it’s borked

programming was a mistake

# whoami

- software / appsec engineering (-ish?)
- infosec (not-so-ish)

- on the side?
  - ~~studies~~, communities, ctf’s, conferences

- I do stupid (fun?) things

- I am not *that* swiss maia (get bingled)

@AtomicMaya
@tech.lgbt

# surely it’s not all borked

# surely it’s not all borked

- if we can trace back a lot of programming design patterns across many languages to “Structured Programming”, the 1972 book written by Dahl, Dijkstra and Hoare
- then yeah

# what’s with the title, Maya?

- been programming for about 9 years now
  - python, c, js, ts, scala, java, swift, golang, dart, php
  - + a bunch of frameworks/libs/dbms’
- and yet, I am woefully underqualified to talk about anything
- (but I can rant, and I will)

# python

- fun interpreted language, very unquirky
- except the lack of typing (like seriously, type hints were added in 3.9)
- it’s slooooow
- pip this, pip that (everything is a package)
- multi-threading? sure

#python

- venv my beloved
  - (I’m cheating on you with Poetry)

- list comprehension is really really fun to work with

#python

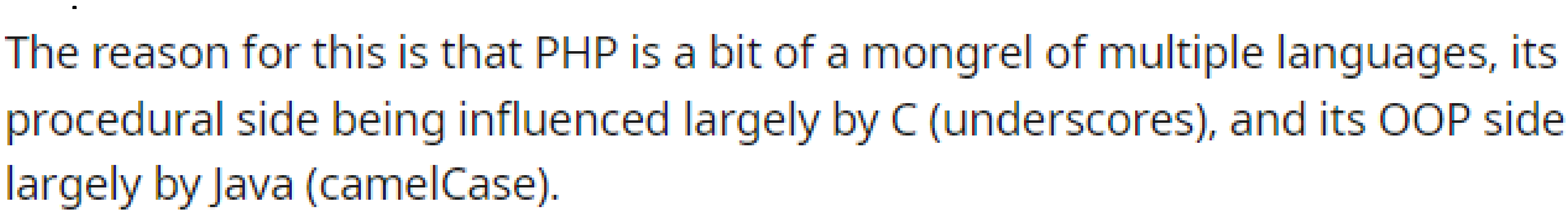
```
return [[reduce(lambda x, y: x ^ y,
[gf_multiplication_7(a, b) for a, b in
zip(fixed_matrix[i],
transpose_square_matrix(matrix=matrix)[j])]) for j
in range(size)] for i in range(size)]
```

#python

- venv my beloved
  - (I’m cheating on you with Poetry)
- list comprehension is really really fun to work with
- testing! it exists
- rated top language to build an API with (not really)

#php

- the easiest language to hate
- untyped by default
- effectively three semantics in a trenchcoat



The reason for this is that PHP is a bit of a mongrel of multiple languages, its procedural side being influenced largely by C (underscores), and its OOP side largely by Java (camelCase).

#php

- the dubious honor of being trashed by its creator
  - “PHP 8 is significantly better because it contains a lot less of my code”

- if you really want “the full Monty” of a rant, check eevee’s blog:
  - https://eev.ee/blog/2012/04/09/php-a-fractal-of-bad-design/

#java

- runs on 3 billion devices (👀 Java card)
- fully cross-OS environment
  - oh wait I have to ship a VM too?
- garbage collection can be finicky
- the dreaded existence of static

