

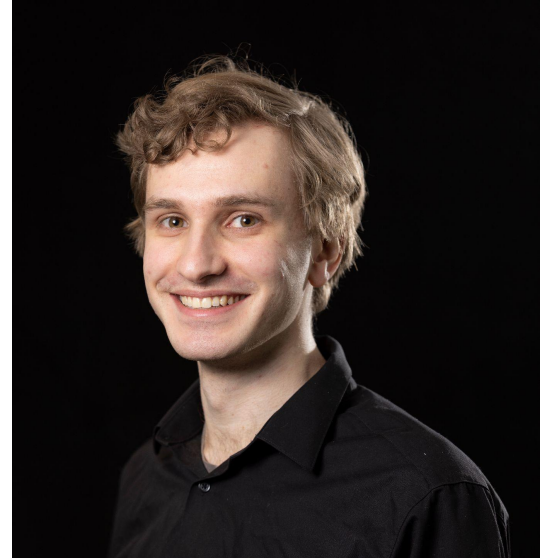
Software is stuk

En nu?

Jerre Starink & Yoep Kortekaas

jerre@UT \$ whoami

- PhD student @ SCS vakgroep Universiteit Twente
 - Malware Analyse
- Twente Hacking Squad lid sinds 2021
 - Reverse Engineering
 - Pwning



yoep@UT \$ whoami

- PhD student @ SCS vakgroep Universiteit Twente
 - Privacy-preserving machine learning
- Twente Hacking Squad lid sinds 2020
 - Cryptografie
 - Reverse Engineering



Twente Hacking Squad

- CTF-team van de Universiteit Twente
- Capture The Flag
 - Cybersecurity puzzels



Bijna alle software
is lek



~~Bijna~~ alle software
is lek



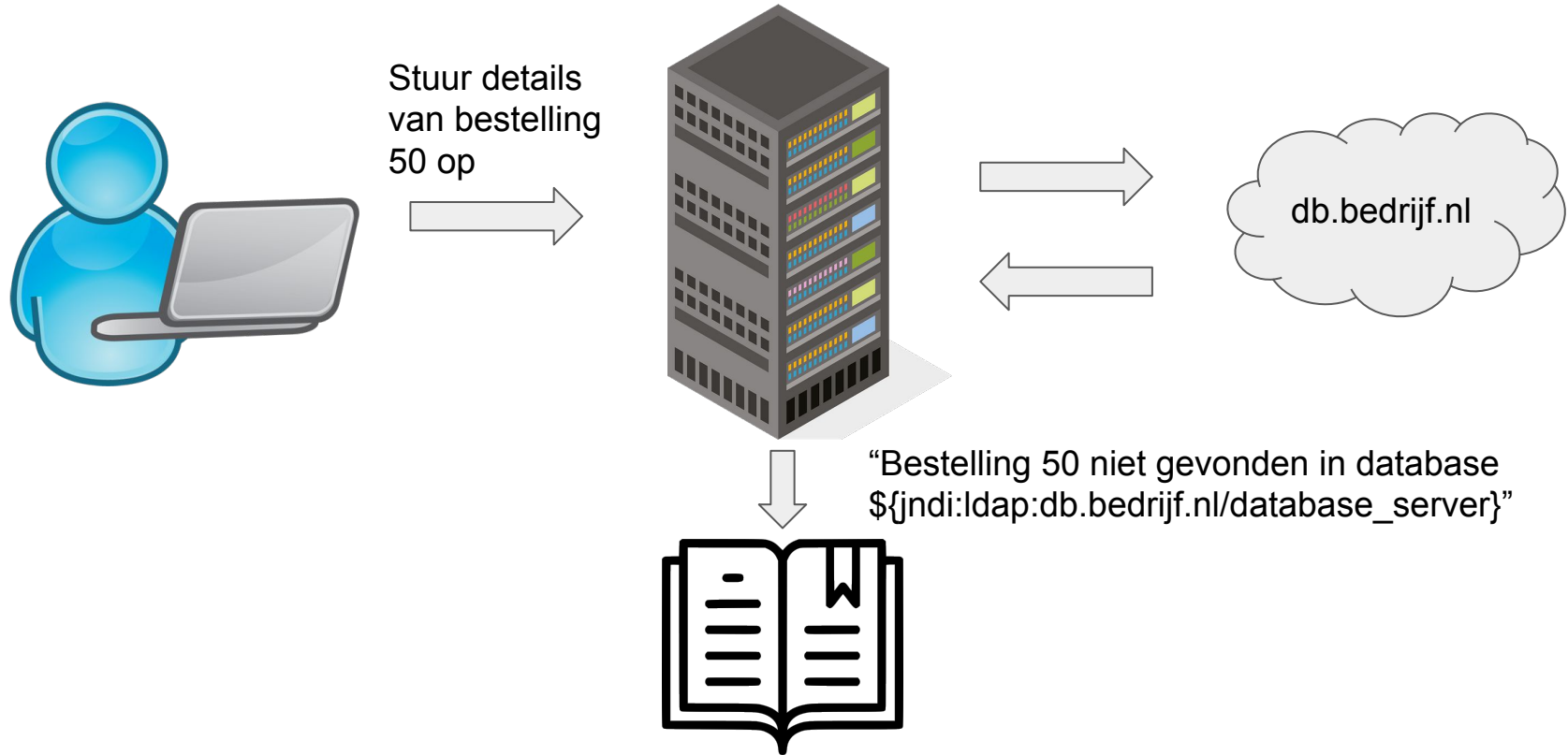
Log4J



Log4J: Wat was er aan de hand

- Log4J: Java Logging Framework
 - Wat is Java
 - Waarvoor gebruik je Log4J?
 - Log4J lookups
- Remote Code Execution
- 10 miljoen pogingen per uur[1]

