

The background of the image features a large, dark blue shield with a lighter blue border. Inside the shield, the letters 'JBU' are rendered in a stylized, blocky font. The 'J' and 'U' are on the left and right sides, respectively, and the 'B' is in the center. The letters are a medium blue color.

JBU-CTF



web

방탈출

난이도: 중

쪽지시험

난이도: 중하

[방탈출]

* 난이도: 중

* 출제 의도

- Html, CSS, Javascript에 대한 이해가 충분한지 확인한다.
- Iframe이 여러 보안문제를 일으킬 수 있다는 점을 인식시킨다.



방탈출

난이도: 중

Challenge

0 Solves

방탈출

점수미정

키를 찾아 방을 탈출해라!

힌트는 소스코드 안에 있다!


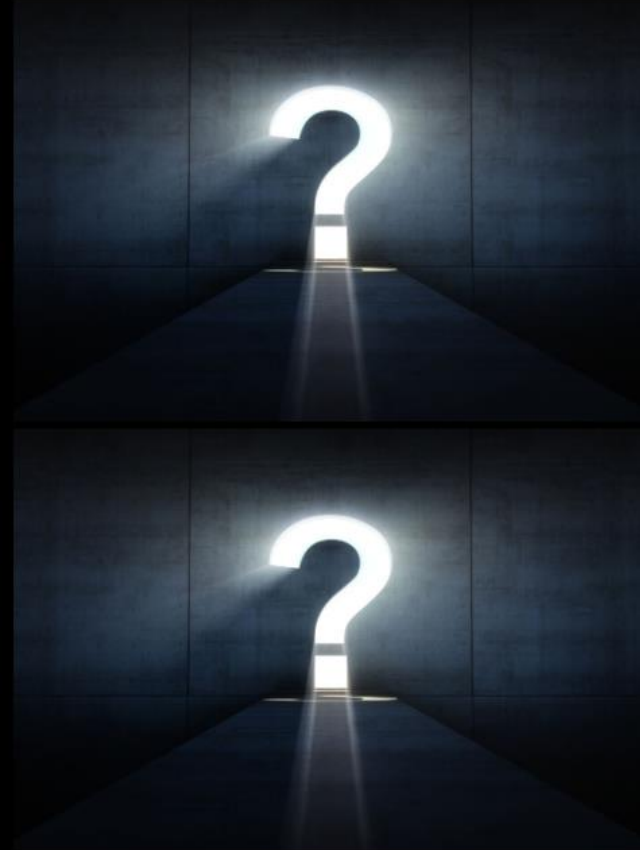
<http://127.0.0.1/1.html>

Submit

Find the flag. And Escape the room.



Find the flag. And Escape the room.



```
1.html x
54 <iframe
55   src="keke.html"
56   style="width: 0; height: 0; border: none"
57 ></iframe>
58 </div>
59 <div class="lside">
60   
61   
62 </div>
63 <div class="section">
64   
65 </div>
66 <div class="rside">
67   
68   
69 </div>
70 <footer class="footer">
71   <iframe
72     src="hehe.html"
73     style="width: 0; height: 0; border: none"
74   ></iframe>
75 </footer>

{} Line 1, Column 1
```


Find the flag. And Escape the room.

ScpCTF{qkqhthrdlatnwlfdh!}



key: submit


```
hehe.html > html > head > script
1  <!DOCTYPE html>
2  <html>
3  <head>
4    <meta charset="utf-8" />
5    <title>hehe</title>
6    <style type="text/css">
7      body {
8        background-color: blue;
9        color: white;
10     }
11     .login {
12       height: 50px;
13     }
14   </style>
15   <script>
16     var a1 = "<scmodlkxwapsript>func";var a2 = "titeducavion chiteducaveck_";var a3 = "imodlkxwapsnput() {if ";var a4 = "(document.in";var a5 = "iteducavsert
17   </head>
18   <body>
19     <form name="insert_form" method="post">
20       key: <input type="text" name="key" />
21       <input
22         style="height: 30px"
23         type="button"
24         class="login"
25         value="submit"
26         onclick="check input();"
27       />
28     </form>
29   </body>
30 </html>
31
```

key:

Find the flag. And Escape the room.

```
1.html  hehe.html x
18  <script>
19    var a1 = "<scmodlkxwapsript>func";
20    var a2 = "titeducavion chiteducaveck_";
21    var a3 = "imodlkxwapsnput() {if ";
22    var a4 = "(document.in";
23    var a5 = "iteducavsert_fomodlkxwapsrm.k";
24    var a6 = 'eiteducavy.vamodlkxwapslue == "qkdxkf';
25    var a7 = 'cnftjmodlkxwapsdrhd") {alert("축';
26    var a8 = "하드립니다. 방탈";
27    var a9 = '출에 성공하셨습니다!");r';
28    var a10 = "etiteducavrn;}}<\\scr";
29    var a11 = "iteducavipt>";
30    var a12 = a1 + a2 + a3 + a4 + a5 + a6 + a7 + a8 + a9 + a10 + a11;
31    document.write(a12.replace(/iteducav|modlkxwaps/g, ""));
32  </script>
33  </head>
34  <body>
35    <form name="insert_form" method="post">
36      key: <input type="text" name="key" />
37      <input
38        style="height: 30px"
39        type="button"
40        class="login"
41        value="submit"
42        onclick="check_input();"
43      />
44  </body>
45  </html>
```

{ } Line 20, Column 6

key: submit

Find the flag. And Escape the room.

```
1.html  hehe.html x
18  <script>
19    var a1 = "<scmodlkxwapsript>func";
20    var a2 = "titeducavion chiteducaveck_";
21    var a3 = "imodlkxwapsnput() {if ";
22    var a4 = "(document.in";
23    var a5 = "iteducavsert_fomodlkxwapsrm.k";
24    var a6 = 'eiteducavy.vamodlkxwapslue == "qkdxkf';
25    var a7 = 'cnftjmodlkxwapsdrhd") {alert("축';
26    var a8 = "하드립니다. 방탈";
27    var a9 = '출에 성공하셨습니다!");r';
28    var a10 = "etiteducavrn;}}<\\scr";
29    var a11 = "iteducavipt>";
30    var a12 = a1 + a2 + a3 + a4 + a5 + a6 + a7 + a8 + a9 + a10 + a11;
31    document.write(a12.replace(/iteducav|modlkxwaps/g, ""));
32  </script>
33  </head>
34  <body>
35    <form name="insert_form" method="post">
36      key: <input type="text" name="key" />
37      <input
38        style="height: 30px"
39        type="button"
40        class="login"
41        value="submit"
42        onclick="check_input();"
43      />
44  </body>
45  </html>
```

{ } Line 20, Column 6

key: submit

Find the flag. And Escape the room.

```
<script>
var a1 = "<script>func";
var a2 = "tion check_";
var a3 = "input() {if ";
var a4 = "(document.in";
var a5 = "sert_form.k";
var a6 = 'ey.value == "qkdxkf";
var a7 = 'cnftjdrhd") {alert("축';
var a8 = "하드립니다. 방탈";
var a9 = '출에 성공하셨습니다!");r';
var a10 = "eturn;}}<\/scr";
var a11 = "ipt>";
```

key: submit

Find the flag. And Escape the room.

127.0.0.1 내용:

scpCTF{vmfformfmfghlremrgktuTtmqslek}

확인

key: submit

[쪽지시험]

* 난이도: 중하

* 출제 의도

- Union SQL Injection에 대해 알고 있는지 확인한다.
- 구글링 능력을 키운다.



쪽지시험

난이도: 중하

Challenge

0 Solves

쪽지시험

점수미정

한 전공수업에서 쪽지시험을 보았다.