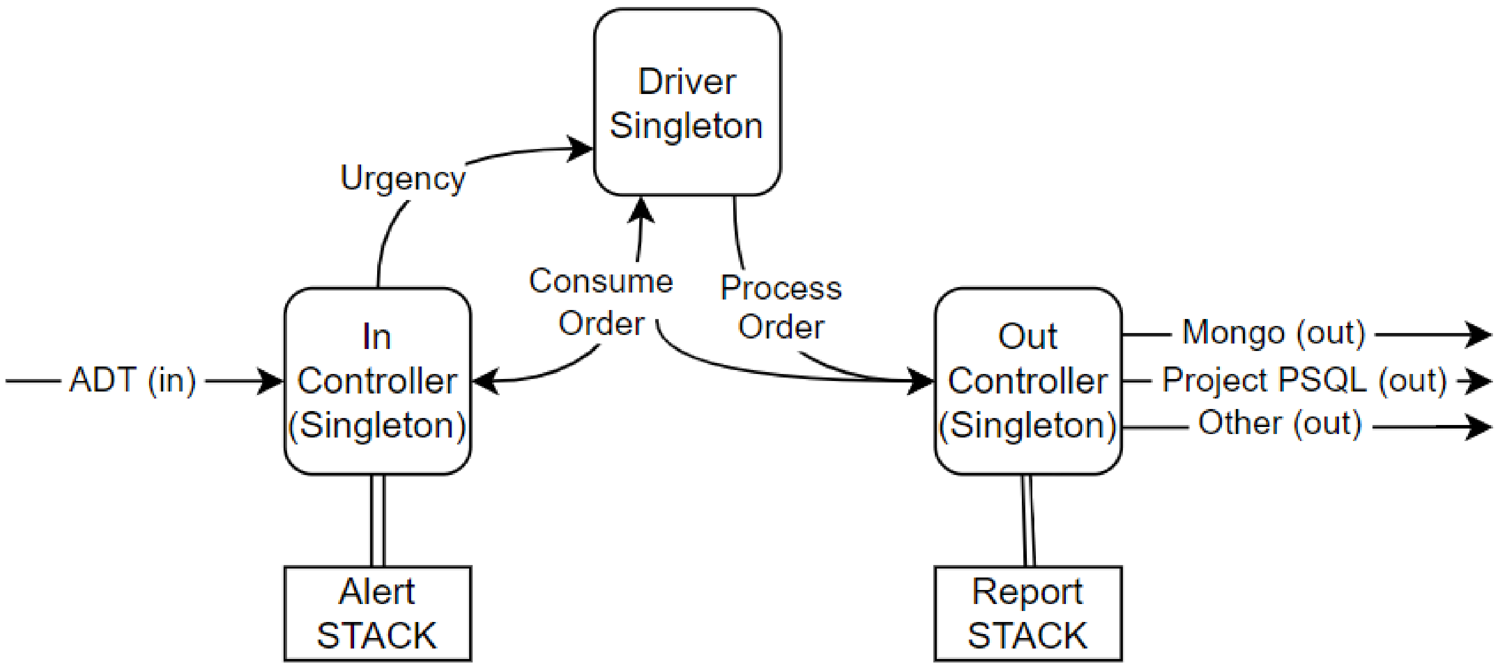
#java (parenthesis)

- EU Commission shenanigans for automated public transportation
- a bit of context
- “It has to be quick! I know, let’s dockerize 15 different Java components and hope for sub-1ms response times!”
- I worked on something called the Risk Assessment Engine

#java (parenthesis)

- main issues
  - alert queueing
  - alert batch processing
  - fully asynchronous

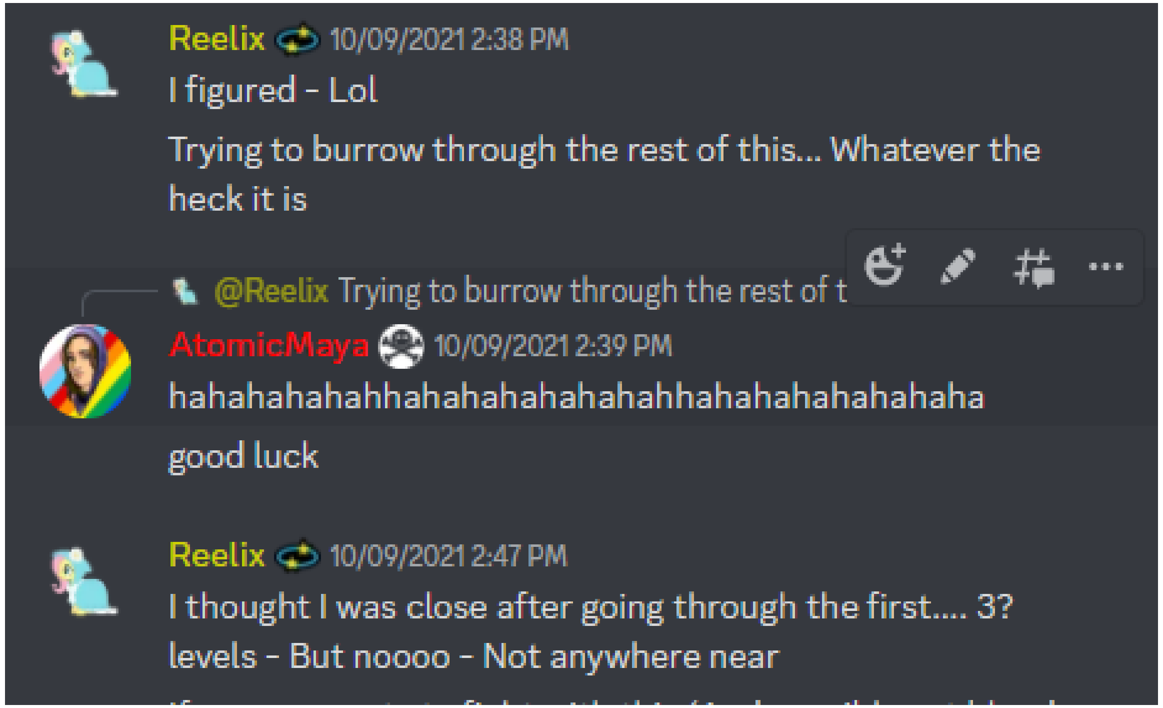
- (all of these are in their own threads btw)



