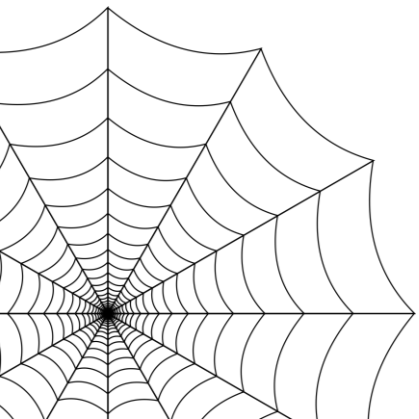
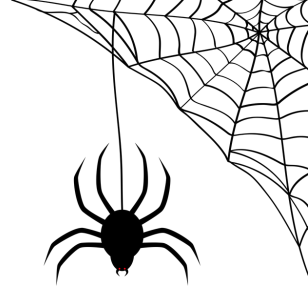


WEB Hacking

웹해킹 교육 3회차

18학번 서연주





<목차>

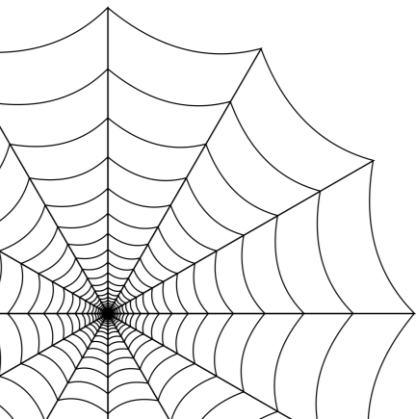
< 00. 시작하기 전에 />

< 01. Basic />

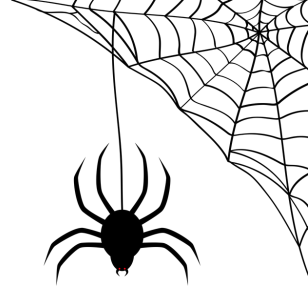
< 02. Practice />

< 03. 마무리 />

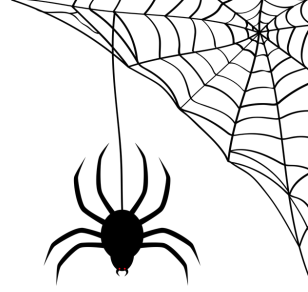
</목차>



00. 시작하기 전에



00. 시작하기 전에



< 2주차 과제 >

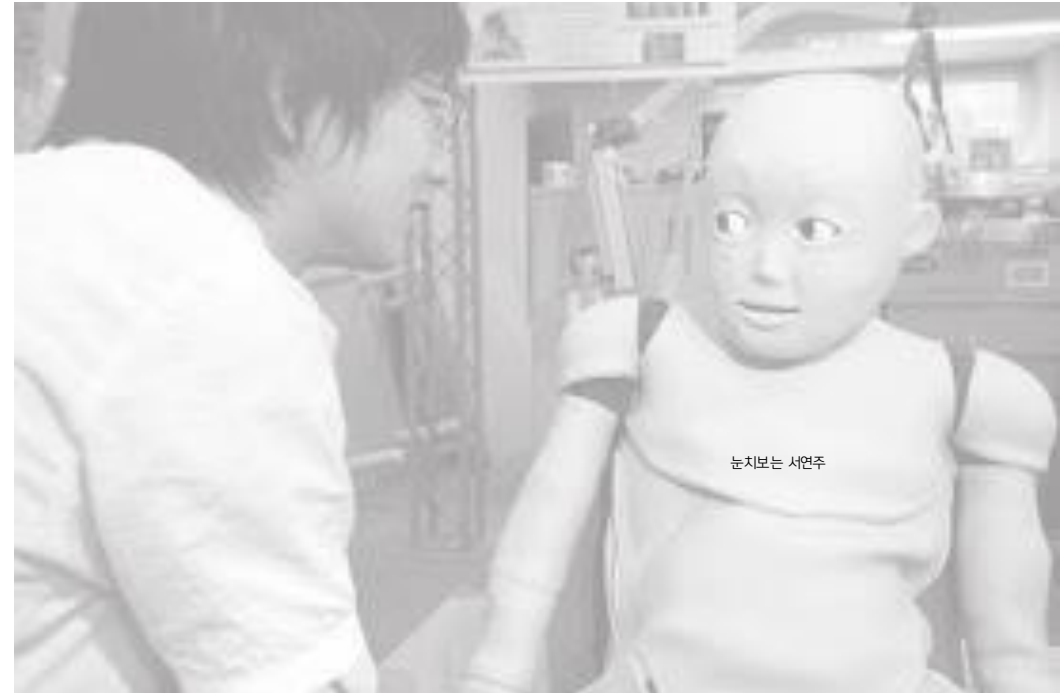
MySQL연동, POST, Session을 이용하여 로그인/로그아웃 기능 구현

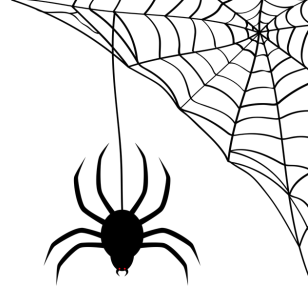
어려웠나요...?

하다가 모르시는게 있거나, 잘 안되신다면 언제든지 연락해주세요!!!

혼자 끄끄 앓는 것보다, 같이 끄끄 앓아봅시다

무슨말이지





⟨01 /⟩

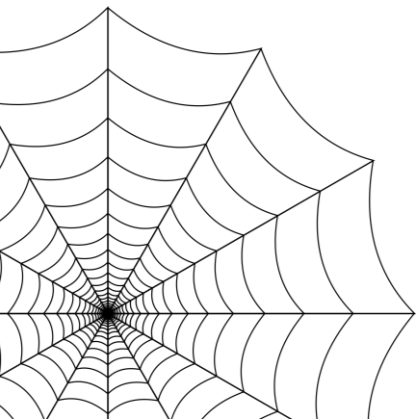
⟨Basic⟩

⟨ Web Hacking /⟩

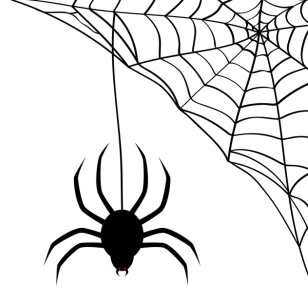
⟨ Encoding & Decoding /⟩

⟨ Tool /⟩

⟨/Basic⟩



01. Basic – Web Hacking



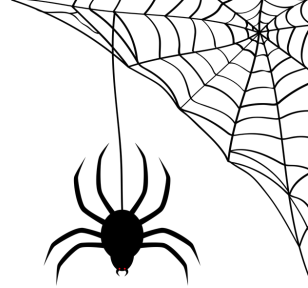
: 웹 사이트의 취약점을 공격하는 기술적 위협,
웹 페이지를 통하여 권한이 없는 시스템에 접근하거나 데이터 유출 및 파괴와 같은 행위

- 해킹 결과를 바로 확인할 수 있음
- 손쉬운 도구, 관련 자료가 많음
- 침입 탐지/차단 시스템, 웹 방화벽 등의 보안 솔루션으로 방어하기 어려움

ex) 고객정보 유출, 계정 도용...

ex) 사이버 캠퍼스 기간 지난 싸강 수강완료로 바꾸기, 수강하지 않는 과목 자료 보기

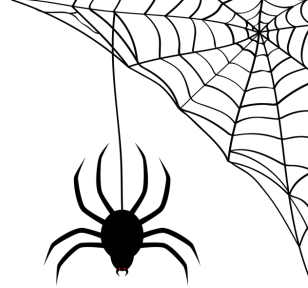
01. Basic – Web Hacking



주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며,
10대 웹 애플리케이션의 취약점 (OWASP TOP 10)을 발표

OWASP Top 10 – 2013(이전)	OWASP Top 10 – 2017(신규)
A1 – 인젝션	A1 – 인젝션
A2 – 인증 및 세션 관리 취약점	A2 – 인증 및 세션 관리 취약점
A3 – 크로스 사이트 스크립팅(XSS)	A3 – 크로스 사이트 스크립팅(XSS)
A4 – 취약한 직접 개체 참조 – A7 통합	A4 – 취약한 접근 제어 (Original category in 2003 2004)
A5 – 보안 설정 오류	A5 – 보안 설정 오류
A6 – 민감 데이터 노출	A6 – 민감 데이터 노출
A7 – 기능 수준의 접근통제 누락	A7 – 공격 방어 취약점(신규)
A8 – 크로스사이트 요청 변조(CSRF)	A8 – 크로스사이트 요청 변조(CSRF)
A9 – 알려진 취약점 있는 컴포넌트 사용	A9 – 알려진 취약점 있는 컴포넌트 사용
A10 – 검증되지 않은 리다이렉트 포워드	A10 – 취약한 API(신규)

01. Basic – Web Hacking



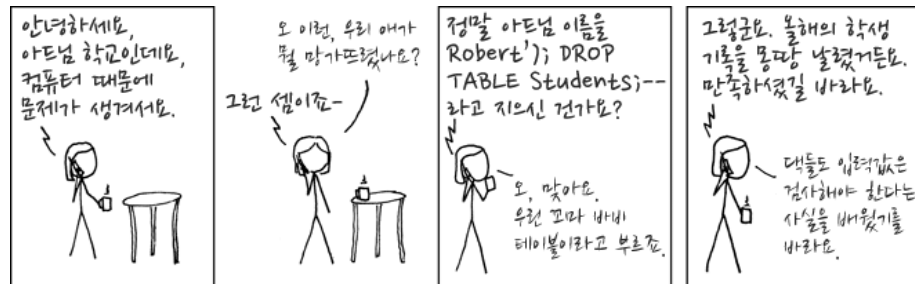
1. Injection

: 공격자에 의해서 취약한 코드를 삽입하고 실행을 변경 → 데이터 손실이나 오염, DoS를 야기

-SQL Injection

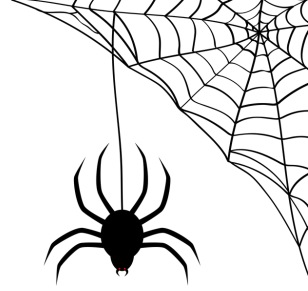
: Structured Query Language

악의적인 SQL문을 실행되게 하여 데이터베이스를 비정상적으로 조작



CC BY-NC 2.5 / 출처 : <http://xkcd.com/327/>

01. Basic – Web Hacking



1=1은 항상 참이기에, 맞는 pw를 치지 않아도!!

```
$username = $_POST["username"];  
$password = $_POST["password"];  
$mysqli->query("SELECT * FROM users WHERE username='{$username}' AND password='{$password}'");
```

