LEVEL LEVEL

Een analyse van onderbelichte risico's van informatielekken in WordPress

Niels de Blaauw
WordCamp Nijmegen
1 september 2018
@NielsdeBlaauw

Wie gelooft er dat 75% van gehackte CMS'en WordPress is?

Introductie AVG Wetgeving.

GROEI VAN WORDPRESS

Als platform en als doelwit

> ***"Last year, WordPress was responsible for 83% of infected content management sites."***
>
> - Luc Princen

Gebaseerd op data van Sucuri Remediation Group

Voorkomen

VOORKOMEN

Standaard adviezen

1. **Alles up to date**

2. **Goede wachtwoorden**

3. **Voldoende logging**

VOORKOMEN

Meer adviezen

- Verander de tabelnaam
- Verstop de versienummers
- Verander de admin username
- Verstop de wp-admin
- Limiteer inlogpogingen
- Disable xml-rpc

Bron: [october 2017 wordpress attack report]

WordPress RestAPI

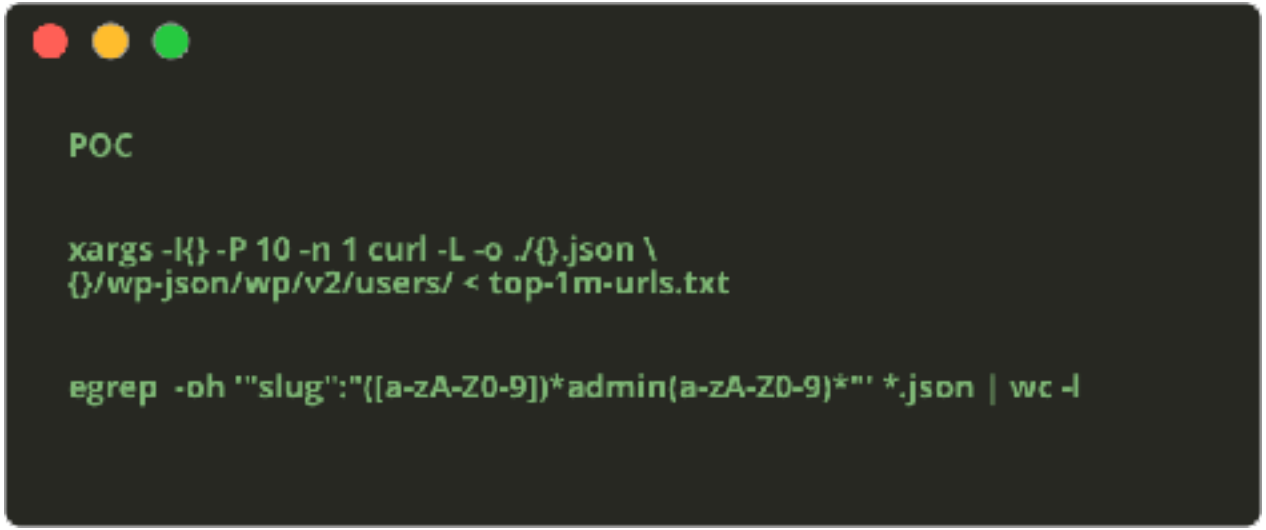
> *The WordPress REST API provides an easy-to-use set of HTTP endpoints that let you access your site's data [..], including users.*

Bron: matt mullenweg state of the word 1015

https://level-level.com/wp-json/wp/v2/users

```
[
  {
    "id":6,
    "name":"niels",
    "url":"https://level-level.com",
    "description":"",
    "link":"https://level-level.com/author/niels/",
    "slug":"niels",
    "avatar_urls":{
      "24":"https://secure.gravatar.com/avatar/edf038c13dd5332a95f76e44b0a10e97?s=24&d=mm&r=g",
      "48":"https://secure.gravatar.com/avatar/edf038c13dd5332a95f76e44b0a10e97?s=48&d=mm&r=g",
      "96":"https://secure.gravatar.com/avatar/edf038c13dd5332a95f76e44b0a10e97?s=96&d=mm&r=g"
    },
    "meta":[

    ],
    "_links":{
      "self":[
        {
          "href":"https://level-level.com/wp-json/wp/v2/users/6"
        }
      ],
      "collection":[
        {
          "href":"https://level-level.com/wp-json/wp/v2/users"
        }
      ]
    }
  }
]
```


POC
xargs -I{} -P 10 -n 1 curl -L -o ./{}.json \
{}/wp-json/wp/v2/users/ < top-1m-urls.txt
egrep -oh '"slug":"[a-zA-Z0-9]*admin[a-zA-Z0-9]*"' *.json | wc -l

Na 1 miljoen sites

156.429 WordPress installaties

752.352 unieke gebruikers

~20% sites met een ‘admin'
die post publiceert.

~30% van sites heeft een gebruiker met ‘admin' als deel van de gebruikersnaam.

