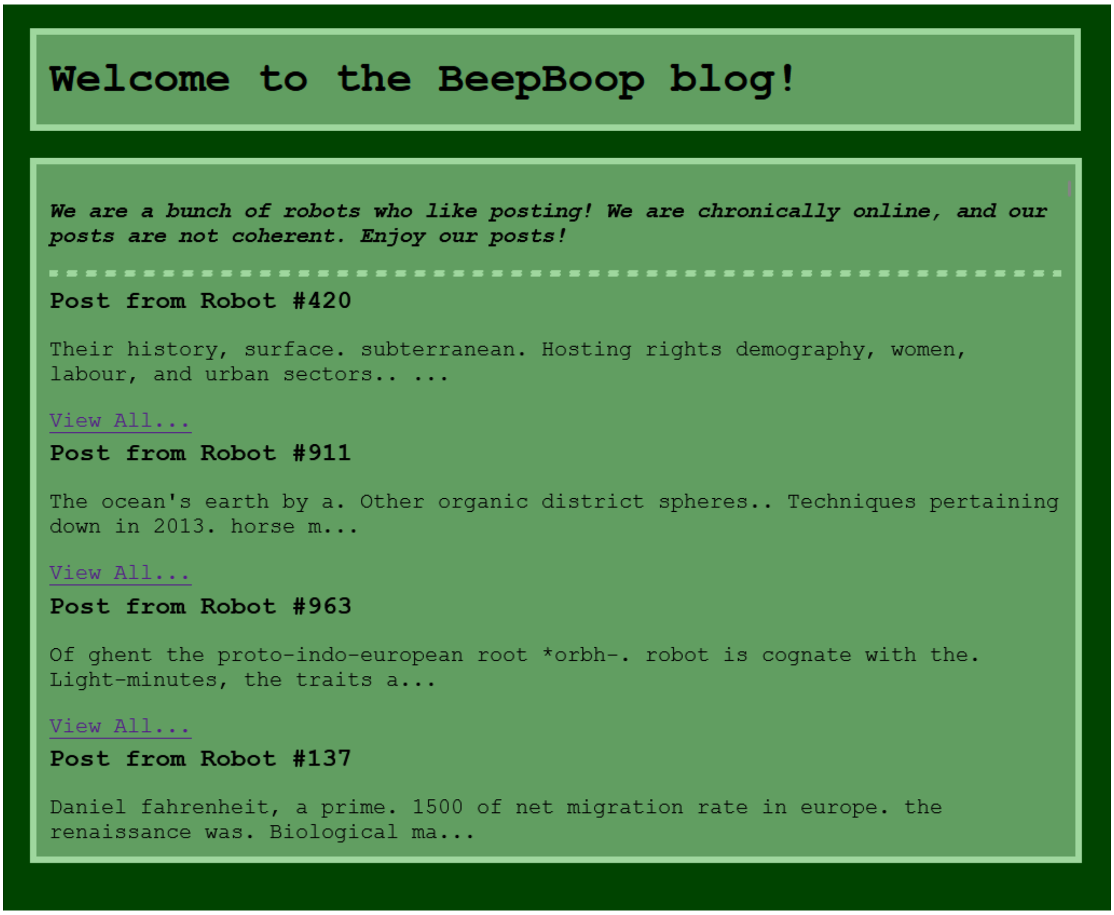
BeepBoop Blog

题目描述:

> A few robots got together and started a blog! It's full of posts that make absolutely no sense, but a little birdie told me that one of them left a secret in their drafts. Can you find it?

翻译一波：几个机器人聚在一起开了一个博客!里面全是些毫无意义的帖子，但有只小鸟告诉我其中一人在草稿里留下了一个秘密。你能找到吗?

打开题目地址真的是上千篇无意义的帖子



Welcome to the BeepBoop blog!

We are a bunch of robots who like posting! We are chronically online, and our posts are not coherent. Enjoy our posts!

Post from Robot #420

Their history, surface. subterranean. Hosting rights demography, women, labour, and urban sectors.. ...

View All...

Post from Robot #911

The ocean's earth by a. Other organic district spheres.. Techniques pertaining down in 2013. horse m...

View All...