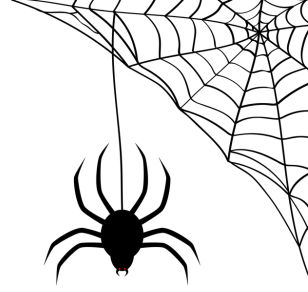
(정상 쿼리문)



```
SELECT * FROM users WHERE username='admin' and password='' OR '1'='1';
```

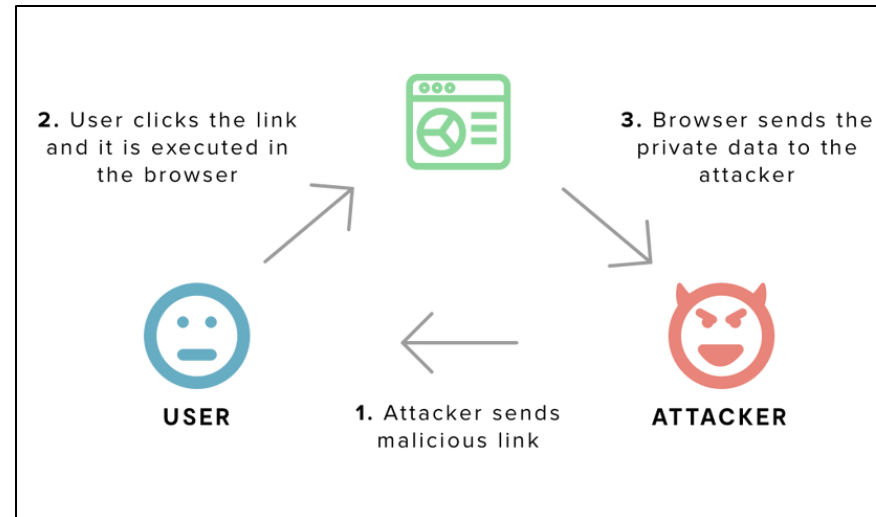
(악의적 SQL문)

01. Basic – Web Hacking

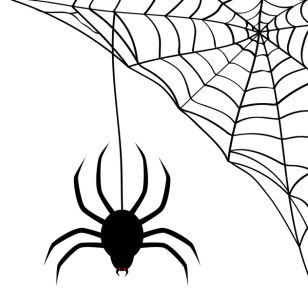


2. 인증 및 세션 관리 취약점

: 인증, 세션 관리와 관련된 기능이 정확하게 구현되어 있지 않아,
공격자가 패스워드, 키 또는 쿠키, 세션 토큰을 해킹하여 인증을 우회
→다른 사용자 ID로 가장



01. Basic - Web Hacking

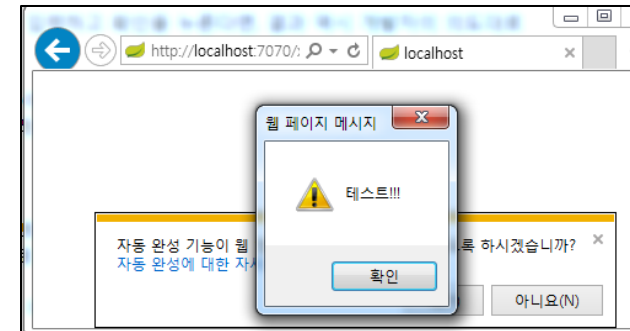
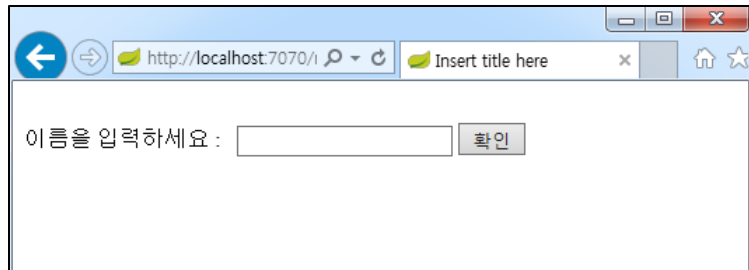


3. XSS (크로스 사이트 스크립팅)

: 게시판 등 사용자의 글쓰기 기능이 존재하는 곳(동적인 HTML페이지) 에 악의적인 목적의 스크립트 삽입

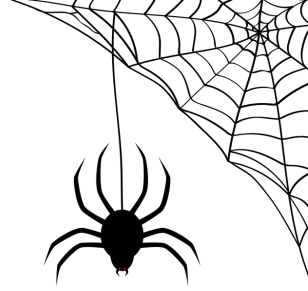
→ 사용자 정보 획득

→ 사용자를 대상으로 한 공격



<https://www.leafcats.com/42>

01. Basic – Encoding & Decoding



Encoding

문자 → 다른 형태나 형식 (컴퓨터가 이해할 수 있는 방식)
(내용에는 변화없이)

정보의 표준화, 보안, 처리 속도 향상, 저장 공간 절약 등

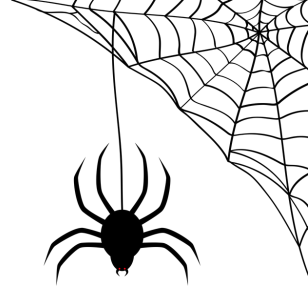
Hello World!



SGVsbG8gV29ybGQh

Decoding

01. Basic - Encoding & Decoding



1. URL Encoding (퍼센트 인코딩)

URL에 문자를 표현하는 문자 인코딩 방법

- 알파벳이나 숫자 등 몇몇 문자를 제외한 값은 특정 단위로 묶어서, 16진수 값으로 인코딩
- 기존 문자열의 HEX값 앞에 % 사용

argos서연주

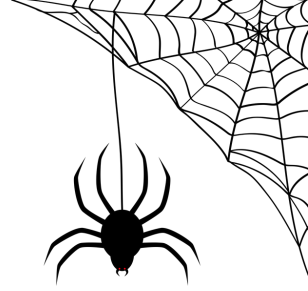


argos%ec%84%9c%ec%97%b0%ec%a3%bc

Url decode, encode해주는 사이트 :

<https://www.convertstring.com/ko/EncodeDecode/UrlEncode>

01. Basic - Encoding & Decoding



2. Base64 Encoding (= 인코딩)

8비트 이진 데이터를 공통 ASCII 영역의 문자들로만 이루어진 일련의 문자열로 바꾸는 인코딩 방식

- 마지막 '='으로 base64인걸 확인

(문자열→ASCII→6bit cut→base64_encode (여기서 남는 비트를 채우기 위해 paddin으로 =))

argos서연주

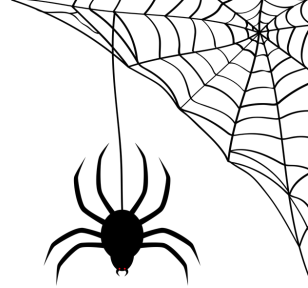


YXJnb3PshJzsl7Dso7wNCg==

Base64 decode, encode해주는 사이트 :

<https://www.convertstring.com/ko/EncodeDecode/Base64Encode>

01. Basic - Tool(설치)

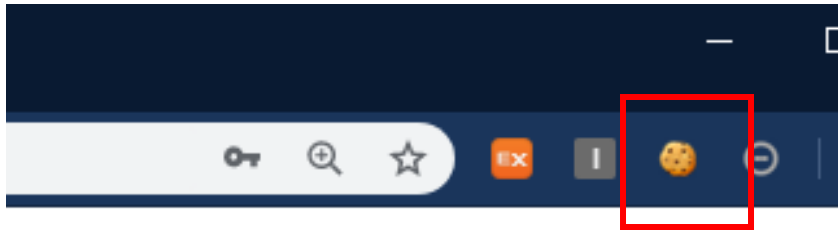


1. EditThisCookie

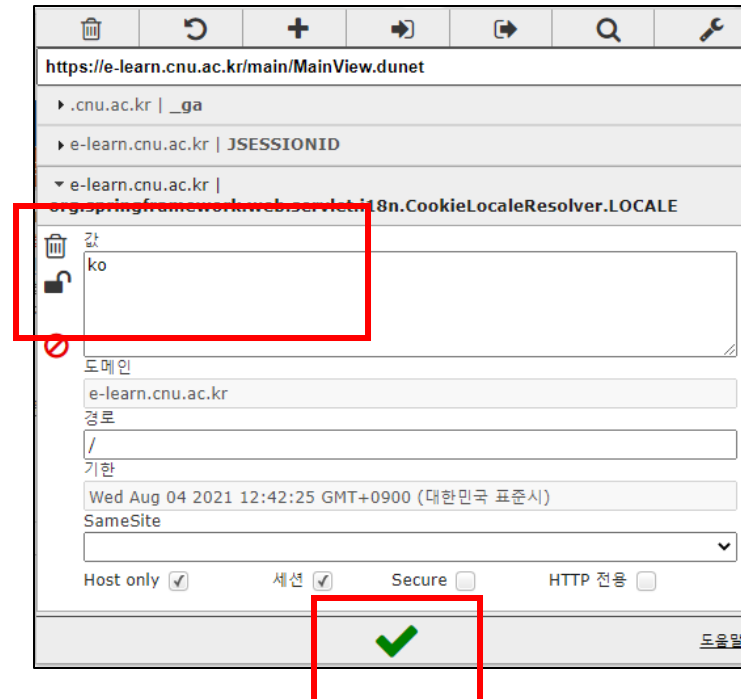
: Chrome 확장 프로그램, 쿠키값을 추가, 편집



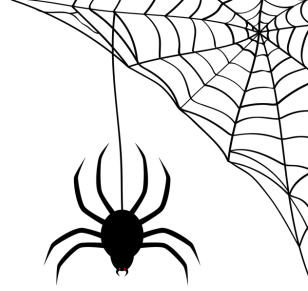
<https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg>



설치 후 북마크 바에서 확인!!