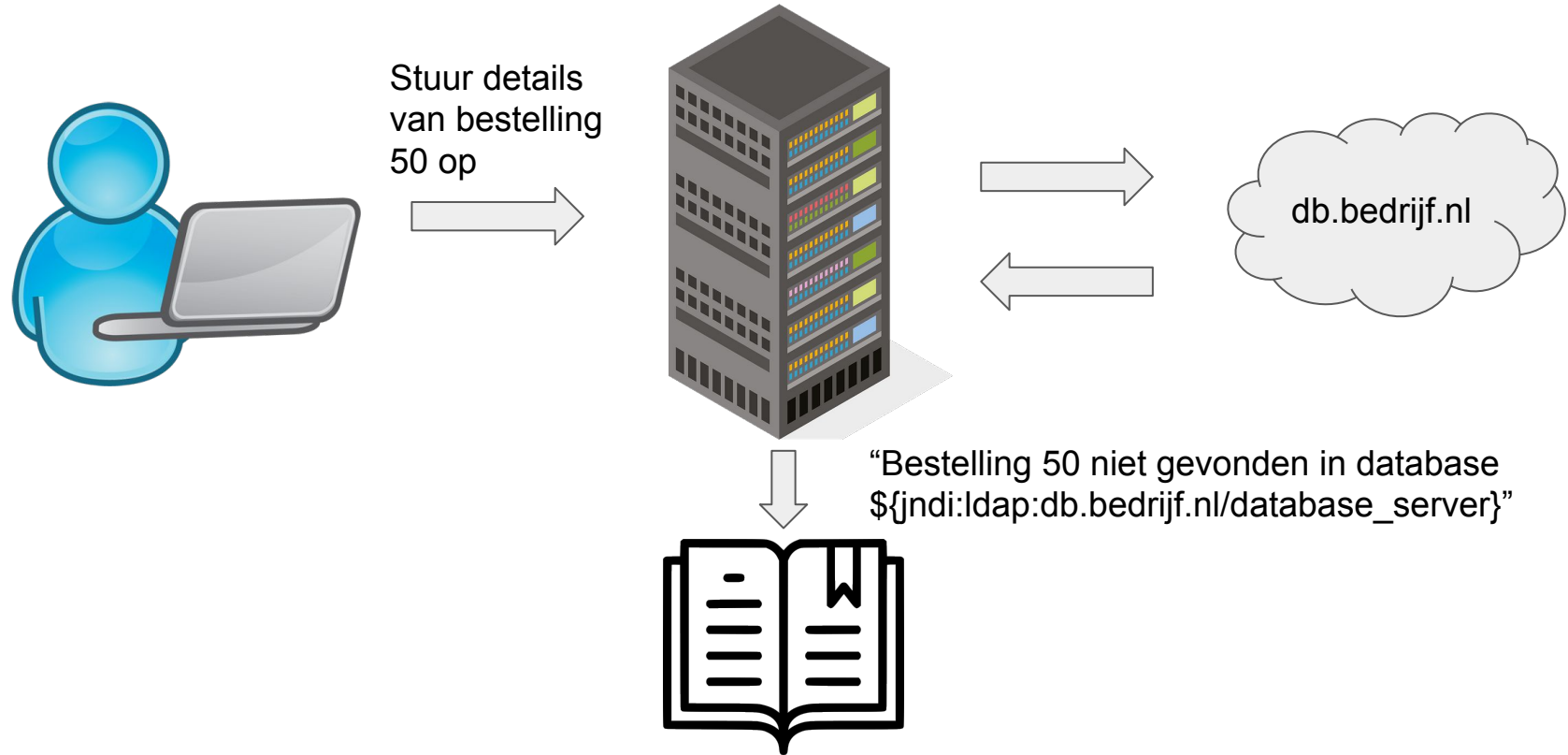
Log4J: Wat was er aan de hand



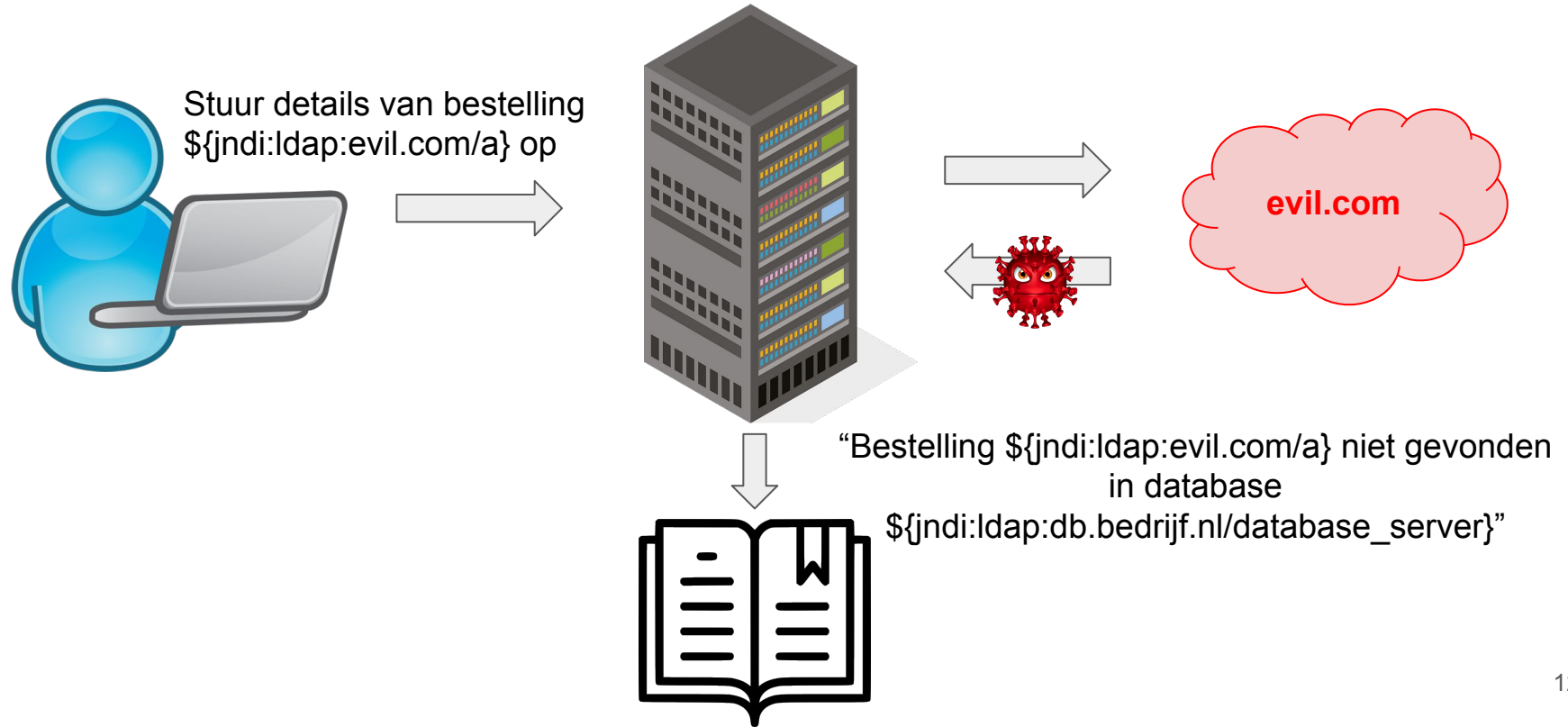
Log4J: Wat was er aan de hand



Log4J: Wat was er aan de hand



Log4J: Wat was er aan de hand



Log4J: Wat was er aan de hand



Log4J: Hoe kan het misbruikt worden

- Crypto Miner
- Defacement
- Foutieve informatie
- Ransomware
- Aanvalsproxy

Log4J: Demo



Log4J: Hoe kan het misbruikt worden

