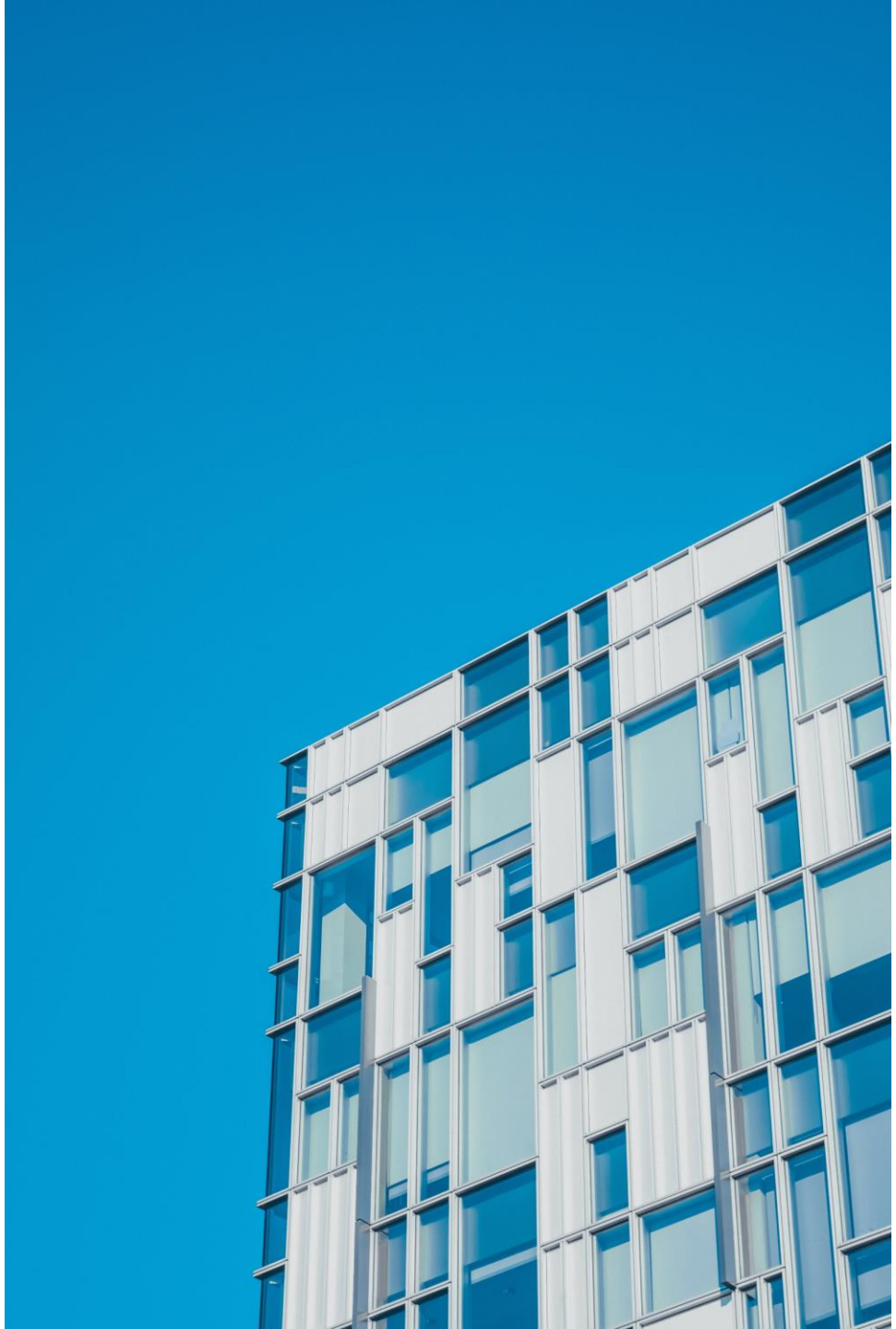
2018

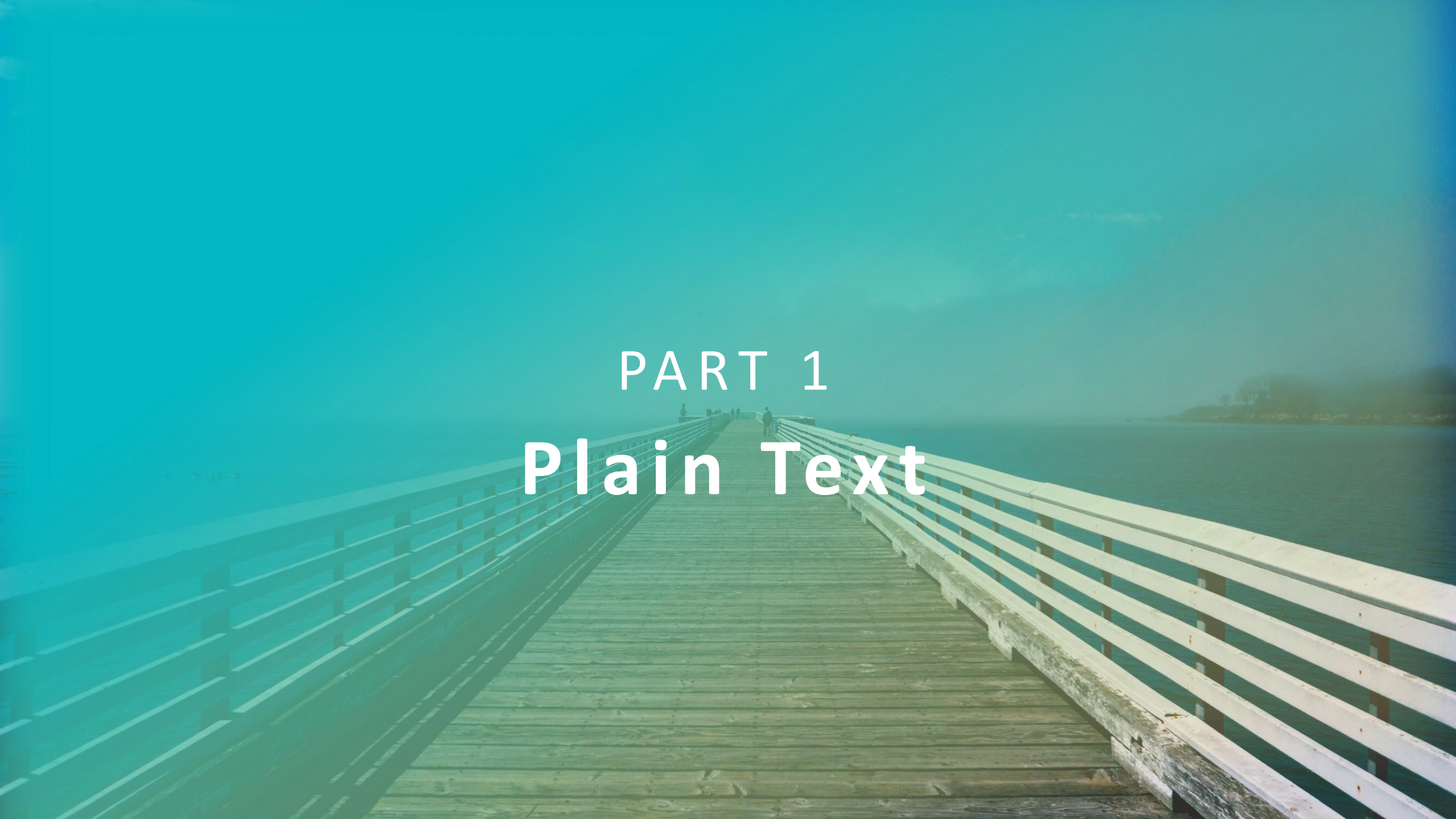
중부대학교 웹서비스 취약점 분석

SUMMER PRESENTATION

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