01. Basic - Tool(설치)



2. Falcon Proxy

: proxy = 대리인

브라우저와 인터넷 서버 사이에서 서버의 기능을 대신해주는 중계 역할 서버

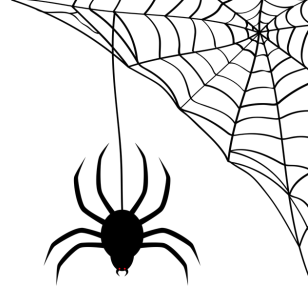
[브라우저에서 서버로 요청 : 브라우저 → 프록시 서버 → 서버]

- 인터넷 속도 향상
- 자신을 숨기거나 보안을 뚫을 때 사용

브라우저의 요청정보, 서버의 응답정보를 상세히 확인 가능
또한 서버로 전송되는 정보 변경 가능

<https://chrome.google.com/webstore/detail/falcon-proxy/gchhimlnjdafdlkojbffdkogjhhkdepf>

사용법 : <https://gsk121.tistory.com/409>



<02/>

<Practice>

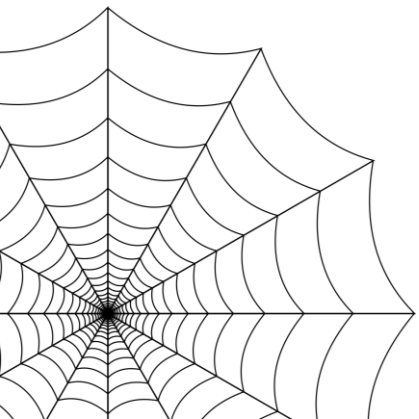
< 실습1 />

< 실습2 - no.1 />

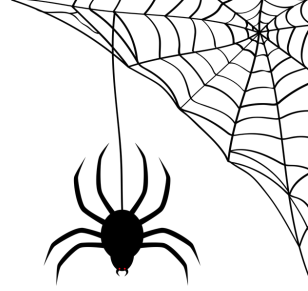
<실습3 - no.14 />

<실습4 - sql injection />

</Practice>



02. Practice



*** 주의 ***

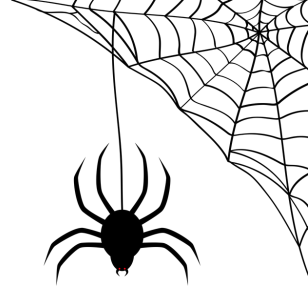
공부, 장난 등의 어떠한 이유로든
서비스 중인 웹 사이트를 공격?

항상 조심하자

툴 사용 또한 조심스럽게



02. Practice - 공부 사이트

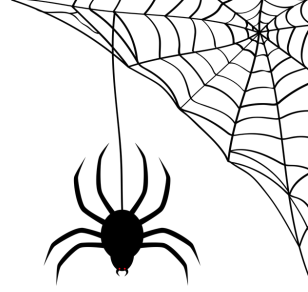


다양한 wargame 사이트

- webhacking.kr
- suninatas.com
- wargame.kr
- www.hackthissite.org/
- www.hacker.org/

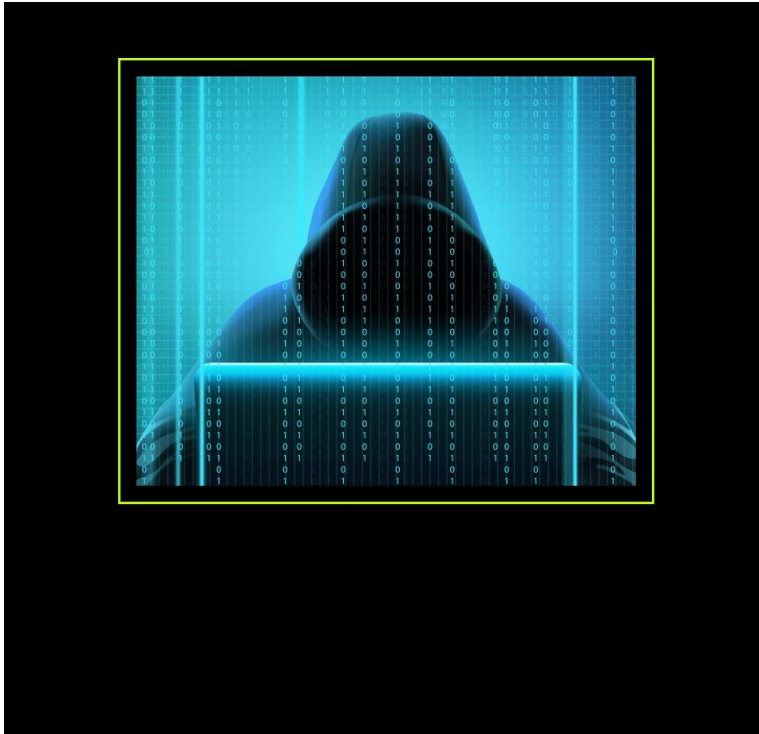
: 웹해킹을 공부할수있는 게임 사이트

02. Practice – 실습1



워게임 사이트에서 풀어보기 전에, 준비한 기본 문제

edu.argos.or.kr/~hololo/3/playground.html 로 접속

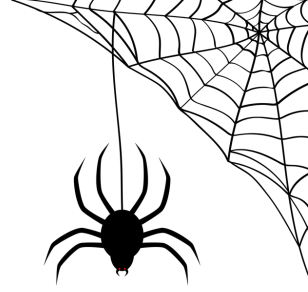


힌트

- 개발자 도구를 이용하라
- 개발자 도구를 열어 HTML을 Edit할 수 있음

제 1 페이지

02. Practice – 실습1



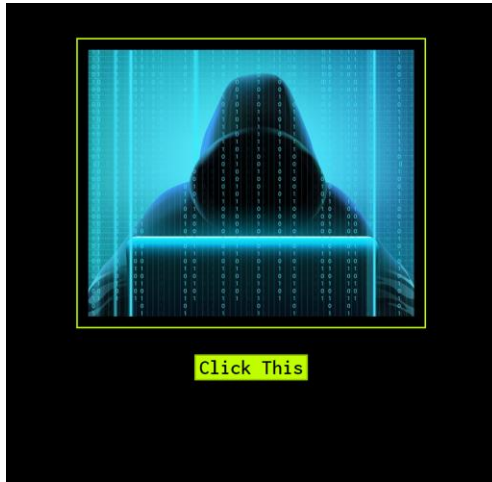
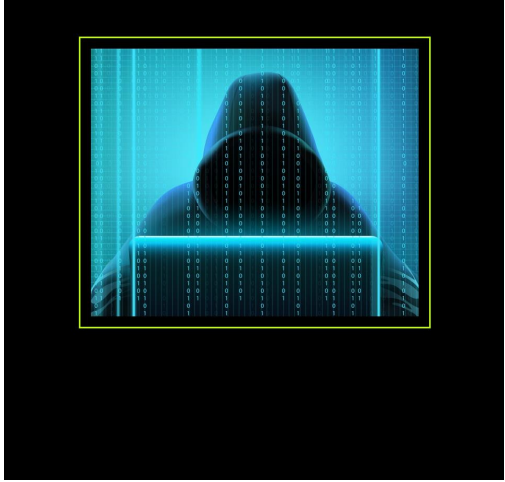
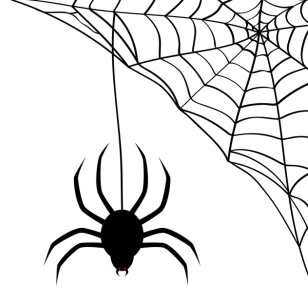
I love Cookie!!??

but now cookie is rotten...

힌트

- cookie가 썩었다?
- 앞에서 설치한 tool을 이용하라
- %는 무슨 Encoding? =은 무슨 Encoding?