#javascript

- untyped
- used everywhere a browser is
  - oh but wait node means running raw on servers too
- super versatile (yay npm)
- no one should have to deal with my javascript
  - (although if you want, uhhhh, DM me)
  - I have great user reviews

#javascript



Reelix 10/09/2021 2:38 PM
I figured - Lol

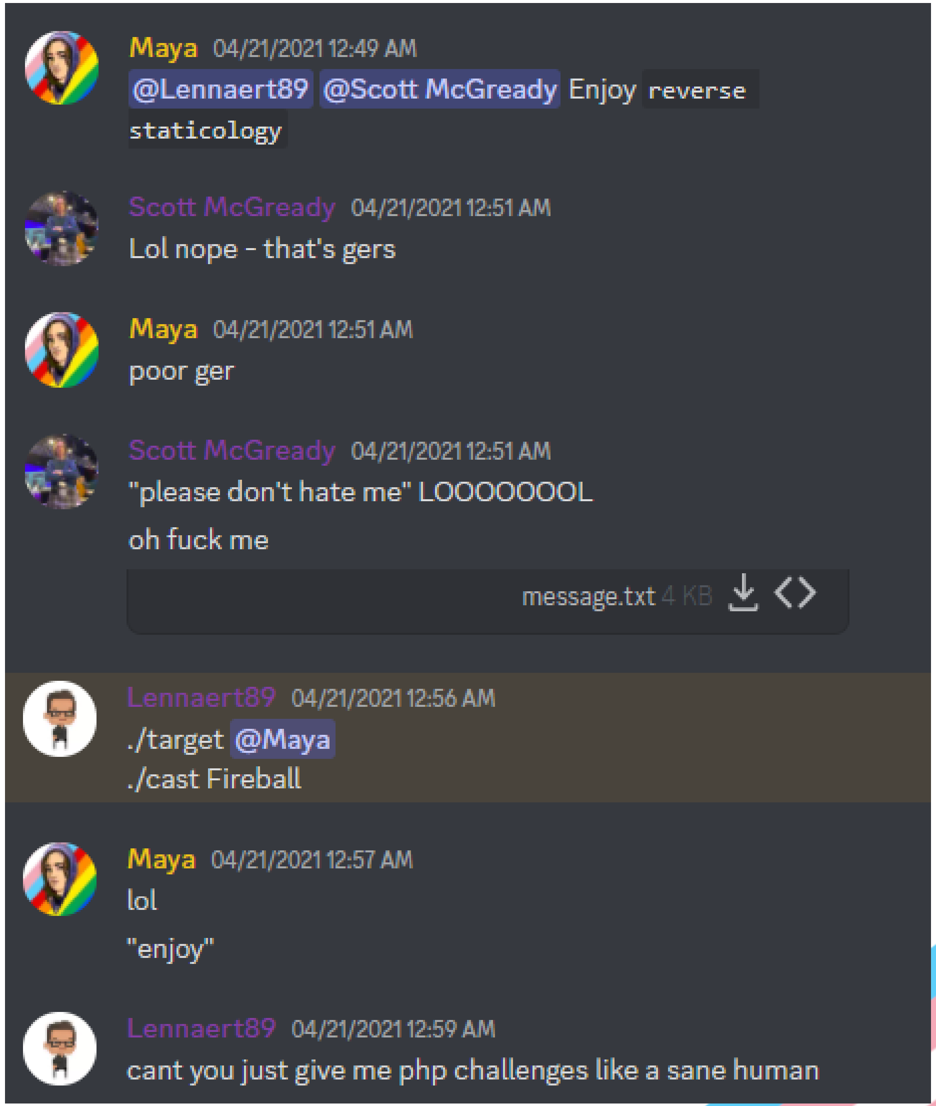
Trying to burrow through the rest of this... Whatever the heck it is

