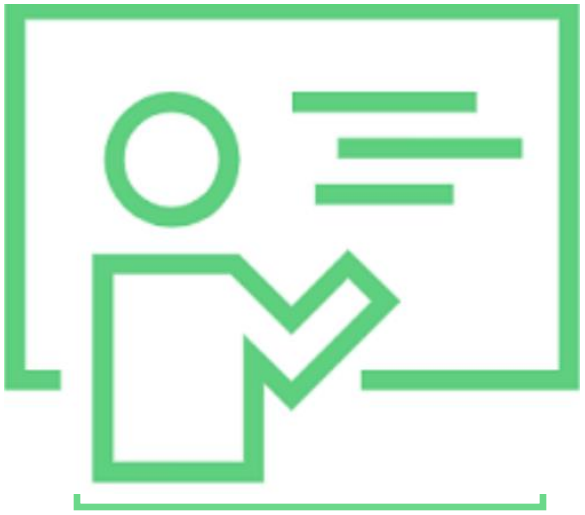


Säkerhet för webutvecklare

Lite av vad ALLA utvecklare borde veta

Stefan Holmberg, Systementor AB

Agenda

- Internet – hur funkar det?
  - Varför det i sin natur är sårbart för s.k MiTM-attacker
  - CIA
  - https
- Lösenord
  - Hur funkar lösenordshantering idag...best practice
  - 10 minuters race - Vi knäcker lösenord
- What to do?
  - OWASP
  - Penetration testing

Om mig

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

- Nästa år:
  - Mer fokus på utbildning: jag tycker det är så roligt...
  - Och jag är bra på det...

Ohhhhhhhh vad sa han precis???

- **Kurser på Distans med start i febuari 2021**

- Affärsmannaskap för utvecklare/konsulter
  - https://education.systementor.se/utbildningar/affman

- Säkerhet för .NET webbutvecklare
  - (Denna kurs borde vara obligatorisk för alla utvecklare)
  - https://education.systementor.se/utbildningar/devsec

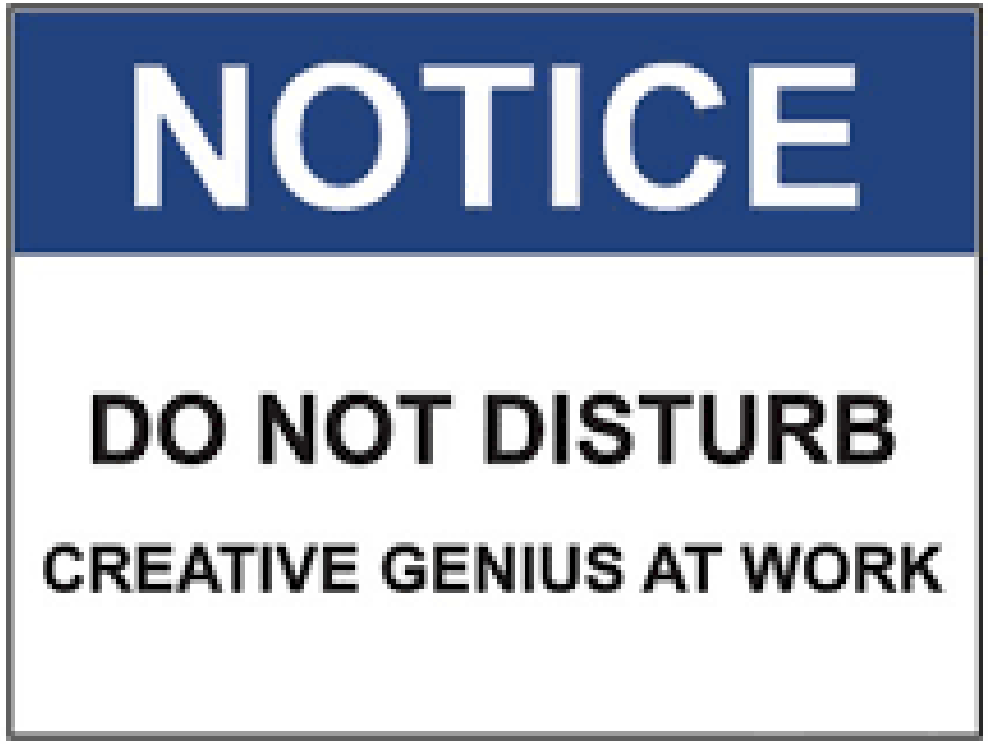
Ok mindre skryt:

- **Jag "tappade" min första burk 2001. En Linuxserver som stod i ett DC i USA. Jag vet än idag inte hur dom kom in och rootade den**

- **Jag tappade min andra burk 2005. Också i USA. En Windows-server med web+SQL Server och det var en KLASSISK SQL Injection...tillsammans med dåligt konfad SQL så kunde dom skapa en Windows-användare (administratör) och logga in med RDP...**

