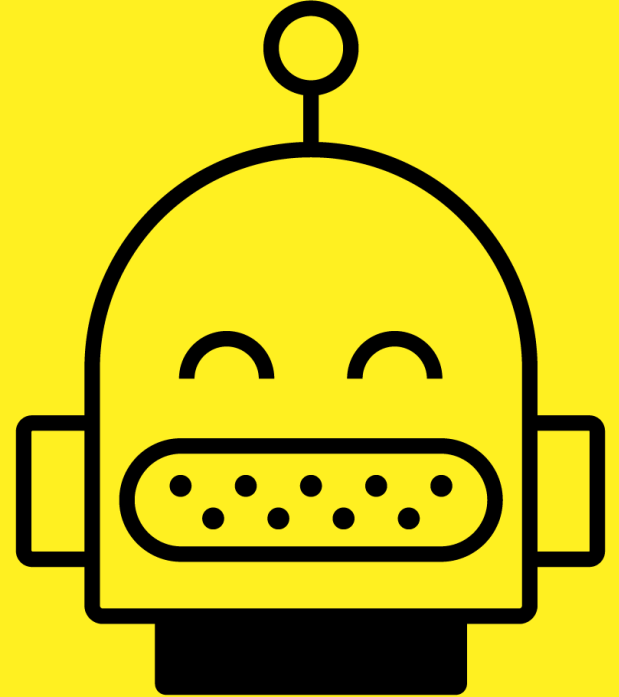




Project Tech

Security



Collegejaar 23/24

Creating Tomorrow

# Agenda

- Het belang van security - voor developers EN voor ontwerpers
- Demonstratie van mogelijke aanvallen
- Praktische tips voor veilige systemen

Is security belangrijk... ... voor een matchingsite?



Figuur 2

# ASHLEY MADISON®

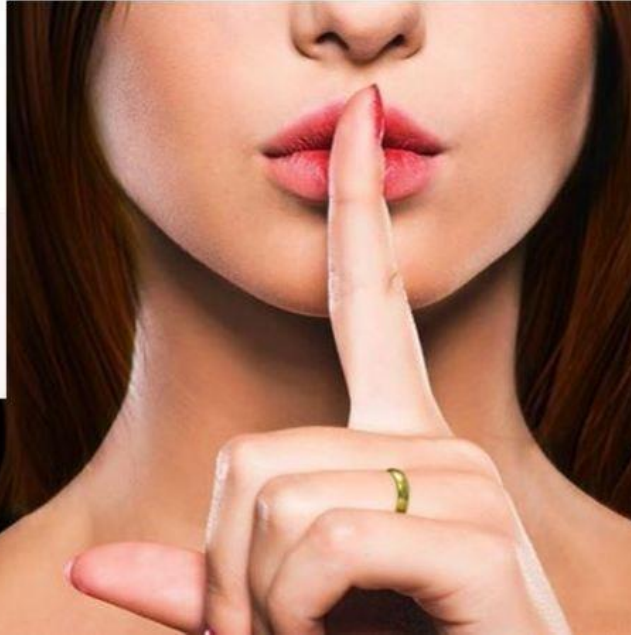
Life is short. Have an affair.®

Begin door ons uw relatiestatus te vertellen:

Selecteer

[Uw matches bekijken »](#)

Meer dan **37.565.000** anonieme leden!



## Ashley Madison

- Datingsite voor 'affaires'
- Gehackt in 2015 door 'The Impact Team'
- Gegevens van 37 miljoen gebruikers online gezet

Figuur 3

## ASHLEY MADISON HACK REVEALS ITS 37 MILLION USERS DEEPEST SEXUAL FANTASIES

[www.independent.co.uk](http://www.independent.co.uk)

### *SOUNDS LEGIT —*

Ashley Madison admits using fembots to  
lure men into spending money

[arstechnica.com](http://arstechnica.com)

Pastor outed on Ashley  
Madison commits suicide

[cnn.com](http://cnn.com)

### *AGAIN?!? —*

Dear Ashley Madison user, I know everything  
about you. Pay up or else

Emails threaten to publish intimate details  
unless members pay a hefty ransom.