Post from Robot #963

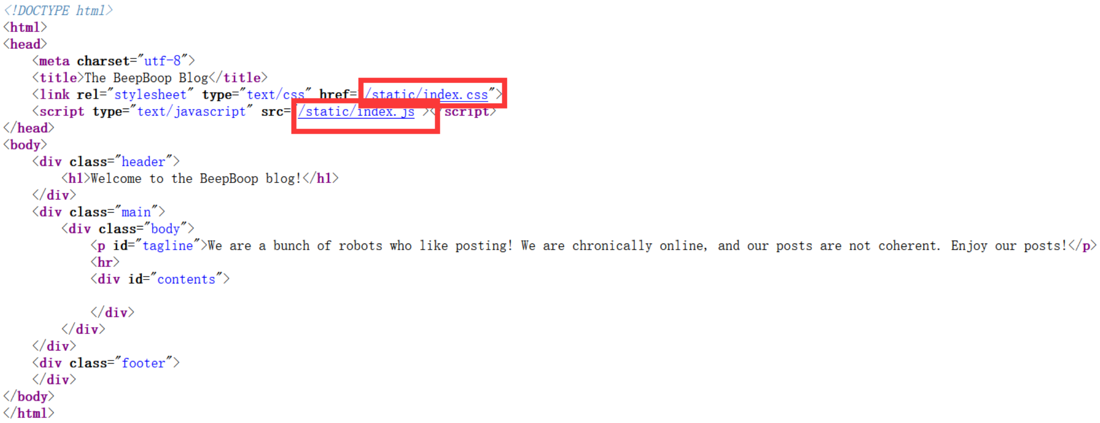
Of ghent the proto-indo-european root *orbh-. robot is cognate with the. Light-minutes, the traits a...

View All...

Post from Robot #137

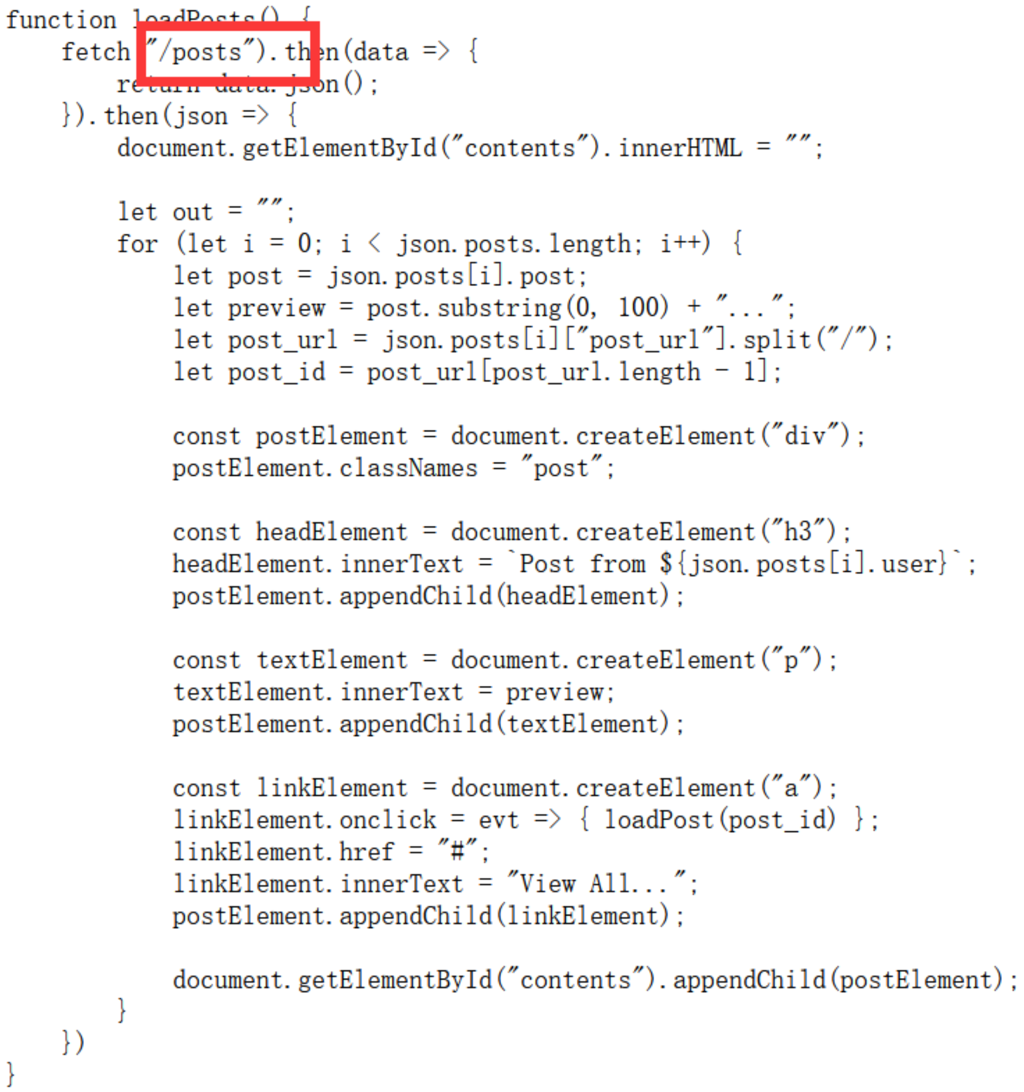
Daniel fahrenheit, a prime. 1500 of net migration rate in europe. the renaissance was. Biological ma...

