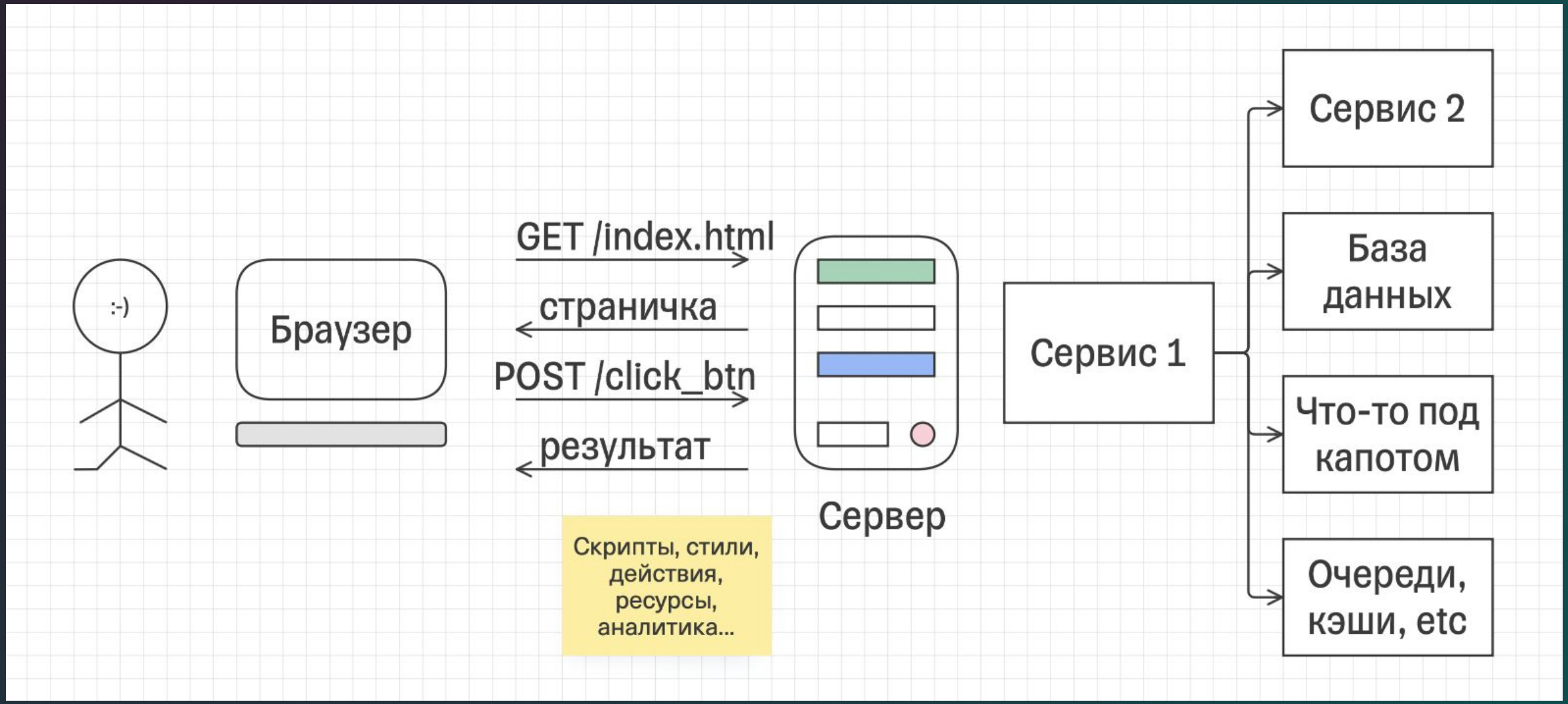
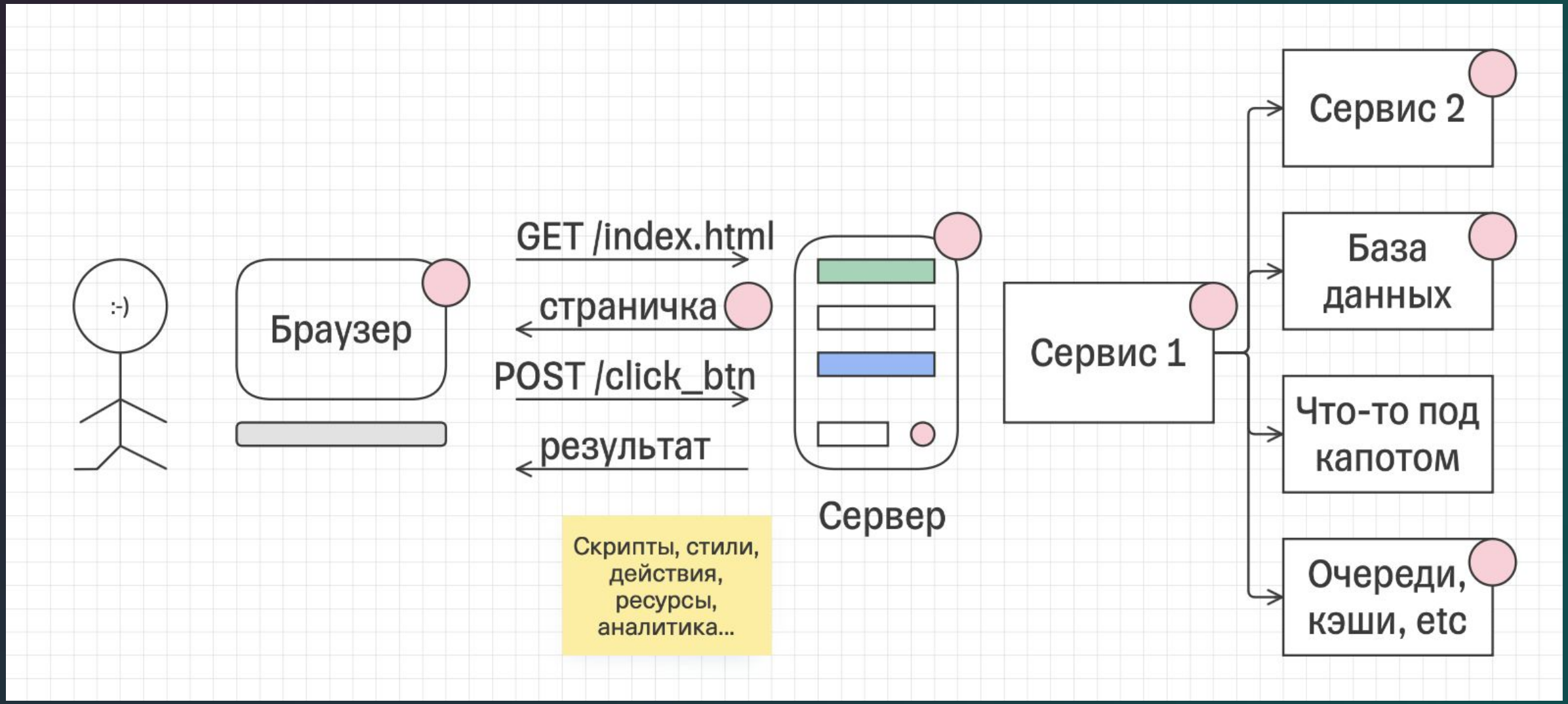
Основы защиты Web-приложений