[arstechnica.com](http://arstechnica.com)

**Overspelsite Ashley Madison wil voor  
11,2 miljoen schikken in datalek-zaak**

[nos.nl](http://nos.nl)

# Slecht werk van de back-end developers?

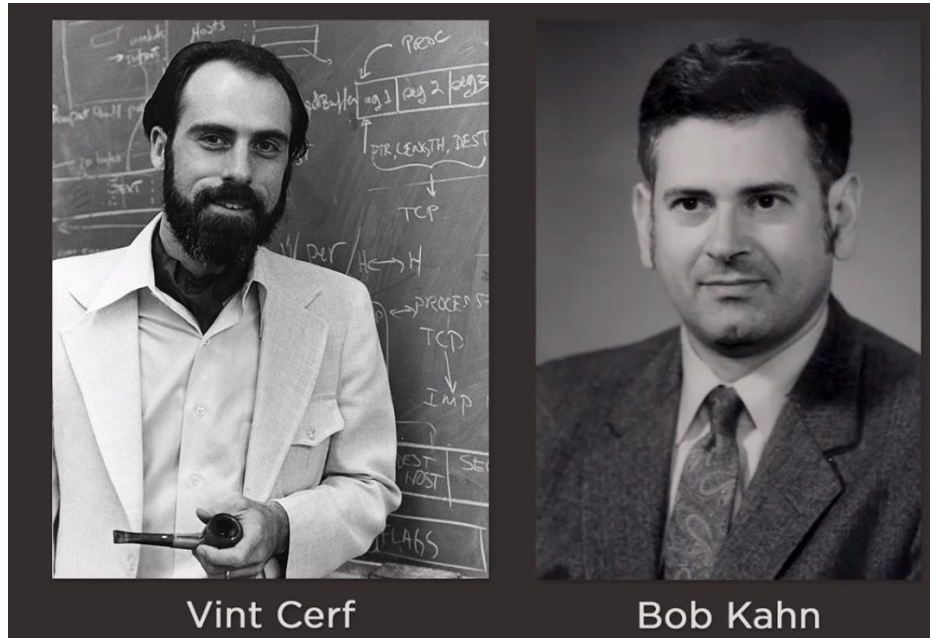
Zeker...

... maar het is ook een ontwerpkeuze om:

- Geld te vragen voor het verwijderen van gebruikersgegevens uit je database, en dat vervolgens niet te doen
- Chatbots in te zetten om je klanten te bedriegen
- Uberhaupt een site voor vreemdgangers te ontwerpen



Figuur 4



Figuur 5

## Het Internet

- ‘Uitgevonden’ in de jaren '70
- Bedoeld voor academisch gebruik
- Nooit voorzien hoe groot het zou worden
- In het ontwerp destijds **GEEN ENKELE AANDACHT** voor beveiliging

# Afluisteren van internetverkeer

Alles wat we over Internet versturen, kan verrassend makkelijk worden afgeluisterd.



Figuur 6

Wi-Fi Pineapple - speciale antenne  
voor afluisteren draadloze  
netwerken

Software voor opvangen en  
analyseren van  
netwerkverkeer



Figuur 7



# Demo



Figuur 6

# Website Geert Wilders gehackt!

*“Daardoor lijkt het bijvoorbeeld net alsof de vroegere Irakese minister van Informatie, Mohammed Saeed al-Sahaf, de nieuwe perschef van Wilders is geworden.”*

[Reijnders, 2005]



Figuur 8

## Wat was er echt aan de hand?

`http://www.geertwilders.nl/index.php?title=`

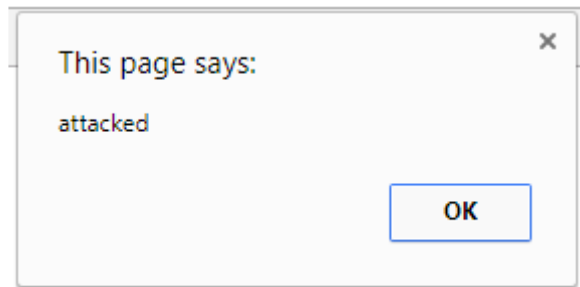
```
<h2>Nieuwe perschef Groep Wilders: `Geert heeft zeer goed  
onafhankelijkheidsverklaring en gaat zeer veel zetels halen.`</h2><br><img  
src=http://www.welovetheiraqiinformationminister.com/images/07-minister.jpg>
```

# Demo Cross Site Scripting

XSS: een hacker kan scripts draaien in de browser van je bezoeker

Voorbeeld code:

```
let txt = "Welcome " + req.query.name  
res.write(txt)
```



Voorbeeld aanval:

Stuur iemand de volgende link:

```
index.js?name=guest<script>alert('attacked')</script>
```

Als je eenmaal javascript in de browser kunt draaien, kun je de hele site overnemen, info uit cookies stelen, etc.

# SQL injection

Voorbeeld code:

```
let userId = rec.query.userid  
let SQL = "SELECT * FROM Users WHERE UserId = " + userId
```

Voorbeeld aanval:

UserId:

Dit geeft de volgende SQL query:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

1=1 is altijd waar, dus deze query geeft alle gebruikers terug.

