

Web Hacking

CONTENTS

Contents 1

– Web 기초

Contents 2

– Cookie & Session

Contents 3

– Password 취약점



WWW

- World Wide Web
- 1989년 팀 버너스리스에 의해 개발됨
- 처음에는 여러 연구소와 대학 간의 문서 공유 목적
- 현재는 정보 공유 뿐만 아니라 다양한 서비스 제공

Contents 1

Web 기초

웹이란?



HTML : 텍스트 & 이미지 등 정적인 콘텐츠

CSS : 콘텐츠에 스타일을 적용하여 꾸밀 수 있음

Java Script : 콘텐츠가 동적으로 보일 수 있게 함

```
<!DOCTYPE html>
<html>
<!-- created 2010-01-01 -->
<head>
  <title>sample</title>
</head>
<body>
  <p>Voluptatem accusantium
  totam rem aperiam.</p>
</body>
</html>
```

HTML

- HyperText Markup Language
- 태그와 콘텐츠로 구성
- 정적인 콘텐츠(이미지, 텍스트)를 표현

CSS



- Cascading Style Sheets
- 스타일 시트 언어
- 사이트의 전체 스타일을 손쉽게 제어



- 객체 지향형 스크립트 언어
- HTML에서 <script> 태그를 이용하여 삽입
- 웹을 동적으로 만들어 줌



CSS

메일 카페 블로그 지식iN 쇼핑 Pay ▶TV 사전 뉴스 증권 부동산 지도 영화 뮤직 책 웹툰 더보기 ▼

Java Script

4 축구결승전 ▼

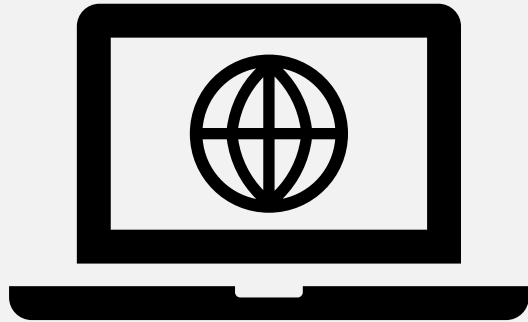
네이버를 더 안전하고 편리하게 이용하세요.

NAVER 로그인

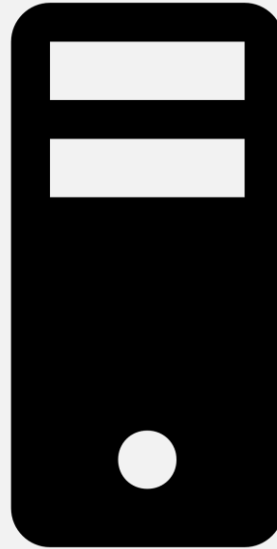
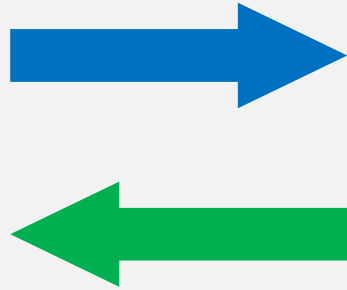
아이디·비밀번호 찾기

회원가입

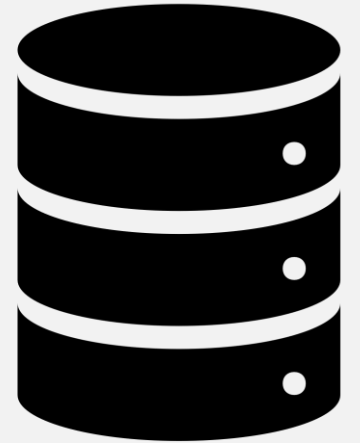
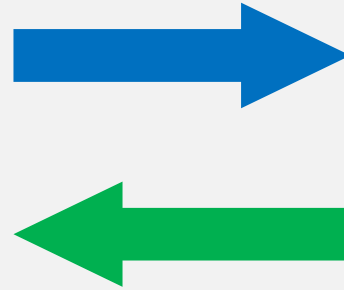
```
<!doctype html>
<html lang="ko">
  <head>...</head>
... <body class> == $0
  <!-- 스킵 내비게이션 -->
  <div class="u_skip">...</div>
  <!-- //스킵 내비게이션 -->
  <div id="PM_ID_ct" class="wrap">...</div>
  <script src="https://pm.pstatic.net/js/c/jindo_v180212.js"></script>
  <script>...</script>
</body>
</html>
```