02. Practice – 실습1(풀이)

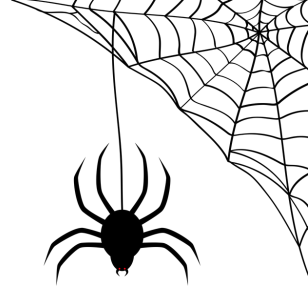


Click This

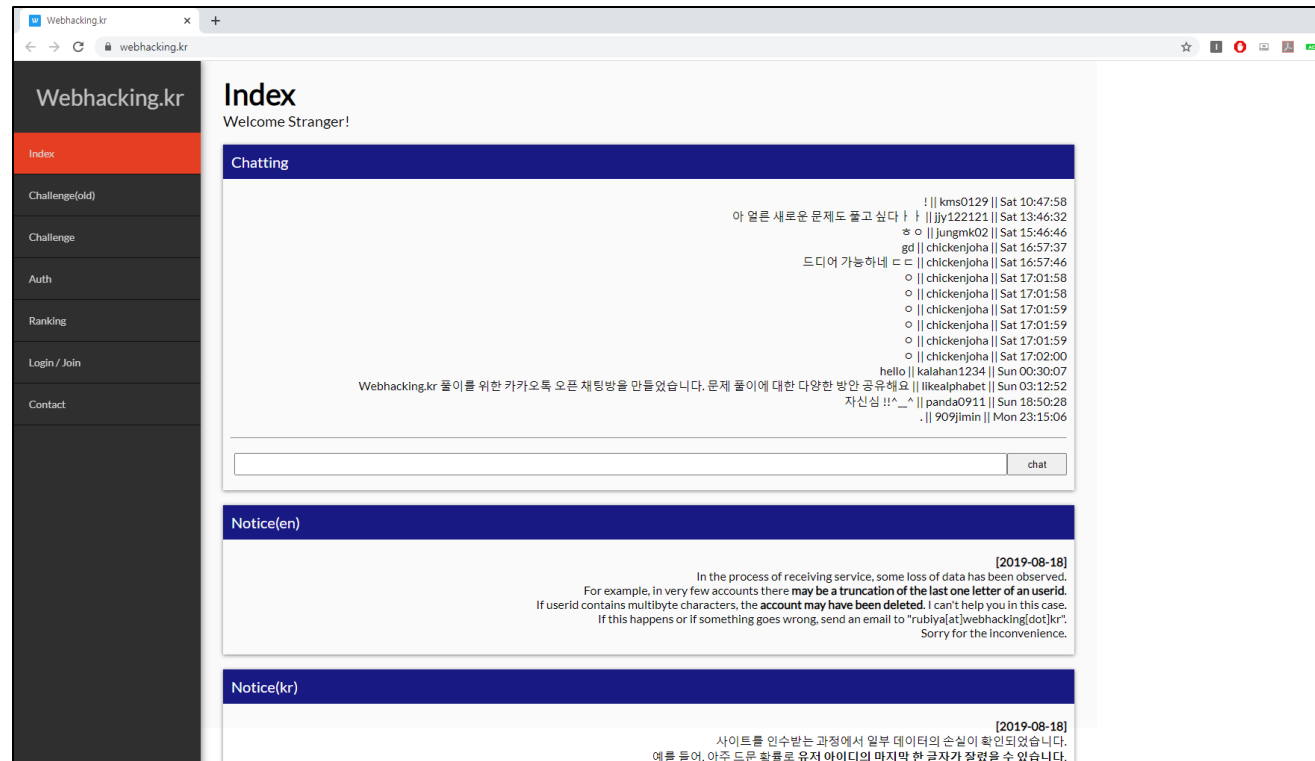
I love Cookie!!??
but now cookie is rotten...

Ha[keD
by
4RG0S

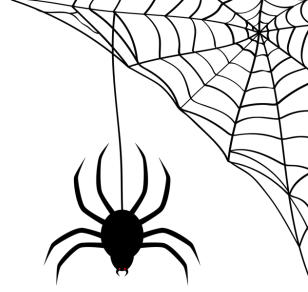
02. Practice – 실습2(no.1)



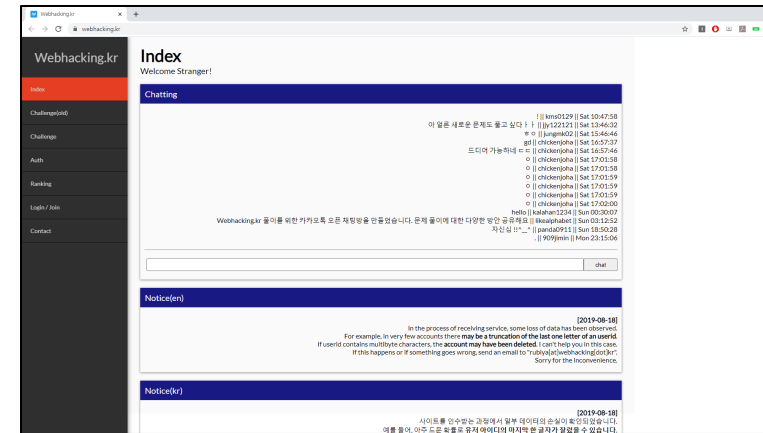
난이도도 다양하고, 좋은 문제들이 많음
웹해킹 입문자들이 많이 이용하는 사이트



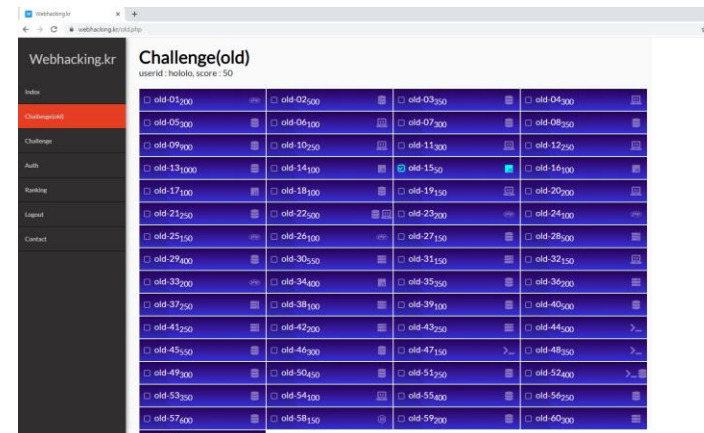
02. Practice – 실습2(no.1)



원래는 webhacking.kr이라는 사이트에서 첫 가입부터 해킹문제
그렇지만...이젠...



-----Challenges-----					
prob1	prob2	prob3	prob4	prob5	prob6
prob7	prob8	prob9	prob10	prob11	prob12
prob13	prob14	prob15	prob16	prob17	prob18
prob19	prob20	prob21	prob22	prob23	prob24
prob25	prob26	prob27	prob28	prob29	prob30
prob31	prob32	prob33	prob34	prob35	prob36
prob37	prob38	prob39	prob40	prob41	prob42
prob43	prob44	prob45	prob46	prob47	prob48
prob49	prob50	prob51	prob52	prob53	prob54
prob55	prob56	prob57	prob58	prob59	prob60
Score : 17350	[300]	[200]	[150]	[400]	[500]
Rank : 110					



02. Practice – 실습2(no.1)

가입합시다!!

<https://webhacking.kr/>

Webhacking.kr

Index

Welcome Stranger!

Chatting

! || kms0129 || Sat 10:47:58
아 열린 새로운 문제도 풀고 싶다 || jjy122121 || Sat 13:46:32
ㅎㅇ || jungmk02 || Sat 15:46:46
gd || chickenjoha || Sat 16:57:37
드디어 가능하네 ㄷㄷ || chickenjoha || Sat 16:57:46
o || chickenjoha || Sat 17:01:58
o || chickenjoha || Sat 17:01:58
o || chickenjoha || Sat 17:01:59
o || chickenjoha || Sat 17:01:59
o || chickenjoha || Sat 17:01:59
o || chickenjoha || Sat 17:02:00
hello || kalahan1234 || Sun 00:30:07
Webhacking.kr 풀이를 위한 카카오톡 오픈 채팅방을 만들었습니다. 문제 풀이에 대한 다양한 방안 공유해요 || likealphabet || Sun 03:12:52
자신심 !!^_^ || panda0911 || Sun 18:50:28
. || 909jimin || Mon 23:15:06

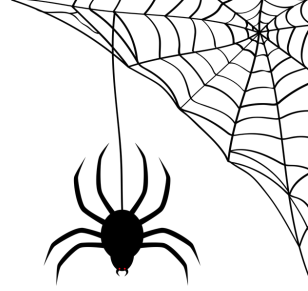
Notice(en)

[2019-08-18]
In the process of receiving service, some loss of data has been observed.
For example, in very few accounts there **may be a truncation of the last one letter of an userid**.
If userid contains multibyte characters, the **account may have been deleted**. I can't help you in this case.
If this happens or if something goes wrong, send an email to "rubiya[at]webhacking[dot]kr".
Sorry for the inconvenience.

Notice(kr)

[2019-08-18]
사이트를 인수받는 과정에서 일부 데이터의 손실이 확인되었습니다.

02. Practice – 실습2(no.1)



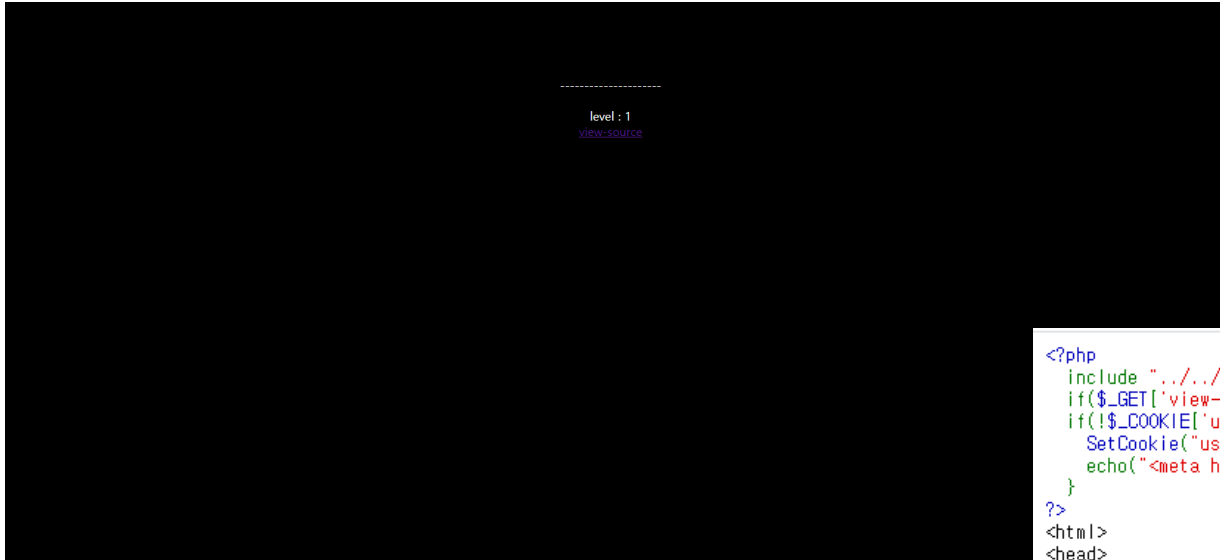
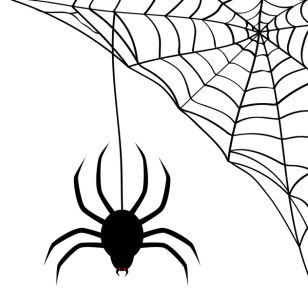
Webhacking.kr Challenge(old)