@Reelix Trying to burrow through the rest of t

AtomicMaya 10/09/2021 2:39 PM
hahahahahahhahahahahahahahhahahahahahahaha

good luck

Reelix 10/09/2021 2:47 PM
I thought I was close after going through the first.... 3? levels - But noooo - Not anywhere near



Maya 04/21/2021 12:49 AM
@Lennaert89 @Scott McGready Enjoy `reverse staticology`

Scott McGready 04/21/2021 12:51 AM
Lol nope - that's gers

Maya 04/21/2021 12:51 AM
poor ger

Scott McGready 04/21/2021 12:51 AM
"please don't hate me" LOOOOOOOL

oh fuck me

message.txt 4 KB

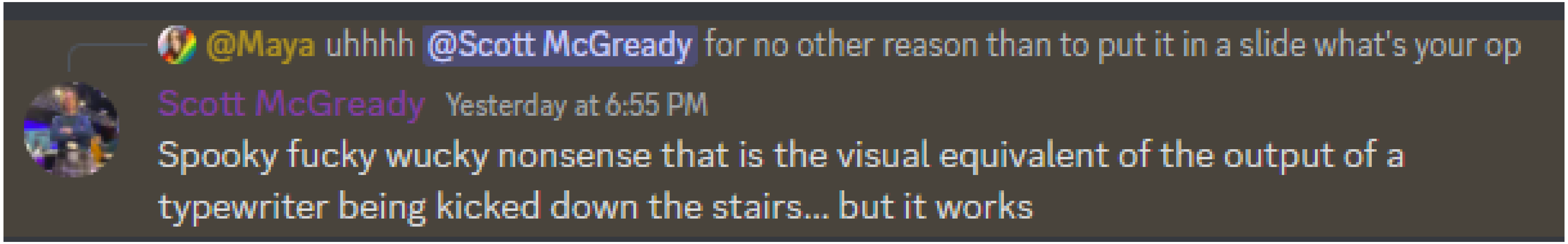
Lennaert89 04/21/2021 12:56 AM
./target @Maya
./cast Fireball

Maya 04/21/2021 12:57 AM
lol

"enjoy"

Lennaert89 04/21/2021 12:59 AM
cant you just give me php challenges like a sane human