  - Båda servrarna var bara..."snälla support. Scratcha dessa och ominstallera"

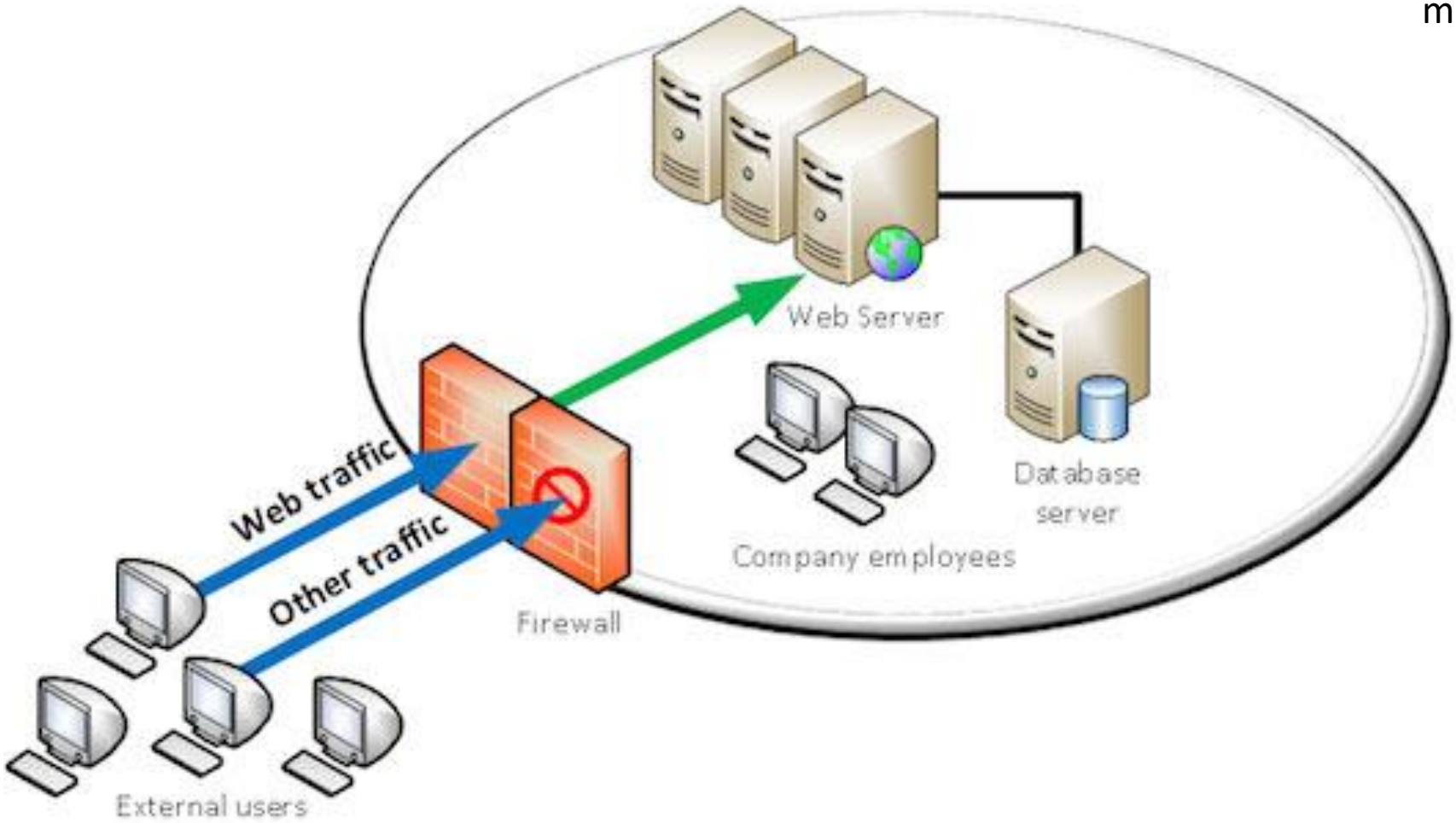
Om seminariet...vad har säkerhet med mig att göra?



Vi har nog svårt med keep up-to-date med alla Javascriptramverk, databasanrop, web frameworks etc etc etc.

