Code Analysis

Now that we have deobfuscated the code, we can start going through it:

Code: javascript

```javascript
'use strict';
function generateSerial() {
  ...SNIP...
  var xhr = new XMLHttpRequest;
  var url = "/serial.php";
  xhr.open("POST", url, true);
  xhr.send(null);
};
```

We see that the `secret.js` file contains only one function, `generateSerial`.

HTTP Requests

Let us look at each line of the `generateSerial` function.

Code Variables

The function starts by defining a variable `xhr`, which creates an object of `XMLHttpRequest`. As we may not know exactly what `XMLHttpRequest` does in JavaScript, let us Google `XMLHttpRequest` to see what it is used for.
After we read about it, we see that it is a JavaScript function that handles web requests.

The second variable defined is the `URL` variable, which contains a URL to `/serial.php`, which should be on the same domain, as no domain was specified.

Code Functions

Next, we see that `xhr.open` is used with `"POST"` and `URL`. We can Google this function once again, and we see that it opens the HTTP request defined '`GET` or `POST`' to the `URL`, and then the next line `xhr.send` would send the request.

So, all `generateSerial` is doing is simply sending a `POST` request to `/serial.php`, without including any `POST` data or retrieving anything in return.

The developers may have implemented this function whenever they need to generate a serial, like when clicking on a certain `Generate Serial` button, for example. However, since we did not see any similar HTML elements that generate serials, the developers must not have used this function yet and kept it for future use.

With the use of code deobfuscation and code analysis, we were able to uncover this function. We can now attempt to replicate its functionality to see if it is handled on the server-side when sending a `POST` request. If the function is enabled and handled on the server-side, we may uncover an unreleased functionality, which usually tends to have bugs and vulnerabilities within them.

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left