



بسم الله الرحمن الرحيم





Laravel Apps Leaking Secrets

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو





فهرست مطالب

مقدمه	۴
Laravel چیست؟	۵
پاسخ وب (فایل پیکربندی واقعی نیست)	۵
دسترسی اولیه	۱۱
اجرا	۱۱
تشخیص‌ها (Detections)	۱۳
IOCs	۱۳





مقدمه

چند وقت پیش، یک تهدیدگر از طریق RDP وارد سیستم شد تا یک ابزار SMTP Cracker را اجرا کند. این ابزار، لیستی از آدرس‌های IP یا URL را برای یافتن سیستم‌های Laravel که به درستی پیکربندی نشده‌اند، اسکن می‌کند. این مهاجمان به دنبال وبسایت‌هایی هستند که Debug Mode در آن‌ها فعال باشد، که به مهاجم اجازه می‌دهد فایل پیکربندی (.env) آن‌ها را مشاهده کند. فایل .env شامل اعتبارنامه‌های AWS، 0365، SendGrid، Twilio و موارد دیگر است.





Laravel چیست؟

Laravel یک چارچوب رایگان و متن باز PHP برای توسعه برنامه‌های وب است که توسط تیلور اتول ایجاد شده است. (منبع: ویکی‌پدیا)

Laravel درایورهایی برای SMTP، Mailgun، Mandrill، Amazon SES، تابع mail در PHP و sendmail فراهم می‌کند و به شما امکان می‌دهد به سرعت ارسال ایمیل را از طریق یک سرویس محلی یا ابری دلخواه شروع کنید. (منبع: مستندات رسمی Laravel)

گزینه دیباگ به طور پیش فرض در سیستم‌های Laravel غیرفعال است، اما به نظر می‌رسد بسیاری از کاربران آن را فعال کرده و عواقب آن را درک نمی‌کنند. در اینجا نمونه‌ای از فعال بودن دیباگ (تنظیم روی true) در فایل پیکربندی env. نشان داده شده است.

```
<tr>
  <td>
    APP_DEBUG
  </td>
  <td>
    <pre class=sf-dump id=sf-dump-2067749625 data-indent-pad=" ">
      "<span class=sf-dump-str title="4 characters": true;/span>
```

پاسخ وب (فایل پیکربندی واقعی نیست)

می‌توانید با بررسی وجود فایل env. در ریشه وب (site.com/.env) یا با ارسال داده‌های تصادفی به وب سرور و بررسی پاسخ، متوجه شوید که آیا دیباگ فعال است یا خیر. در پاسخ، گزینه دیباگ و همچنین تمام اطلاعات فایل env. که شامل secret ها می‌باشد را مشاهده خواهید کرد.





در اینجا نمونه‌ای از پاسخ وب با دیباگ فعال آورده شده است:

```
    AWS_ACCESS_KEY_ID
  </td>
  <td>
    <pre class=sf-dump id=sf-dump-1797855799 data-indent-pad=" ">
      "<span class=sf-dump-str title="20 characters">[REDACTED]</span>
    </pre>
    <script>
      Sfdump("sf-dump-1797855799")
    </script>
  </td>
</tr>
<tr>
  <td>
    AWS_SECRET_ACCESS_KEY
  </td>
  <td>
    <pre class=sf-dump id=sf-dump-706539060 data-indent-pad=" ">
      "<span class=sf-dump-str title="40 characters">[REDACTED]</span>
    </pre>
    <script>
      Sfdump("sf-dump-706539060")
    </script>
  </td>
</tr>
<tr>
  <td>
    AWS_DEFAULT_REGION
  </td>
  <td>
    <pre class=sf-dump id=sf-dump-840748221 data-indent-pad=" ">
      "<span class=sf-dump-str title="9 characters">us-east-1</span>
```