"Det fixar IT-säkerhetstekniker"

"Sätt upp en firewall och skydda min fantastiska skapelse"



Riskförståelse #1: Så funkar Internet

- När ni ändå är här...jag har lite semesterbilder jag kan visa … ;)

- Note to stefan
- C:\Users\stefan\OneDrive - Systementor Aktiebolag\WebSecurity\New York

Dvs...kommunikation

- Är INTE point to point.
- Min dator vet INTE hur den ska hitta till harenet.ad.jp i Japan tex...
- Min dator kan gå ett steg (default gateway)
- Sen bestämmer nästa part (router) var jag ska gå vidare
- Går igenom ett antal mellanhänder (routers)

tracert www.harenet.ad.jp

```
 1     2 ms     *        2 ms  RT-AC66U_B1-5620 [192.168.1.1]
 2     4 ms    70 ms     4 ms  31-209-4-161.cust.bredband2.com [31.209.4.161]
 3     4 ms     4 ms     4 ms  83-233-72-5.cust.bredband2.com [83.233.72.5]
 4    17 ms     3 ms     4 ms  83-233-72-4.cust.bredband2.com [83.233.72.4]
 5    52 ms     3 ms     3 ms  hu0707-sto-mar36-cr1.se.bredband2.net [83.233.9.202]
 6     4 ms     *       31 ms  100.64.11.1
 7     4 ms     6 ms     6 ms  et-0-0-61.edge1.Stockholm1.Level3.net [213.249.107.21]
 8     *        *        *     Request timed out.
 9     6 ms     5 ms     6 ms  ae-13.r01.stocse01.se.bb.gin.ntt.net [129.250.9.49]
10    38 ms    91 ms   137 ms  ae-8.r24.amstnl02.nl.bb.gin.ntt.net [129.250.3.68]
11    52 ms    88 ms    39 ms  ae-3.r25.amstnl02.nl.bb.gin.ntt.net [129.250.4.69]
12     *      112 ms   112 ms  ae-5.r24.asbnva02.us.bb.gin.ntt.net [129.250.6.162]
13   214 ms   168 ms   195 ms  ae-2.r24.snjsca04.us.bb.gin.ntt.net [129.250.6.237]
14   193 ms   171 ms   244 ms  ae-0.r25.snjsca04.us.bb.gin.ntt.net [129.250.3.147]
15   277 ms   274 ms     *     ae-21.r30.tokyjp05.jp.bb.gin.ntt.net [129.250.5.77]
16   334 ms   273 ms   329 ms  ae-2.r02.tokyjp05.jp.bb.gin.ntt.net [129.250.3.22]
17     *        *        *     Request timed out.
18   299 ms   502 ms   286 ms  r033.tr9.kct.ne.jp [211.125.119.33]
19   327 ms   282 ms   360 ms  r026.tr9.kct.ne.jp [211.125.119.26]
20   320 ms   274 ms   273 ms  r106.tr9.kct.ne.jp [211.125.119.106]
21   342 ms   278 ms   320 ms  103-14-13-3.c2.ptr.chiroro.ne.jp [103.14.13.3]
```

Routande protokoll => MiTM

Routande protokoll => MiTM

Tänk er att jag är på semester i New York. Det är innan Internet-eran så när jag har slut på pengar skickar jag ett vykort med ett meddelande till min pappa i Sverige.

”Hej Pappa! Slut på pengar...Skicka några tusen dollar i ett brev tillbaka till mig (Stefan Room 12, Hotel The Golden Puck, 12 3rd Avenue, NY)”

Hur färdas mitt vykort?
- jag lämnar det i receptionen
- personal lägger det på lådan
- lådan töms av postpersonal
- till lokala postkontoret
- till NY post Office Central
- till flygplatsen
- säck bärs in i flygplanet
- landar Arlanda

etc etc etc

Ganska många mellansteg (routes, HOPS)

Vad kan tex personalen i receptionen göra???

INTERNET ÄR ALLTSÅ SOM GJORT FÖR MiTM

Både tjuvlyssna … och förändra/förvanska information
Näääää? Jooooo

Note to Stefan: C:\Users\stefan\OneDrive - Systementor Aktiebolag\WebSecurity

- https://www.theregister.com/2011/01/25/tunisia_facebook_password_slurping/

T.o.m World peace and freedom really IS at stake!

Ok...och doomsday warnings aside

What happens if...

Er sajt delaktig i malwaredistribution
Badwill/stämningar etc etc

Er sajt delaktig i spridande av virus
Badwill/stämningar etc etc

Det går att tjyvlyssna och sno besökares konton (id och lösen). Badwill/stämningar etc etc

Enkel lösning...

HTTPS alltid (certifikat)