- Crypto Miner
- Defacement
- Foutieve informatie
- Ransomware
- Aanvalsproxy



Leuker kunnen we het niet maken,
wel makkelijker





Gehackt worden:

Leuker kunnen we het niet maken,
wel ~~makkelijker~~ *moeilijker*

Hoe kan je jezelf voorbereiden

Basis:

- Updates
- Backups
- Security training
- Penetratie testen
- Administratie

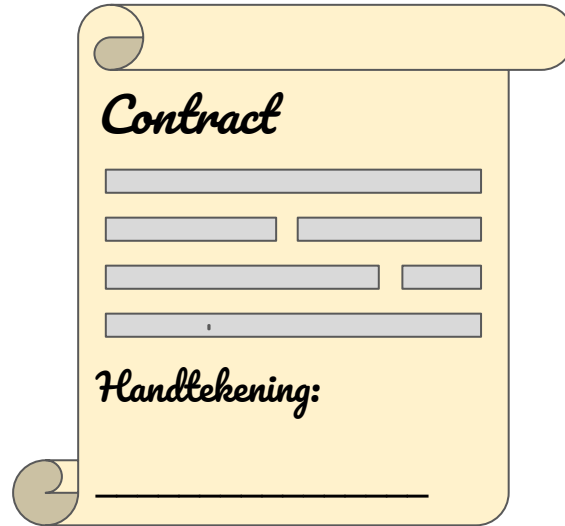
Volgende Stap:

