존재 확인

패스워드	<input type="password"/>
패스워드 확인	<input type="password"/>

Step 2. 통신 시 패스워드에 대한 암호화가 이루어지지 않음

0820	5f 70 61 73 73 77 6f 72	64 22 0d 0a 0d 0a 74 65	password".....te
0830	73 74 0d 0a 2d 2d 2d 2d	2d 2d 57 65 62 4b 69 74	st..... --WebKit
0840	46 6f 72 6d 42 6f 75 6e	64 61 72 79 61 52 44 6b	FormBoun daryaRdk

감사합니다