H*cking WASM Debugging

Lessons from h*cking/solving WASM challs

ByamB4

$ whoami

- **2021**
  Graduated MUST-SICT via cybersecurity

- **2021, 2022, 2023**
  Haruul Zangi /cybersecurity/ 3 time champion

- **International competition**
  Black Hat MEA 12th place /Saudi Arabia
  VolgaCTF 8th place /Russia
  ACSC 53th place /Asia
  ICC 3rd place /America

WASM

ByamB4

$ wasm --about

- **Web + Assembly**
- **Compiles from various language**
  - Go, Rust, C, C++, ...
- **Use existing complex libraries**
  - Complex 3D engine, blockchain
- **Security in mind**
  - Sandbox system, isolated memory
  - Less dynamic than JS, injection, memory management, so hard

WASM

ByamB4

$ wasm --cases

- WASM video games are becoming very common
  - Newgrounds, Kongregate, ...
- Unity3D and Unreal engine 4 can now both target WASM
- Retargeted desktop applications
- 3D applications

$ wasm --hack

- Web becomes traditional way to reverse back to ASM
- radare2
- JEB decompiler
- Wabt (WASM binary toolkit)
- Cetus (more like a cheat engine)

ByamB4

$ wasm --hack

```
0x001e5c1     i32.const 32
0x001e5c3     i32.add
0x001e5c4     global.set $global0
0x001e5c6   )
0x001e5c9   (func $func388 (param $var0 i32) (param $var1 i32) (result i32)
0x001e5c9     (local $var2 i32)
0x001e5c9     (local $var3 i32)
0x001e5cc     block $label0
0x001e5ce       local.get $var1
0x001e5d0       i32.const -1
0x001e5d2       i32.eq
0x001e5d3       if
0x001e5d5         i32.const 9617972
0x001e5da         i32.const 4
0x001e5dc         i32.const 0
0x001e5de         call $func1683
0x001e5e1         i32.load
0x001e5e4         local.tee $var0
0x001e5e6         i32.const 4
0x001e5e8         i32.const 5632
0x001e5eb         call $func1683
0x001e5ee         i32.load offset=5632
0x001e5f2         i32.eqz
0x001e5f3         br_if $label0
0x001e5f5         local.get $var0
0x001e5f7         i32.const 4
0x001e5f9         i32.const 5636
0x001e5fc         call $func1683
0x001e5ff         i32.load offset=5636
0x001e603         br_if $label0
0x001e605         local.get $var0
0x001e607         i32.const 1
0x001e609         i32.store offset=5632
0x001e60d         global.get $global3
0x001e60f         if
```

```
(module
 (table 0 anyfunc)
 (memory $0 1)
 (export "memory" (memory $0))
 (export "factorial" (func $factorial))
 (func $factorial (; 0 ;) (param $0 i32) (result i32)
  (local $1 i32)
  (local $2 i32)
  (set_local $2
   (i32.const 1)
  )
  (block $label$0
   (br_if $label$0
    (i32.lt_s
     (get_local $0)
     (i32.const 2)
    )
   )
   (set_local $2
    (i32.const 1)
   )
   (loop $label$1
    (set_local $2
     (i32.mul
      (get_local $0)
      (get_local $2)
     )
    )
    (set_local $1
     (i32.gt_s
      (get_local $0)
      (i32.const 2)
     )
    )
    (set_local $0
     (i32.add
      (get_local $0)
      (i32.const -1)
     )
    )
    (br_if $label$1
     (get_local $1)
    )
   )
  )
  (get_local $2)
 )
)
```