Егоров Антон
developer @ T-Bank

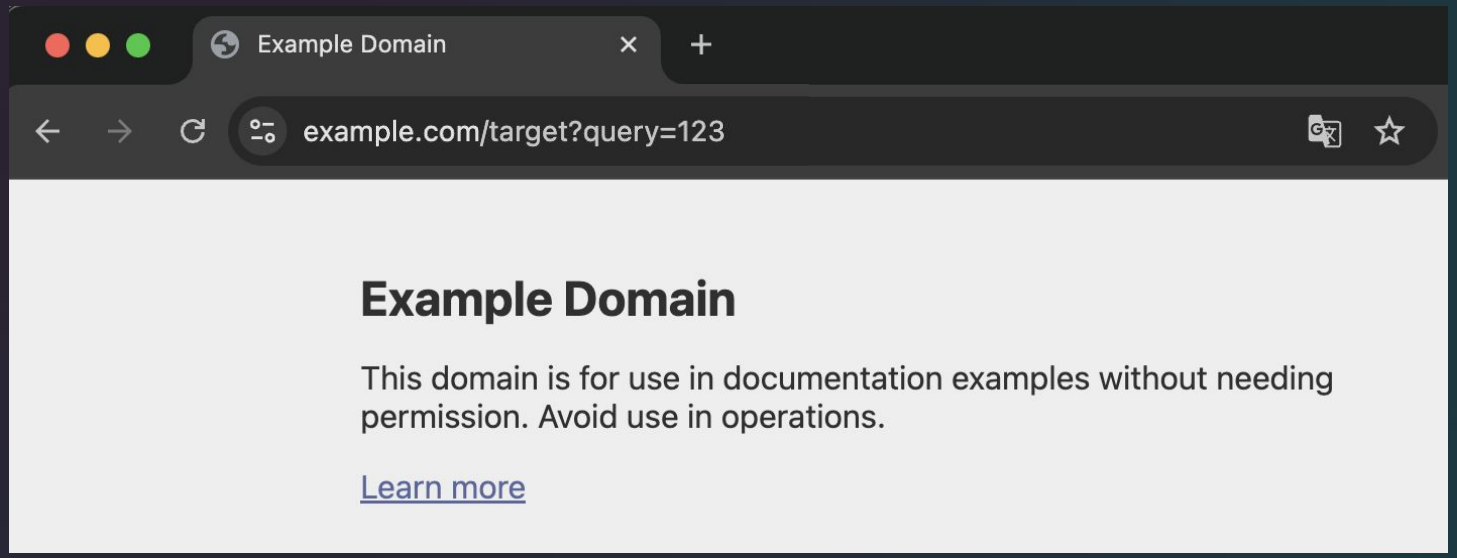
О web-приложениях



О web-приложениях



Запросы на сервер – HTTP




```HTTP
GET /target?query=123 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 AppleWebKit/605.1.15 (KHTML, like Gecko) Safari/605.1.15
Accept: */*
```

Запросы на сервер

HTTP

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 1234
Set-Cookie: PHPSESSID=1234...

