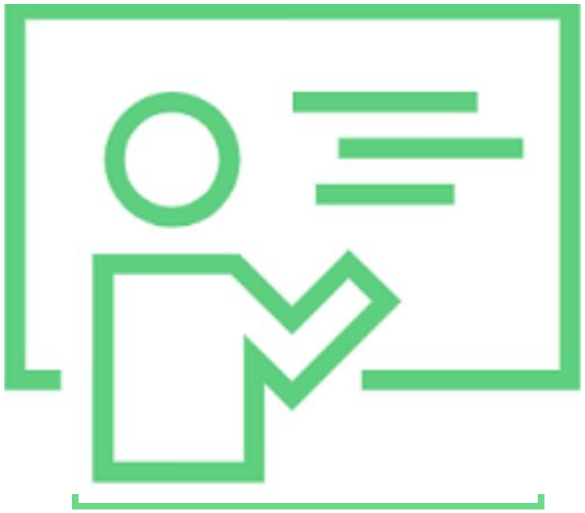


Lunchkodning med Stefan

Lösenordsknäckning i C#

Kod från https://github.com/aspcodenet/WebSec2Demo

Stefan Holmberg, Systementor AB

```
0 references
public class PasswordCracker
{
    // På samma sätt som https://en.wikipedia.org/wiki/List_of_data_breaches
    //DVS Säg att vi fått tag på
    /*
     *
     *Id    UserId  HashedPassword
    2   stefan  5F4DCC3B5AA765D61D8327DEB882CF99
    3   oliver  6DBD0FE19C9A301C4708287780DF41A2
    4   josefine    C1A93BDFFE7D5062BA3489BBD21E59DC
    */
    1 reference
    public string Solve(string hashedPassword)
    {
        //Ok - nu ska vi KODA logik för att göra det omöjliga
        return null;
    }
}
```

Agenda

- Hur kan applikationer lagra lösenord
  - klartext?
  - krypterat?
  - hashat? ← BEST PRACTICE

- Recept
  - Om hashning är “safe” - hur kan vi knäcka såna lösenord?
  - Teori - så kan vi göra!
  - Vi kodar… och knäcker lösenord!
  - Kod får ni på https://github.com/aspcodenet/WebSec2Demo

- Vad kan vi göra för att skydda oss! Bara jättekort idag
  - SALT
  - MFA

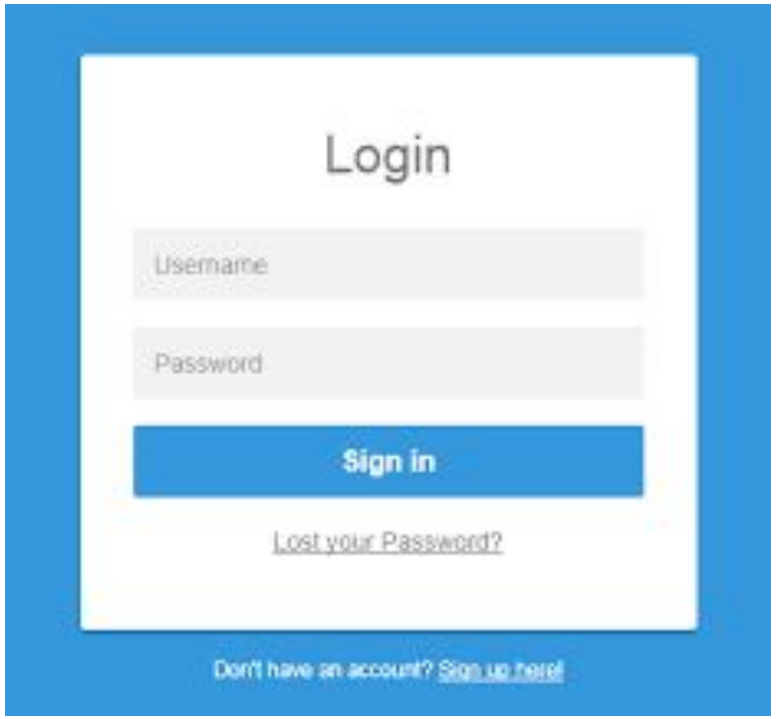
Om mig

- Eget företag i 23 år
  - Konsultat som Webutvecklare(.NET stack) bank/finans/ecommerce
  - Utbildar inom IT (.NET, IOT, Säkerhet, Java)
  - SAAS tjänster Cloud
  - ~~Äger/driver gym~~
  - Investeringar