- Containerisatie
- Infrastructure as Code
- Infiltratie detectie

Oracle: Ghostly Signatures



Oracle: Ghostly Signatures

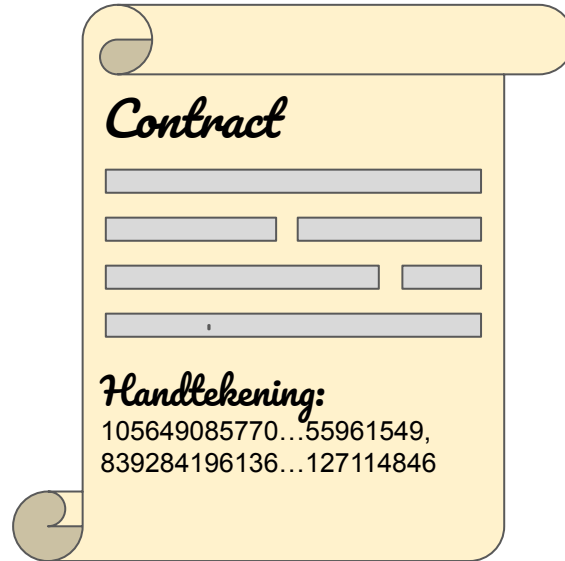


Oracle: Ghostly Signatures

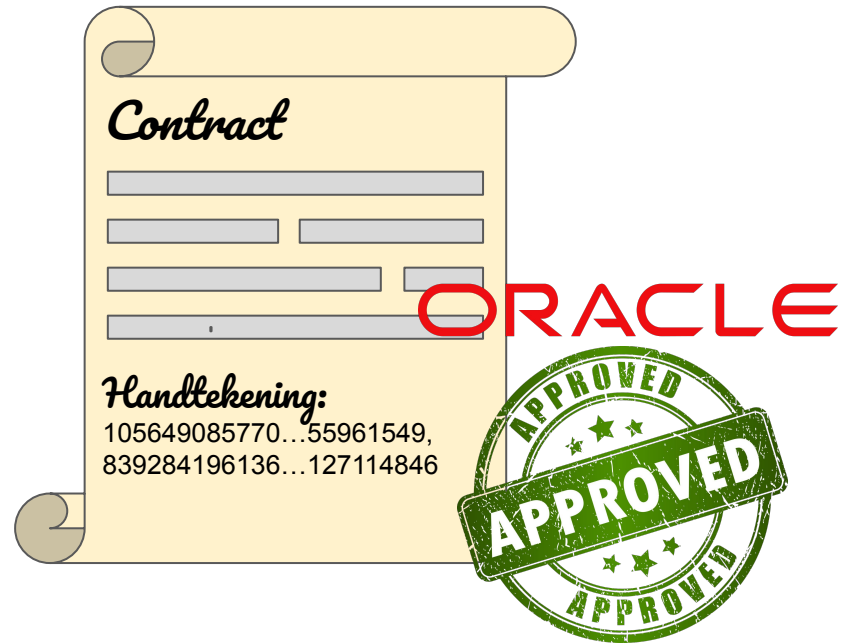


10564908577005981512544318
33031470075896282669392461
7305408352692851555961549,
83928419613626119610376417
49261341436578836568673289
8524595542136424127114846

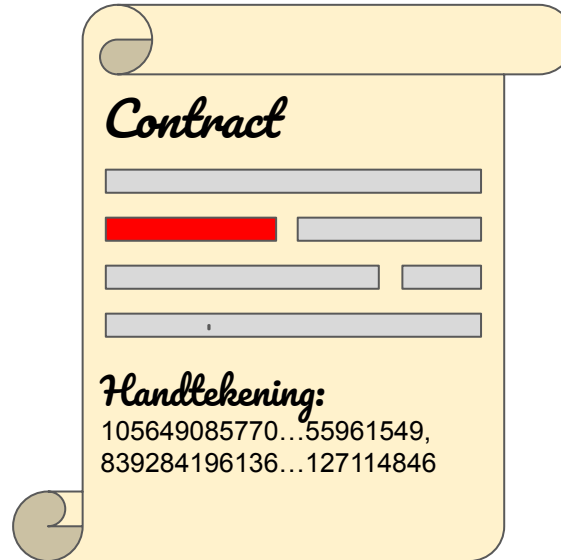
Oracle: Ghostly Signatures



Oracle: Ghostly Signatures



Oracle: Ghostly Signatures



Oracle: Ghostly Signatures



Oracle: Ghostly Signatures

- Digitale handtekeningen zijn moeilijk te vervalsen
 - Er is altijd maar één handtekening juist.
 - Zonder de “geheime sleutel” is domweg gokken totdat je het juiste getal vind de enige manier.
 - Hele grote getallen zijn moeilijk te raden.

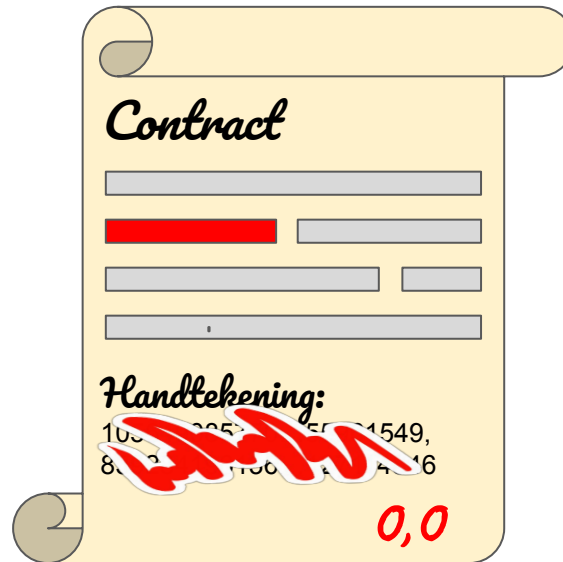
Oracle: Ghostly Signatures

- De theorie klopt.
- Maar de implementatie had een fout...