Table of Contents





PART 1

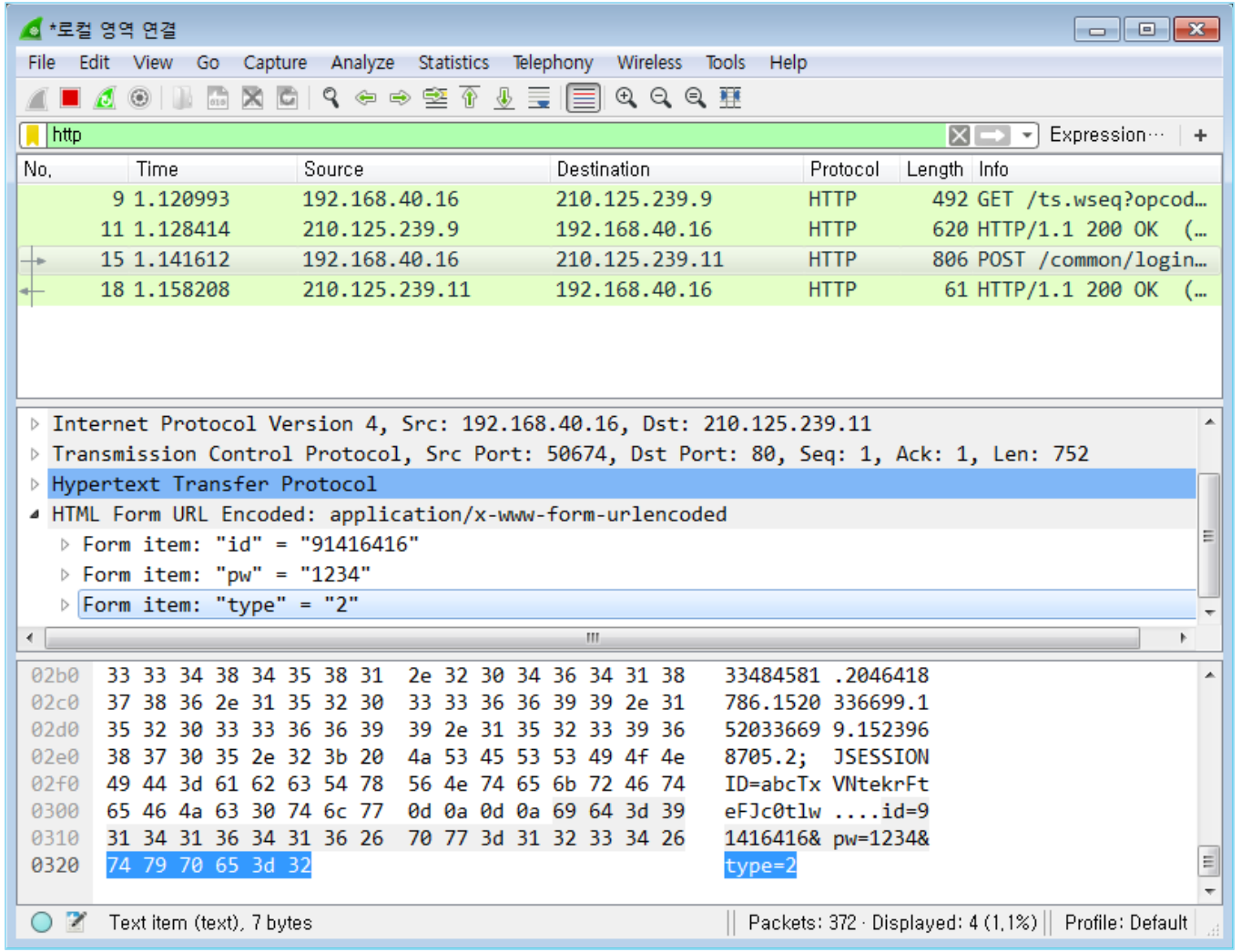
Plain Text

PlainText

Process #1

PlainText

Process #2



Scenario #MITM

Normal case

SERVER

