# Hoe veilig is jouw Joomla! Website!?
## Een hacker's perspectief!

**Door**: Luca Congiu & Johan van der Velde
**JoomlaDagen Nederland 2025 - 4 oktober 2025**

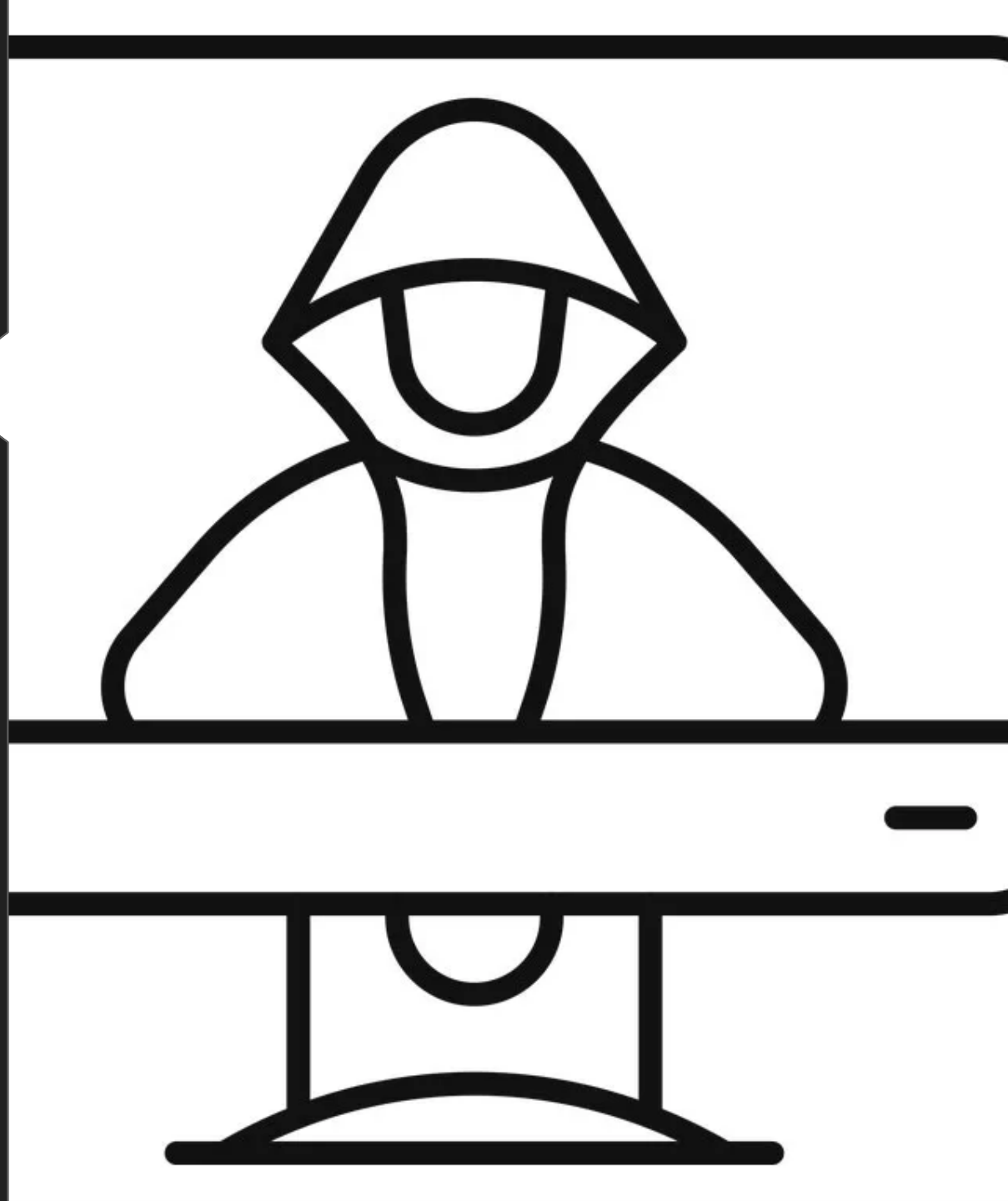
Even voorstellen

# Luca Congiu

Woonachtig in Limburg

Ethical Hacker – Pentester / red teamer

Startende ondernemer



Even voorstellen

# Johan van der Velde

Hoensbroek - Limburg

**Information Risk & Security Officer**

Passie voor Joomla! - Lid Joomla! Community

Werk met Joomla! sinds versie 1.0 (2005)