<!doctype html>
<html>
    <head><title> Page title </title></head>
    <body>Your HTML markup here
    <....>
    </body>
</html>
```

Запросы на сервер – ресурсы

HTTP

```
GET /assets/index.js HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 AppleWebKit/605.1.15 (KHTML, like Gecko) Safari/605.1.15
Accept: */*
```

HTTP

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=UTF-8
Content-Length: 123

<h1>Not Found... =( <h1>
```

HTTP

```
GET /assets/main_styles.css HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 AppleWebKit/605.1.15 (KHTML, like Gecko) Safari/605.1.15
Accept: */*
```

Запросы на сервер – жмем кнопку

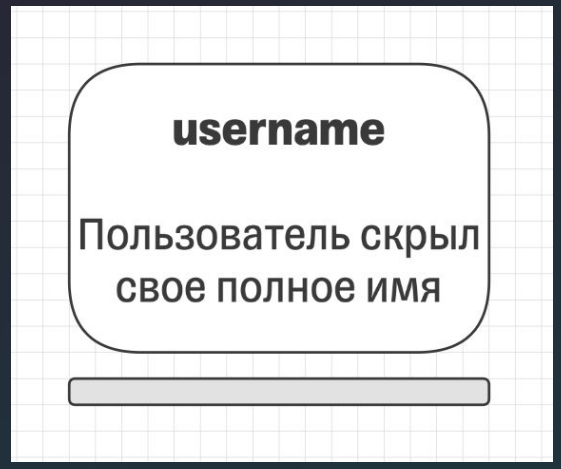
```HTTP
POST /target?query=123 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 AppleWebKit/605.1.15 (KHTML, like Gecko) Safari/605.1.15
Accept: application/json
Content-Type: application/json
Content-Length: 42
Authorization: Bearer {your_token}
Cookie: PHPSESSID=12345678.........

   {"field1": "test", "other": 123, ...
```

Запросы на сервер – жмем кнопку

```HTTP
POST /target?query=123 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 AppleWebKit/605.1.15 (KHTML, like Gecko) Safari/605.1.15
Accept: application/json
Content-Type: application/json
Content-Length: 42
Authorization: Bearer {your_token}
Cookie: PHPSESSID=12345678.........

   {"field1": "test", "other": 123, ...
```

Раскрытие данных в ответе

Пример. В браузере отрисовывается только username, но сервер возвращает избыточные данные



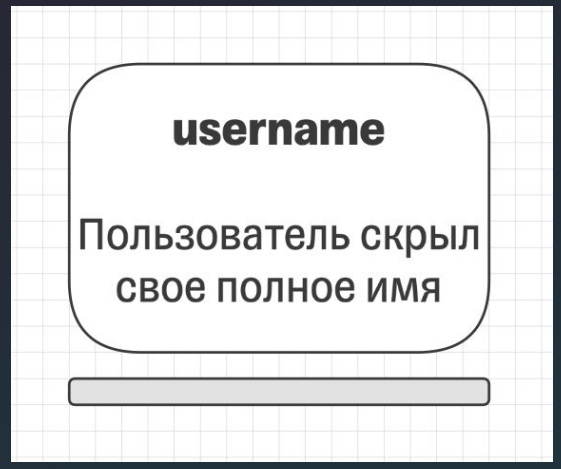

```
GET /get_username?user_id=123 HTTP/1.1
Host: example.com
Accept: application/json
User-Agent: curl/1.2.3
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 123
```

```
{
    "username": "anonymous",
    "full_name": "Печкин Игорь Иванович"
}
```

Раскрытие данных в ответе

Пример. В браузере отрисовывается только username, но сервер возвращает избыточные данные




```
GET /get_username?user_id=123 HTTP/1.1
Host: example.com
Accept: application/json
User-Agent: curl/1.2.3
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 123
```