primes.wasm.wasm ×

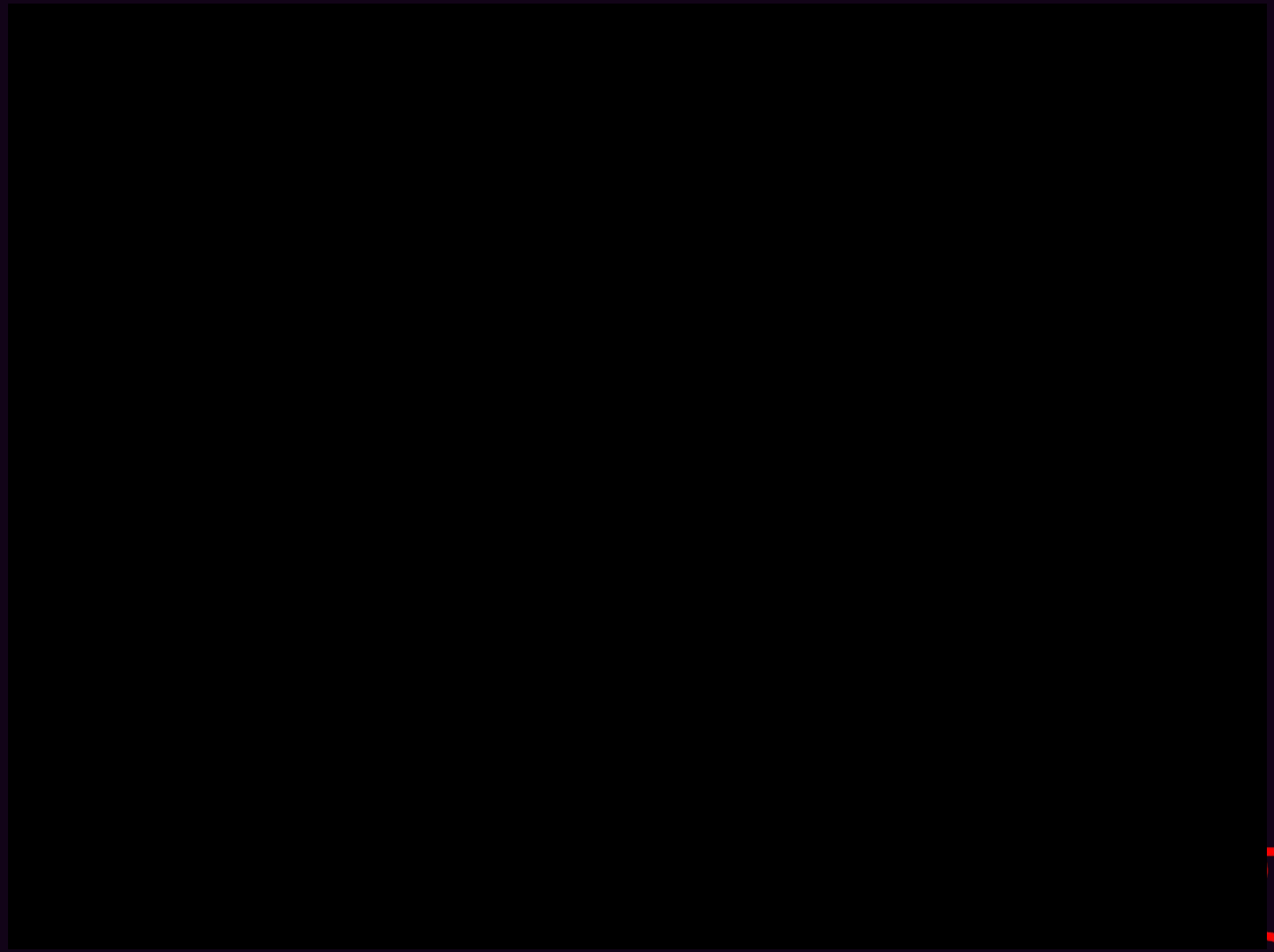
```
1   (module
2     (type $t0 (func (result i32)))
3     (func $a (type $t0) (result i32)
4       (local $l0 i32) (local $l1 i32) (loca
5       i32.const 2
6       set_local $l0
7       loop $L0
8         get_local $l0
9         i32.const 2
10        i32.gt_u
11        if $I1
12          block $B2
13            get_local $l0
14            set_local $l2
15            loop $L3 (result i32)
16              get_local $l0
17              get_local $l2
18              i32.const -1
```