Schrijf stap voor stap handleidingen (Nederlands)

www.vandervelde-web.nl

Mede initiatiefnemer JUG043 Maastricht

www.jug043.nl

Mede organisator JoomlaDagen NL 2025

# Wie heeft al eens een hack meegemaakt?


HACKED!
Hi Master (: Your System 0wNed By Turkish Hackers!
redLine & rudeb0y & Ejder & The_Bekir & SaCReDSeeR & ASH ouNed you!
next target: microsoft.com
TiTHacK.CoM & SavSaK.CoM

# Hoe veilig is Jouw Joomla Website!?
## Een hackersperspectief!

- **Doel van presentatie**
  - Inzicht geven in veiligheid Joomla! website, vanuit perspectief van etical hacker!
- **Onderwerpen**
  - Waarom is ook Jouw Joomla! website interessant?
  - Hoe denken hackers en hoe gaan ze te werk?
  - **Praktijkvoorbeeld:** Hoe een hacker binnen komt in een Joomla 4 website!
  - Veel voorkomende beveiligingsfouten
  - Cyber hygiëne: de eerste verdedigingslinie
  - Extra beveiligingsmaatregelen
  - Wat te doen bij een hack?

# Waarom is jouw Joomla website interessant?

- Hackers willen gegeven achterhalen, zoals:
  - Persoonsgegevens (gebruikersnamen, wachtwoorden, e-mailadressen, telefoonnummers etc.)
  - Bankgegevens (bankrekeningnummers, creditcard gegevens - via webshop)
  - Bedrijfsgegevens / bedrijfsgeheimen (starten ransomware aanval)
- Hackers willen daarmee:
  - Financiële voordelen behalen (verkoop (persoons)gegevens op darkweb)
  - Website down brengen / verstoren organisaties
  - E-mails versturen via jou website, denk aan spam of phising berichten
  - Misbruik maken van servercapaciteit / VPS
- Scriptkiddies die aan het experimenteren zijn (defacing)

# Hoe denken hackers, hoe gaan ze te werk?

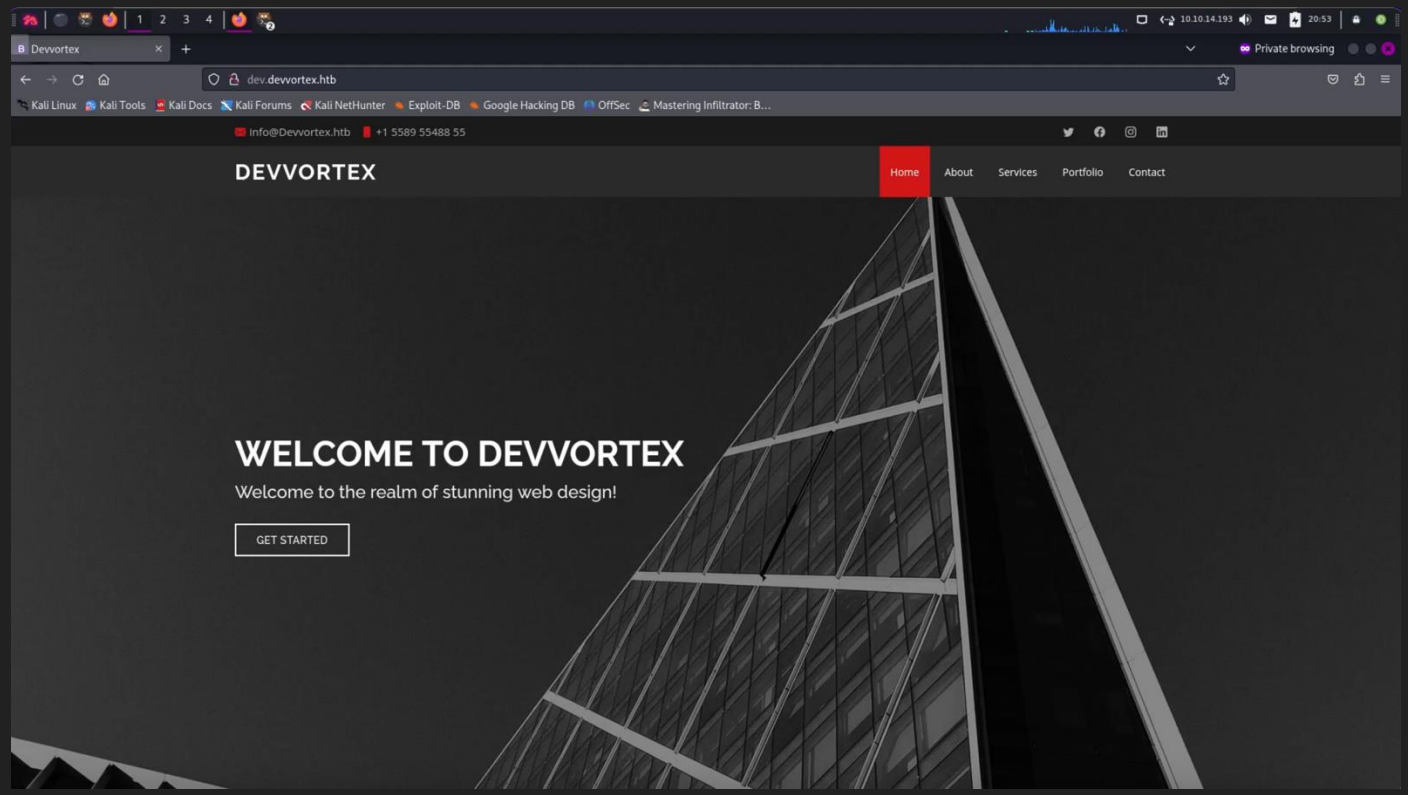
- **Fase 1 verkennen:**
  Hackers verzamelen informatie over het doelwit zonder argwaan te wekken.
- **Fase 2 bewapenen:**
  Hackers bepalen welke technieken en tools ze nodig hebben om binnen te dringen.
- **Fase 3 toegang verkrijgen:**
  Hackers gebruiken phishing, malware, kwetsbaarheden of andere methoden om toegang te krijgen.
- **Fase 4 toegang behouden:**
  Hackers installeren achterdeurtjes om hun toegang te behouden.
- **Fase 5 datadiefstal:**
  Hackers stelen (bedrijfs)data van organisaties en verkopen deze / chantagedoeleinden.