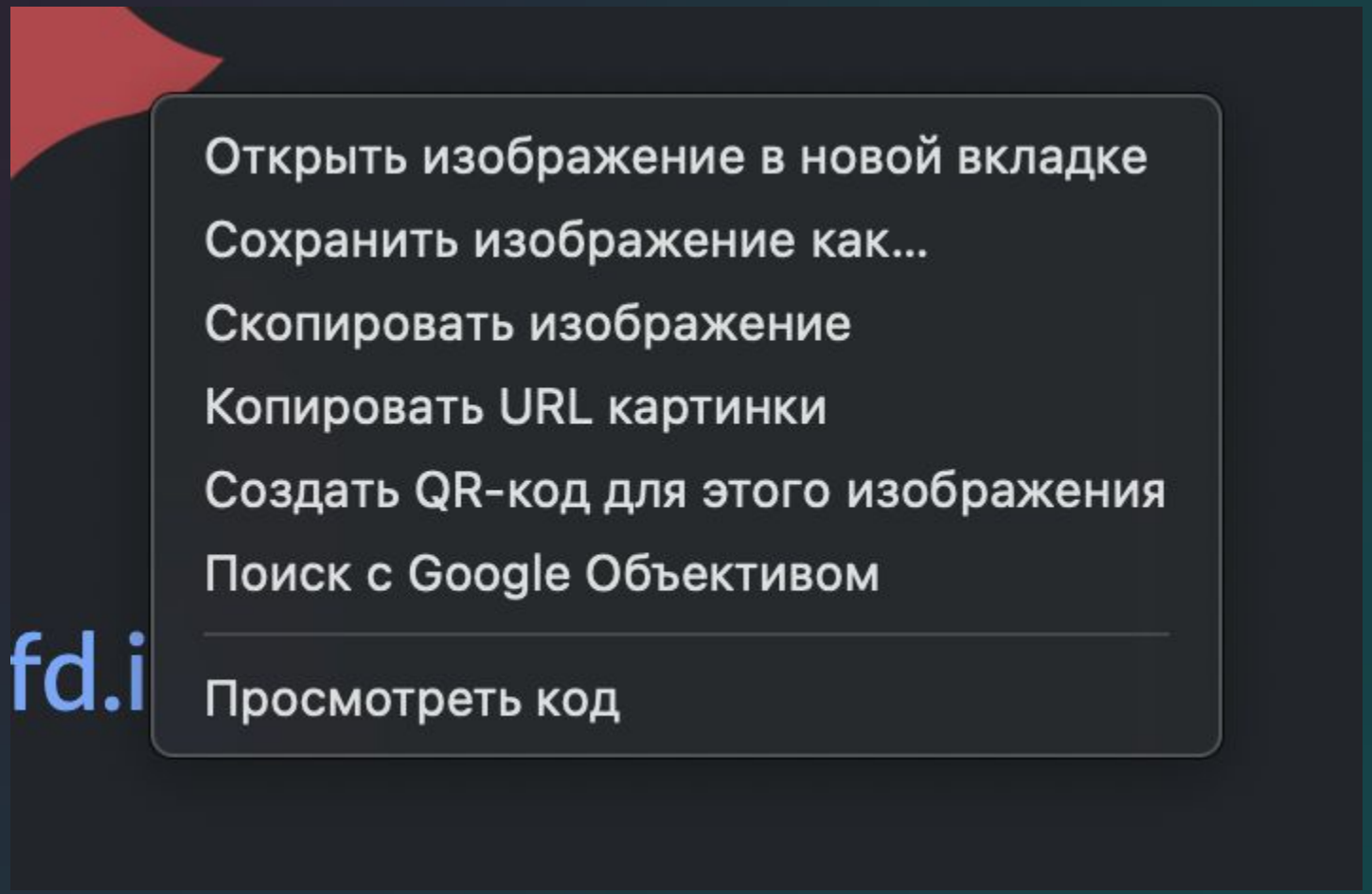
```
{
    "username": "anonymous",
    "full_name": "Печкин Игорь Иванович"
}
```

Раскрытие данных в ответе

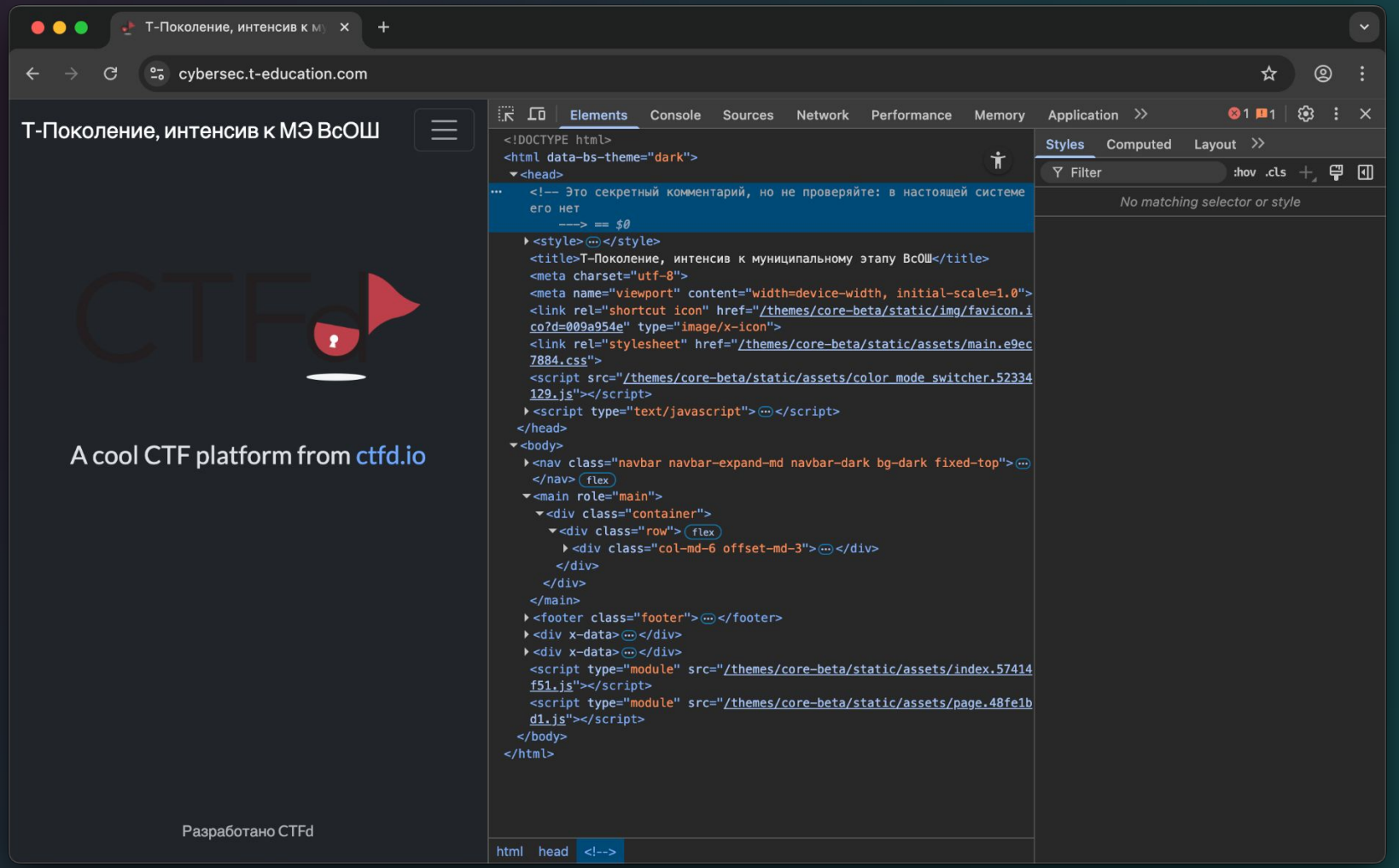
JavaScript

```
function sendPostRequest(password, data) {
    const url = '/auth/admin';

    if (password === 'very_secret_admin_password') {
        fetch('/auth/admin', {
            method: 'POST',
            headers: {
                'Content-Type': 'application/json'
            },
            body: JSON.stringify({ password })
        })
        .then(data => {
            alert('Успех:', data);
        })
        .catch(error => {
            console.error('Ошибка:', error);
        });
    } else {
        alert('Неправильный пароль.');
    }
}
```