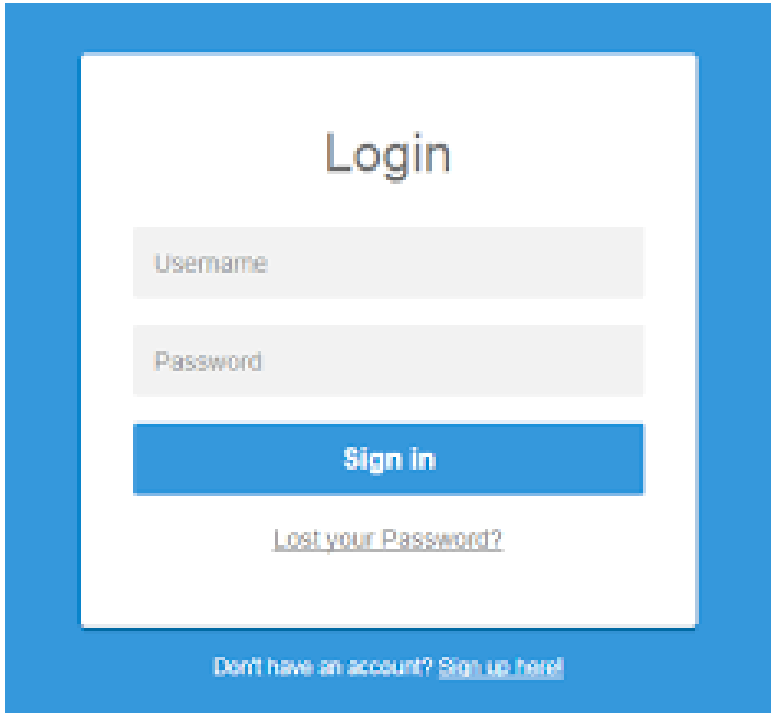
Confidentiality (kryptering)
Integrity (checksum/hash)
Authentication (cert = prata med rätt part)

(vi går in på allt detta i detalj på kursen Säkerhet för .NET webbutvecklare)

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...

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

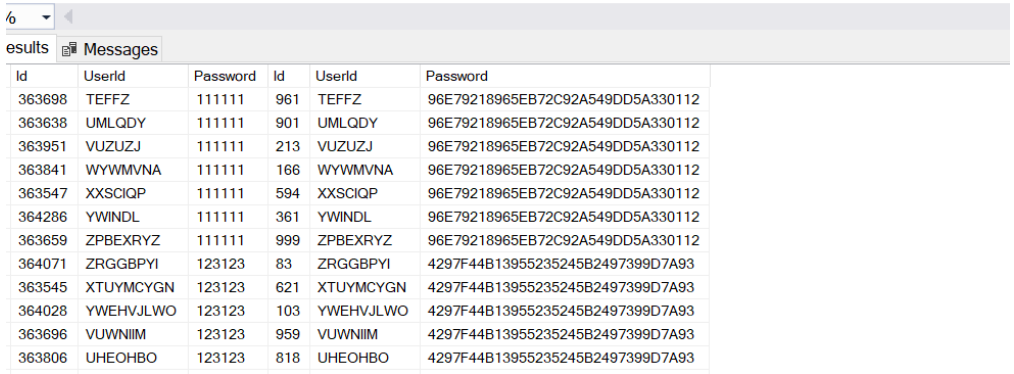
	Id	UserId	Password
1	1	WQVJEX	5B1B68A9ABF4D2CD155C81A9225FD158
2	2	ALVMN	5B1B68A9ABF4D2CD155C81A9225FD158
3	3	VRHGKAPWCG	185662EA4FD642D37CB02520DFBDBECD
4	4	BDJDIUREQ	8AFA847F50A716E64932D995C8E7435A
5	5	WZXCIWNUZC	D6CA20CF73048F6E7B818E6DE220CDCB
6	6	GSULKXRFYK	3FC0A7ACF087F549AC2B266BAF94B8B1
7	7	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

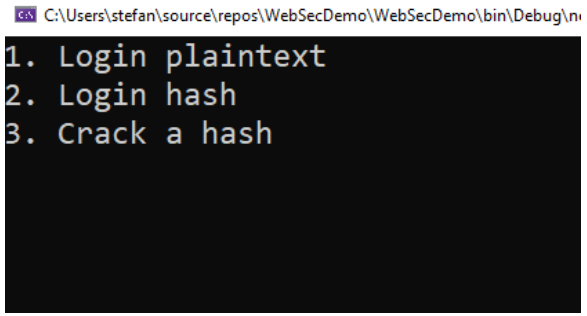
1. Ladda ner med common passwords....alltså seriöst det finns filer med miljontals poster

2. Skapa hashar på alla dom posterna...

3. Matcha mot

4. Träff!? Japp...bara att logga in

Vi kodar...



https://github.com/aspcodenet/WebSecDemo

Ok what about 12-åringen … Hashcat…

- cd /mnt/c/users/stefan/downloads/hashcat-5.0.0
- del md5.pot
- hashcat -a 0 -m 0 --potfile-path md5.pot demo2.txt rockyou.txt

Kvar...

- Hur undviker man hashcat-attacker
- Andra typer av threats... OWASP
- Authentication/authorisation
  - MFA
  - Automatiska verktyg
  - Det går inte att pentesta bristande Authorisation... = Code Review måste till

Boka in mig för konsultation – hur kan jag hjälpa er i ert projekt?

stefan.holmberg@systementor.se
070 – 431 49 65