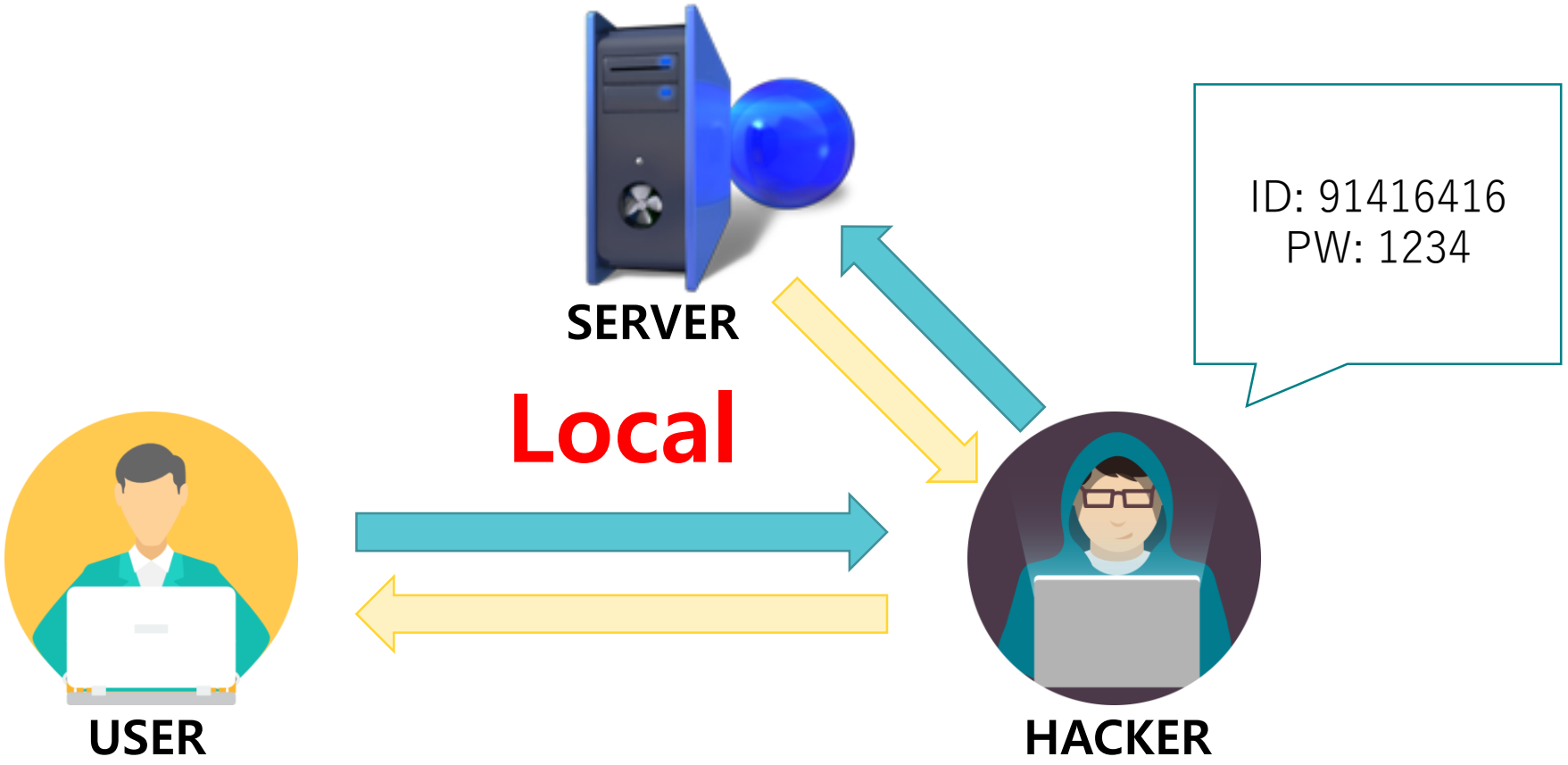
Local

USER

HACKER

Scenario #MITM

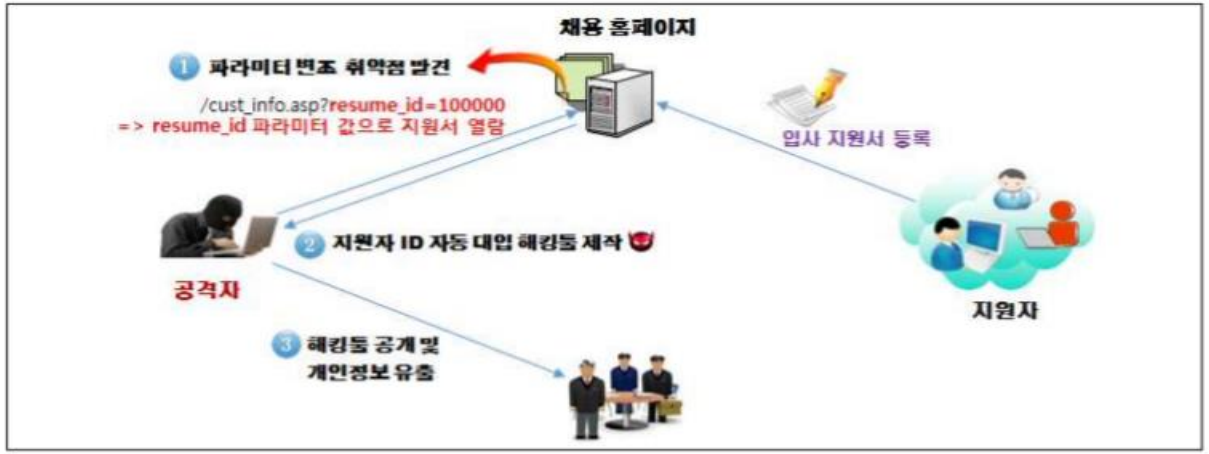
Abnormal case




PART 2
사이버강의실

Parameter Manipulation

Theory