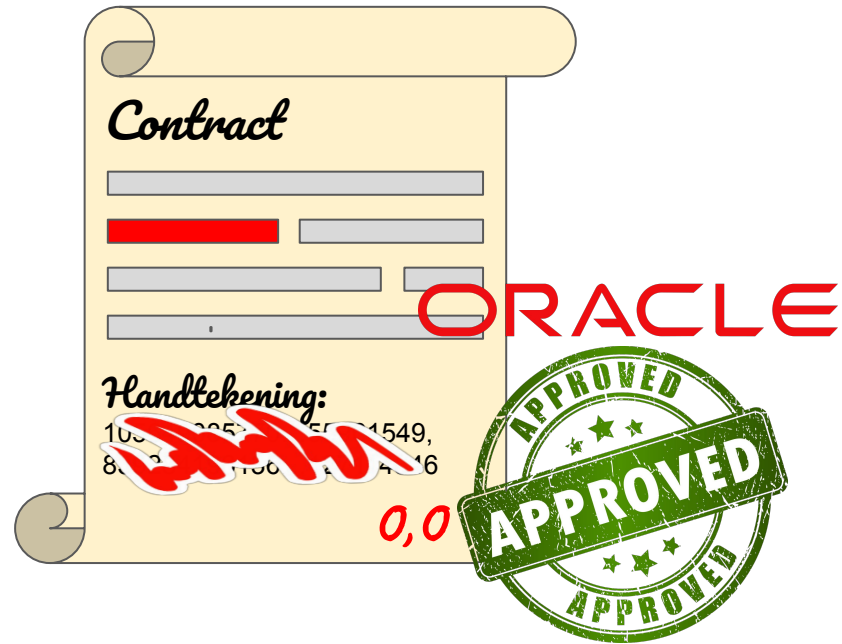
Oracle: Ghostly Signatures



Oracle: Ghostly Signatures



Oracle: Ghostly Signatures





Gehackt worden:

Leuker kunnen we het niet maken,
wel ~~makkelijker~~ *moeilijker*

Hoe kan je jezelf voorbereiden

Basis:

- Updates
- Backups
- Security training
- Penetratie testen
- Administratie

Volgende Stap:

- Containerisatie
- Infrastructure as Code
- Infiltratie detectie

Microsoft: Office Macros



Microsoft Office: A problem of macro scale

- Oude techniek gemaakt in 1993 (Office 3)
- Een manier om documenten interactief te maken
 - Bijv. Automatisch invullen van Excel Sheets
- Veel bedrijven gebruiken het voor automatisatie