클라이언트



서버

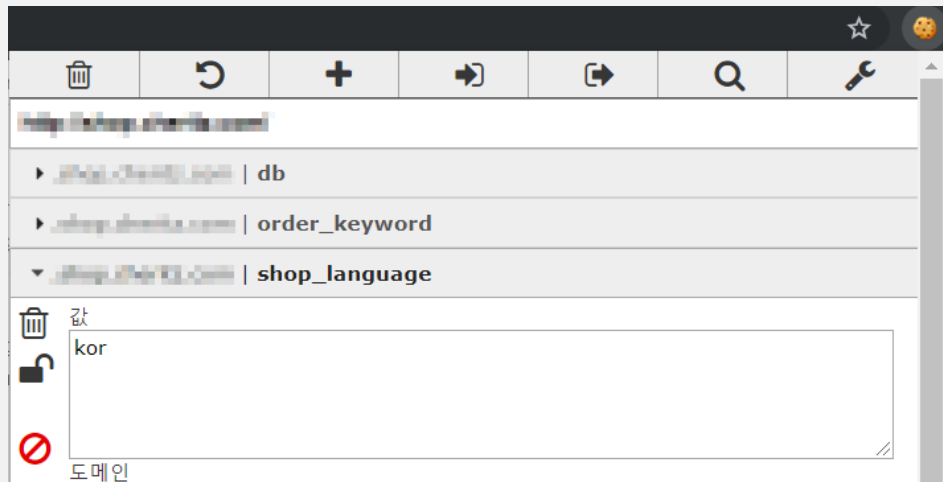


데이터베이스

- http 프로토콜의 특징이자 약점을 보완하기 위해 사용
- 클라이언트와 서버 간의 인증 유지
- 차이점은 **저장되는 위치**
쿠키는 클라이언트, 세션은 서버에 저장