Как искать?

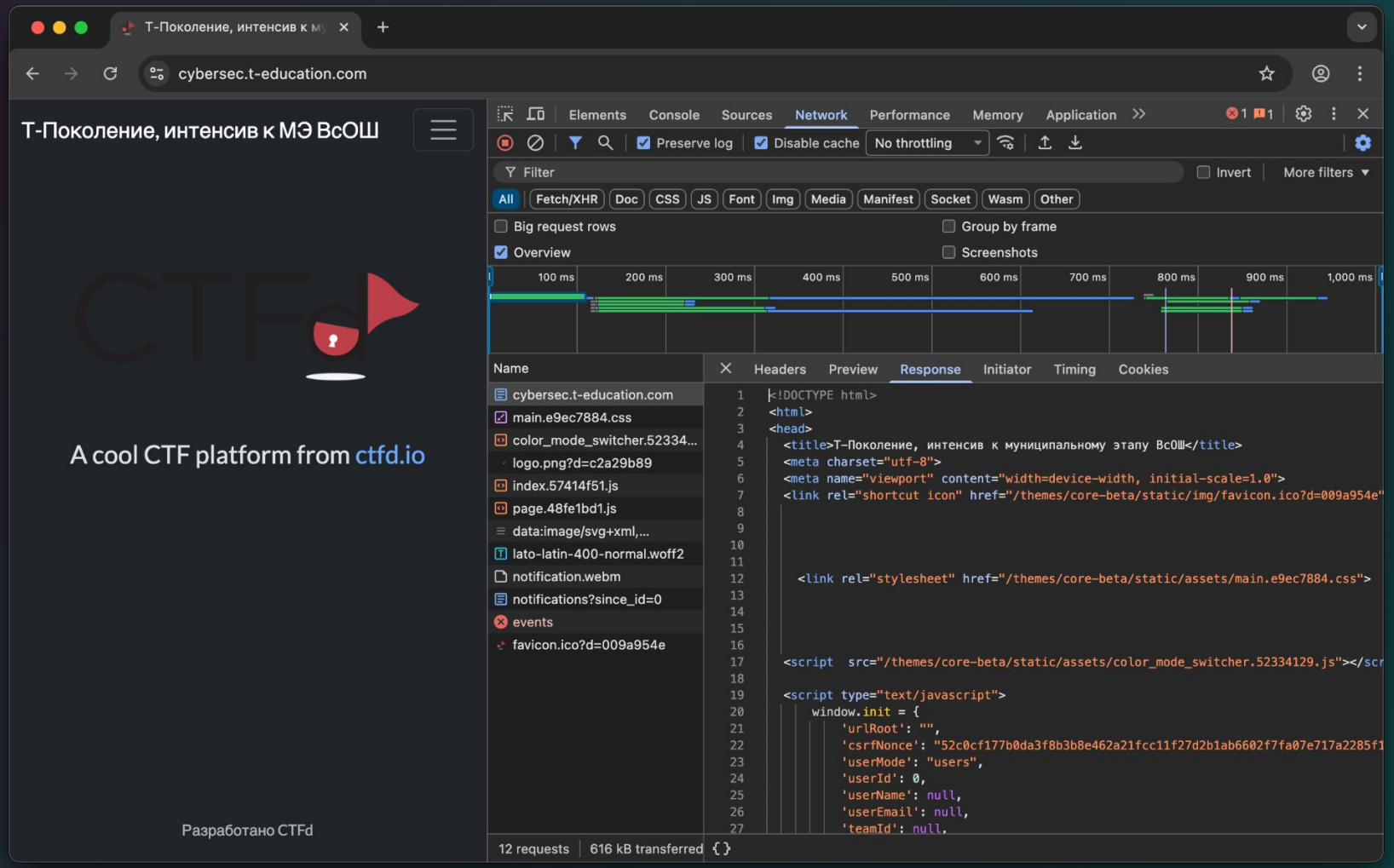

Открыть изображение в новой вкладке
Сохранить изображение как...
Скопировать изображение
Копировать URL картинки
Создать QR-код для этого изображения
Поиск с Google Объективом
Просмотреть код
fd.i

Как искать?