Lösenord

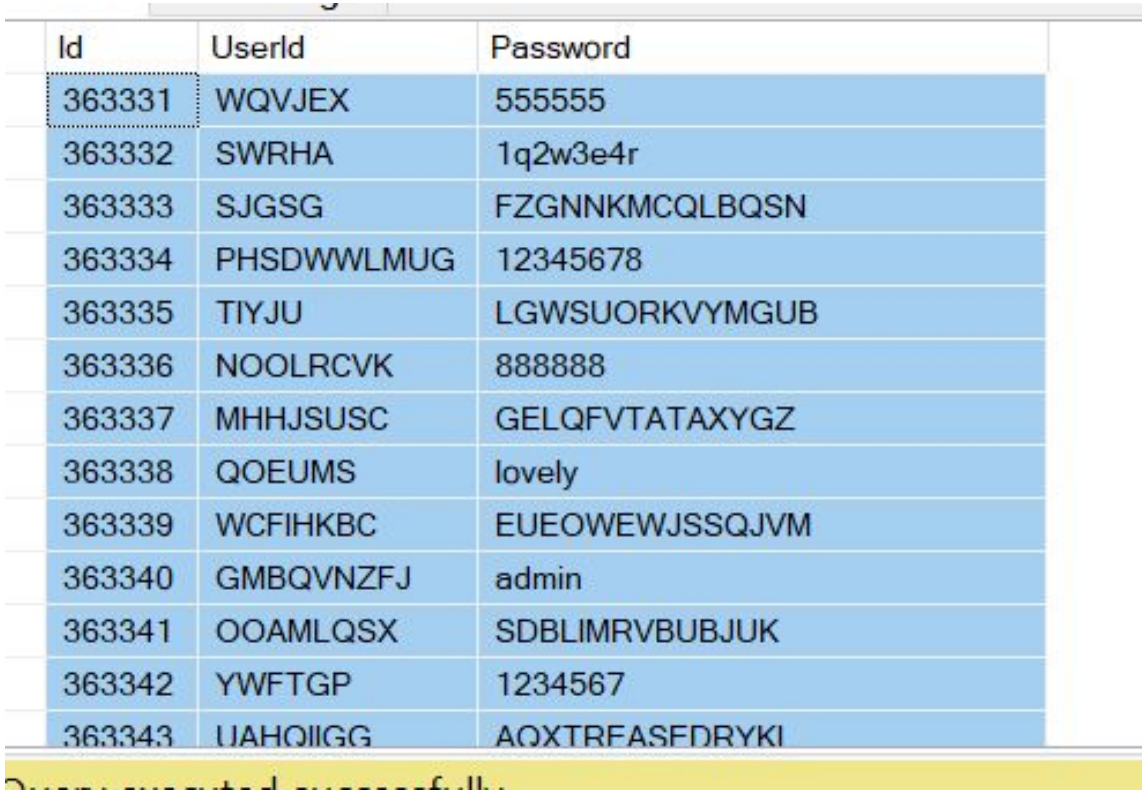
Best practice today

Var lagras dom?
Hur? Kryptering?
Nyckel?



Plaintext

Of course not...



Id	UserId	Password
363331	WQVJEX	555555
363332	SWRHA	1q2w3e4r
363333	SJGSG	FZGNNKMCQLBQSN
363334	PHSDWWLMUG	12345678
363335	TIYJU	LGWSUORKVYMGUB
363336	NOOLRCVK	888888
363337	MHHJSUSC	GELQFVTATAXYGZ
363338	QOEUMS	lovely
363339	WCFIHKBC	EUEOWEWJSSQJVM
363340	GMBQVNZFJ	admin
363341	OOAMLQSX	SDBLIMRVBUBJUK
363342	YWFTGP	1234567
363343	UAHQIIGG	AQXTREASEDRYKI

Men kryptering då? FARLIGT: om den enda krypteringsnyckeln försvinner så är allt läckt!

Hashing

Algoritm (er) för
ONE way defuscation.

Dvs det **går inte** att från
en hashtext räkna ut vad
originalet är…

Ex hasha 2,7GB Linux ISO. Såklart
all information INTE finns i 32bytes HASH

Vid skapande av konto:
beräkna en HASH för
lösenordet som
användaren valt. Spara
HASH i databasen