userid : hololo, score : 50

<input type="checkbox"/> old-01 ₂₀₀	<input type="checkbox"/> old-02 ₅₀₀	<input type="checkbox"/> old-03 ₃₅₀	<input type="checkbox"/> old-04 ₃₀₀
<input type="checkbox"/> old-05 ₃₀₀	<input type="checkbox"/> old-06 ₁₀₀	<input type="checkbox"/> old-07 ₃₀₀	<input type="checkbox"/> old-08 ₃₅₀
<input type="checkbox"/> old-09 ₉₀₀	<input type="checkbox"/> old-10 ₂₅₀	<input type="checkbox"/> old-11 ₃₀₀	<input type="checkbox"/> old-12 ₂₅₀
<input type="checkbox"/> old-13 ₁₀₀₀	<input type="checkbox"/> old-14 ₁₀₀	<input checked="" type="checkbox"/> old-15 ₅₀	<input type="checkbox"/> old-16 ₁₀₀
<input type="checkbox"/> old-17 ₁₀₀	<input type="checkbox"/> old-18 ₁₀₀	<input type="checkbox"/> old-19 ₁₅₀	<input type="checkbox"/> old-20 ₂₀₀
<input type="checkbox"/> old-21 ₂₅₀	<input type="checkbox"/> old-22 ₅₀₀	<input type="checkbox"/> old-23 ₂₀₀	<input type="checkbox"/> old-24 ₁₀₀
<input type="checkbox"/> old-25 ₁₅₀	<input type="checkbox"/> old-26 ₁₀₀	<input type="checkbox"/> old-27 ₁₅₀	<input type="checkbox"/> old-28 ₅₀₀
<input type="checkbox"/> old-29 ₄₀₀	<input type="checkbox"/> old-30 ₅₅₀	<input type="checkbox"/> old-31 ₁₅₀	<input type="checkbox"/> old-32 ₁₅₀
<input type="checkbox"/> old-33 ₂₀₀	<input type="checkbox"/> old-34 ₄₀₀	<input type="checkbox"/> old-35 ₃₅₀	<input type="checkbox"/> old-36 ₂₀₀
<input type="checkbox"/> old-37 ₂₅₀	<input type="checkbox"/> old-38 ₁₀₀	<input type="checkbox"/> old-39 ₁₀₀	<input type="checkbox"/> old-40 ₅₀₀
<input type="checkbox"/> old-41 ₂₅₀	<input type="checkbox"/> old-42 ₂₀₀	<input type="checkbox"/> old-43 ₂₅₀	<input type="checkbox"/> old-44 ₅₀₀
<input type="checkbox"/> old-45 ₅₅₀	<input type="checkbox"/> old-46 ₃₀₀	<input type="checkbox"/> old-47 ₁₅₀	<input type="checkbox"/> old-48 ₃₅₀
<input type="checkbox"/> old-49 ₃₀₀	<input type="checkbox"/> old-50 ₄₅₀	<input type="checkbox"/> old-51 ₂₅₀	<input type="checkbox"/> old-52 ₄₀₀
<input type="checkbox"/> old-53 ₃₅₀	<input type="checkbox"/> old-54 ₁₀₀	<input type="checkbox"/> old-55 ₄₀₀	<input type="checkbox"/> old-56 ₂₅₀
<input type="checkbox"/> old-57 ₆₀₀	<input type="checkbox"/> old-58 ₁₅₀	<input type="checkbox"/> old-59 ₂₀₀	<input type="checkbox"/> old-60 ₃₀₀
<input type="checkbox"/> old-61 ₂₀₀			

엄청 많은 문제들(old), 배점도 다양

02. Practice – 실습2(no.1)

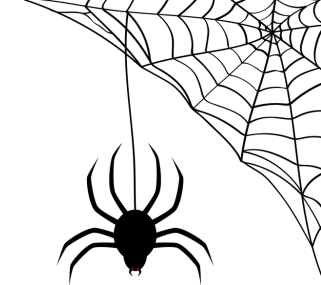


뭘 할지 모르겠다? → 페이지 소스

이지만, 현재는 source를 줌

```
<?php
include "../././config.php";
if($_GET['view-source'] == 1){ view_source(); }
if(!$_COOKIE['user_lv']){
    SetCookie("user_lv","1",time()+86400*30,"/challenge/web-01/");
    echo("<meta http-equiv=refresh content=0>");
}
?>
<html>
<head>
<title>Challenge 1</title>
</head>
<body bgcolor=black>
<center>
<br><br><br><br><br>
<font color=white>
-----<br>
<?php
if(!is_numeric($_COOKIE['user_lv'])) $_COOKIE['user_lv']=1;
if($_COOKIE['user_lv']>=6) $_COOKIE['user_lv']=1;
if($_COOKIE['user_lv']>5) solve(1);
echo "<br>level : ".$_COOKIE['user_lv'];
?>
<br>
<a href=./?view-source=1>view-source</a>
</body>
</html>
```

02. Practice – 실습2(no.1)



우리가 왜 Front-End언어를 자세히 배웠는가?

- 페이지 소스 분석
- 정답 찾기 / 해킹

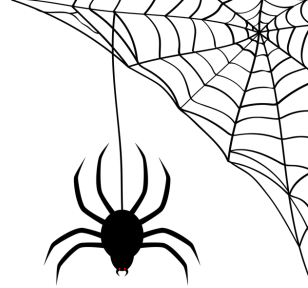
```
<?php
include "../././config.php";
if($_GET['view-source'] == 1){ view_source(); }
if(!$_COOKIE['user_lv']){
    SetCookie("user_lv","1",time()+86400*30,"/challenge/web-01/");
    echo("<meta http-equiv=refresh content=0>");
}
?>
<html>
<head>
<title>Challenge 1</title>
</head>
<body bgcolor=black>
<center>
<br><br><br><br><br>
<font color=white>
-----<br>
<?php
    if(!is_numeric($_COOKIE['user_lv'])) $_COOKIE['user_lv']=1;
    if($_COOKIE['user_lv']>=6) $_COOKIE['user_lv']=1;
    if($_COOKIE['user_lv']>5) solve(1);
    echo "<br>level : {$_COOKIE['user_lv']}";
?>
<br>
<a href=./?view-source=1>view-source</a>
</body>
</html>
```

source code

페이지 소스를 보면 우리가 해야 할 것

- 1) solve라는 함수나, flag를 보여줄 만한 함수/부분 찾기
- 2) 1주위의 코드 분석
- 3) 모르는 함수가 있으면 구글링해서
어떤 함수인지 / 어떤 인자가 필요한지 공부

02. Practice – 실습2(no.1)



```
<?php
include "../././config.php";
if($_GET['view-source'] == 1){ view_source(); }
if(!$_COOKIE['user_lv']){
    SetCookie("user_lv", "1", time()+86400*30, "/challenge/web-01/");
    echo("<meta http-equiv=refresh content=0>");
}
```

```
?>
<html>
<head>
<title>Challenge 1</title>
</head>
<body bgcolor=black>
<center>
<br><br><br><br><br>
<font color=white>
-----<br>
```

```
<?php
if(!is_numeric($_COOKIE['user_lv'])) $_COOKIE['user_lv']=1;
if($_COOKIE['user_lv']>=6) $_COOKIE['user_lv']=1;
if($_COOKIE['user_lv']>5) solve(1);
echo "<br>level : {$_COOKIE['user_lv']}";
?>
<br>
<a href=./?view-source=1>view-source</a>
</body>
</html>
```

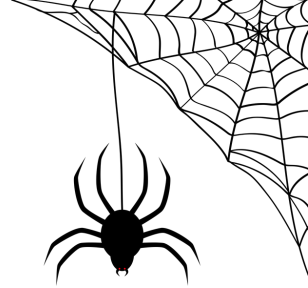
분석의 방향

'user_lv'라는 쿠키가 없으면 생성
setCookie함수 사용

solve(1)

\$_COOKIE['user_lv']>5

02. Practice – 실습2(no.1)



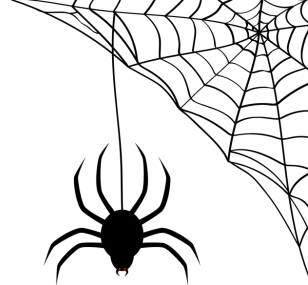
```
<?php
include "../config.php";
if($_GET['view-source'] == 1){ view_source(); }
if(!$_COOKIE['user_lv']){
    SetCookie("user_lv", "1", time()+86400*30, "/challenge/web-01/");
    echo("<meta http-equiv=refresh content=0>");
}
?>
<html>
<head>
<title>Challenge 1</title>
</head>
<body bgcolor=black>
<center>
<br><br><br><br><br>
<font color=white>
```

```
-----<br>
<?php
if(!is_numeric($_COOKIE['user_lv'])) $_COOKIE['user_lv']=1;
if($_COOKIE['user_lv']>=6) $_COOKIE['user_lv']=1;
if($_COOKIE['user_lv']>5) solve(1);
echo "<br>level : {$_COOKIE['user_lv']}";
?>
<br>
```

```
<a href=./?view-source=1>view-source</a>
</body>
</html>
```

‘user_lv’라는 쿠키가 6이상이면 1을 넣어줌
5초과면 solve()?

