Laravel APP_KEY

From Public Leak to RCE

Guillaume VALADON - @guedou

Laravel

a PHP-based **web framework**

use APP_KEY for encryption/decryption

decryption transparently **deserialize objects**

many gadget chains exist 💥

leak of APP_KEY **may lead to RCE**

Laravel: CVE-2018-15133

Applications: CVE-2024-5555, CVE-2024-55556…

Synacktiv Research

650,000 Laravel public instances

from Shodan, in summer 2024

dorks to retrieve leaked APP_KEY

Google, GitHub…

~400 instances with an immediate RCE 💥

~6000 valid APP_KEY

Hold my beer

GitGuardian Public Monitoring

GitGuardian monitors GitHub live
every public commits are scanned

260,000 APP_KEY leaked on GitHub
since 2018

~600 instances with an immediate RCE 💥
interesting improvement!

APP_KEY + APP_URL = <3

APP_URL defines the **application host**

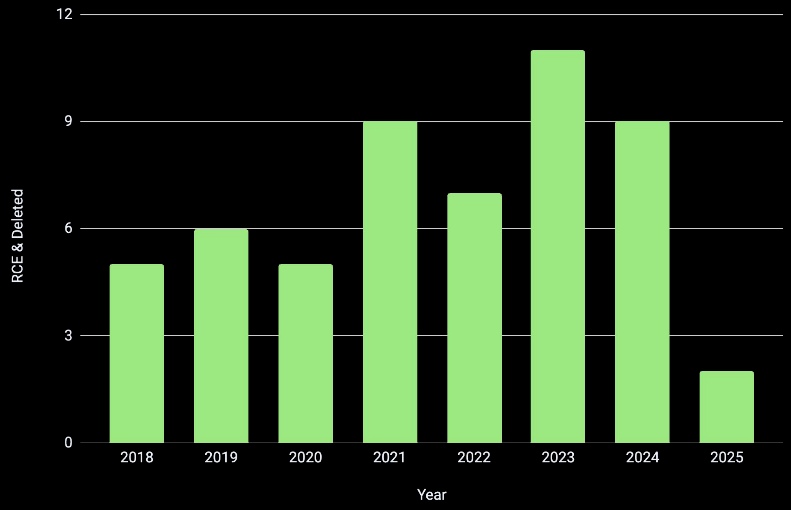
i.e. https://www.sstic.org

~28,000 unique APP_URL / APP_KEY found on GitHub

10% are valid

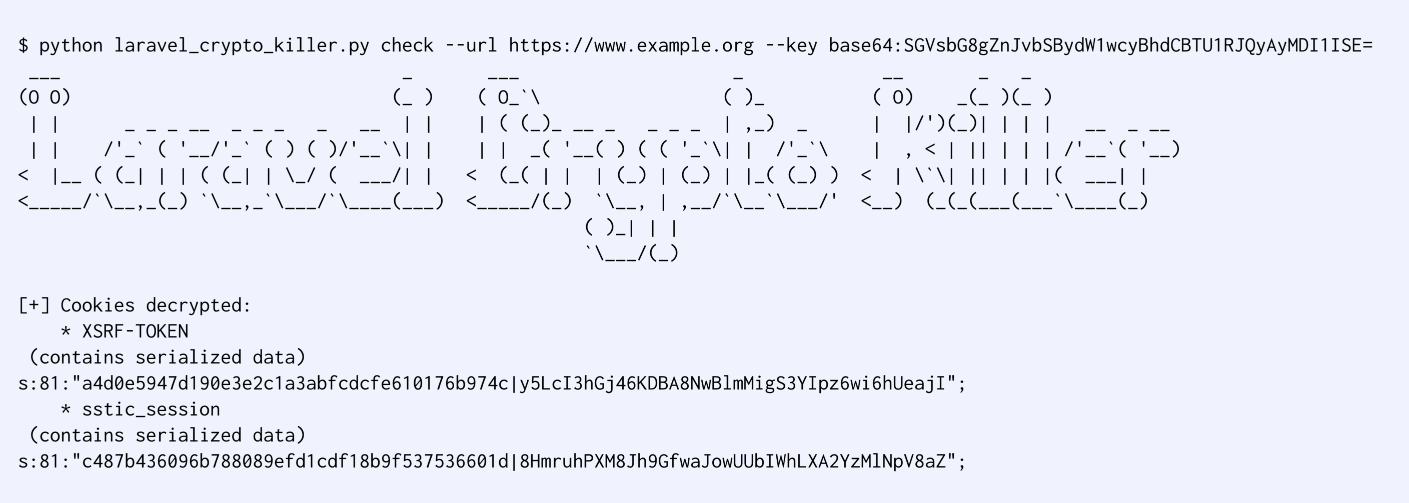
~120 instances with an immediate RCE 💥

50 deleted from GitHub



GitGuardian

Further Information



```
$ python laravel_crypto_killer.py check --url https://www.example.org --key base64:SGVsbG8gZnJvbSBydW1wcyBhdCBTU1RJQyAyMDI1ISE=
 ___                                _       ___                    _             __       _   _
(O O)                              (_ )    ( O_`\                 ( )_          ( O)    _(_ )(_ )
 | |      _ _ _ __  _ _ _   _   __  | |    | ( (_)_ __ _   _ _ _  | ,_)  _      |  |/')(_)| | | |   __  _ __
 | |    /'_` ( '__/'_` ( ) ( )/'__`\| |    | |  _( '__( ) ( ( '_`\| |  /'_`\    |  , < | || | | | /'__`( '__)
<  |__ ( (_| | | ( (_| | \_/ (  ___/| |   <  (_( | |  | (_) | (_) | |_( (_) )  <  | \`\| || | | |(  ___| |