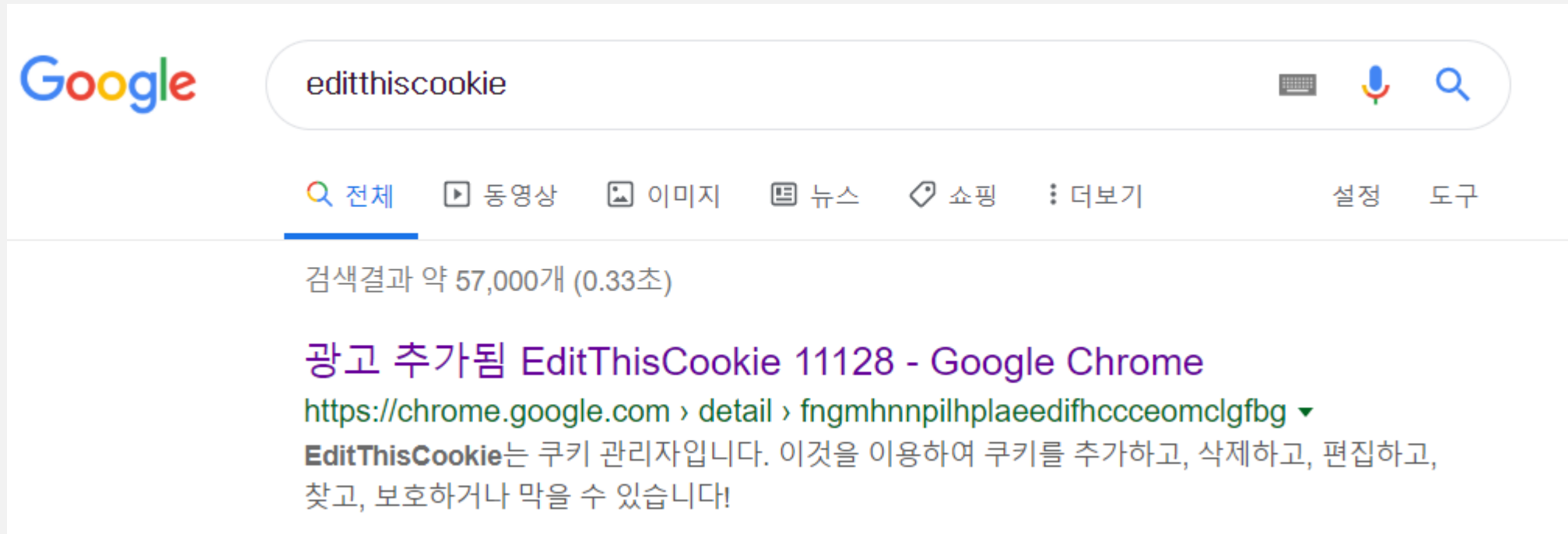


- 쿠키를 이용하여 웹 사이트의 동작을 제어
ex) 팝업 창 - 오늘은 다시 보지 않음
- 쿠키는 클라이언트에 저장
임의로 수정, 삭제하는 것이 가능
이로 인하여 발생하는 것이 '쿠키 변조'
- 쿠키 관리를 도와주는 도구 존재
Chrome의 'EditThisCookie'

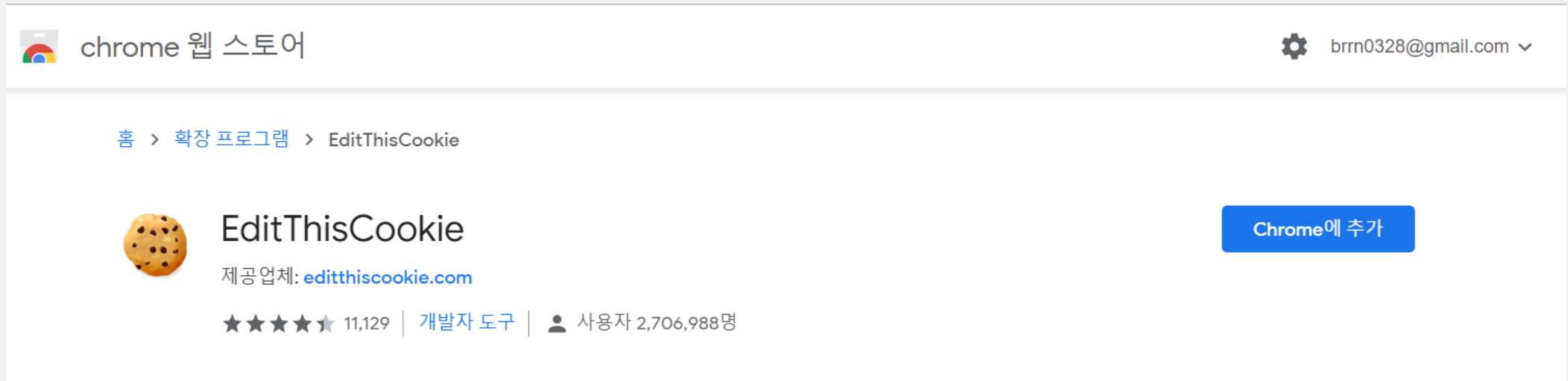


```
onClick="closeWin()" alt="오늘이창그만보기">  
  
function closeWin (){  
    setCookie("Notice_20160628", "done", 1);  
    self.close();  
}
```

1. Google에서 EditThisCookie 검색




2. Chrome에 추가



Contents 2


Cookie & Session

EditThisCookie

전체 삭제 

<https://www.naver.com/>

- ▶ .naver.com | **_naver_usersession_**
- ▶ .naver.com | **ASID**
- ▶ .naver.com | **BMR**
- ▶ .naver.com | **NNB**
- ▶ .naver.com | **nx_ssl**
- ▶ .naver.com | **page_uid**
- ▼ www.naver.com | **PM_CK_loc** 쿠키 이름