Microsoft Office: A problem of macro scale



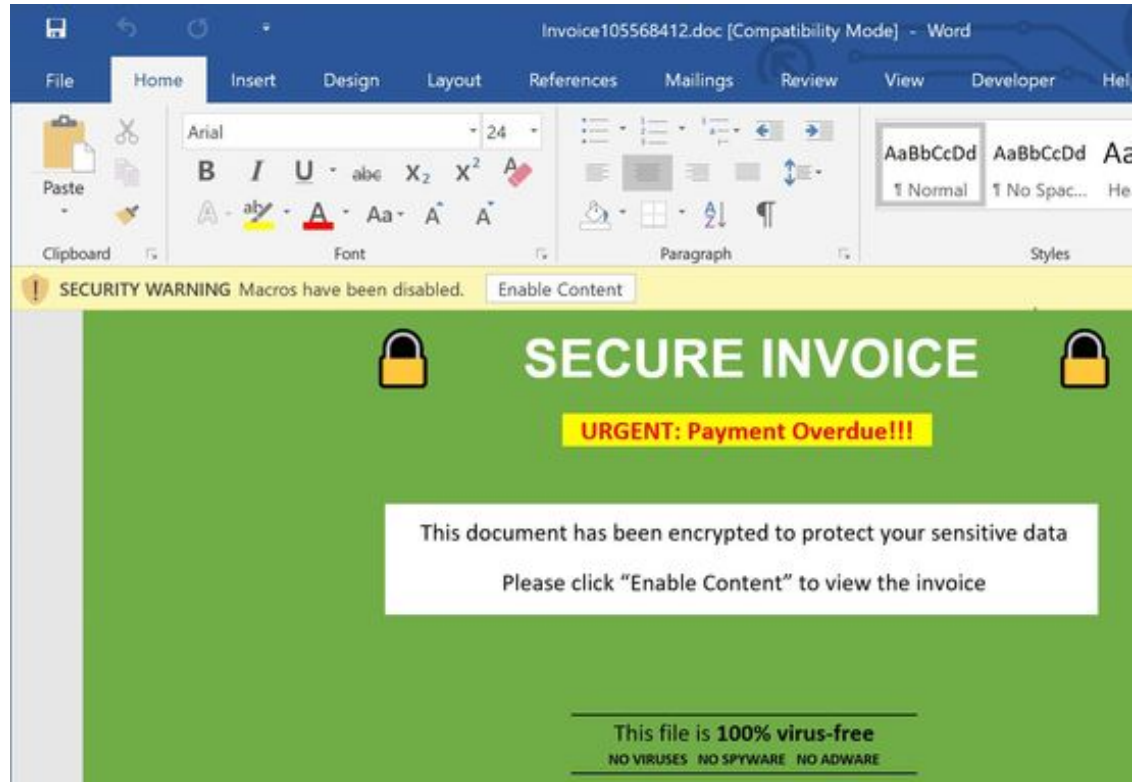
Aandelen.xlsx



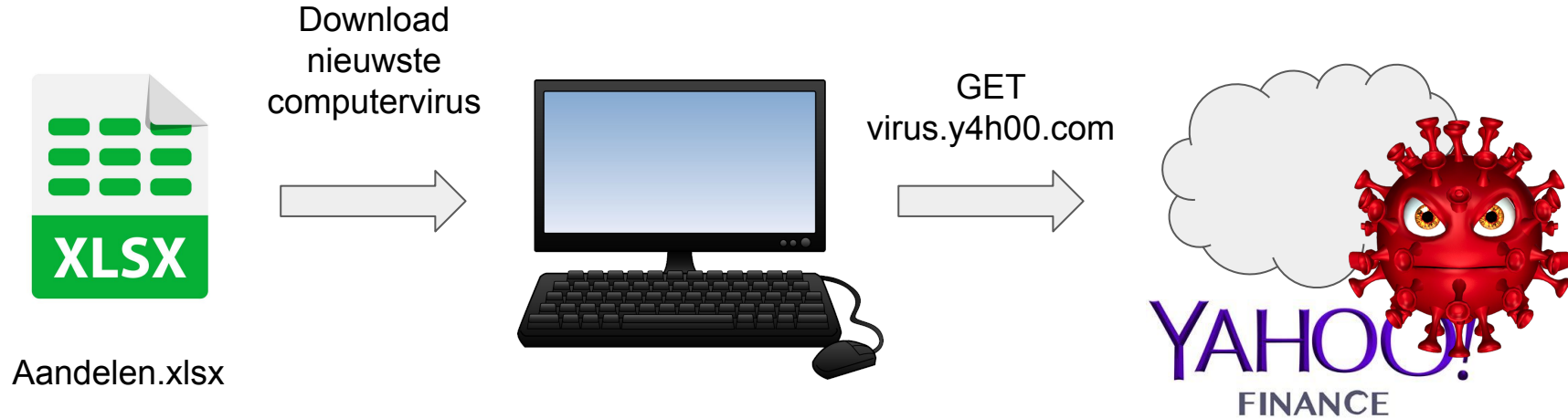
Microsoft Office: A problem of macro scale



It's not a
bug, it's
a feature!



Microsoft Office: A problem of macro scale



MS Office Macros: Demo

Microsoft Office: A problem of macro scale (4)

- Mensen klikken snel op “Alles Accepteren” zonder er over na te denken
- Hackers maken hier graag misbruik van
- Gevolgen zijn vergelijkbaar met die van Log4J



Gehackt worden:

Leuker kunnen we het niet maken,
wel ~~makkelijker~~ *moeilijker*

Hoe kan je jezelf voorbereiden

Basis:

- Updates
- Backups
- Security training
- Penetratie testen
- Administratie

Volgende Stap:

- Containerisatie
- Infrastructure as Code
- Infiltratie detectie

SQL Injection

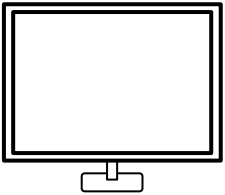


SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks

SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login



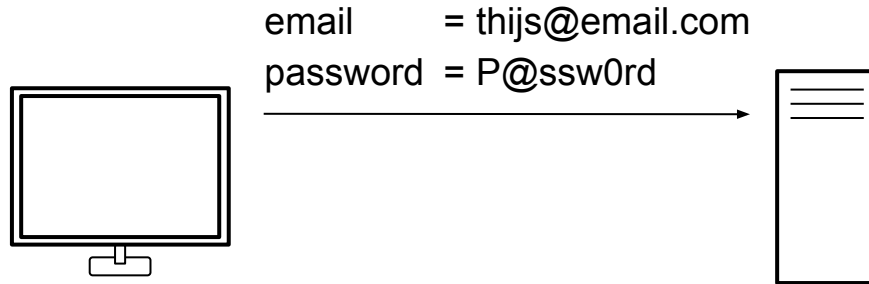
Login

Email

Password

SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login



Login

Email

Password

SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login

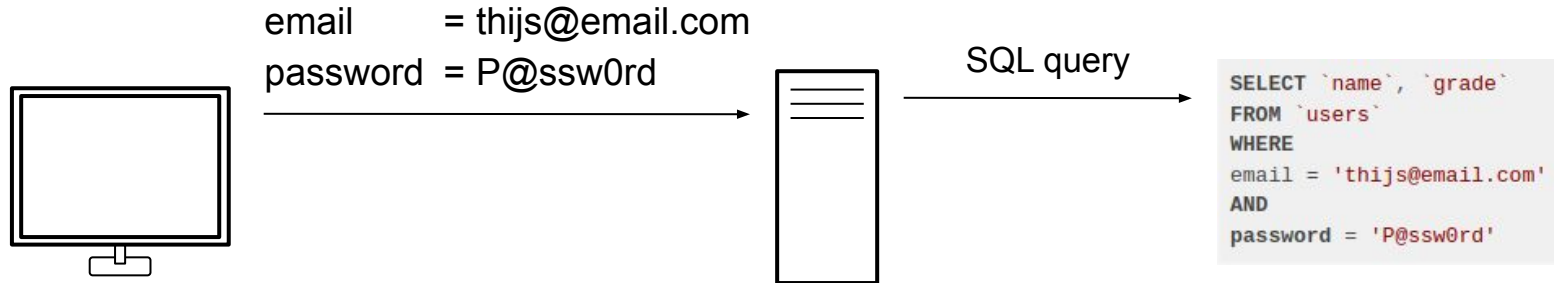
Login

Email

thijs@email.com

Password

Submit



SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login

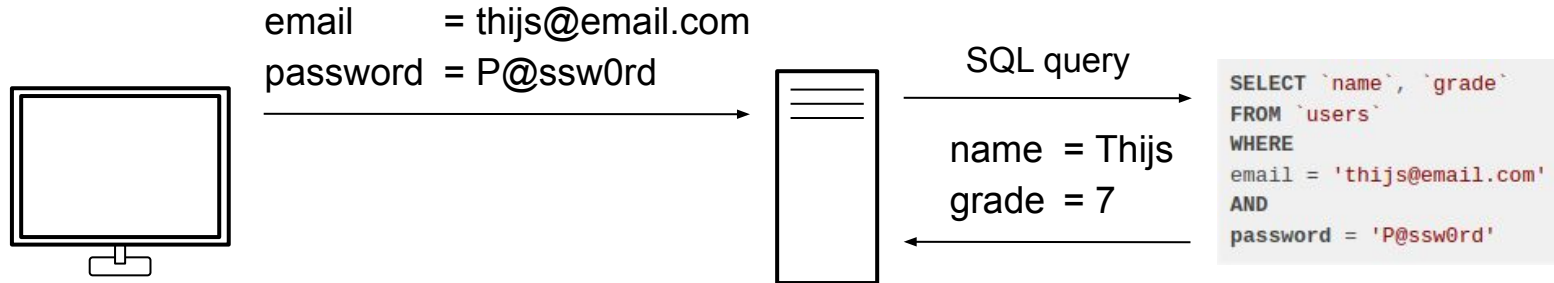
Login

Email

thijs@email.com

Password

Submit



SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login

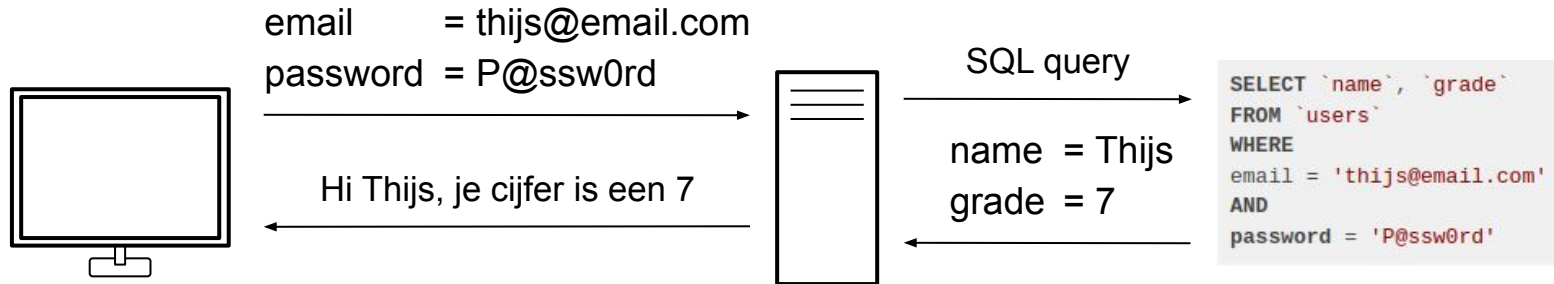
Login

Email

thijs@email.com

Password

Submit



SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login
- Invoer manipuleren om toegang te verkrijgen

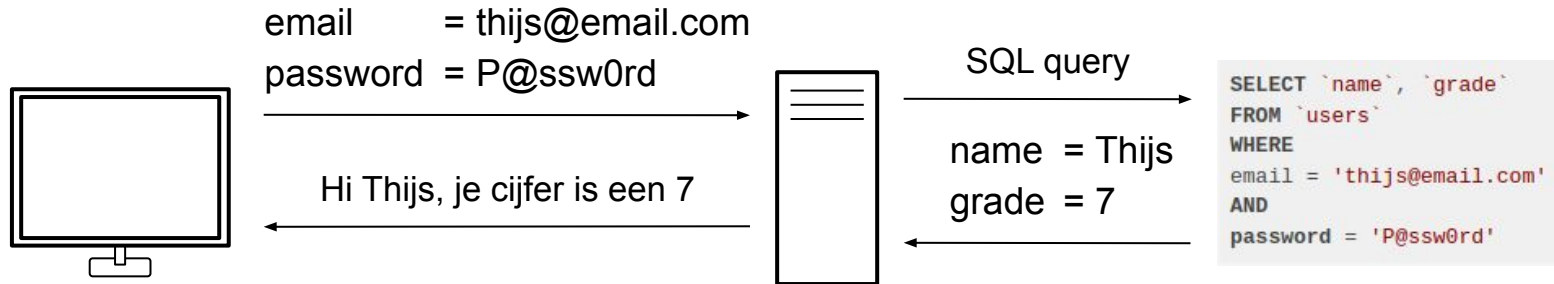
Login

Email

thijs@email.com

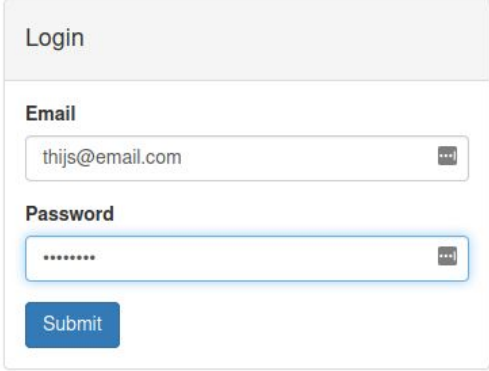
Password

Submit



SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login
- Invoer manipuleren om toegang te verkrijgen