WASM

ByamB4

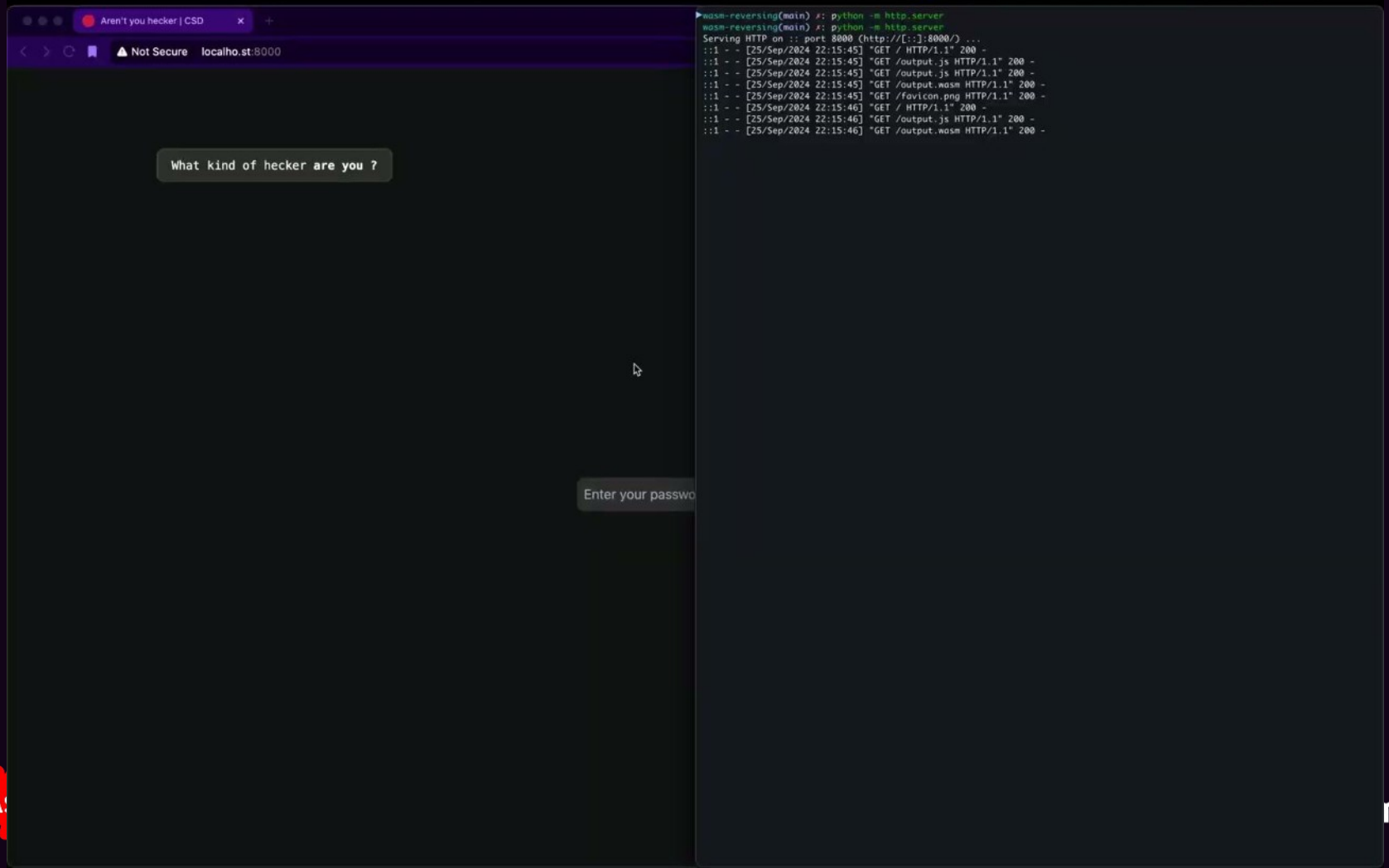
$ wasm --demo1

- **Solving CTF like challenge**
- **Method 1: debugging**
- **Method 2: overwriting wasm**