# Veel voorkomende aanvalsmethoden

- Brute-force aanvallen (wachtwoorden achterhalen – daarmee toegang verkrijgen)
- Backdoor in Joomla! / extensies / templates of bestanden
- SQL Injecties (admin account toevoegen)
- Cross-site scripting (XSS)
- Malware en backdoors
- Misconfiguratie van
  - Configuration.php
  - File uploadfunctionaliteit
- Kwetsbaarheden in Joomla! / extensies / templates

# Voorbeeld: Hoe een hacker binnen komt

- Hack van een Joomla! 4 website (in 6:31minuten!)




# Veel gemaakte fouten

- Onveilige wachtwoorden gebruiken
- Geen Multifactor Authenticatie gebruiken (MFA)
- Joomla! & Joomla! extensies niet frequent updaten
- Onveilige instellingen en configuraties
- Geen SSL certificaat gebruikt
- Geen (Web Application) Firewall extensie geïnstalleerd
- Verkeerde instellingen back-up toegepast
- Gebrek aan regelmatige beveiligingsscans / penetratietest

# Cyberhygiëne: eerste verdedigingslinie

- Gebruik sterke & unieke wachtwoorden incl. MFA oplossing / Fysiek token (Yubikey)
- Joomla! en Joomla! extensies frequent updaten
- Gebruik veilige extensies / templates (Joomla Extension Directory en Joomla Template Directory)
- Gebruik alleen stabiele Joomla! versies voor productie websites (geen testversies)
- Gebruik betrouwbare hostingprovider (ISO 27001 gecertificeerd)
- Installeer een (Web Application) Firewall extensie (RSFirewall of Akeeba Admintools)
  - Handleiding installeren Akeeba Admintools – Joomla 5
- Maak regelmatig back-ups & test ook je back-up d.m.v. restore (Akeeba Backup)
  - Handleiding backup maken - Joomla 5
  - Handleiding backup terugzetten - Joomla 5

# Cyberhygiëne: eerste verdedigingslinie

- Gebruik SSL certificaten
- Gebruik SFTP account voor filetransfer
- Controleer regelmatig logfiles
- Monitor verdachte activiteiten via:
  - Akeeba Panopticon
  - YourSites
  - Watchful
  - mySites.guru