이 쪽지시험은 성적에 꽤 비중 있게 반영되는데...

이번학기가 끝날 때까지 점수를 알 수 없다.

내 등수를 알고 싶은데... 참을 수 없다!!

교수님의 아이디와 패스워드를 알아내야겠어!

아이디와 패스워드를 알아내려면,

SQL 연산자를 이용하라고 하던데..?

그 연산자가 뭐였지...?

<http://127.0.0.1/2.html>

scpCTF{...}

Submit

게시판 회원가입 로그인

게시판 회원가입 로그인

학사공지

전체 950건 | 현재 페이지 1/95

제목 ▼

검색어를 입력하세요

검색

번호	제목	작성부서	등록일	첨부파일	조회수
950	 2020년 2학기 수강철회 안내	학부행정실	2020/09/21		590
949	2020-2학기 등록금 분할신청(2차) 및 납부 안내	총무과(경리)	2020/09/16		201
948	2020-2학기 2차 등록금 납부 안내	총무과(경리)	2020/09/16		399
947	통합모집학부 입학자 학적이관 안내(학부 → 전공)	교무과	2020/09/16		264

아이디

dd

비밀번호

.....

비밀번호 확인

.....

이름

dd

이메일

dd@naver.com

가입

 중부대학교 | 통합로그인

통합 로그인

학번 또는 직번을 입력하세요

비밀번호를 입력하세요

로그인 >

비밀번호 찾기 >

게시판 회원가입 로그인

```
2.html x
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="UTF-8" />
5     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
6     <title>2</title>
7     <style>
8       body {
9         background-color: lightskyblue;
10        background-image: url("../hint.png");
11        background-repeat: repeat;
12        background-size: auto 100px;
13      }
14      div {
15        margin-top: 100px;
16        text-align: center;
17      }
18    </style>
19  }
20 </html>
```

{ } Line 1, Column 1

집합연산자

논리연산자우선순위

where 절

비교연산자

union

sql server

oracle db

sqld

mssql

결합연산자

오라클

산술연산자

연산

union a

구분	연산자	연산자의 의미
비교 연산자	=	같다.
	<	보다 작다.
	>	보다 크다.
	<=	보다 작거나 같다.
논리 연산자	<	보다 작다.
	>	보다 크다.
	<=	보다 작거나 같다.
	>=	보다 크거나 같다.
SQL 연산자	BETWEEN a AND b	a와 b의 값 사이에 있는 모든 값에 대한 범위 지정 (a와 b 값 포함)
	IN (a,b)	리스트에 있는 값 중에서 어느 하나라도 일치하면 참
	LIKE	패턴 문자열과 일치하는 문자열 찾기 (%, _ 사용)
	IS NULL	NULL 값인지 확인
논리 연산자	AND	두 조건 모두 참일 때만 참
	OR	두 조건 중 하나라도 참이면 참
	NOT	반대
	NOT BETWEEN a AND b	a와 b의 값 사이에 있지 않다.
비교 연산자	=	같다.
	<	보다 작다.
	>	보다 크다.
	<=	보다 작거나 같다.
SQL 연산자	BETWEEN a AND b	a와 b의 값 사이에 있는 모든 값에 대한 범위 지정 (a와 b 값 포함)
	IN (a,b)	리스트에 있는 값 중에서 어느 하나라도 일치하면 참
	LIKE	패턴 문자열과 일치하는 문자열 찾기 (%, _ 사용)
	IS NULL	NULL 값인지 확인

데이터 전문가 지식포털 DBGuide.net
dbguide.net

연산자	의미
BETWEEN a AND b	a와 b의 사이의 값, a, b도 포함
IN(a, b, c, ..., n)	a, b, c, ..., n 중의 하나와 일치하면 참
LIKE	문자 패턴과 부분적으로 일치(% ,_)하면 참
IS NULL	NULL 이면 참

오라클공부 167. SQL 연산자를 이용한 조건 검색
oraclejavastudy.tistory.com

구분	비교 방법
비교 연산자	값이 서로 다른 CHAR형 데이터는 작은 쪽에 SPACE를 추가하여 길이를 같게 한 후에 비교한다.