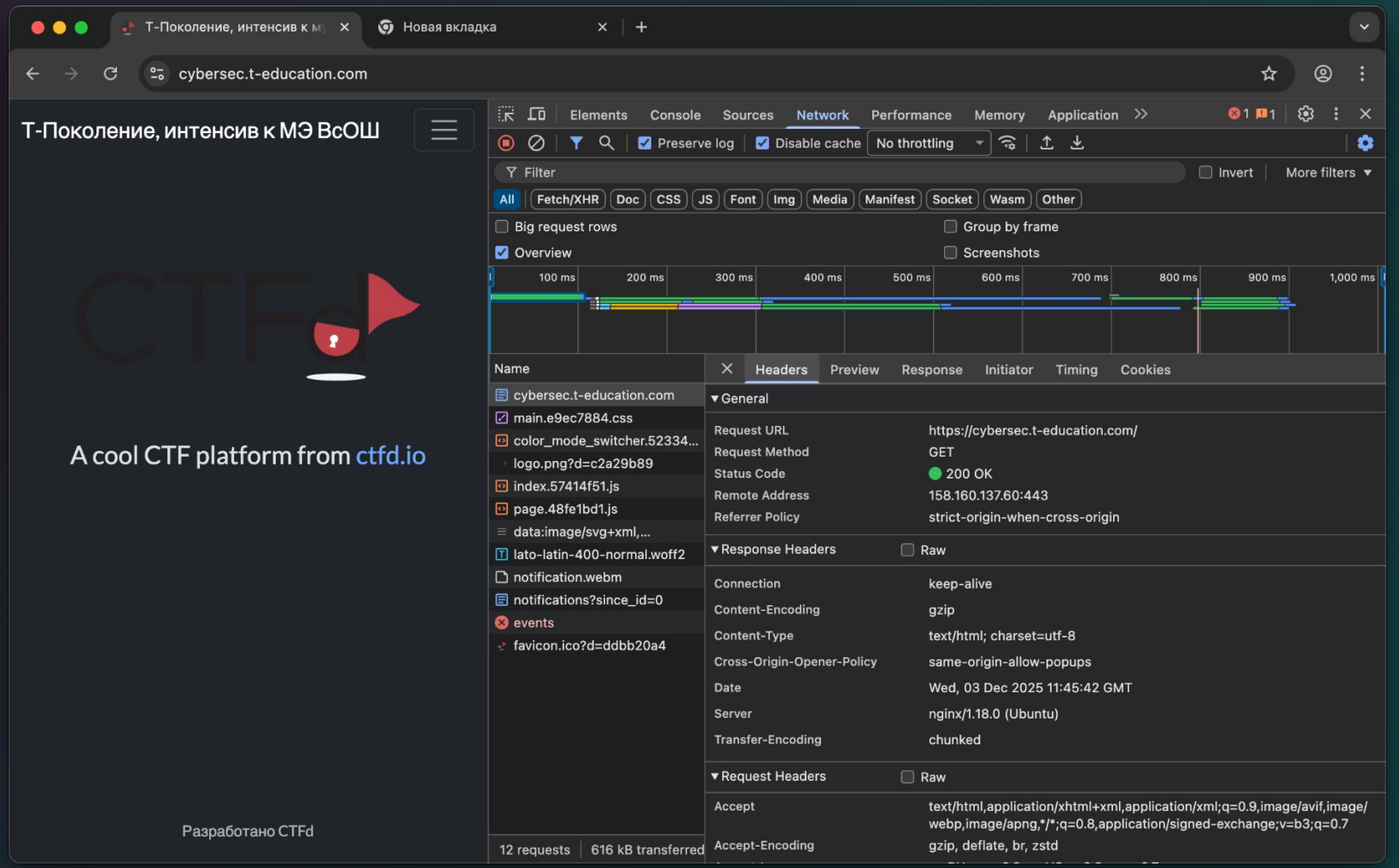

Т-Поколение, интенсив к м
cybersec.t-education.com
Т-Поколение, интенсив к МЭ ВсОШ
A cool CTF platform from ctfd.io
Разработано CTFd
Elements
Console
Sources
Network
Performance
Memory
Application
<!DOCTYPE html>
<html data-bs-theme="dark">
<head>
<!-- Это секретный комментарий, но не проверяйте: в настоящей системе его нет
---> == $0
<style></style>
<title>Т-Поколение, интенсив к муниципальному этапу ВсОШ</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link rel="shortcut icon" href="/themes/core-beta/static/img/favicon.ico?d=009a954e" type="image/x-icon">
<link rel="stylesheet" href="/themes/core-beta/static/assets/main.e9ec7884.css">
<script src="/themes/core-beta/static/assets/color_mode_switcher.52334129.js"></script>
<script type="text/javascript"></script>
</head>
<body>
<nav class="navbar navbar-expand-md navbar-dark bg-dark fixed-top"></nav>
<main role="main">