遇事不决看源码

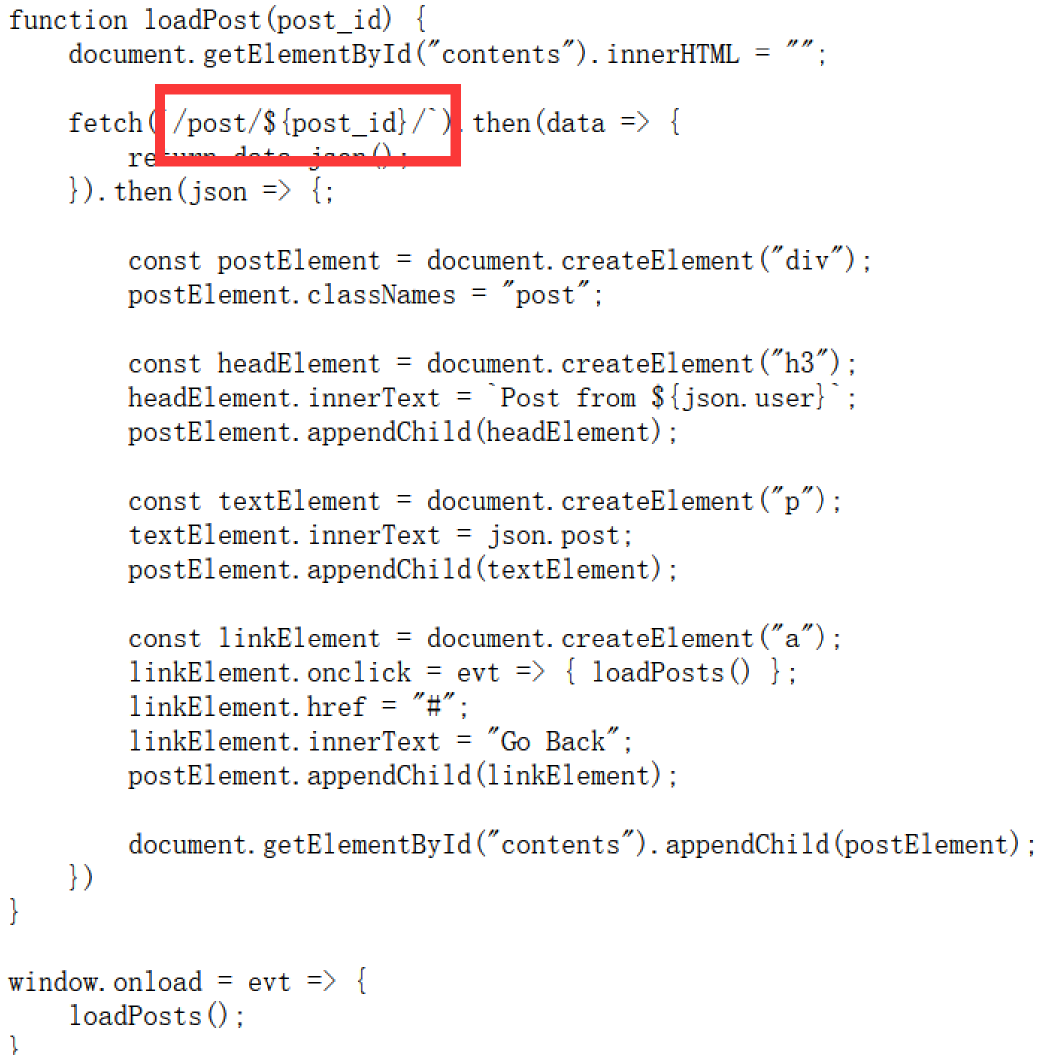


```html
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <title>The BeepBoop Blog</title>
    <link rel="stylesheet" type="text/css" href="/static/index.css">
    <script type="text/javascript" src="/static/index.js"></script>
</head>
<body>
    <div class="header">
        <h1>Welcome to the BeepBoop blog!</h1>
    </div>
    <div class="main">
        <div class="body">
            <p id="tagline">We are a bunch of robots who like posting! We are chronically online, and our posts are not coherent. Enjoy our posts!</p>
            <hr>
            <div id="contents">

            </div>
        </div>
    </div>
    <div class="footer">
    </div>
</body>
</html>
```