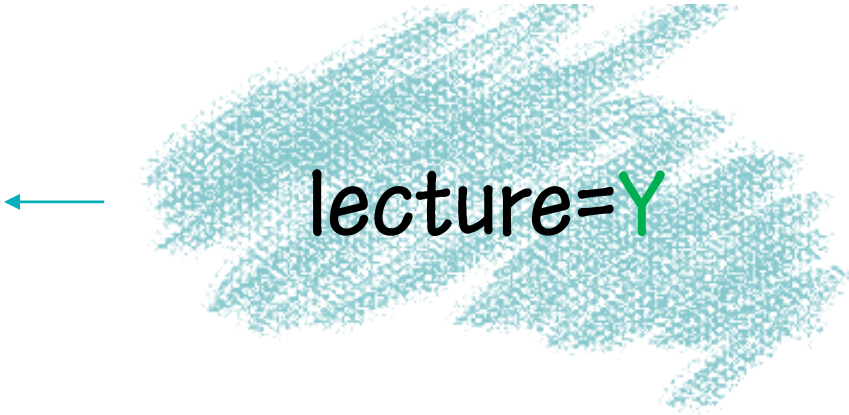


[그림 1] 파라미터 변조를 통한 입사 지원서 유출

KrCERT/CC
인터넷 침해 대응 센터

Cyber Lecture Room

Parameter manipulation



>> 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?