개별 삭제 

값
34900677677b40cfae8a978ab9f64735a6d9b9c3a82cb948b6f6fb33af0636cd

쿠키 값


도메인
www.naver.com

경로
/

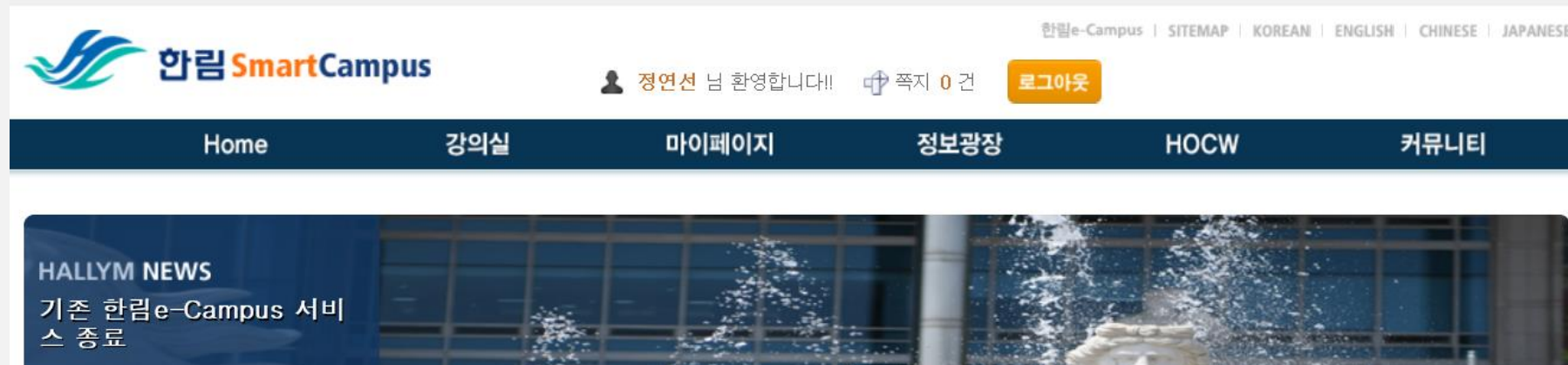
기한
Sun Sep 08 2019 15:07:23 GMT+0900 (한국 표준시)

SameSite

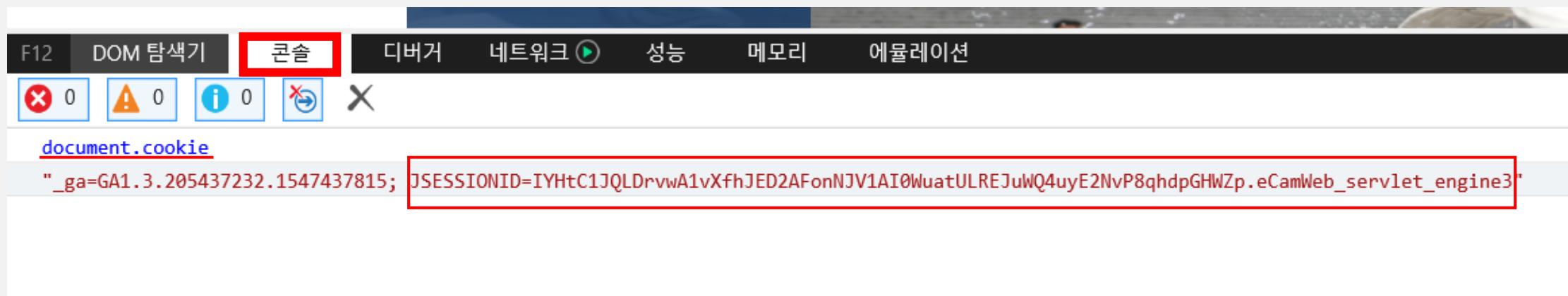
Host only ☒ 세션 ☐ Secure ☐ HTTP 전용 ☒

 도움말

1. Internet Explore에서 스마트 캠퍼스 로그인



2. 개발자 환경(F12)에서 쿠키 값(Session ID) 확인



3. Chrome에서 스마트 캠퍼스 접속

The screenshot shows the Hallym SmartCampus website interface. The header includes the Hallym SmartCampus logo, a user ID field, and navigation links for Home, 강의실 (Classroom), 마이페이지 (My Page), and 정보광장 (Information Plaza). The main content area features a video player with the title 'HALLYM NEWS' and a description '기존 한림e-Campus 서비스 종료' (Existing Hallym e-Campus service ends). The footer contains links for 공지사항 (Notice), S.Campus, 학사 (Academics), 일반대학원 (General Graduate School), 특수대학원 (Special Graduate School), and MORE, along with the HOCW logo.