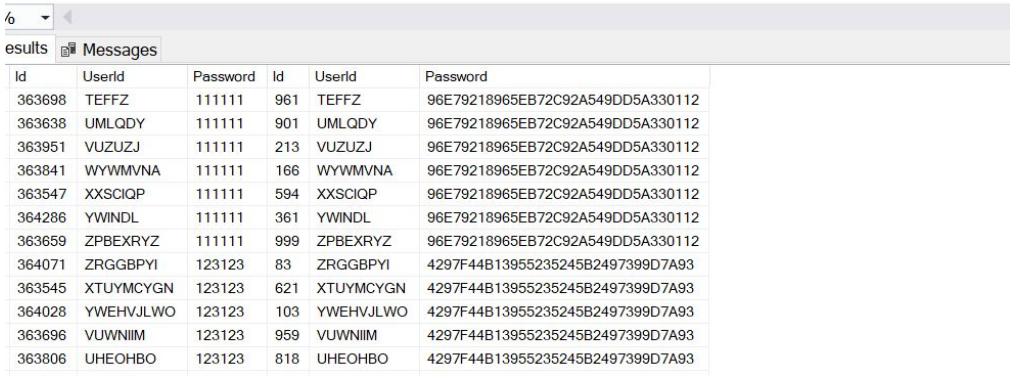
	Id	UserId	Password
1	1	WQVJEX	5B1B68A9ABF4D2CD155C81A9225FD158
2	2	ALVMN	5B1B68A9ABF4D2CD155C81A9225FD158
3	3	VRHGKAPWCG	185662EA4FD642D37CB02520DFBDBECD
4	4	BDJDIUREQ	8AFA847F50A716E64932D995C8E7435A
5	5	WZXCIWNUZC	D6CA20CF73048F6E7B818E6DE220CDCB
6	6	GSULKXRFYK	3FC0A7ACF087F549AC2B266BAF94B8B1
7	7	BRBSOCQU	8774E19D95316C1C011E8F521933C5FE
8	8	ESIOF	6EEA9B7EF19179A06954EDD0F6C05CEB
9	9	IUYLIAAWS	B61D5B3E913E49620ACF104ACC20EE22
10	10	ZWPWZGOKFG	8AFA847F50A716E64932D995C8E7435A
11	11	ZIZMPI	466F936A391433072E5C6F701D9B7E12

Vid login - beräkna en
HASH av det användaren
skrivit in...och jämför det
med vad vi har i databasen!

Svaghet???

- Samma algoritm => samma hash alltid...

```
select * from accounts join HashedAccounts
on accounts.userid=HashedAccounts.Userid
order by accounts.password
```



esults Messages

Id	UserId	Password	Id	UserId	Password
363698	TEFFZ	111111	961	TEFFZ	96E79218965EB72C92A549DD5A330112
363638	UMLQDY	111111	901	UMLQDY	96E79218965EB72C92A549DD5A330112
363951	VUZUZJ	111111	213	VUZUZJ	96E79218965EB72C92A549DD5A330112
363841	WYWMVNA	111111	166	WYWMVNA	96E79218965EB72C92A549DD5A330112
363547	XXSCIQP	111111	594	XXSCIQP	96E79218965EB72C92A549DD5A330112
364286	YWINDL	111111	361	YWINDL	96E79218965EB72C92A549DD5A330112
363659	ZPBEXRYZ	111111	999	ZPBEXRYZ	96E79218965EB72C92A549DD5A330112
364071	ZRGGBPYI	123123	83	ZRGGBPYI	4297F44B13955235245B2497399D7A93
363545	XTUYMCYGN	123123	621	XTUYMCYGN	4297F44B13955235245B2497399D7A93
364028	YWEHVJLWO	123123	103	YWEHVJLWO	4297F44B13955235245B2497399D7A93
363696	VUWNIIM	123123	959	VUWNIIM	4297F44B13955235245B2497399D7A93
363806	UHEOHBO	123123	818	UHEOHBO	4297F44B13955235245B2497399D7A93

- Även oberoende av site osv!!! https://hashes.org

Låt oss säga att nån kommer över din lösenordsfil

4	BDJDIUREQ	8AFA847F50A716E64932D995C8E7435A
5	WZXCIWNUZC	D6CA20CF73048F6E7B818E6DE220CDCB
6	GSULKXRFYK	3FC0A7ACF087F549AC2B266BAF94B8B1
7	BRBSOCQU	8774E19D95316C1C011E8F521933C5FE
8	ESIOF	6EEA9B7EF19179A06954EDD0F6C05CEB
9	IUYLIAAWS	B61D5B3E913E49620ACF104ACC20EE22
10	ZWPWZGOKFG	8AFA847F50A716E64932D995C8E7435A
11	ZIZMPI	466F936A391433072E5C6F701D9B7E12
12	ALMLD	7C6A180B36896A0A8C02787EEAFB0E4C
13	OMIPHNW	B8D98B7844530FAB6116D6707C867F84
14	OSLVD	F379EAF3C831B04DE153469D1BEC345E
15	MAMLJADSTR	CC0E37A6F06CB7289AB818309BF86560
16	XMYPFLKXM	5B1B68A9ABF4D2CD155C81A9225FD158

1. Ladda ner med common passwords....alltså seriöst det finns filer med miljontals poster

2. Skapa hashar på alla dom posterna...

3. Matcha mot

4. Träff!? Japp...bara att logga in

Men ingen kommer över en lösenordsfil

https://en.wikipedia.org/wiki/List_of_data_breaches