Wat als er gebruikersnamen en wachtwoorden in de database staan?

# Demo SQL injection



Figuur 11

# Wat te doen?

## 1. Houd je software up to date



- Installeer de nieuwste versie(s) van je software
- Controleer je gebruikte node modules
  - `npm audit`
  - `npm update`

```
Windows PowerShell
PS D:\Surfdrive\Blok Tech\backend\nodecode> npm audit
# npm audit report

dicer *
Severity: high
Crash in HeaderParser in dicer - https://github.com/advisories/GHSA-wm7h-9275-46v2
No fix available
node_modules/dicer
  busboy <=0.3.1
  Depends on vulnerable versions of dicer
    node_modules/busboy
      multer <=2.0.0-rc.3
      Depends on vulnerable versions of busboy
        node_modules/multer

3 high severity vulnerabilities

Some issues need review, and may require choosing
a different dependency.
PS D:\Surfdrive\Blok Tech\backend\nodecode> |
```

Dependabot alerts · ivo-online · nodecode

Search or jump to... Pull requests Issues Codespaces Marketplace Explore

ivo-online / nodecode Public

<> Code Issues Pull requests Actions Projects Wiki Security 1 Insights Settings

Overview

Reporting

Policy

Advisories

Vulnerability alerts

Dependabot 1

Code scanning

### Dependabot alerts

isopen

1 Open 0 Closed Package Ecosystem Manifest

Crash in HeaderParser in dicer **High**

#1 opened 5 days ago • Detected in dicer (npm) · package-lock.json

Dependabot alerts surface known security vulnerabilities in some dependency manifest files. Dependabot security updates automatically keep your application up-to-date by updating dependencies in response to these alerts. Dependabot version updates can also help keep dependencies up-to-date.

Crash in HeaderParser in dicer · 1

github.com/ivo-online/nodecode/security/dependabot/1

Search or jump to... Pull requests Issues Codespaces Marketplace Explore

ivo-online / nodecode Public

<> Code Issues Pull requests Actions Projects Wiki Security 1 Insights Settings

Dependabot alerts / #1

## Crash in HeaderParser in dicer #1

**Open** Opened 5 days ago on dicer (npm) · package-lock.json

| Package     | Affected versions | Patched version |
|-------------|-------------------|-----------------|
| dicer (npm) | <= 0.3.1          | None            |

This affects all versions of package dicer. A malicious attacker can send a modified form to server, and crash the nodejs service. A complete denial of service can be achieved by sending the malicious form in a loop.

dependabot[bot] opened this 5 days ago

Dismiss alert

Severity

**High** 7.5 / 10

CVSS base metrics

|                     |           |
|---------------------|-----------|
| Attack vector       | Network   |
| Attack complexity   | Low       |
| Privileges required | None      |
| User interaction    | None      |
| Scope               | Unchanged |

# Wat te doen?

## 2. Versleutel communicatie (encryptie)



- Gebruik bestaande protocollen en standaarden
- B.v. HTTPS (SSL/TLS) en SSH
- Sta er op dat je netwerkbeheerders het ondersteunen!



# Wat te doen?



## 3. Controleer alle variabelen die van buiten je programma komen

- input van gebruikers
- data vanuit andere systemen, sites of APIs
- parameters die worden meegegeven in de URL

Verwijder alle mogelijke code, voordat je iets met de informatie doet

# Sanitise your inputs

- Valideer (ook) in de backend: validatie in de frontend is gebruiksvriendelijk, maar een hacker gebruikt echt niet jouw frontend om je site te hacken.
- Verwijder code met standaard modules zoals **xss**  
<https://jssxss.com/en/index.html>

```
const xss = require('xss')
const html = xss('<script>alert("hack");</script>')
console.log(html)
```

```
&lt;script&gt;alert("hack");&lt;/script&gt;
```

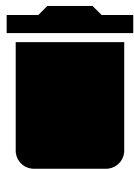
## Sanitise your inputs #2

Behalve code verwijderen, kun je ook checken of de data wel klopt. Is een e-mailadres echt een e-mailadres, bevat een getal alleen cijfers, heeft een postcode een geldig format etc.

- Gebruik in formulieren het juiste `<input type="...">` voor het soort data dat je wilt hebben.
- Gebruik een validator zoals **Validator.js**  
<https://github.com/validatorjs/validator.js>

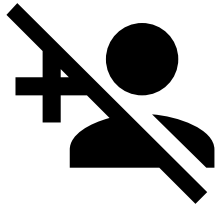
# Wat te doen?

## 4. Zet geen info voor developers live



- commentaar
- links naar verborgen pagina's
- versies van software / systemen
- zet je wachtwoorden (`.env`) niet op GitHub!