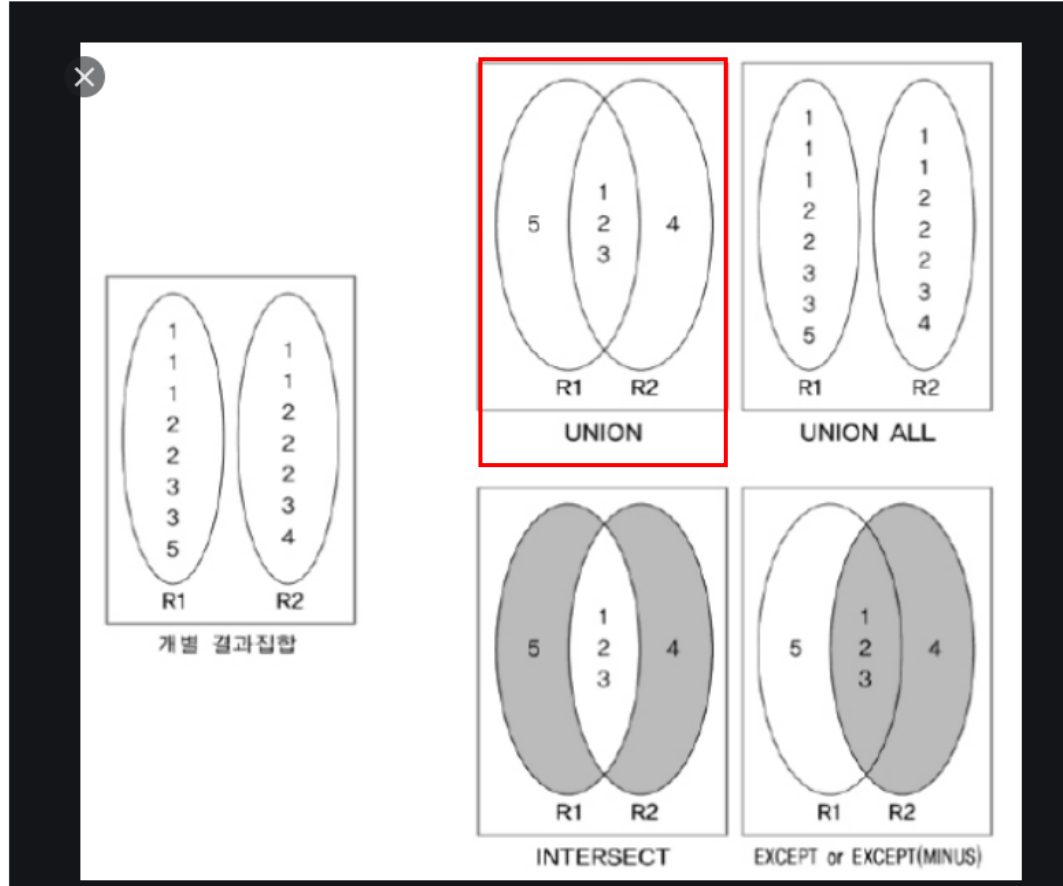
종류	연산자	연산자의 의미
비교 연산자	=	같다.
	<	보다 작다.
	>	보다 크다.
	<=	보다 작거나 같다.
논리 연산자	AND	두 조건 모두 참일 때만 참
	OR	두 조건 중 하나라도 참이면 참
	NOT	반대
	NOT BETWEEN a AND b	a와 b의 값 사이에 있지 않다.
SQL 연산자	BETWEEN a AND b	a와 b의 값 사이에 있는 모든 값에 대한 범위 지정 (a와 b 값 포함)
	IN (a,b)	리스트에 있는 값 중에서 어느 하나라도 일치하면 참
	LIKE	패턴 문자열과 일치하는 문자열 찾기 (%, _ 사용)
	IS NULL	NULL 값인지 확인