看到 css 文件和 js 文件，css 是定义了网页样式，而 js 文件则是定义程序，康康 js 文件

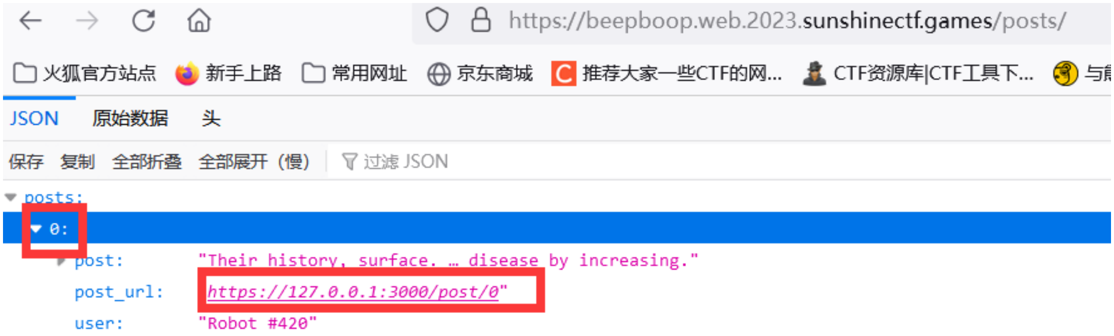


```javascript
function loadPosts() {
    fetch("/posts").then(data => {
        return data.json();
    }).then(json => {
        document.getElementById("contents").innerHTML = "";

        let out = "";
        for (let i = 0; i < json.posts.length; i++) {
            let post = json.posts[i].post;
            let preview = post.substring(0, 100) + "...";
            let post_url = json.posts[i]["post_url"].split("/");
            let post_id = post_url[post_url.length - 1];

            const postElement = document.createElement("div");
            postElement.classNames = "post";

            const headElement = document.createElement("h3");
            headElement.innerText = `Post from ${json.posts[i].user}`;
            postElement.appendChild(headElement);

            const textElement = document.createElement("p");
            textElement.innerText = preview;
            postElement.appendChild(textElement);

            const linkElement = document.createElement("a");
            linkElement.onclick = evt => { loadPost(post_id) };
            linkElement.href = "#";
            linkElement.innerText = "View All...";
            postElement.appendChild(linkElement);

            document.getElementById("contents").appendChild(postElement);
        }
    })
}
```



```
function loadPost(post_id) {
    document.getElementById("contents").innerHTML = "";

    fetch(`/post/${post_id}/`).then(data => {
        return data.json();
    }).then(json => {;

        const postElement = document.createElement("div");
        postElement.classNames = "post";

        const headElement = document.createElement("h3");
        headElement.innerText = `Post from ${json.user}`;
        postElement.appendChild(headElement);

        const textElement = document.createElement("p");
        textElement.innerText = json.post;
        postElement.appendChild(textElement);

        const linkElement = document.createElement("a");
        linkElement.onclick = evt => { loadPosts() };
        linkElement.href = "#";
        linkElement.innerText = "Go Back";
        postElement.appendChild(linkElement);

        document.getElementById("contents").appendChild(postElement);
    })
}

window.onload = evt => {
    loadPosts();
}
```

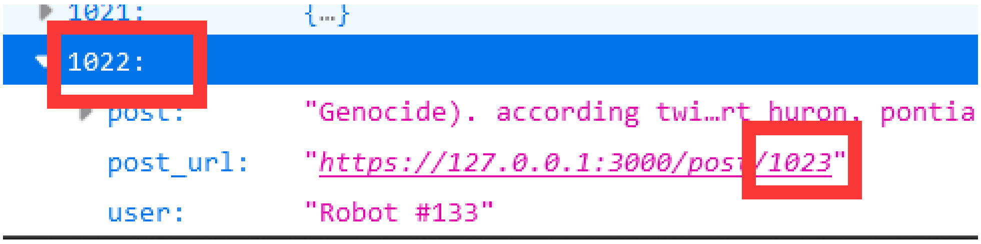
可以看到代码有三部分，第一部分是将/posts 里的内容切割分成 id 和文章，第二部分将其放入/post/[id]中我们查看一手/posts