WASM

ByamB4

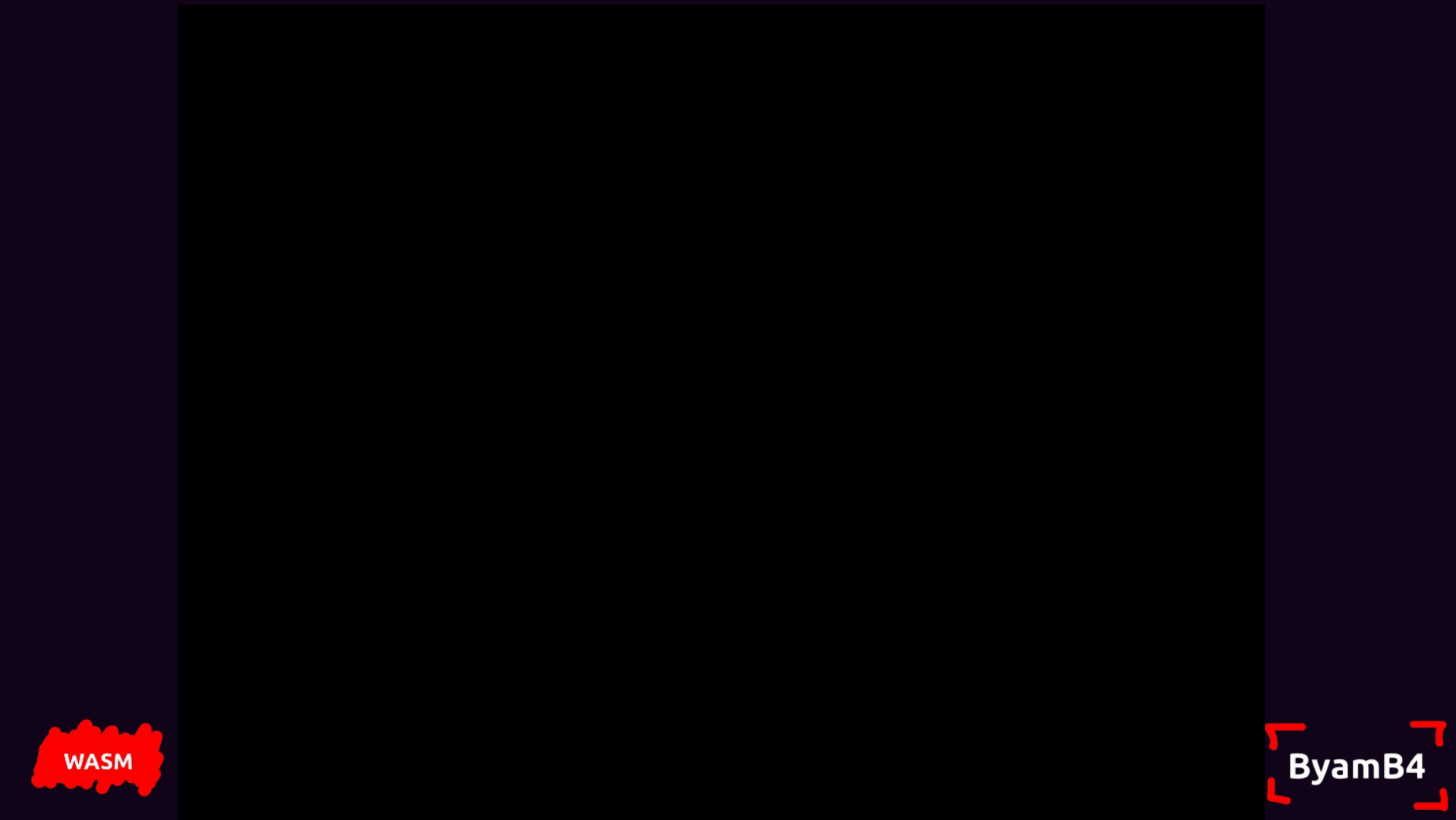

iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
Wed Sep 25 22:17
Aren't you hecker | CSD
Not Secure localho.st:8000
What kind of hecker are you ?
Enter your passwo
wasm-reversing(main) ✗: python -m http.server
wasm-reversing(main) ✗: python -m http.server
Serving HTTP on :: port 8000 (http://[::]:8000/) ...
::1 - - [25/Sep/2024 22:15:45] "GET / HTTP/1.1" 200 -
::1 - - [25/Sep/2024 22:15:45] "GET /output.js HTTP/1.1" 200 -
::1 - - [25/Sep/2024 22:15:45] "GET /output.js HTTP/1.1" 200 -
::1 - - [25/Sep/2024 22:15:45] "GET /output.wasm HTTP/1.1" 200 -
::1 - - [25/Sep/2024 22:15:45] "GET /favicon.png HTTP/1.1" 200 -
::1 - - [25/Sep/2024 22:15:46] "GET / HTTP/1.1" 200 -
::1 - - [25/Sep/2024 22:15:46] "GET /output.js HTTP/1.1" 200 -
::1 - - [25/Sep/2024 22:15:46] "GET /output.wasm HTTP/1.1" 200 -

$ wasm --demo2

- **Trying real life game**

- **https://github.com/GMH-Code/Quake-WASM**

- **https://quake.m-h.org.uk/**


WASM
ByamB4