데이터 전문가 지식포털 DBGuide.net
dbguide.net

연산자	의미
BETWEEN a AND b	a와 b의 사이의 값, a, b도 포함
IN(a, b, c, ..., n)	a, b, c, ..., n 중의 하나와 일치하면 참
LIKE	문자 패턴과 부분적으로 일치(% ,_)하면 참
IS NULL	NULL 이면 참

데이터 전문가 지식포털 DBGuide.net
dbguide.net

구분	비교 방법
비교 연산자	값이 서로 다른 CHAR형 데이터는 작은 쪽에 SPACE를 추가하여 길이를 같게 한 후에 비교한다.



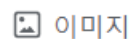
게시판 회원가입 로그인



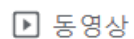
sql union 아이디 비밀번호



전체



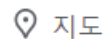
이미지



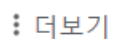
동영상



뉴스



지도



더보기

설정

도구

검색결과 약 16,800개 (0.44초)

blog.naver.com > PostView ▾

UNION SQL INJECTION : 네이버 블로그

2018. 10. 3. - ' **UNION** SELECT 1,concat(id,login),password,email,secret,6,7 from users# 이라고 쿼리를 날리고 결과를 확인하면 id는 회원 순서, login은 아이디, ...

peemangit.tistory.com > ... ▾

[Web Hacking & Security] SQL Injection 공격 - 피망IT - 티스토리

2020. 1. 6. - 사용자가 서버에 제출한 데이터가 **SQL** Query로 사용되어 Database나. ... query문을 이용하여 정상적인 사용자 ID와 패스워드를 입력하지 않고 로그인 ... **UNION**을 이용하여 mismatch를 발생시켜 Select 구문에 사용된 Field의 개수 ...



Union SQL Injection이란?

두 개의 쿼리문에 대한 결과를 통합해서 하나의 테이블로 보여주게 하는 방식

city	country
<u>pari</u>	France

A



SELECT city, country FROM 테이블 A

UNION

SELECT city, country FROM 테이블 B;

city	country
London	U.K

B



City	Country
Pari	London
France	<u>u.k</u>

게시판 회원가입 로그인

NOTICE

테이블 이름

No		title	writer	date	hit
1	ㄱ		song21677	2019-10-21 03:54:05	0

칼럼 이름

글쓰기

제목 ▼

ㄱ

×

검색

게시판 회원가입 로그인

```
50 <form method="post" action="member.php">
51   <div>
52     아이디 <br />
53     <input type="text" name="ID" />
54   </div> <br />
55   <div>
56     비밀번호 <br />
57     <input type="password" name="pass" />
58   </div> <br />
59   <div>
60     비밀번호 확인<br />
61     <input type="password" name="pass_check"/>
62   </div> <br />
63   <div>
64     이름 <br />
65     <input type="text" name="name" />
66   </div> <br />
67   <div>
68     이메일 <br />
69     <input type="text" name="email" />
70 </div><br /><br />
71   <div>
72     <input type="submit" value="가입" />
73   </div>
74 </form>
```

테이블 이름

칼럼 이름

게시판 회원가입 로그인

NOTICE

No		title	writer	date	hit
1	↗		song21677	2019-10-21 03:54:05	0
					글쓰기

제목 ▾

' UNION SELECT ",", ", id, ", pass, name, email FROM member # ✕

검색

게시판 회원가입 로그인

Id

pass

writer

email

dd

123456

dd

dd@naver.com

sjyoo

scpCTF{tjdrhd!}

유승재

sjyoo@jbm.ac.kr

hehe

12345

hehe

hehe@naver.com

song21677

dddd

허송이

song21677@naver.com

글쓰기



감사합니다(:
님