02. Practice – 실습2(no.1)



```
<?php
include "../config.php";
if($_GET['view-source'] == 1){ view_source(); }
if(!$_COOKIE['user_lv']){
    SetCookie("user_lv", "1", time()+86400*30, "/challenge/web-01/");
    echo("<meta http-equiv=refresh content=0>");
}
?>
<html>
<head>
<title>Challenge 1</title>
</head>
<body bgcolor=black>
<center>
<br><br><br><br><br>
<font color=white>
-----<br>
<?php
    if(!is_numeric($_COOKIE['user_lv'])) $_COOKIE['user_lv']=1;
    if($_COOKIE['user_lv']>=6) $_COOKIE['user_lv']=1;
    if($_COOKIE['user_lv']>5) solve(1);
    echo "<br>level : {$_COOKIE['user_lv']}";
?>
<br>
<a href=./?view-source=1>view-source</a>
</body>
</html>
```

source code

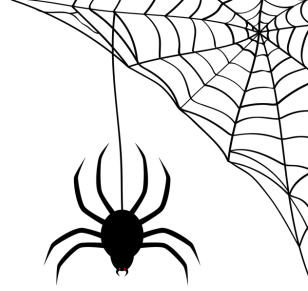
풀 수 있습니다!!

(오히려 앞에서 풀었던 문제보다 쉬울 수도..?)

힌트

- 앞에서 썼던 tool?
- 숫자 장난
- 숫자엔 자연수 뿐만 아니라…?

02. Practice – 실습2(no.1)



https://webhacking.kr/challenge/web-01/

webhacking.kr | PHPSESSID

webhacking.kr | user_iv

도메인: webhacking.kr

경로: /challenge/web-01/

기한: Thu Sep 03 2020 12:56:42 GMT+0900 (대한민국 표준시)

SameSite: Strict

Host only ☒ 세션 ☐ Secure ☐ HTTP 전용 ☐

webhacking.kr 내용:

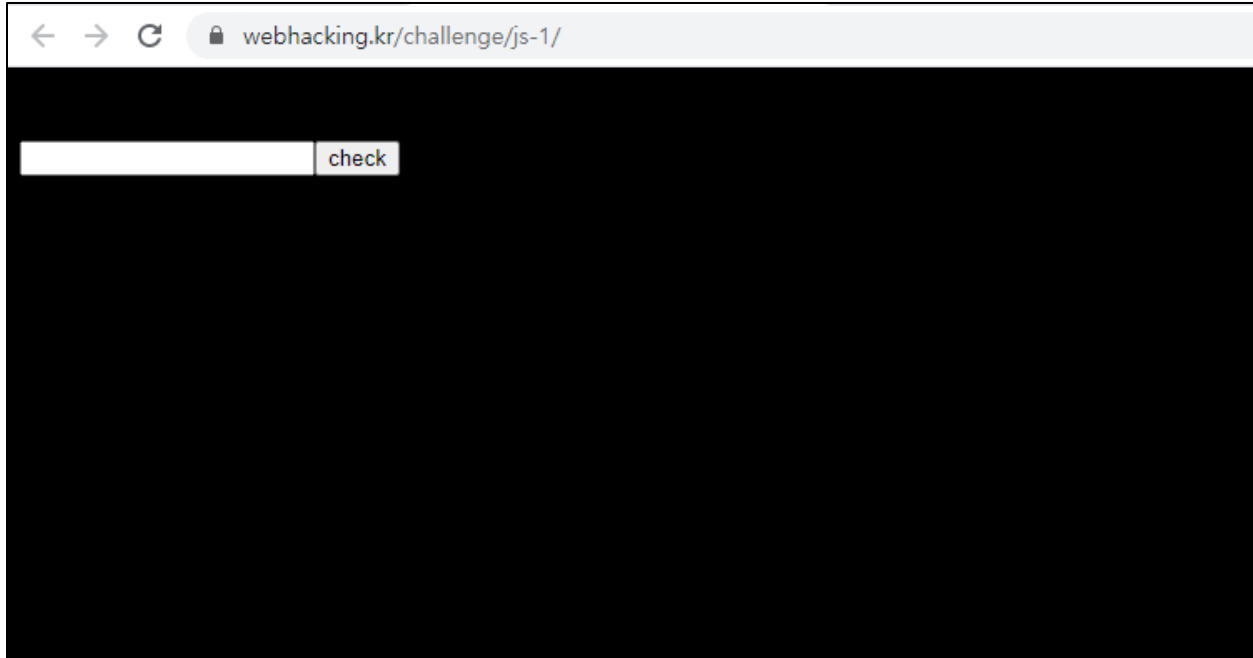
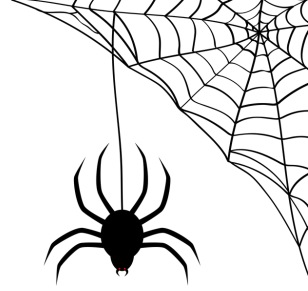
old-01 Pwned!

확인

old-01 Pwned. You got 200point. Congratz!

level : 5.5
[view-source](#)

02. Practice – 실습3(no.14)

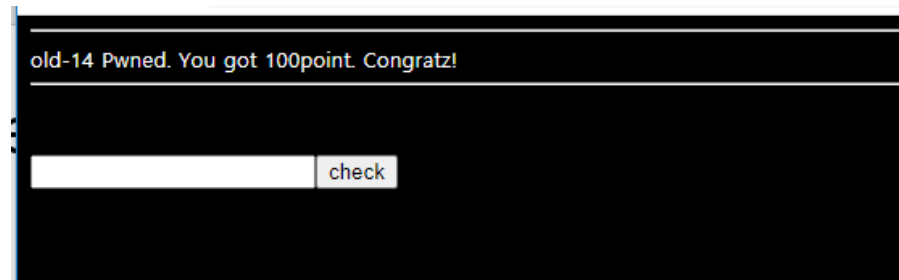
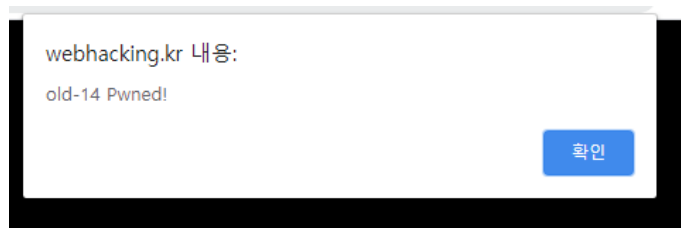


또 다른 문제!!

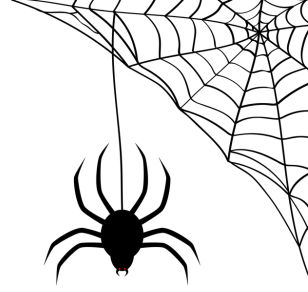
이번엔 혼자 먼저 풀어봅시다!!

힌트

- 항상 '개발자 도구' 를 이용
- 이번엔 console창을 써볼까..

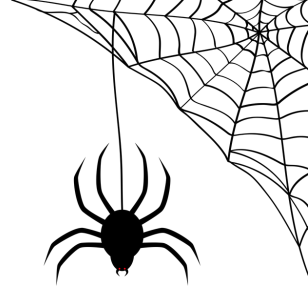


02. Practice – 실습3(no.14)



```
Elements Console Sources Network Performance Memory Application Security
<html>
  <head>...</head>
  <body cz-shortcut-listen="true"> == $0
    <br>
    <br>
    <form name="pw">
      <input type="text" name="input_pwd">
      <input type="button" value="check" onclick="ck()">
    </form>
    <script>
      function ck(){
        var ul=document.URL;
        ul=ul.indexOf(".kr");
        ul=ul*30;
        if(ul==pw.input_pwd.value) { location.href="?" + ul * pw.input_pwd.value; }
        else { alert("Wrong"); }
      }
    </script>
  </body>
</html>
```

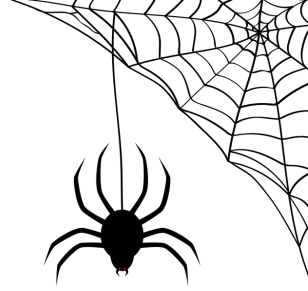
02. Practice – 실습3(no.14)



```
Elements  Console  Sources  Network  Performance  Memory  Application  Security

<html>
  <head>...</head>
  <body cz-shortcut-listen="true"> == $0
    <br>
    <br>
    <form name="pw">
      <input type="text" name="input_pwd">
      <input type="button" value="check" onclick="ck()">
    </form>
    <script>
      function ck(){
        var ul=document.URL;
        ul=ul.indexOf(".kr");
        ul=ul*30;
        if(ul==pw.input_pwd.value) { location.href="?" + ul * pw.input_pwd.value; }
        else { alert("Wrong"); }
      }
    </script>
  </body>
</html>
```

02. Practice – sql Injection



* 복습

- 테이블 조회하기

: 테이블의 모든 데이터 → select * from (테이블명);

특정 컬럼 데이터만 → select (컬럼명) from (테이블명);

조건에 따라 특정 컬럼만 → select (컬럼명) from (테이블명) where (조건);

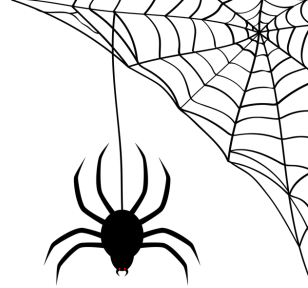
```
mysql> select * from table1;
+-----+-----+-----+
| no | id      | pw      |
+-----+-----+-----+
| 1  | argos   | argos   |
| 2  | web     | hacking |
| 3  | hololo  | hololo  |
+-----+-----+-----+
3 rows in set (0.00 sec)
```

```
mysql> select id from table1 where pw="hacking";
+----+
| id |
+----+
| web |
+----+
1 row in set (0.01 sec)
```

select (보고싶은 정보의 컬럼명) from (테이블명) where (컬럼명)=“들어있는 값”;