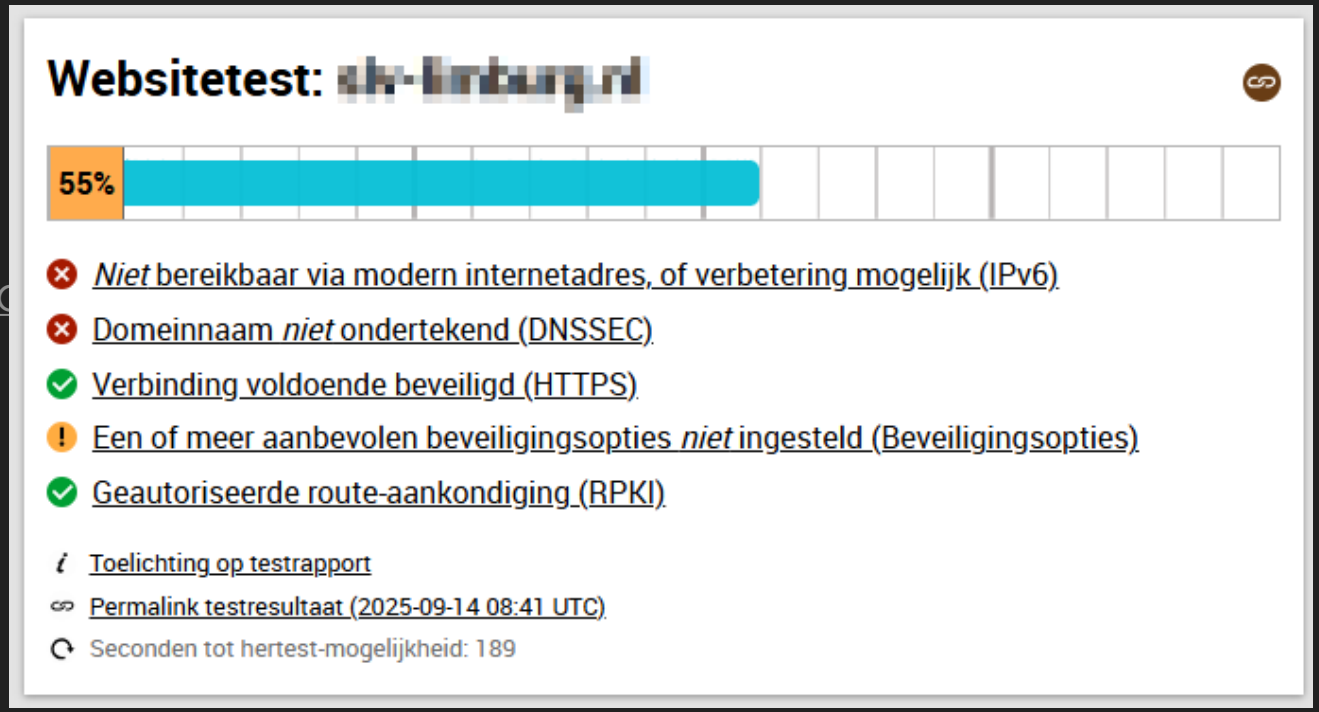
# Wat te doen bij een hack?

- Blijf kalm & onderneem direct actie!
- Website offline halen & controleren op malware
- Veilige back-up terugzetten (restore actie)
- Beveiliging aanscherpen!
- Wachtwoorden resetten
  - (s)FTP account -> gebruik SFTP
  - Database account \ naam
  - Joomla! gebruiker accounts (SuperVisor)
- Joomla! en Joomla! extensies updaten
- MFA inschakelen (ook voor webhostingomgeving)
- Informeer je webhoster over de hack!

KEEP
CALM
AND
DON'T
PANIC

# Tips en Tricks

- Zorg dat je een goed back-up strategie hebt
- Zorg dat je ook regelmatig een restore test uitvoert
- Scan je website met online tools:
  - www.internet.nl
  - www.ssllabs.com
  - https://developer.mozilla.org/en-US/
- Bezoek informatie sessies JUG's



# Handige links

- Directe link Akeeba Backup voor Joomla!:
  https://www.akeeba.com/products/akeeba-backup.html
- Directe link Akeeba Admin Tools voor Joomla!:
  https://www.akeeba.com/products/admin-tools.html
- Joomla Admin checklist Joomill
  https://www.joomill-extensions.com/extensions/admin-checklist
- Testen website via Internet.nl
  https://internet.nl/
- Testen website via Mozilla Observatory
  https://developer.mozilla.org/en-US/observatory
- 15 tips om jou Joomla website veilig te houden
  15 tips om jou Joomla website veilig te houden
- Bezoek JUGs in Nederland
  https://joomlacommunity.nl/agenda/joomla-gebruikersgroepen

**Bedankt voor de aandacht**


**Luca Congiu**

- Mail: luca@zerolink.nl
- LinkedIn: https://www.linkedin.com/in/luca-congiu/

**Johan van der Velde**

- Mail: info@vandervelde-web.nl
- Website: www.vandervelde-web.nl
- LinkedIn: https://www.linkedin.com/in/johanvandervelde/


Mocht je nog vragen hebben, neem dan gerust contact met ons op!

Kortingscode Akeeba: **32EF9400**

**geeft korting van 25% op elk product of bundel**
**geldig is tot 1 januari 2026**

# Q & A sessie

# Deze JoomlaDagen zijn mogelijk gemaakt door:






















Dank!!