<_____/`\__,_(_) `\__,_`\___/`\____(___)  <_____/(_)  `\__, | ,__/`\__`\___/'  <__)  (_(_(___(___`\____(_)
                                                     ( )_| | |
                                                     `\___/(_)

[+] Cookies decrypted:
    * XSRF-TOKEN
 (contains serialized data)
s:81:"a4d0e5947d190e3e2c1a3abfcdcfe610176b974c|y5LcI3hGj46KDBA8NwBlmMigS3YIpz6wi6hUeajI";
    * sstic_session
 (contains serialized data)
s:81:"c487b436096b788089efd1cdf18b9f537536601d|8HmruhPXM8Jh9GfwaJowUUbIWhLXA2YzMlNpV8aZ";
```

MISC

LE MAGAZINE DE LA CYBERSÉCURITÉ
OFFENSIVE ET DÉFENSIVE

N°139
MAI / JUIN 2025

FRANCE MÉTRO. : 14,90 € - BEL 15,90 € - CH 22,30 CHF
TOM 1900 XPF - CAN 24,50 $CAD

L 19018 - 139 - F: 14,90 € - RD

SMSI / JURIDIQUE
Retour d'expérience sur la conformité au règlement européen DORA

MFA / FIDO2
Renforcez la sécurité de vos connexions RDP avec une YubiKey

IA / RÉTRO-INGÉNIERIE
Analyse de malware assistée par Intelligence Artificielle

PENTEST / WEB / PHP

SÉCURITÉ DU FRAMEWORK LARAVEL

COMMENT UNE SIMPLE CLÉ PEUT-ELLE COMPROMETTRE LA SÉCURITÉ DE VOS APPLICATIONS ?

- Utilisation du chiffrement
- Vulnérabilités & failles
- Analyse des attaques autour du leak d'APP_KEY

SURVEILLANCE / RÉSEAU SOCIAL
Collecter des données issues de Snapchat à partir de la dissection de son API

CTI / CYBERCRIMINALITÉ
Explorer la distribution de malwares via la navigation sur le Web

GOUVERNANCE / CONFORMITÉ
Anticiper pour mieux protéger : le rôle central de l'analyse des risques en DevSecOps

https://github.com/synacktiv/laravel-crypto-killer/

Thank you

Question Time 🔥

in Guillaume VALADON - @guedou

GitGuardian