<footer class="footer"></footer>
<div x-data>
<div x-data>
<script type="module" src="/themes/core-beta/static/assets/index.57414f51.js"></script>
<script type="module" src="/themes/core-beta/static/assets/page.48fe1bd1.js"></script>
</body>
</html>
Styles
Computed
Layout
Filter
:hov .cls
No matching selector or style
html
head
<!-->

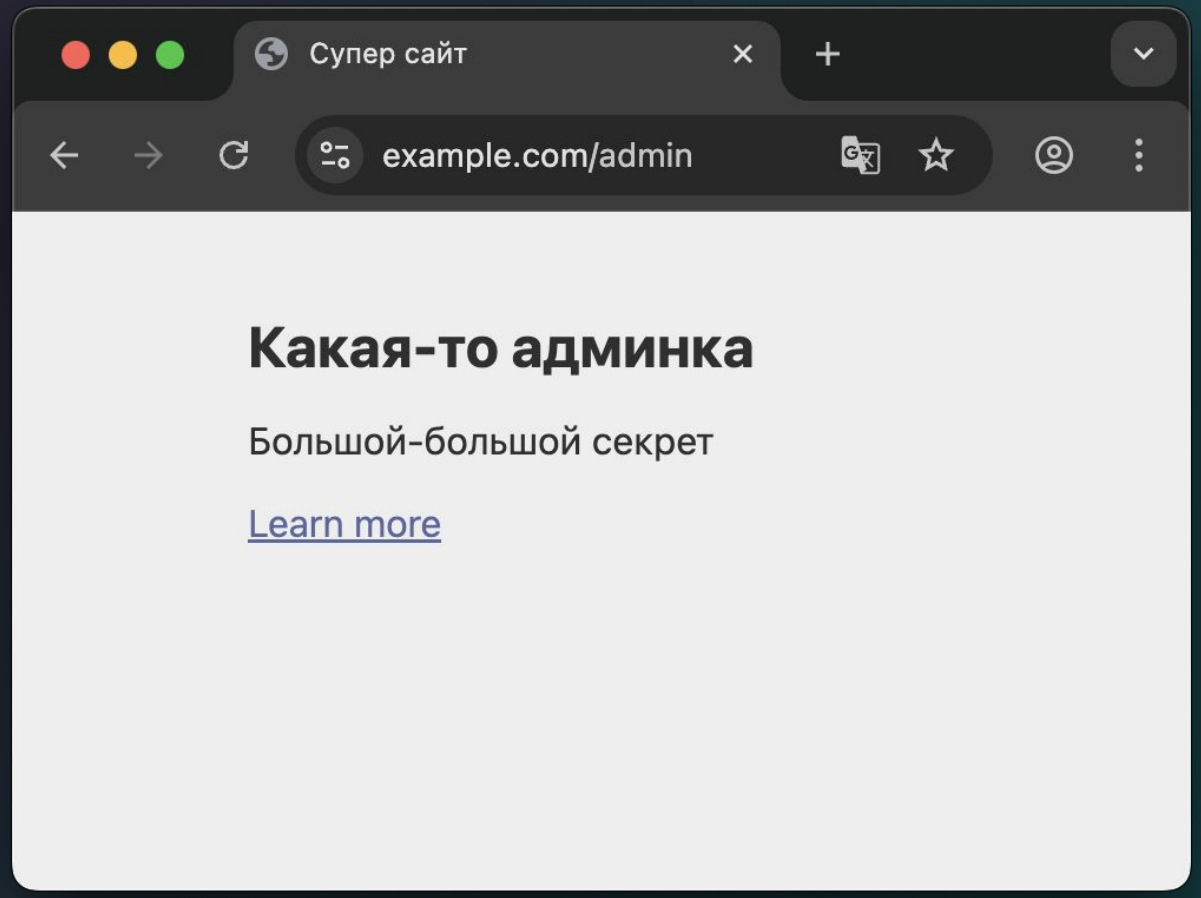
Как искать?


Т-Поколение, интенсив к МЭ ВсОШ
cybersec.t-education.com
Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
Socket
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
100 ms
200 ms
300 ms
400 ms
500 ms
600 ms
700 ms
800 ms
900 ms
1,000 ms
Name
cybersec.t-education.com
main.e9ec7884.css
color_mode_switcher.52334...
logo.png?d=c2a29b89
index.57414f51.js
page.48fe1bd1.js
data:image/svg+xml,...
lato-latin-400-normal.woff2
notification.webm
notifications?since_id=0
events
favicon.ico?d=009a954e
Headers
Preview
Response
Initiator
Timing
Cookies
A cool CTF platform from ctfd.io
Разработано CTFd
12 requests
616 kB transferred

Как искать?