#javascript

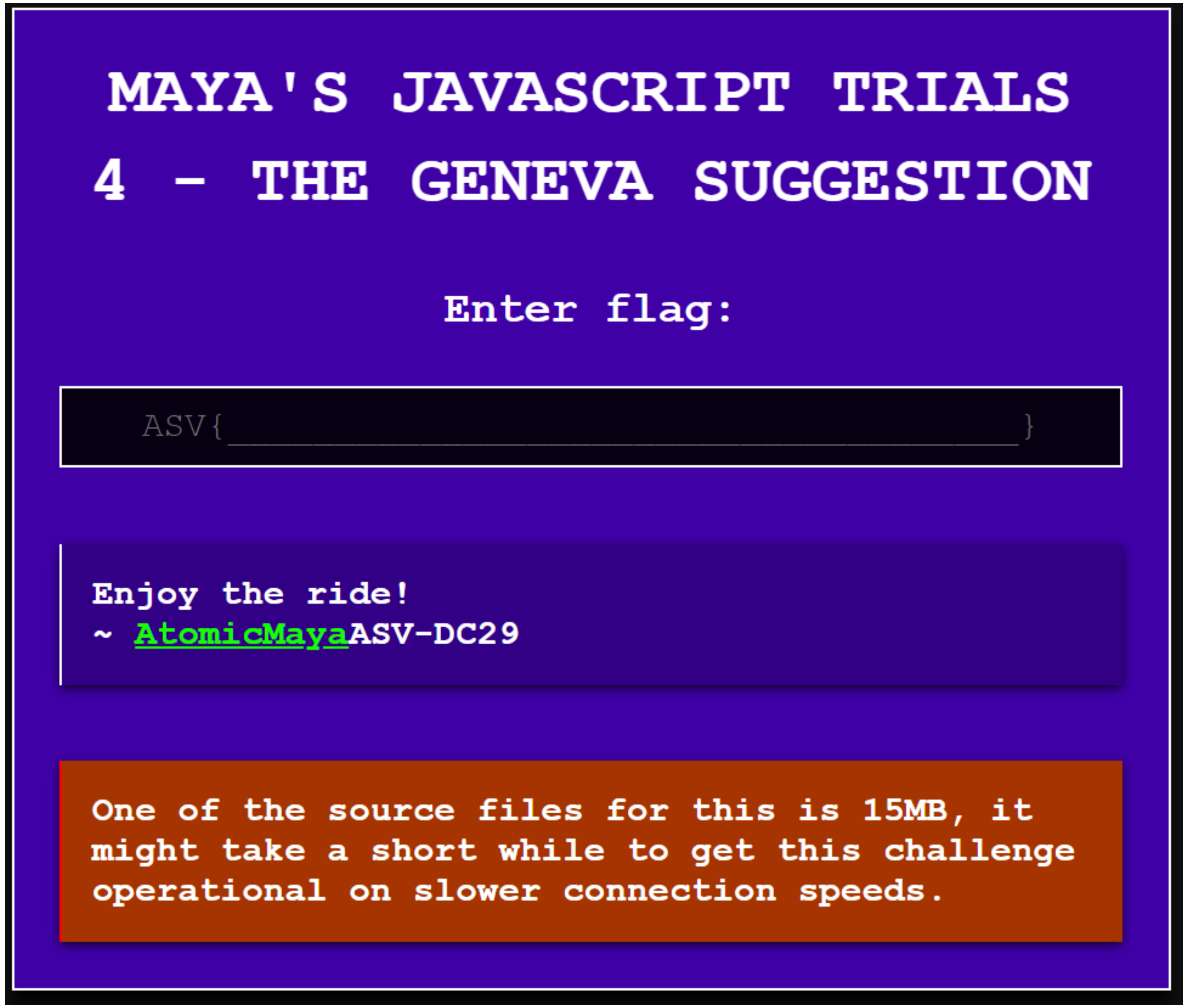


@Maya uhhhh @Scott McGready for no other reason than to put it in a slide what's your op

Scott McGready Yesterday at 6:55 PM

Spooky fucky wucky nonsense that is the visual equivalent of the output of a typewriter being kicked down the stairs... but it works

#javascript (or rather JSFUCK)



MAYA'S JAVASCRIPT TRIALS

4 - THE GENEVA SUGGESTION

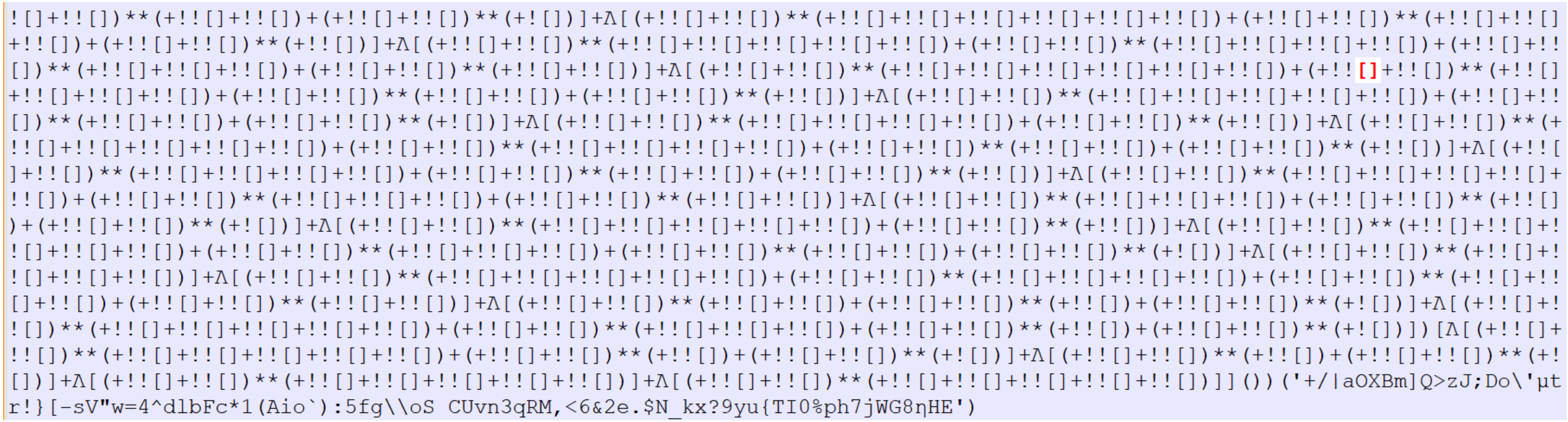
Enter flag:

ASV{_______________________________________}

Enjoy the ride!
~ AtomicMayaASV-DC29

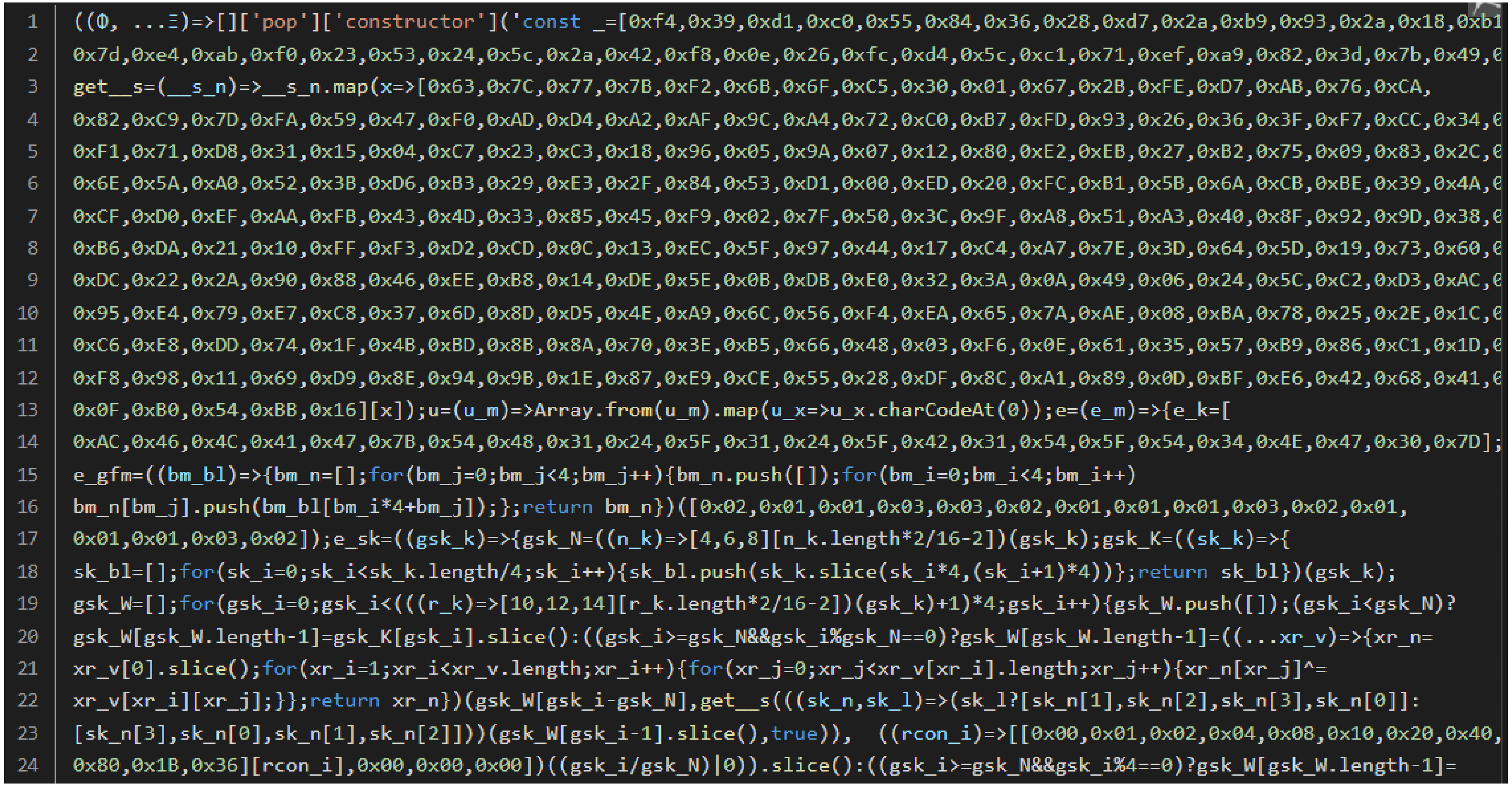
One of the source files for this is 15MB, it might take a short while to get this challenge operational on slower connection speeds.