# Wat te doen?



## 5. Verwerk en bewaar geen gegevens die je niet nodig hebt

- geen onnodige persoonsgegevens vragen
- anonimiseer

# Wat te doen?



6. Bewaar een hash in plaats van een wachtwoord

# Password Hash


geheim => \$2b\$10\$3k9m5HOUOMPh1.K.FUUIsOGCDPmd5h2Om9dRHlj7j2xOM1SUKBse2

- Een hash is een rekensom op basis van de oorspronkelijke tekst
- Bewaar een hash in plaats van een wachtwoord in je database: als de database wordt gehackt, zijn de wachtwoorden nog veilig
- Het narekenen van een hash kost relatief veel rekentijd. Hackers die 1 voor 1 wachtwoorden proberen (een brute force attack) worden hiermee afgeremd
- Gebruik **Bcryptjs**  
<https://github.com/dcodeIO/bcrypt.js>

| RANK | PASSWORD   | CHANGE FROM 2015 |
|------|------------|------------------|
| 1    | 123456     | Unchanged        |
| 2    | password   | Unchanged        |
| 3    | 12345      | 2 ↗              |
| 4    | 12345678   | 1 ↘              |
| 5    | football   | 2 ↗              |
| 6    | qwerty     | 2 ↘              |
| 7    | 1234567890 | 5 ↗              |
| 8    | 1234567    | 1 ↗              |
| 9    | princess   | 12 ↗             |
| 10   | 1234       | 2 ↘              |
| 11   | login      | 9 ↗              |
| 12   | welcome    | 1 ↘              |
| 13   | solo       | 10 ↗             |
| 14   | abc123     | 1 ↘              |
| 15   | admin      | NEW              |
| 16   | 121212     | NEW              |
| 17   | flower     | NEW              |
| 18   | password   | 6 ↗              |
| 19   | dragon     | 3 ↘              |

Figuur 9

# Samenvatting

- 
- A background image showing two hands, one from the left and one from the right, with fingers interlaced to form a heart shape. The hands are light-skinned and the person is wearing a pink sleeve. The background is a solid light blue.
- 🕒 Houd je software up to date
  - 🔒 Versleutel communicatie en gegevens
  - 🔍 Controleer alle variabelen die van buiten je programma komen
  - 🗑️ Verwijder info voor developers in de productie omgeving
  - 🚫 Verwerk en bewaar geen gegevens die je niet nodig hebt
  - 🔑 Sla een hash op in plaats van wachtwoorden



# Bronvermelding

- Maarten Reijnders, 15 maart 2005, Website Wilders kwetsbaar voor 'low-tech hack', Webwereld, verkregen op 27-9-2017 van <http://webwereld.nl/e-commerce/22574-website-wilders-kwetsbaar-voor--low-tech-hack>
- Figuur 1: Gerd Altmann, 10-9-2009, online dating love heart web, online afbeelding, <https://pixabay.com/illustrations/online-dating-love-heart-web-4465754/>
- Figuur 2: What could possibly go wrong? online afbeelding, <https://software.intel.com/en-us/blogs/2013/01/06/benign-data-races-what-could-possibly-go-wrong>
- Figuur 3: NOS, 17-7-2017, Ashley Madison, online afbeelding, <https://nos.nl/artikel/2183699-overspelsite-ashley-madison-wil-voor-11-2-miljoen-schikken-in-datalek-zaak.html>
- Figuur 4: z.d., Who's to blame, online afbeelding, <https://www.deancoulson.co.uk/whos-to-blame/>
- Figuur 5: Code.org, 28-6-2016, What is the Internet?, online video, <https://www.youtube.com/watch?v=Dxcc6ycZ73M>
- Figuur 6: Wireshark, z.d., online afbeelding, <https://www.wireshark.org/>
- Figuur 7: Hak5, z.d., WiFi pineapple, online afbeelding, <https://hakshop.com/products/wifi-pineapple?variant=11303796101>
- Figuur 8: z.d., Muhammed Saeed al-Sahaf, online afbeelding, <http://www.welovetheiraqiinformationminister.com/>
- Figuur 9: Morgan, Announcing our Worst Passwords of 2016, retrieved on 31-10-2019 from <https://www.teamsid.com/worst-passwords-2016>
- Figuur 10: z.d., Datingsite kiezen, online afbeelding, <https://www.datingsitekiezen.nl/nieuws/deze-banen-geven-je-het-meeste-succes-op-datingsites/>
- Figuur 11: z.d., Raspberry Pi 4, online afbeelding, <https://www.raspberrypi.com/products/>