در اینجا نمونه‌ای از یک فایل .env آورده شده است:

```
APP_NAME=[REDACTED]
APP_ENV=[REDACTED]
APP_KEY=[REDACTED]
APP_DEBUG=true
APP_URL=[REDACTED]

LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=[REDACTED]
DB_USERNAME=[REDACTED]
DB_PASSWORD=[REDACTED]

BROADCAST_DRIVER=log
CACHE_DRIVER=file
QUEUE_CONNECTION=sync
SESSION_DRIVER=file
SESSION_LIFETIME=120

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=ssl://smtp.googlemail.com
MAIL_PORT=465
MAIL_USERNAME=[REDACTED]
MAIL_PASSWORD=[REDACTED]
MAIL_ENCRYPTION=null
MAIL_FROM_ADDRESS=[REDACTED]
MAIL_FROM_NAME="[REDACTED]"

AWS_ACCESS_KEY_ID=[REDACTED]
AWS_SECRET_ACCESS_KEY=[REDACTED]
AWS_DEFAULT_REGION=us-east-1
AWS_BUCKET=[REDACTED]

PUSHER_APP_ID=[REDACTED]
PUSHER_APP_KEY=[REDACTED]
PUSHER_APP_SECRET=[REDACTED]
PUSHER_APP_CLUSTER=mt1

MIX_PUSHER_APP_KEY="${PUSHER_APP_KEY}"
MIX_PUSHER_APP_CLUSTER="${PUSHER_APP_CLUSTER}"

FILESYSTEM_DRIVER=public

FIREBASE_PUSH_NOTIFICATION_KEY=[REDACTED]

JAVA_BRIDGE_URL=[REDACTED]
JAVA_BRIDGE_DRIVER=Pjb62
JAVA_BRIDGE_RESOURCE_PATH="/tmp/lib"
JAVA_BRIDGE_KEY_STORE_PATH="/tmp/lib"

CYBER_SOURCE_ACCESS_KEY=[REDACTED]
CYBER_SOURCE_PROFILE_ID=[REDACTED]
```





اسکرپت SMTP Cracker که اتفاقاً یک Cracker نیست و فقط اعتبارنامه‌های SMTP را دریافت نمی‌کند، از روش‌های فوق برای خزیدن در لیستی از IP/ها/URLها استفاده می‌کند و به دنبال رشته‌های خاصی در پاسخ می‌گردد، مانند PayPal، AWS_KEY، SES_KEY، Twilio، sendgrid، office365، zoho، mailgun و دیگر موارد.

در اینجا بخشی از اسکرپت آورده شده است که در آن به دنبال یک رشته در mailhost می‌گردد و secretها را در فایل مناسب خروجی می‌دهد.

```
else:
    # mod aws
    if '.amazonaws.com' in mailhost:
        getcountry = reg('email-smtp.(.*?).amazonaws.com', mailhost)[0]
        build = 'URL: '+str(url)+'\nMETHOD: '+str(method)+'\nMAILHOST: '
        remover = str(build).replace('\r', '')
        save = open('Results/'+getcountry[:2]+'\.txt', 'a')
        save.write(remover+'\n\n')
        save.close()
        remover = str(build).replace('\r', '')
        save2 = open('Results/smtplib_aws.txt', 'a')
        save2.write(remover+'\n\n')
        save2.close()
    elif 'sendgrid' in mailhost:
        build = 'URL: '+str(url)+'\nMETHOD: '+str(method)+'\nMAILHOST: '
        remover = str(build).replace('\r', '')
        save = open('Results/sendgrid.txt', 'a')
        save.write(remover+'\n\n')
        save.close()
    elif 'office365' in mailhost:
        build = 'URL: '+str(url)+'\nMETHOD: '+str(method)+'\nMAILHOST: '
        remover = str(build).replace('\r', '')
        save = open('Results/office.txt', 'a')
        save.write(remover+'\n\n')
        save.close()
    elif '1and1' in mailhost or 'lund1' in mailhost:
        build = 'URL: '+str(url)+'\nMETHOD: '+str(method)+'\nMAILHOST: '
        remover = str(build).replace('\r', '')
        save = open('Results/1and1.txt', 'a')
        save.write(remover+'\n\n')
        save.close()
    elif 'zoho' in mailhost:
        build = 'URL: '+str(url)+'\nMETHOD: '+str(method)+'\nMAILHOST: '
        remover = str(build).replace('\r', '')
        save = open('Results/zoho.txt', 'a')
        save.write(remover+'\n\n')
        save.close()
    elif 'mandrillapp' in mailhost:
        build = 'URL: '+str(url)+'\nMETHOD: '+str(method)+'\nMAILHOST: '
        remover = str(build).replace('\r', '')
```





خروجی اسکریپت در پوشه‌ای به نام Results ذخیره می‌شود. نتایج به گروه‌های مختلفی تقسیم می‌شوند، همانطور که در تصویر زیر مشاهده می‌کنید.