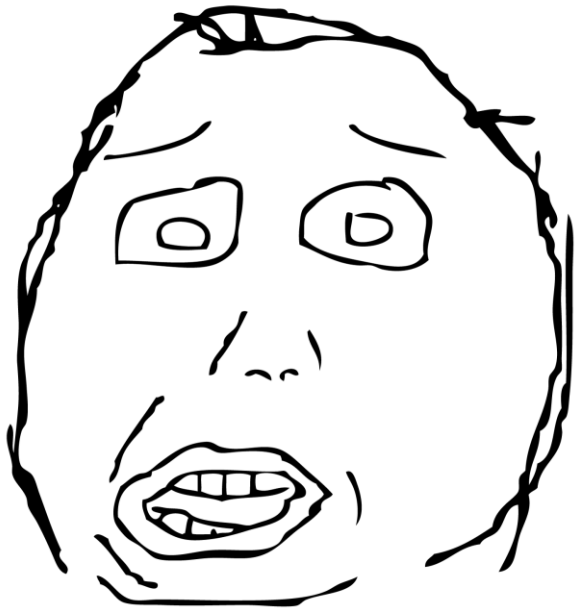
>> Lecture.js

```
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

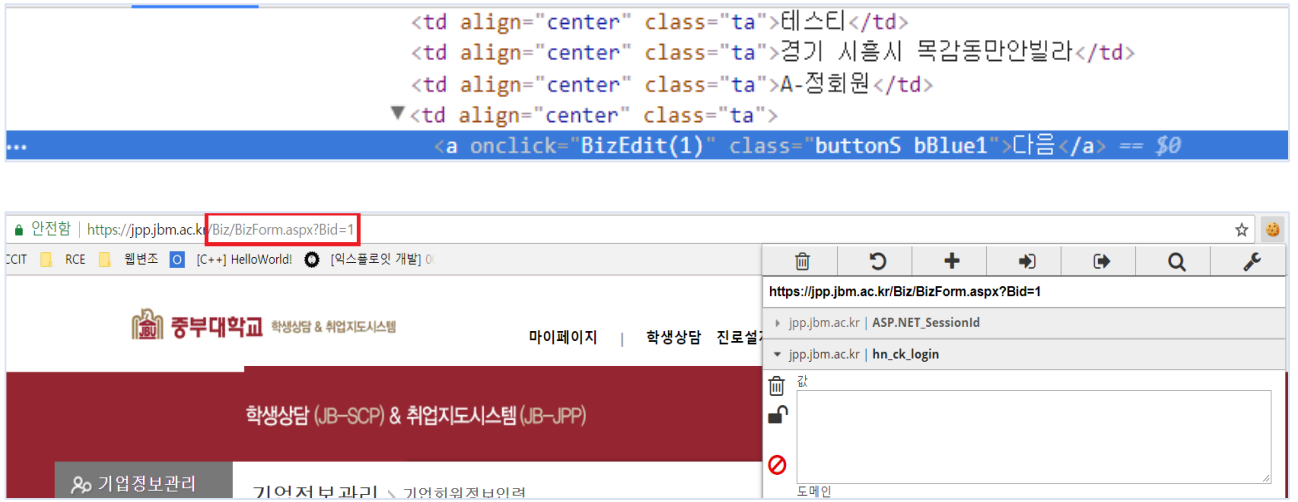
기업 로그인

조건부 권한

JPP Login System

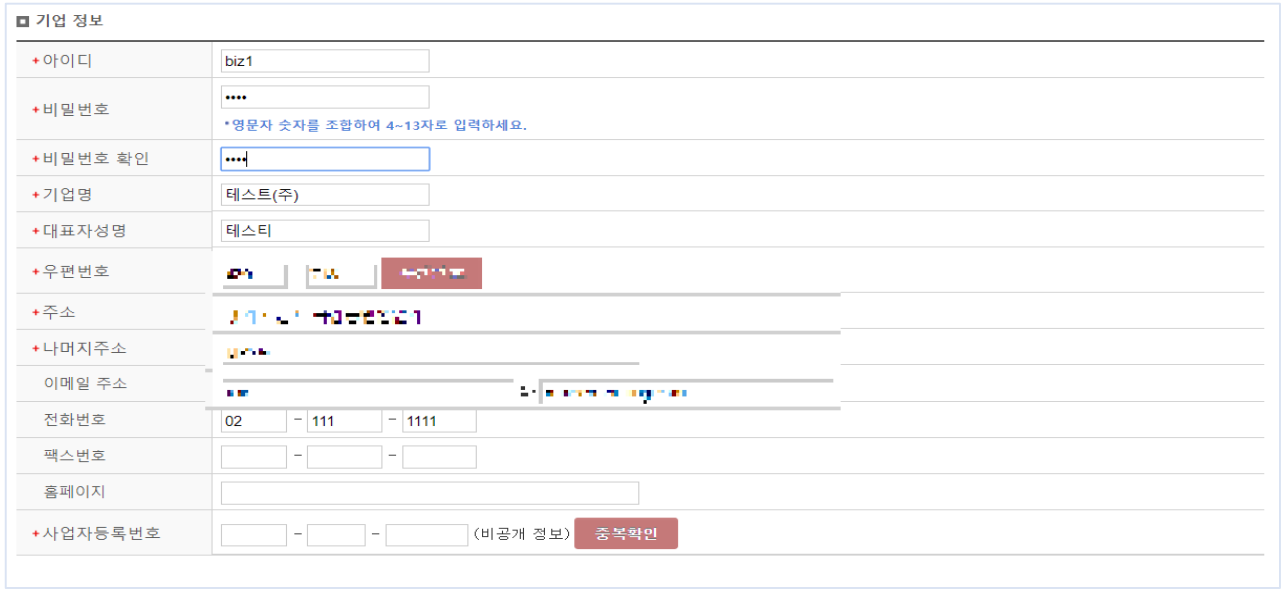
검색 → 수정/등록 → 로그인

JPP Login System



검색 → 수정/등록 → 로그인

JPP Login System



검색 → 수정/등록 → 로그인

JPP Login System

검색 → 수정/등록 → 로그인

Part4
정보 유출

Information is important

- 학번(사번)
- 이름
- 단과-대학
- 학년
- 전화번호
- 핸드폰번호
- 메일주소
- 주소(상세주소 제외)

Information is important

- 학번
- 이름
- 사진
- 졸업성적
- 이력서
- IP
- 이수학점
- 학년
- 핸드폰 번호
- 비밀번호
- 상세주소
- 이메일
- 성적조작

Welcome to the real world!

-컬럼명 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>
```