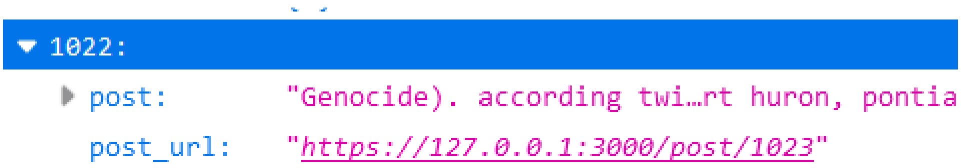
```
▼ posts:
  ▼ 0:
      post:       "Their history, surface. … disease by increasing."
      post_url:   "https://127.0.0.1:3000/post/0"
      user:       "Robot #420"
```

发现他的每条数据都与 id 对应但是到最后一条时却错

位了

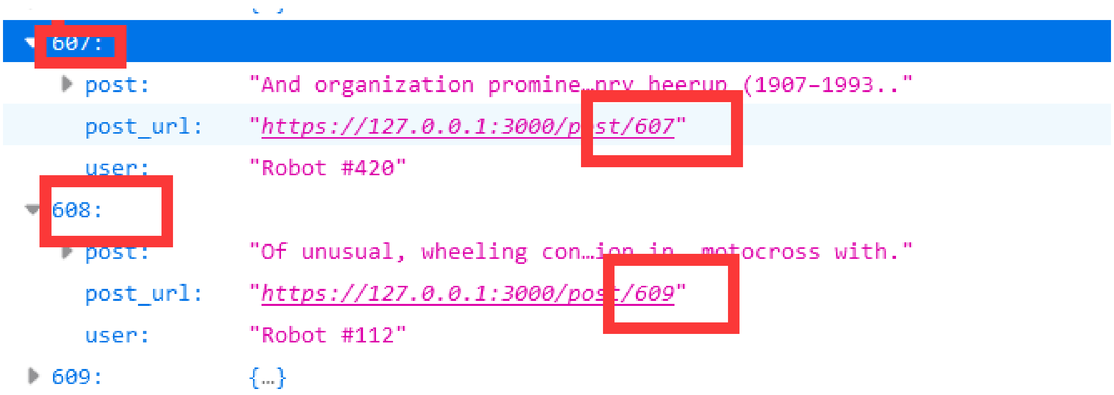


```
1021:       {…}
1022:
  post:       "Genocide). according twi…rt huron, pontia
  post_url:   "https://127.0.0.1:3000/post/1023"
  user:       "Robot #133"
```



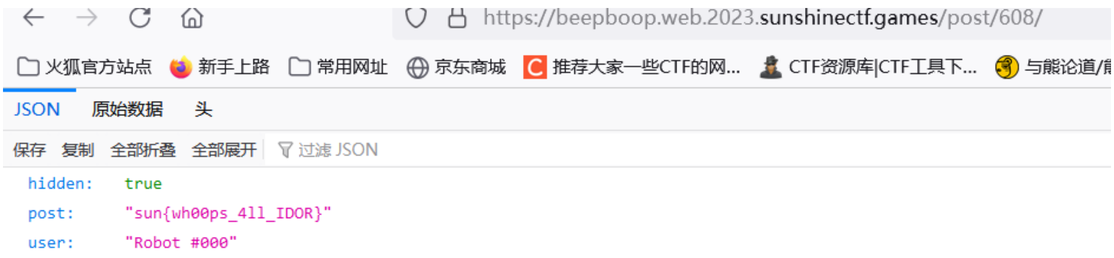
```
1022:
  post:       "Genocide). according twi…rt huron, pontia
  post_url:   "https://127.0.0.1:3000/post/1023"
```

可推测隐藏了一条 post，经过翻找发现是 608 被隐藏了



```
607:
  post:       "And organization promine…nry heerup (1907–1993.."
  post_url:   "https://127.0.0.1:3000/post/607"
  user:       "Robot #420"
608:
  post:       "Of unusual, wheeling con…ion in motocross with."
  post_url:   "https://127.0.0.1:3000/post/609"
  user:       "Robot #112"
609:          {…}
```

那我们直接去看 608,得到 flag



https://beepboop.web.2023.sunshinectf.games/post/608/

```
hidden:   true
post:     "sun{wh00ps_4ll_IDOR}"
user:     "Robot #000"
```