Name
not_vulnerable.txt
SMTP_RANDOM.txt
aws_access_key_secret.txt
us-east.txt
sendgrid.txt
aws_unknown_region.txt
smtp_aws.txt
TWILLIO.txt
mailgun.txt
us-west.txt
office.txt
zoho.txt
mandrill.txt
eu-west.txt
paypal_sandbox.txt
ap-south.txt
ap-northeast.txt





در داخل آن فایل‌ها، secretها و روش استفاده شده برای استخراج اطلاعات قرار دارد. این یک مثال جزئی از فایل sendgrid است:

```
1 URL: http://[REDACTED]:80
2 METHOD: debug
3 MAILHOST: smtp.sendgrid.net
4 MAILPORT: 587
5 MAILUSER: [REDACTED]
6 MAILPASS: [REDACTED]
7 MAILFROM: [REDACTED]
8 FROMNAME: [REDACTED]
9
10 URL: http://[REDACTED]:80
11 METHOD: debug
12 MAILHOST: smtp.sendgrid.net
13 MAILPORT: 465
14 MAILUSER: apikey
15 MAILPASS: [REDACTED]
16 MAILFROM:
17 FROMNAME:
18
19 URL: http://[REDACTED]:80
20 METHOD: /.env
21 MAILHOST: smtp.sendgrid.net
22 MAILPORT: 587
23 MAILUSER: apikey
24 MAILPASS: [REDACTED]
25 MAILFROM:
26 FROMNAME:
27
28 URL: http://[REDACTED]:80
29 METHOD: debug
30 MAILHOST: smtp.sendgrid.net
31 MAILPORT: 587
32 MAILUSER: apikey
33 MAILPASS: [REDACTED]
34 MAILFROM:
```





این یک مثال جزئی از فایل متنی office365 است:

```
1 URL: http://[REDACTED]:80
2 METHOD: /.env
3 MAILHOST: smtp.office365.com
4 MAILPORT: 587
5 MAILUSER: [REDACTED]
6 MAILPASS: [REDACTED]
7 MAILFROM:
8 FROMNAME:
9
10 URL: http://[REDACTED]:80
11 METHOD: debug
12 MAILHOST: smtp.office365.com
13 MAILPORT: 587
14 MAILUSER: [REDACTED]
15 MAILPASS: [REDACTED]
16 MAILFROM: [REDACTED]
17 FROMNAME: [REDACTED]
18
19 URL: http://[REDACTED]:1:80
20 METHOD: debug
21 MAILHOST: smtp.office365.com
22 MAILPORT: 587
23 MAILUSER: [REDACTED]
24 MAILPASS: [REDACTED]
25 MAILFROM:
```

ما در حال تماس با بیش از ۱۰۰ نفر/سازمان هستیم که سیستم‌هایشان از طریق دیباگ Laravel موارد مهمی را نشت می‌دهند، به این امید که این مشکل را برطرف کرده و رمزهای عبور خود را تغییر دهند.

دسترسی اولیه

ورود RDP به عنوان Local Administrator از آدرس 64.86.198[.]22 بود و هیچ تلاشی مبنی بر Brute Force از این IP مشاهده نشد.

اجرا

مهاجم پایتون ۲.۷ را نصب و از آن برای اجرای اسکریپت SMTP استفاده کرد.





```
commandLine      pip install bs4
currentDirectory C:\\Python27\\Scripts\\
hashes           SHA1=3B8F65BDBC2AE4D6785F5B294A4F495C3
                 026
image            C:\\Python27\\Scripts\\pip.exe
integrityLevel   High
loginGuid        {008cde44-071e-601f-0273-ce0f00000000}
loginId          0xfce7302
parentCommandLine \"C:\\Windows\\System32\\cmd.exe\"
```





تشخیص‌ها (Detections)

درخواست‌های وب به مسیر root/.env یا داده‌های ارسالی (post data) که شامل 0x[:androxgh0st (یک رشته Hardcode شده در smtp.py) باشد.

IOCs

File

filename	smtp.py
md5	39e1ec2c704bcd57034da4ac288446e
sha1	352e9c78f08574adbaa0aaf49c19d5853bb4be36
sha256	478290f801dafc9086810f857c123d74690920a4c44fb573cd01463c1b6fb432

Network

type	value	comment
ip-src	64.86.198.22	RDP Unauthorized Access

```
Valid Accounts - T1078
Python - T1059.006
Scripting - T1064
User Execution - T1204
Graphical User Interface - T1061
Command and Scripting Interpreter - T1059
```

منبع:

<https://thedfirreport.com/2021/02/28/laravel-debug-leaking-secrets/>

