

15E

dontpwn.me, en webapplikasjon for å forenkle bruk av sterke passord

Innhold

- Problembeskrivelse
- Hva kan vi gjøre selv for å begrense skadeomfanget?
- Hva med brukernavn, kan noe gjøres der?
- Løsningen
- Suksessfaktorer
- Demonstrasjon
- Lisens

Problembeskrivelse

- Datainnbrudd
- Brute force
- Id tyveri
- Brukernavn og passord kommer støtt og stadig på avveie!

Hva kan vi gjøre selv for å begrense skadeomfanget?

- Jo, begynne å bruke gode passord
- Hvorfor er dette så vanskelig?
 - Vanskelig å huske
 - Vanskelig å oppbevare sikkert
 - Trenger verktøy

Hva kjennetegner sterke passord?

- Lengde
- Tegnsett
- Tilfeldighet
- Mønster
- Bør ikke forekomme i ordlister

Hva med brukernavn, kan noe gjøres der?

- Ja, vi kan lage bedre brukernavn også, selv om vi tvinges til å bruke epostadresse som brukernavn!
 - Gmail identifikator

Løsningen

- Vi lager et verktøy!!

Suksessfaktorer

- Må kunne lage skikkelige passord, med varierende grad av styrke
- Må kunne tilby noe ekstra:
 - Generering av brukernavn (gmail-identifikator)
 - Mulighet for å sjekke om brukernavn har forekommet i kjente datainnbrukk
 - Mulighet for å sjekke om passord finnes i ordliste
 - Mulighet for å lagre passord på sikker måte (kryptering)
 - Mulighet for å automatisk logge inn på diverse tjenester, derav slipper man å huske passord og brukernavn
 - «Mobile first!»



dont
pwn
.me

Navnevalg

- dontpwn.me
 - «Ikke ei meg»: henspeiling til applikasjonens ønske om å forebygge at man «blir eid», at brukernavn og passord kommer på avveie. Eventuelt at man begrenser skade dersom brukernavn og passord kommer på avveie.
 - Ordspill: www.haveibeenpwned.com Her kan man sjekke om man har blitt «eid»
 - Ledig domenenavn, enkelt og relativt kort domenenavn

Demo

Lisens

Dokumentasjon

- CC BY-SA

Kildekode

- GNU GPL v3.0