GEBRUIKERSNAMEN

Top ~~10~~ 11

1. Admin
2. Editor
3. Alex
4. David
5. Chris
6. Administrator
7. Webmaster
8. Guest
9. Daniel
10. Michael
11. Laura

> *The WordPress project doesn't consider usernames or user ids to be private or secure information. A username is part of your online identity.*

Bron: why are disclosures of usernames or user ids not a security issue

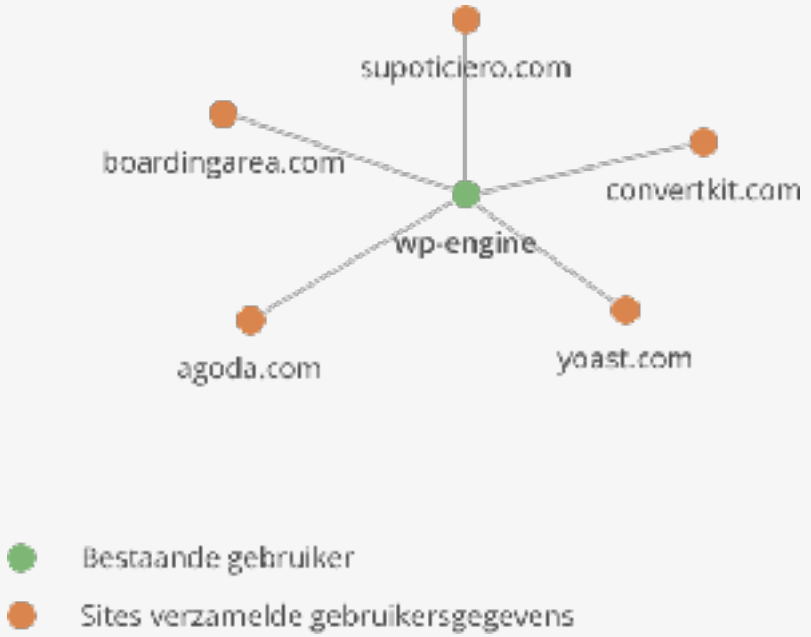
KWETSBARE GRAVATAR URLS

https://secure.gravatar.com/avatar/
edf038c13dd5332a93f76e44b0a10e97?s=48&d=mm&r=g

Username	Website	Email	Gravatar
niels_deblaauw	https://level-level.com	niels@level-level.com	edf038c13dd5332a93f76e44b0a10e97
high_roller	https://casino-in-malta.nl	niels@level-level.com	edf038c13dd5332a93f76e44b0a10e97

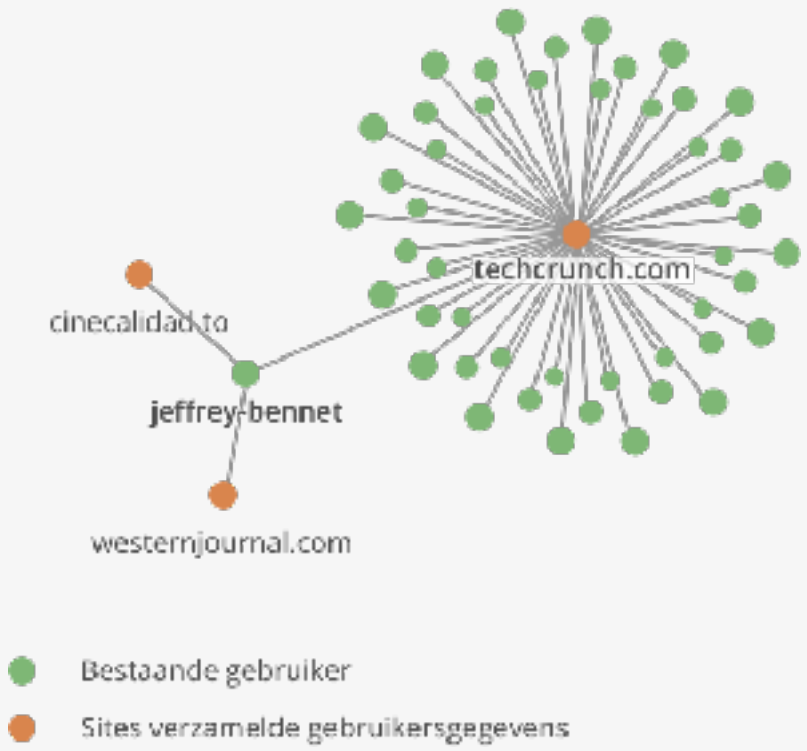
VERZAMELING

Gebruikersgegevens op websites



BEVEILIGING

Gebruikersgegevens op websites



Meer dan 2/3 gebruikt hetzelfde wachtwoord op meerdere, totaal ongerelateerde websites.

Bron: science of password selection

"In other words, 86% of subscribers were using passwords already leaked in other data breaches and available to attackers in plain text."

Bron: 86 of passwords are terrible and other statistics

Sinds 1 januari 2018 zijn 33 ‘authenticated' kwetsbaarheden gepubliceerd.

Bron: authenticated search wpvulndb

[...] strengere eisen aan de registratie van de datalekken in een organisatie. Organisaties moeten alle datalekken documenteren.

Takeaway

CONCLUSIE

Dus:

- **Sla geen data op die je niet nodig hebt**
- **Deel geen data die anderen niet nodig hebben**

Een analyse van onderbelichte risico's van informatielekken in WordPress

Niels de Blaauw
WordCamp Nijmegen 2018

LEVEL LEVEL

Resources

- **Nog in te vullen:** Voorbeeld

  http://voorbeeld.com