#javascript (or rather JSFUCK)



```
![]+!![])**(+!![]+!![])+(+!![]+!![])**(+![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![]
+!![])+(+!![]+!![])**(+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![]+!![]+!![])+(+!![]+!!
[])**(+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]
+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![])+(+!![]+!![])**(+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![])+(+!![]+!!
[])**(+!![]+!![])+(+!![]+!![])**(+![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![])]+Λ[(+!![]+!![])**(+
!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![])+(+!![]+!![])**(+!![])]+Λ[(+!![
]+!![])**(+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![])+(+!![]+!![])**(+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+
!![])+(+!![]+!![])**(+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![])+(+!![]+!![])**(+!![]
)+(+!![]+!![])**(+![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!
![]+!![]+!![])+(+!![]+!![])**(+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![])+(+!![]+!![])**(+![])]+Λ[(+!![]+!![])**(+!![]+!
![]+!![]+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!!
[]+!![])+(+!![]+!![])**(+!![]+!![])]+Λ[(+!![]+!![])**(+!![]+!![])+(+!![]+!![])**(+!![])+(+!![]+!![])**(+![])]+Λ[(+!![]+!
![])**(+!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![]+!![]+!![])+(+!![]+!![])**(+!![])+(+!![]+!![])**(+![])])[Λ[(+!![]+
!![])**(+!![]+!![]+!![]+!![]+!![])+(+!![]+!![])**(+!![])+(+!![]+!![])**(+![])]+Λ[(+!![]+!![])**(+!![])+(+!![]+!![])**(+!
[])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![])]+Λ[(+!![]+!![])**(+!![]+!![]+!![]+!![]+!![])]]())('+/|aOXBm]Q>zJ;Do\'µt
r!}[-sV"w=4^dlbFc*1(Aio`):5fg\\oS CUvn3qRM,<6&2e.$N_kx?9yu{TI0%ph7jWG8ηHE')
```