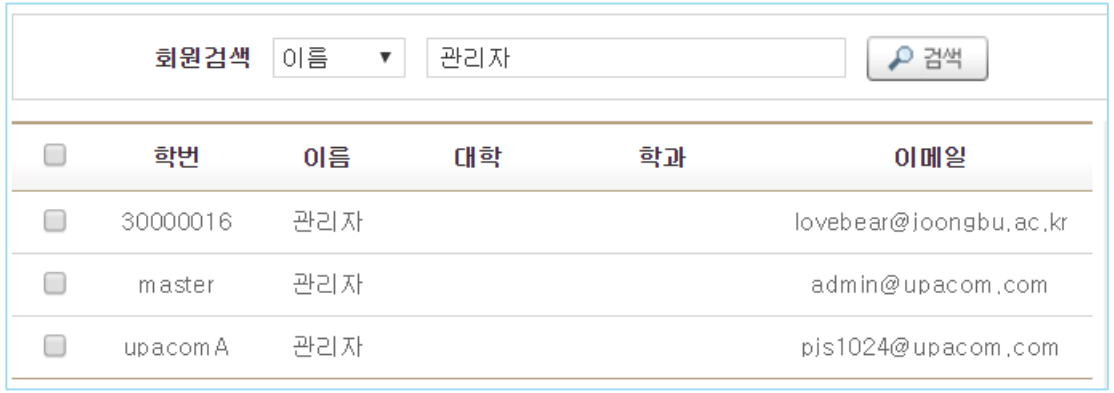
```
SELECT MBER_CD, MBER_NM · · · , EMAIL FROM `TABLE_NAME` WHERE $search_field=$search_text
```

Welcome to the real world!