The Chrome DevTools Cookie Inspector is open, displaying the cookies for the URL `https://smart.hallym.ac.kr/index.jsp`. The cookies list shows a cookie named `JSESSIONID` with the value `J7feH1EuSZCzxVcKSe4iSFHDo2H9b70oIChWUejFK1vTGVhWy0Dv5ffSY3hx1VhR.eCamWeb_servlet_engine3`. A red box highlights this cookie, and a red text label '비로그인시 기존 JSESSIONID' (Existing JSESSIONID when not logged in) is placed next to it. The cookie details section shows the domain as `smart.hallym.ac.kr`, the path as `/`, the expiration time as `Mon Sep 07 2020 20:25:39 GMT+0900 (한국 표준시)`, and the SameSite attribute as `SameSite`. The cookie is marked as 'Host only' and 'Secure'.

4. EditThisCookie를 사용하여 쿠키 변조

The screenshot shows the Hallym SmartCampus website interface. The top navigation bar includes links for Home, 강의실 (Classroom), 마이페이지 (My Page), and 정보광장 (Information Plaza). A sidebar on the left displays 'HALLYM NEWS' with a headline about the end of the Hallym e-Campus service. The main content area features a large image of a fountain. The EditThisCookie extension is open on the right, displaying the URL 'https://smart.hallym.ac.kr/index.jsp'. The cookie list shows a 'JSESSIONID' cookie with the value 'IYHtC1JQLDrvwA1vXfhJED2AFonNJV1AI0WuatULREJuWQ4uyE2NvP8qhdpGHWZp.eCamWeb_servlet_engine3'. A red box highlights this value, and a red text overlay reads 'IE에서 가져온 JSESSIONID로 저장' (Save as JSESSIONID from IE). The extension's settings show the domain as 'smart.hallym.ac.kr' and the path as '/'. The 'Host only' checkbox is checked, and the 'Secure' checkbox is unchecked. A green checkmark icon is visible in the bottom right corner of the extension's interface.

5. Chrome에서도 로그인 세션 획득



세션 고정 & 예측

세션 고정

- 사용자가 접속할 때마다 동일한 Session ID를 발행하여 발생
ex) PHPSESSION, JESSID 등
- 쿠키가 유출된 경우 세션이 도용될 수 있음
따라서 매번 기존의 세션 파기 후 새로운 Session ID 발행

세션 예측

- 특정 패턴을 기반으로 Session ID를 만들 때 발생
ex) IP Address, 단순히 숫자가 1씩 증가
- Brute force 등을 통해 유효한 세션 도용 가능
따라서 Session ID를 발행 시 마다 예측할 수 없도록 생성

Name	Value	Domain	Path	Expires / Max-Age
PHPSESSID	no688n...	shoppi...	/	N/A
_ga	GA1.3.3...	.boardli...	/	2021-06-23T08:49:38.000Z
_gat	1	.boardli...	/	2019-06-24T08:50:38.000Z
_gid	GA1.3.1...	.boardli...	/	2019-06-25T08:49:38.000Z
check_stats	1	shoppi...	/	N/A
boardli...	...	boardli...	/	N/A

※위 사이트는 취약점과 관련 없는 예시 사이트입니다.

