

나는 어떻게 회원가입 API를 짜야하나요?

: 사용자에게 어떤 **비밀번호**를 권장해야 할까?

발표 내용이 정리된 글입니다

github.com/joungeun/why/blob/e8ba734a12d2d344e7b6a282d247f0c841b8f4b8/Why%20can%20only%20write%20certain%20special%20characters%20in%20passwords.md

사용자에게 어떤 **비밀번호**를 권장해야 할까?

여러분이 자주 사용하시는 비밀번호 형식은 무엇인가요?

또는 가장 많이 본 비밀번호 형식은 무엇인가요?

사용자에게 어떤 *비밀번호*를 권장해야 할까?

- * 8~12자 이내 영문,숫자,특수문자 중 2가지 이상을 조합해야 합니다.
- * 사용 불가 특수 문자: ' " + / \ ; : - _ ^ & () < > 제외

내가 짜는 회원가입 API는 좋지 않은 API인가?

사용자에게 어떤 **비밀번호**를 권장해야 할까?

ID/PW

* 아이디

* 비밀번호

8~16자리 영문 대소문자, 숫자, 특수문자 중 3가지 이상 조합

사람인 

대문자, 소문자 숫자, 특수문자 등을 조합

8자리 이상

coupang

회원정보를 입력해주세요



아이디(이메일)

이메일을 입력하세요.



- × 영문/숫자/특수문자 2가지 이상 조합 (8~20자)
- × 3개 이상 연속되거나 동일한 문자/숫자 제외
- × 아이디(이메일) 제외

쿠팡 

사용자에게 어떤 **비밀번호**를 권장해야 할까?

NIST (미국 국립표준 기술 연구소)

내용:

비밀번호 변경하신지 3개월이 지났습니다.
비밀번호를 변경해주세요.

확인

90일 주기로 비밀번호를 변경하라

사용자에게 어떤 **비밀번호**를 권장해야 할까?



빌 버 (Bill Burr)
특징: 비밀번호에 특수문자 쓰게 함

후회돼요

사용자에게 어떤 **비밀번호**를 권장해야 할까?



2003년 가이드라인이
오히려 보안에
취약할 수 있다는 사실!!

○ㄷ!!!!!!!



사용자에게 어떤 **비밀번호**를 권장해야 할까?

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-63-3>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

사용자에게 어떤 **비밀번호**를 권장해야 할까?

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-63-3>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

검증자는 패스워드에 대해 구성 규칙을 요구해서는 안 된다.
(생성 규칙의 복잡성 높이지 마.)

검증자는 패스워드를 임의로 변경하라고 요구해선 안 된다.
(주기적 변경 요구 금지.)

사용자에게 어떤 **비밀번호**를 권장해야 할까?

KISA(한국 인터넷진흥원)에서도...

두 종류 이상의 문자구성과 8자리 이상의 길이로 구성된 문자열

※ 문자종류는 알파벳 대문자와 소문자, 특수문자, 숫자의 4가지임

또는

10자리 이상의 길이로 구성된 문자열

※ 숫자로만 구성할 경우 취약할 수 있음

사용자에게 어떤 *비밀번호*를 권장해야 할까?

결론

Monkey1!



monkeyspringbootmouseschool
(MonkeySpringBootMouseSchool)

사용자에게 어떤 *비밀번호*를 권장해야 할까?

결론

글자수 제한

블랙리스트 사용

근데 특수문자 제한은 좋지 않다는 말을 드리고 싶습니다 제가 찾아보면서 느끼는 건데, 특수문자 제한은 사용자에게 보안에 대한 의문을 불러일으킵니다

보통 문자 혹은 문자열간 구분자로 사용한 특수문자는 못쓰게 막더라구요 ㅎㅎ.....

아 저것도 좀 표준으로 통일시킬 수 없을까요

동일 비번 쓰는데 어디서는 @가 안되고 어디서는 #가 안되고.....

비번에 특문은 필수면서 -;

님

LINK IP 09-16 언급 · 공감 신고

제님 전 bitwarden으로 생성해서 쓰는데요, 사이트에서 허용하지 않은 문자가 있는지 한번 검토해서 만약 있으면 다른 특수문자로 대체해넣기 번거롭네요.

님

LINK IP 09-16 언급 · 공감 신고

님
절대적인 표준은 아니지만
보안에 별로 효과가 없다니
그러니까 어떤 특수문자들

님

LINK IP 09-16 대댓글 · 공감 신고

SQL 인젝션 등 여러 보안 이슈로 저런 특수 문자 제한을 걸어 둔 것이라고 설득을 해 주고 싶습니다...만... 다 변명입니다. 심지어 패스워드는 원문 그대로 DB에 저장되지도 않기 때문에 문제가 될 수 없습니다.

님

LINK IP 09-16 언급 · 공감 신고

❤ 1

솔직히 SQL 인젝션 때문에 특수문자에 저런 제한을 걸어야 한다는 건, 해당 사이트가 보안이 취약하다고 자랑하는 것과 같다고 생각합니다. 쿼리 내에서 특수 문자는 이스케이프 되어야 하는 게 기본이거든요.

님

LINK IP 09-16 언급 · 공감 신고

@... 가까운 클리앙만 해도 비번 제약 없고.. 뭐 메일 사이트에서 메일 제목이나 본문에 온갖 특수문자 넣어서 전송해도 잘 가고.... 말씀 하신대로 저장도 평문 저장도 아닌데 어찌된 영문으로 저런 제약들이 생겨났나 의문입니다.

LINK IP 09-16 대댓글 · 공감 신고

사실 평문으로 쿼리를 만들어 쓰는 데서나 저게 보안 문제가 되는 건데.. 바꿔말하면 개발자 수준이 개판이란 뜻입니다.

LINK IP 09-16 언급 · 공감 신고

하긴... 그리고보니 IT (특히 웹) 기반한 서비스 회사들에서는 저런 메세지들 잘 못본 거 같네요.

2020.06.22 09:13

사이트도 올해 새로 수주를 해서 개편을 했는데 황당하게도 비밀번호에 &를 못넣더라구요. 근게 개편 전에는 & 넣는 게 가능해서 원래 비밀번호에 &가 있었던 저는 그대로 잘 쓰고 있긴 정보 수정 부분(수정 전에 기존 비밀번호를 입력하는 부분)에서 자꾸 에러가 나서 전화해 있으면 안된다고...

어보니 보안 강화라는 황당한 답변을 받았네요. 정녕 올해 만든 사이트가 맞는 건지...

를 낮추는 행위이니 '보안 약화' 인데 말이죠. 보안 강화란 도

문자가 제한되면 경우의 수가 줄어들어서 더 보안에 취약해지
화합니다. 뭐 딱히 전문성 있는 답변을 기대한 건 아니지만...