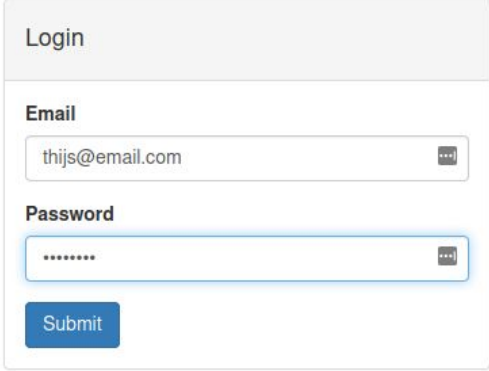


The image shows a web login interface. At the top is a header with the word 'Login'. Below it are two input fields: 'Email' containing 'thijs@email.com' and 'Password' containing a masked password '*****'. Both fields have a small icon on the right side. Below the password field is a blue 'Submit' button.

```
SELECT `name`, `grade`  
FROM `users`  
WHERE  
email = '<email>'  
AND  
password = '<password>'
```

SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login
- Invoer manipuleren om toegang te verkrijgen



The image shows a web login interface. At the top is a header with the word 'Login'. Below it are two input fields: 'Email' containing 'thijs@email.com' and 'Password' containing a masked password '*****'. Both fields have a small 'x' icon to clear the input. Below the password field is a blue 'Submit' button.

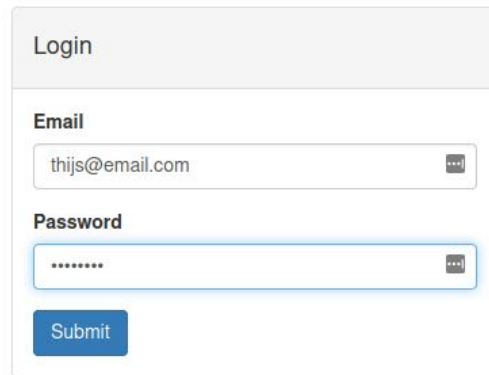
```
SELECT `name`, `grade`  
FROM `users`  
WHERE  
email = '<email>'  
AND  
password = '<password>'
```



```
SELECT `name`, `grade`  
FROM `users`  
WHERE  
email = '<email>'  
AND  
password = 'incorrect'  
  
FALSE
```

SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login
- Invoer manipuleren om toegang te verkrijgen
 - Door een ' karakter toe te voegen, sluiten we het wachtwoord veld af, en kunnen we onze eigen code uitvoeren die **TRUE** terug geeft.



The image shows a web login interface. At the top is a header with the word 'Login'. Below it are two input fields: 'Email' containing 'thijs@email.com' and 'Password' containing '*****'. Both fields have a small '...' icon on the right. Below the password field is a blue 'Submit' button.

```
SELECT `name`, `grade`  
FROM `users`  
WHERE  
email = '<email>'  
AND  
password = '<password>'
```



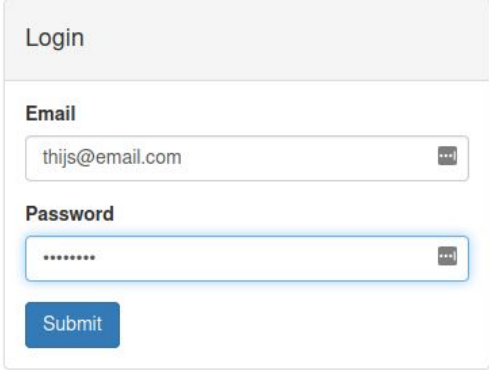
```
SELECT `name`, `grade`  
FROM `users`  
WHERE  
email = '<email>'  
AND  
password = 'incorrect' OR '1'='1'
```

TRUE

SQL-injection - De basis

- Invoer van gebruiker wordt vertrouwd, en naar een database doorgestuurd zonder (goede) checks
- Voorbeeld - Website login
- Invoer manipuleren om toegang te verkrijgen
 - Door een ' karakter toe te voegen, sluiten we het wachtwoord veld af, en kunnen we onze eigen code uitvoeren die **TRUE** terug geeft.
- Invoer moet opgeschoond worden:

`incorrect' OR '1'='1` $\longrightarrow$ `incorrect\' OR \'1\'=\'1`



The image shows a web login form. At the top is a header with the word 'Login'. Below it are two input fields: 'Email' containing 'thijs@email.com' and 'Password' containing seven dots. Both fields have a small icon on the right side. Below the password field is a blue 'Submit' button.

SQL Injection: Demo



Conclusie

- Software is stuk
- Blijf up-to-date
- Maak backups
- Creëer bewustzijn
 - Trainingen
 - Pen testing



Gehackt worden:

Leuker kunnen we het niet maken,
wel ~~makkelijker~~ *moeilijker*