조건

02. Practice – sql Injection



〈조건〉

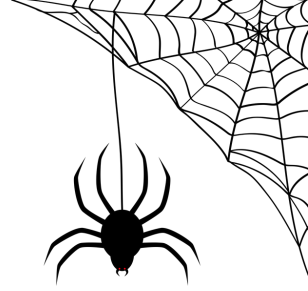
select id from table1 where id="web" and pw="hacking";

and 연산

참이면

id 출력

02. Practice – sql Injection

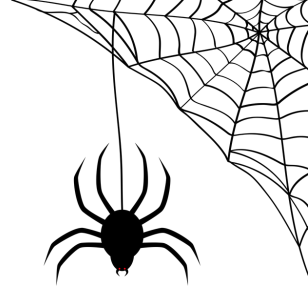


```
SELECT * FROM users WHERE username='admin' and password=' OR 1=1 --'
```

받는 입력은 'username' 과 'password'

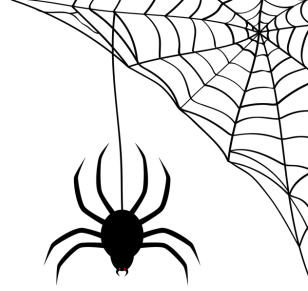
Username	admin
Password	' OR '1' = '1

02. Practice – sql Injection(no.18)



```
<br>
<br>
<center>
  <h1>SQL INJECTION</h1>
  <form method="get" action="index.php">
    <table border="0" align="center" cellpadding="10" cellspacing="0">
      <tbody>
        <tr>
          <td>
            <input type="text" name="no">
          </td>
          <td>
            <input type="submit">
          </td>
        </tr>
      </tbody>
    </table>
  </form>
  <a style="background:gray;color:black;width:100;font-size:9pt;">
    <b>RESULT</b>
    <br>
    <br>
    <br>
    <a href="?view_source=1">view-source</a>
  </center>
</body>
</html>
```

02. Practice – sql Injection(no.18)



```
<br>
<br>
<center>
  <h1>SQL INJECTION</h1>
  <form method="get" action="index.php">
    <table border="0" align="center" cellpadding="10" cellspacing="0">
      <tbody>
        <tr>
          <td>
            <input type="text" name="no">
          </td>
          <td>
            <input type="submit">
          </td>
        </tr>
      </tbody>
    </table>
  </form>
  <a style="background:gray;color:black;width:100;font-size:9pt;">
    <b>RESULT</b>
    <br>
  </a>
  <br>
  <br>
  <a href="?view_source=1">view-source</a>
</center>
</body>
</html>
```

‘입력받은 input의 name’ = ‘입력값’

webhacking.kr/challenge/web-32/index.php?no=hololo

SQL INJECTION

[view-source](#)

A black and white line drawing of a spider on a web. The spider is positioned in the lower-left quadrant, facing right. It has a rounded body and eight legs. A single strand of web extends from the spider towards the upper-left corner. In the upper-right quadrant, there is a large, intricate spider web with a central spiral and several concentric rings. The background is plain white.

```
if($_GET[no])
{
```

② eregi("A",B) → B에 A가 속해있다면, 참
exit() 해당 페이지 종료

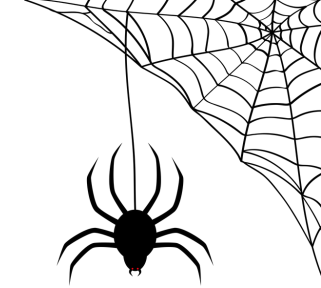
```
if(ereg(" |/(|(|)|)|t|&|union|select|from|0x",$_GET[no])) exit("no hack");
```

```
$q=mysql_fetch_array(mysql_query("select id from challenge18_table where id='guest' and no=$_GET[no]"));
```

<pre> if(\$q[0]=="guest") echo ("hi guest"); if(\$q[0]=="admin") { @solve(); echo ("hi admin!"); } </pre>	<p>③ <challenge18_table0이라는 테이블에서 id='guest' 이고 no= '받아온 값' 인 곳에서 id를 가져옴></p> <p>→ mysql_fetch_array() (받아온 정보의 한 row씩 배열에 저장)</p> <p>→ &q (저번의 row)</p>
---	---

④ 만약 admin0이면 solve()

02. Practice – sql Injection(no.18)



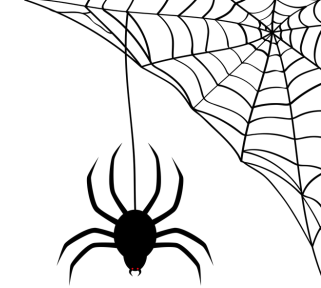
결론 : 우리가 바꿀 수 있는 부분? == &_GET[no]

→바꿔서 admin이 포함된 열이 \$q에 저장되도록 !!

```
<a style=background:gray;color:black;width:100;font-size:9pt;><b>RESULT</b><br>
<?
if($_GET[no])
{
if(eregi(" |/(|#|)|#t|#|&|union|select|from|0x",$_GET[no])) exit("no hack");
$q=@mysql_fetch_array(mysql_query("select id from challenge18_table where id='guest' and no=$_GET[no]"));
if($q[0]=="guest") echo ("hi guest");
if($q[0]=="admin")
{
@solve();
echo ("hi admin!");
}
}
?>
</a>
```

어떻게 해야지 admin의 정보를 뺏을 수 있게 하지?

02. Practice – sql Injection(no.18)



결론 : 우리가 바꿀 수 있는 부분? == &_GET[no]

→바꿔서 admin이 포함된 열이 \$q에 저장되도록 !!

1. 공백 입력

SQL INJECTION

제출

RESULT
no hack

select id from challenge18_table where id='guest' and no='1';
→ \$q = 'guest'

and 연산
↓
guest

< challenge18_table >

id	no
guest	1
...	...

2. 1 입력

SQL INJECTION

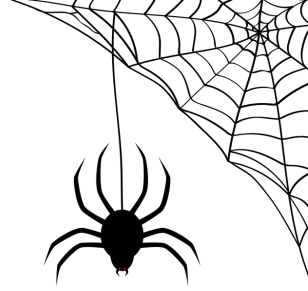
제출

RESULT
hi guest

```
if($q[0]=="guest") echo ("hi guest");
```

admin은 어디에?

02. Practice – sql Injection(no.18)



만약 no의 옵션이 AUTO_INCREMENT라면? 2 또는 다른 숫자? (guest가 10이었으니)

select id from challenge18_table where id='guest' and no=2;

이면 admin이 나올까?

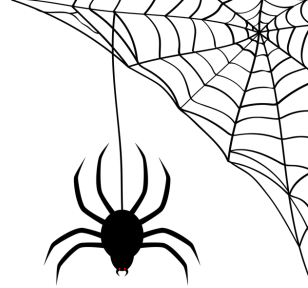


admin을 뽑아내는 데에, 거짓!
id='admin'이어야 함

우리가 조작할 수 있는 부분은

```
y(mysql_query("select id from challenge18_table where id='guest' and no=$_GET[no]"));
```

02. Practice – sql Injection(no.18)



```
y(mysql_query("select id from challenge18_table where id='guest' and no=$_GET[no]"));
```



앞의 id= 'guest' 를 무효화!!

참고

sql에서의 연산 순서 : 괄호 > not > and > or

→ A and B or C 그러므로 C만 참이면 전체가 참!!

①

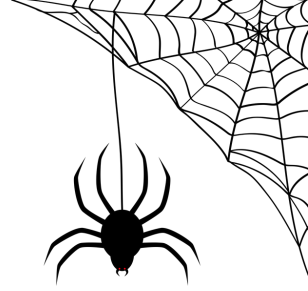
where id= 'guest' and no=-1 or no=2

guest에 거짓!!

admin에 참!!

→ admin만 추출!!

02. Practice – sql Injection(no.18)



no= '여기에 우리가 입력하는 값'

-1 or no=2

라고 입력하면 될까?



```
<a style=background:gray;color:black;width:100;font-size:9pt;><b>RESULT</b><br>
<?
if($_GET[no])
{
if(ereg(" |/|\\(|\\)|#|t|\\||&|union|select|from|0x",$_GET[no])) exit("no hack");
$q=@mysql_fetch_array(mysql_query("select id from challenge18_table where id='guest' and no=$_GET[no]"));
if($q[0]=="guest") echo ("hi guest");
if($q[0]=="admin")
{
@solve();
echo ("hi admin!");
}
}

?>
</a>
```

공백, /, \, (, &
등등의 문자가 포함되어있으면
exit!!