- 세션의 만료 기간을 정하지 않아 발생
세션의 종료 시간을 설정해주어야 안전
- 만료되지 않은 세션으로 인하여 불법적인 접근 가능

- 회원 가입 시 안전한 계정 및 패스워드 규칙이 사용되지 않아서 발생한다.
해커가 추측을 통한 로그인 시도를 통해 권한 획득
- 쉽게 예측할 수 있는 계정 및 패스워드를 사용 하는 경우 발생한다.
이름의 이니셜, 생일, 1234 등 연속된 숫자
- 기본 계정을 사용할 경우 발생한다.
admin / admin 과 같은 초기 계정을 그대로 사용
- <https://howsecureismypassword.net>

취약한 계정	취약한 패스워드
admin, guest, test root, user 등	aaaa, 1234,1111 test, password 등

안전한 패스워드 가이드 라인

- 패스워드 최소 길이 설정

영어 대문자, 소문자, 숫자, 특수문자 중 2종류를 조합하여 10자리 이상

영어 대문자, 소문자, 숫자, 특수문자 중 3종류를 조합하여 8자리 이상

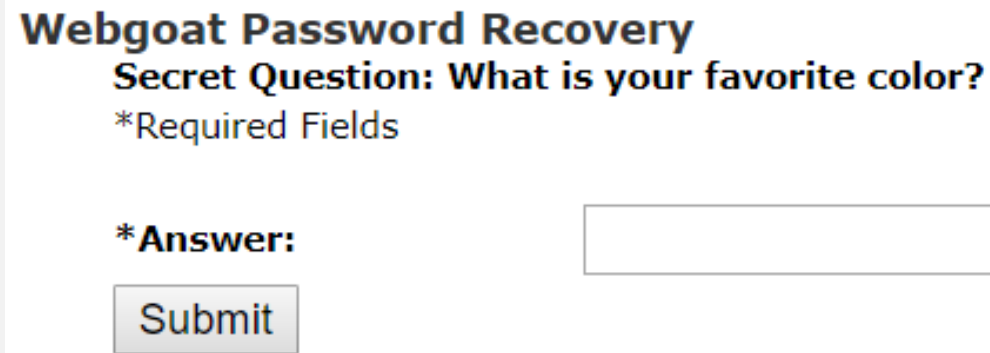
- 추측하기 어려운 패스워드

생일, 전화번호, 아이디와 비슷한 패스워드는 포함 되지 않도록 함

qwer, asdf, 1234 등 키보드 상에서 나란히 있는 문자열이 포함 되지 않도록 함

- 주기적인 변경

비밀번호에 유효기간을 설정하고 최소 6개월 마다 변경



The image shows a web form titled "Webgoat Password Recovery". Below the title is a "Secret Question: What is your favorite color?". Underneath this is the text "*Required Fields". Further down, there is a label "*Answer:" followed by a text input field. At the bottom of the form is a "Submit" button.

- 패스워드 복구 로직이 취약하여 패스워드가 유출
공격자가 예측할 수 있거나 쉽게 얻을 수 있는 정보를 기반한 질문은 위험
- 패스워드 복구 질문이 단순하여 예측할 수 있는 경우 발생
ex) 출신 초등학교, 생일, 회원 가입 시 사용한 이메일 등
- 패스워드 복구 로직 통과 이후, 패스워드 알려주는 방식도 주의
바로 웹 사이트에서 보여주기 보다는 인증된 이메일, SMS를 통해 확인하는 것이 안전

- 특정 웹 서비스를 반복적으로 요청하는 것
ex) 로그인, 메일발송, 게시판 글쓰기 등
- 패킷을 모니터링하여 공격을 감지하는 시스템이 필요
공격이 허용될 시, 패스워드를 무차별 대입(Brute Force)하여 로그인하거나
서버 다운 가능성이 있음


A screenshot of a webmail interface. The '받는사람' (To) field is highlighted with a green border and contains a question mark icon. The '참조' (Cc) field is empty. The '제목' (Subject) field is empty. The '파일첨부' (Attachments) section shows '내 PC' (My PC) and '네이버 클라우드' (Naver Cloud) options. Below these fields is a rich text editor toolbar with various icons for text formatting, alignment, and linking. The main body of the email is empty.

A screenshot of the Google login page. The Google logo is at the top, followed by the text '로그인' (Login) and 'Google 계정 사용' (Use Google Account). Below this is a large input field for the email or phone number, with the placeholder text '이메일 또는 휴대전화' (Email or phone number). Below the input field is a link that says '이메일을 잊으셨나요?' (Forgot your email?). At the bottom, there is a link for '계정 만들기' (Create account) and a blue '다음' (Next) button.