Find admin password

OracleDB

- ‘_’ 는 한 개의 데이터
- ‘%’ 는 한 개 이상의 데이터



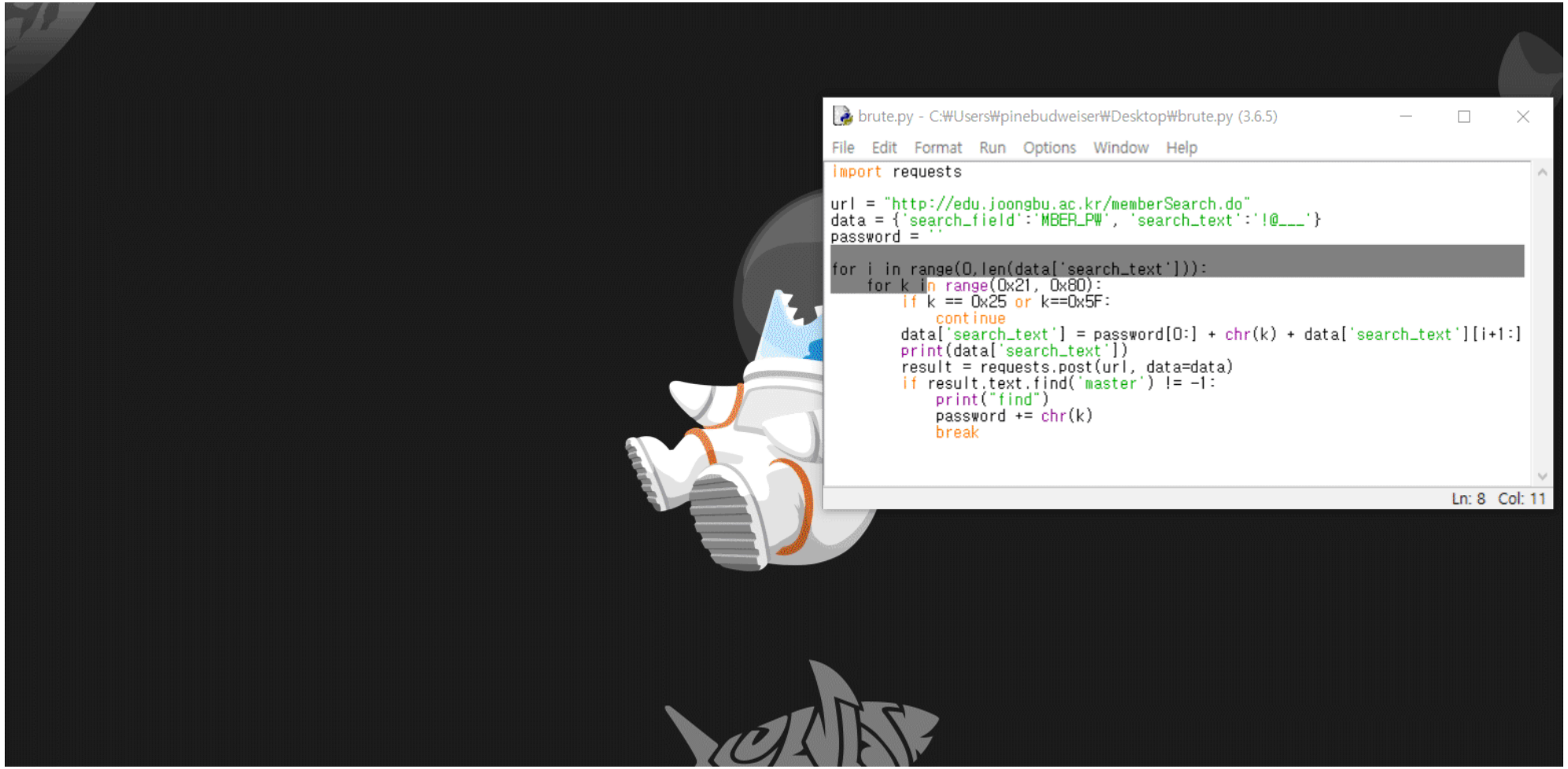
MBER_NM -> MBER_PW

_@___(5글자)

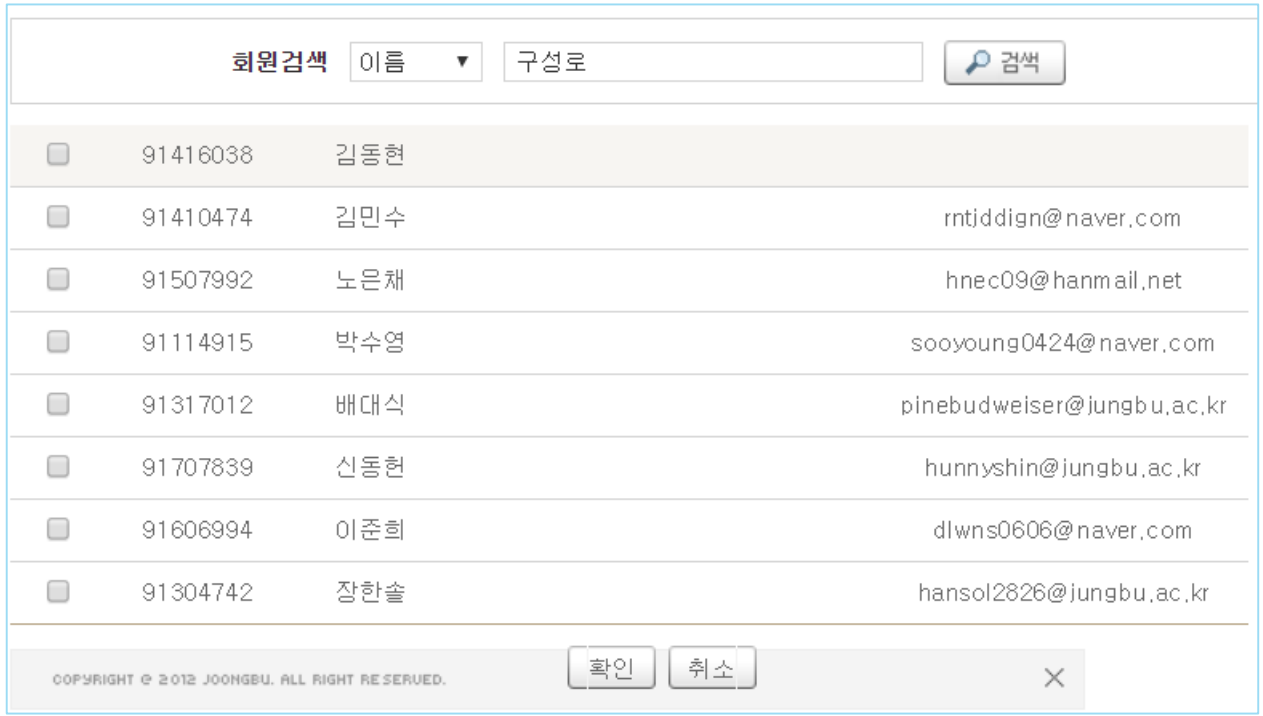
A-Za-z0-9… brute force

Welcome to the real world!

Find admin password



Welcome to the real world!



MEMBER_NM → ADDR

Welcome to the real world!

인재정보 : 6158 건

이름	이력서	학과(계열)	경력/희망연봉	지역	수정일
류** (女,1998)	[redacted]	산업디자인학전공	[redacted]	[redacted]	2018-04-23
원** (男,1996)	[redacted]	자동차관리학과	[redacted]	[redacted]	2018-04-21
최** (男,1996)	[redacted]	자동차관리학과	[redacted]	[redacted]	2018-04-19
김** (女,1997)	[redacted]	연극영화학전공	[redacted]	[redacted]	2018-04-19

시험_평가조회

시험시간 : 30분, 총인원 : 134명, 제출인원 : 126명, 미제출인원 : 0명, 미응시인원 : 8명

전체 | 응시자 | 미응시자 | 오프라인

정렬 : 이름 ▼ 시험상태 : 전체 ▼ 이름 ▼ 검색

학번	이름	평가여부	점수/총점	응시상태	제출일자	IP	시험지	평가
[redacted]	[redacted]	평가완료	18 / 30	응시	2018-04-27 01:22:33	[redacted]		보기
[redacted]	[redacted]	평가완료	20 / 30	응시	2018-04-27 16:33:44	[redacted]		보기
[redacted]	[redacted]	평가완료	26 / 30	응시	2018-04-27 15:58:01	[redacted]		보기

Welcome to the real world!