공백대신 쓸 문자? (공백 필터링 우회 문자)

%0a

%09

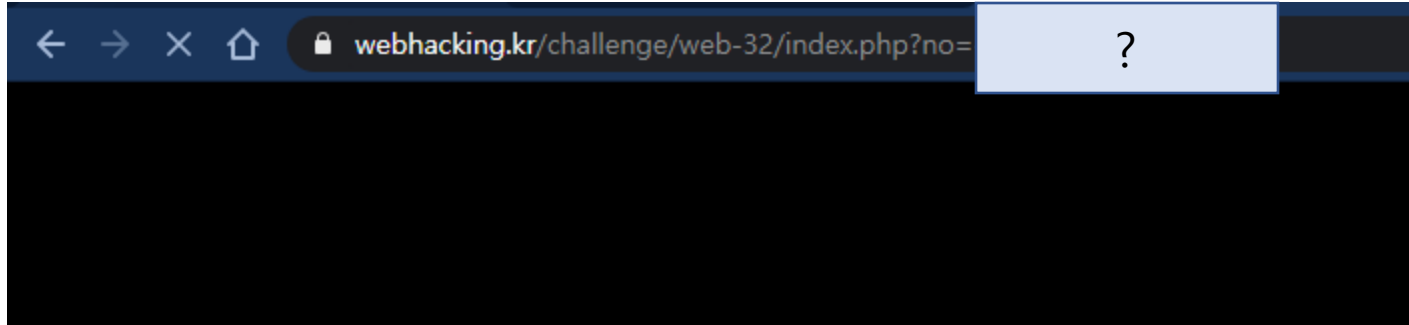
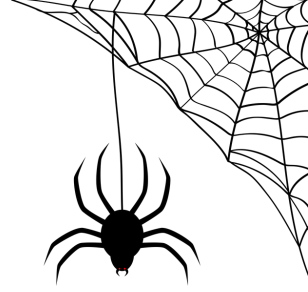
%0d

등등

그러므로 url에 직접

url encoding을 고려하여 입력

02. Practice – sql Injection(no.18)



SQL INJECTION

제출

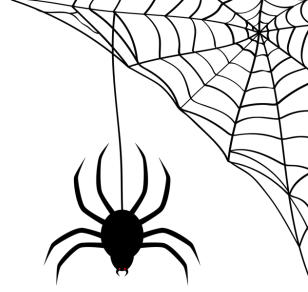
RESULT

old-18 Pwned. You got 100point. Congratz!

hi admin!

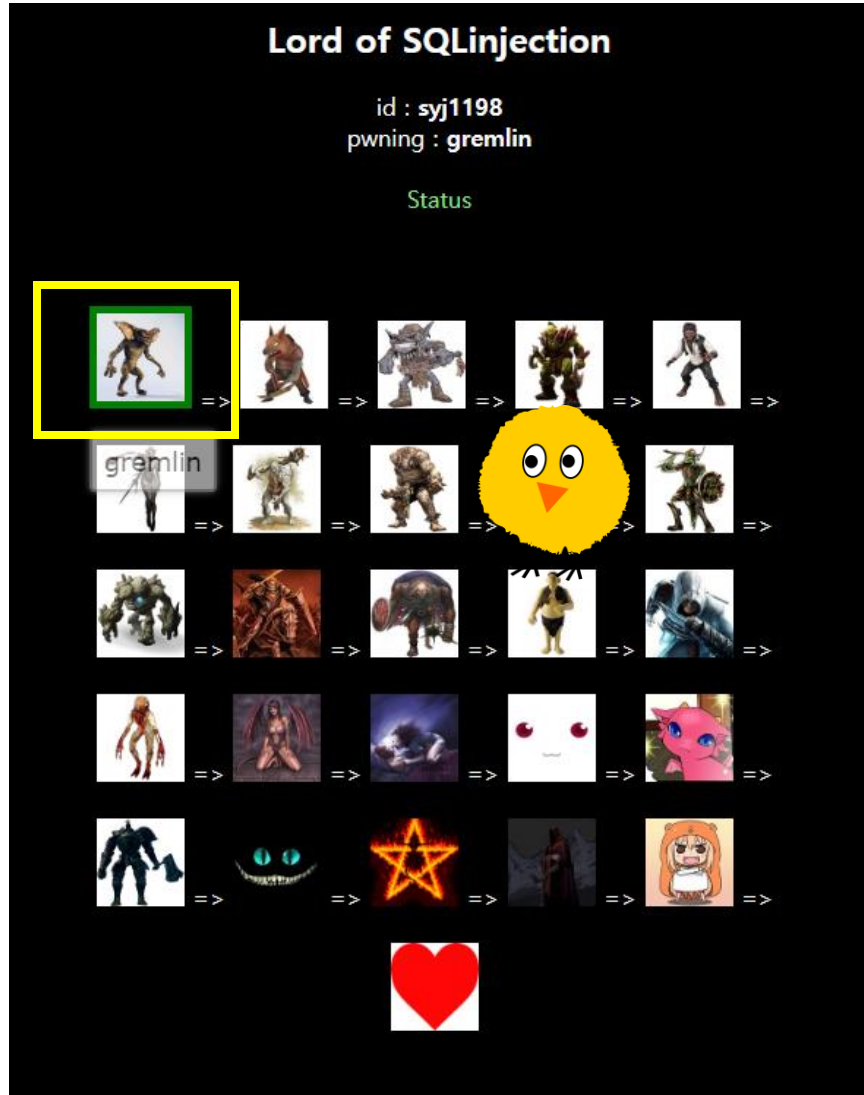
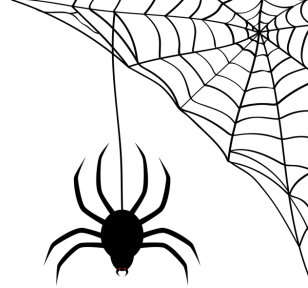
[view-source](#)

03. 마무리



- 많은 문제를 풀어볼 것
- 사실 문제의 write up (풀이)가 구글링하면 다 나오지만,
그걸 보고, 아무 의미도 모른 채 그대로 따라하는 건 공부 X
보고, 함수와 태그를 하나하나 해석하며 자신의 것으로 만들자!!
- 구글링하면 나오는 write up처럼
자신만의 풀이법을 블로그에 적으며, 기록을 남기는 게 좋다!!
- 문제를 어느 순서로 풀지 모르겠으면 저에게 연락

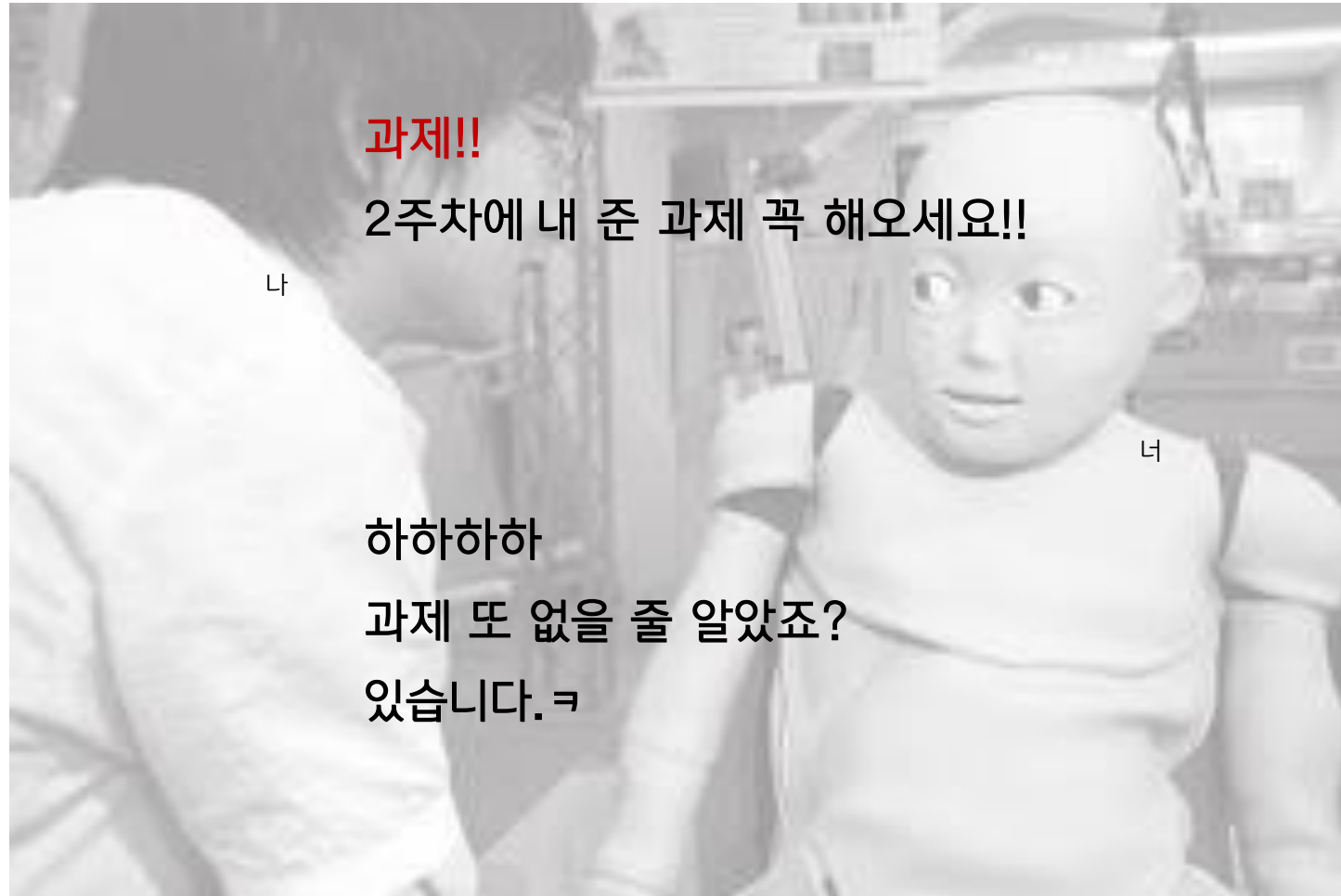
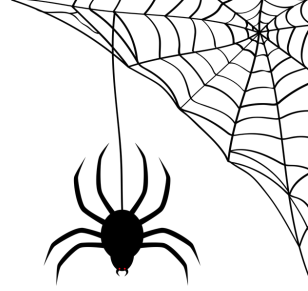
03. 그리고 과제



과제!!

<https://los.eagle-jump.org/>에서
회원가입을 한 후,
gremlin문제 풀어오기
(sql Injection 문제)

03. 그리고 과제



Q&A