1) CAPCHA

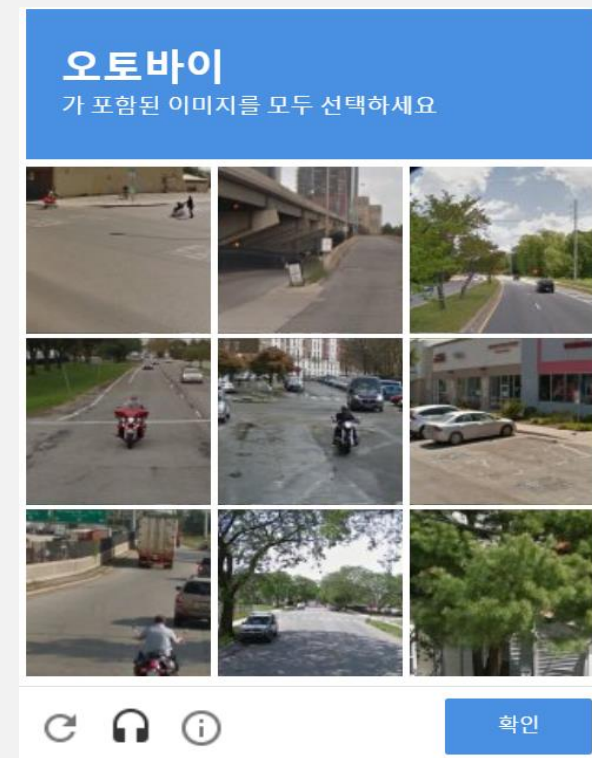
- 자동화 스크립트 혹은 툴을 이용하지 못하도록 CAPCHA를 이용하여 특정 요청을 반드시 수동으로 하도록 강제함

☐ 로봇이 아닙니다.


reCAPTCHA
개인정보 보호 · 약관

페이지 정보

Google의 시스템이 컴퓨터 네트워크에서 비정상적인 트래픽을 감지했습니다. 이 페이지는 로봇이 아니라 실제 사용자가 요청을 보내고 있는지를 확인하는 페이지입니다. [왜 이런 현상이 발생하는 거죠?](#)



2) 반복 행위 방어

- 요청을 반복하여 할 수 없도록 과도한 요청 시 제지할 수 있는 방안 마련

안전을 위해 비밀번호와 자동입력 방지문자를 입력해주세요.
[앗, 로그인이 안 되나요?](#)

아이디

비밀번호

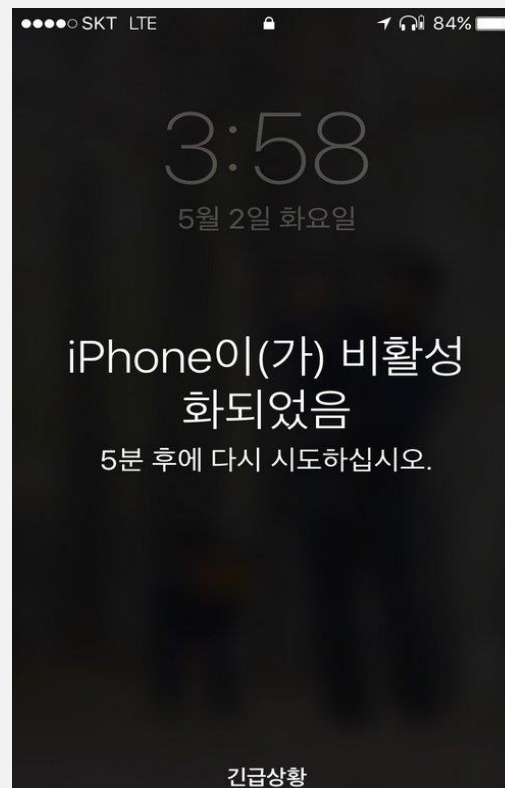
아래 이미지를 보이는 대로 입력해주세요.

5 V 3 H F

새로고침

음성으로 듣기

자동입력 방지문자



감사합니다