추천의뢰 스크랩 뒤로

제목	이력서 (수정일 : 2018-06-28)	
	이름	손**(남자)
	생년월일	[illegible]
	휴대폰	[illegible]
	E-mail	[illegible]
	주소	[illegible]

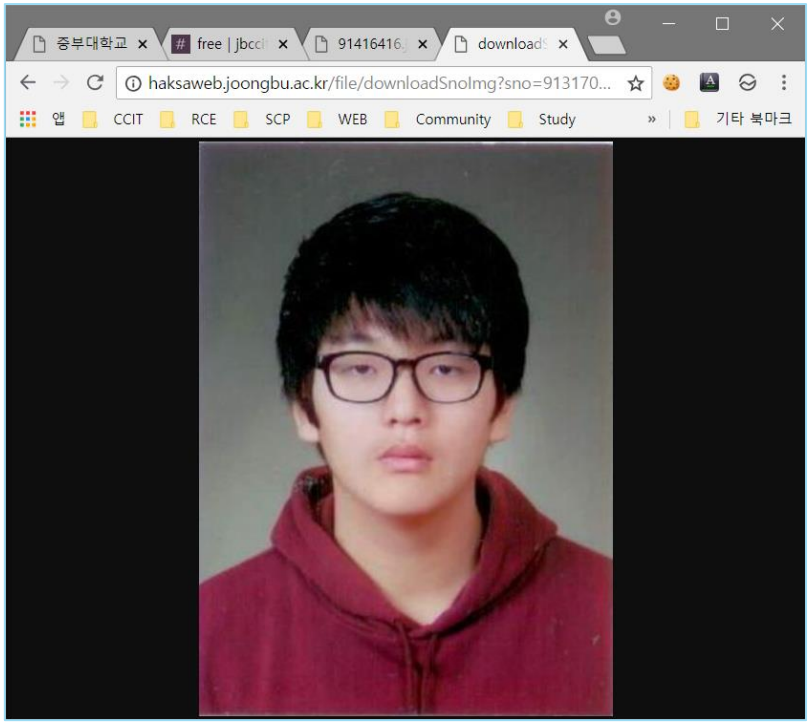
기본항목

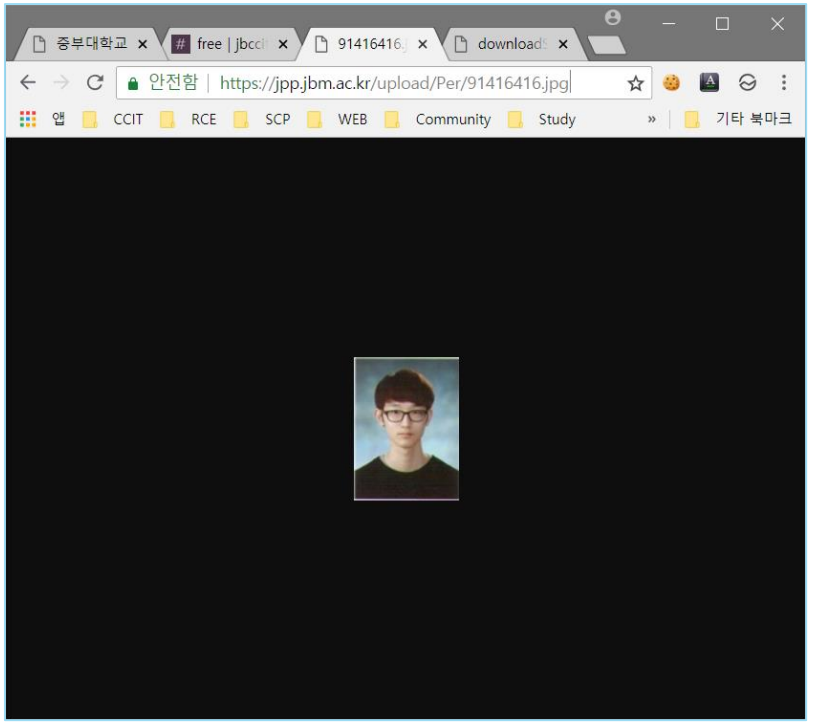
보훈대상여부	비대상	장애여부	[illegible]
병역사항	[illegible]	졸업예정일	
희망지역	[illegible]	희망연봉	[illegible]
지원분야	[illegible]		

학력정보

학과	[illegible]	전공	[illegible]
현재학기	[illegible]	학적상태	[illegible]
총취득학점	[illegible]	평균평점	[illegible]
구분	[illegible]	출신고교	

Welcome to the real world!





- http://haksaweb.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 이미지들은 4월 제보 후 7월에 제작된 이미지입니다.

"

당신의 정보는 소중합니다

신뢰 되지 않은 사이트에 정보를 기입 시 최소한의 정보를 기입해주세요

"


Thank You