#javascript (or rather JSFUCK)



```
((Φ, ...Ξ)=>[]['pop']['constructor']('const _=[0xf4,0x39,0xd1,0xc0,0x55,0x84,0x36,0x28,0xd7,0x2a,0xb9,0x93,0x2a,0x18,0xb1
0x7d,0xe4,0xab,0xf0,0x23,0x53,0x24,0x5c,0x2a,0x42,0xf8,0x0e,0x26,0xfc,0xd4,0x5c,0xc1,0x71,0xef,0xa9,0x82,0x3d,0x7b,0x49,0
get__s=(__s_n)=>__s_n.map(x=>[0x63,0x7C,0x77,0x7B,0xF2,0x6B,0x6F,0xC5,0x30,0x01,0x67,0x2B,0xFE,0xD7,0xAB,0x76,0xCA,
0x82,0xC9,0x7D,0xFA,0x59,0x47,0xF0,0xAD,0xD4,0xA2,0xAF,0x9C,0xA4,0x72,0xC0,0xB7,0xFD,0x93,0x26,0x36,0x3F,0xF7,0xCC,0x34,0
0xF1,0x71,0xD8,0x31,0x15,0x04,0xC7,0x23,0xC3,0x18,0x96,0x05,0x9A,0x07,0x12,0x80,0xE2,0xEB,0x27,0xB2,0x75,0x09,0x83,0x2C,0
0x6E,0x5A,0xA0,0x52,0x3B,0xD6,0xB3,0x29,0xE3,0x2F,0x84,0x53,0xD1,0x00,0xED,0x20,0xFC,0xB1,0x5B,0x6A,0xCB,0xBE,0x39,0x4A,0
0xCF,0xD0,0xEF,0xAA,0xFB,0x43,0x4D,0x33,0x85,0x45,0xF9,0x02,0x7F,0x50,0x3C,0x9F,0xA8,0x51,0xA3,0x40,0x8F,0x92,0x9D,0x38,0
0xB6,0xDA,0x21,0x10,0xFF,0xF3,0xD2,0xCD,0x0C,0x13,0xEC,0x5F,0x97,0x44,0x17,0xC4,0xA7,0x7E,0x3D,0x64,0x5D,0x19,0x73,0x60,0
0xDC,0x22,0x2A,0x90,0x88,0x46,0xEE,0xB8,0x14,0xDE,0x5E,0x0B,0xDB,0xE0,0x32,0x3A,0x0A,0x49,0x06,0x24,0x5C,0xC2,0xD3,0xAC,0
0x95,0xE4,0x79,0xE7,0xC8,0x37,0x6D,0x8D,0xD5,0x4E,0xA9,0x6C,0x56,0xF4,0xEA,0x65,0x7A,0xAE,0x08,0xBA,0x78,0x25,0x2E,0x1C,0
0xC6,0xE8,0xDD,0x74,0x1F,0x4B,0xBD,0x8B,0x8A,0x70,0x3E,0xB5,0x66,0x48,0x03,0xF6,0x0E,0x61,0x35,0x57,0xB9,0x86,0xC1,0x1D,0
0xF8,0x98,0x11,0x69,0xD9,0x8E,0x94,0x9B,0x1E,0x87,0xE9,0xCE,0x55,0x28,0xDF,0x8C,0xA1,0x89,0x0D,0xBF,0xE6,0x42,0x68,0x41,0
0x0F,0xB0,0x54,0xBB,0x16][x]);u=(u_m)=>Array.from(u_m).map(u_x=>u_x.charCodeAt(0));e=(e_m)=>{e_k=[
0xAC,0x46,0x4C,0x41,0x47,0x7B,0x54,0x48,0x31,0x24,0x5F,0x31,0x24,0x5F,0x42,0x31,0x54,0x5F,0x54,0x34,0x4E,0x47,0x30,0x7D];
e_gfm=((bm_bl)=>{bm_n=[];for(bm_j=0;bm_j<4;bm_j++){bm_n.push([]);for(bm_i=0;bm_i<4;bm_i++)
bm_n[bm_j].push(bm_bl[bm_i*4+bm_j]);};return bm_n})([0x02,0x01,0x01,0x03,0x03,0x02,0x01,0x01,0x01,0x03,0x02,0x01,
0x01,0x01,0x03,0x02]);e_sk=((gsk_k)=>{gsk_N=((n_k)=>[4,6,8][n_k.length*2/16-2])(gsk_k);gsk_K=((sk_k)=>{
sk_bl=[];for(sk_i=0;sk_i<sk_k.length/4;sk_i++){sk_bl.push(sk_k.slice(sk_i*4,(sk_i+1)*4))};return sk_bl})(gsk_k);
gsk_W=[];for(gsk_i=0;gsk_i<(((r_k)=>[10,12,14][r_k.length*2/16-2])(gsk_k)+1)*4;gsk_i++){gsk_W.push([]);(gsk_i<gsk_N)?
gsk_W[gsk_W.length-1]=gsk_K[gsk_i].slice():((gsk_i>=gsk_N&&gsk_i%gsk_N==0)?gsk_W[gsk_W.length-1]=((...xr_v)=>{xr_n=
xr_v[0].slice();for(xr_i=1;xr_i<xr_v.length;xr_i++){for(xr_j=0;xr_j<xr_v[xr_i].length;xr_j++){xr_n[xr_j]^=
xr_v[xr_i][xr_j];}};return xr_n})(gsk_W[gsk_i-gsk_N],get__s(((sk_n,sk_l)=>(sk_l?[sk_n[1],sk_n[2],sk_n[3],sk_n[0]]:
[sk_n[3],sk_n[0],sk_n[1],sk_n[2]]))(gsk_W[gsk_i-1].slice(),true)),  ((rcon_i)=>[[0x00,0x01,0x02,0x04,0x08,0x10,0x20,0x40,
0x80,0x1B,0x36][rcon_i],0x00,0x00,0x00])((gsk_i/gsk_N)|0)).slice():((gsk_i>=gsk_N&&gsk_i%4==0)?gsk_W[gsk_W.length-1]=
```

I could also talk about Golang

- but it’s really cool though
- it is garbage-collected but it can be wonky
- dealing with panic’s is a really wild approach

I could also talk about Rust

- but I don’t want to get stabbed
- my only issue is how it handles JSON, but ¯_(ツ)_/¯
  - (I know it’s not designed for it)
- crabs are cool