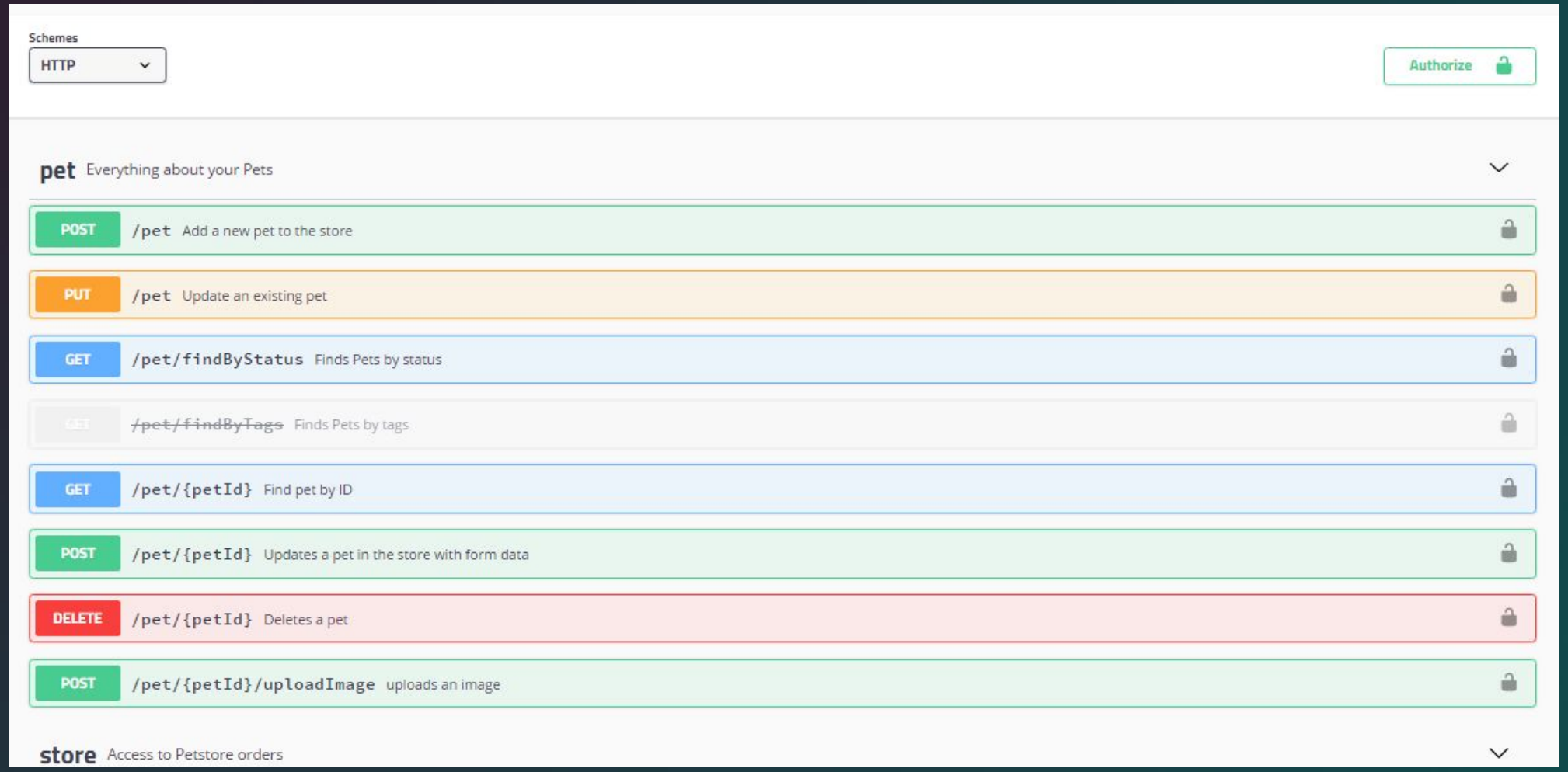

Т-Поколение, интенсив к МЭ ВсОШ
A cool CTF platform from ctfd.io
Разработано CTFd
cybersec.t-education.com
Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
Socket
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
100 ms
200 ms
300 ms
400 ms
500 ms
600 ms
700 ms
800 ms
900 ms
1,000 ms
Name
cybersec.t-education.com
main.e9ec7884.css
color_mode_switcher.52334...
logo.png?d=c2a29b89
index.57414f51.js
page.48fe1bd1.js
data:image/svg+xml,...
lato-latin-400-normal.woff2
notification.webm
notifications?since_id=0
events
favicon.ico?d=ddbb20a4
12 requests
616 kB transferred
Headers
Preview
Response
Initiator
Timing
Cookies
General
Request URL
https://cybersec.t-education.com/
Request Method
GET
Status Code
200 OK
Remote Address
158.160.137.60:443
Referrer Policy
strict-origin-when-cross-origin
Response Headers
Raw
Connection
keep-alive
Content-Encoding
gzip
Content-Type
text/html; charset=utf-8
Cross-Origin-Opener-Policy
same-origin-allow-popups
Date
Wed, 03 Dec 2025 11:45:42 GMT
Server
nginx/1.18.0 (Ubuntu)
Transfer-Encoding
chunked
Request Headers
Raw
Accept
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding
gzip, deflate, br, zstd

Отсутствие контроля доступа



Отсутствие контроля доступа

/docs – Swagger UI. Раскрытие структуры API



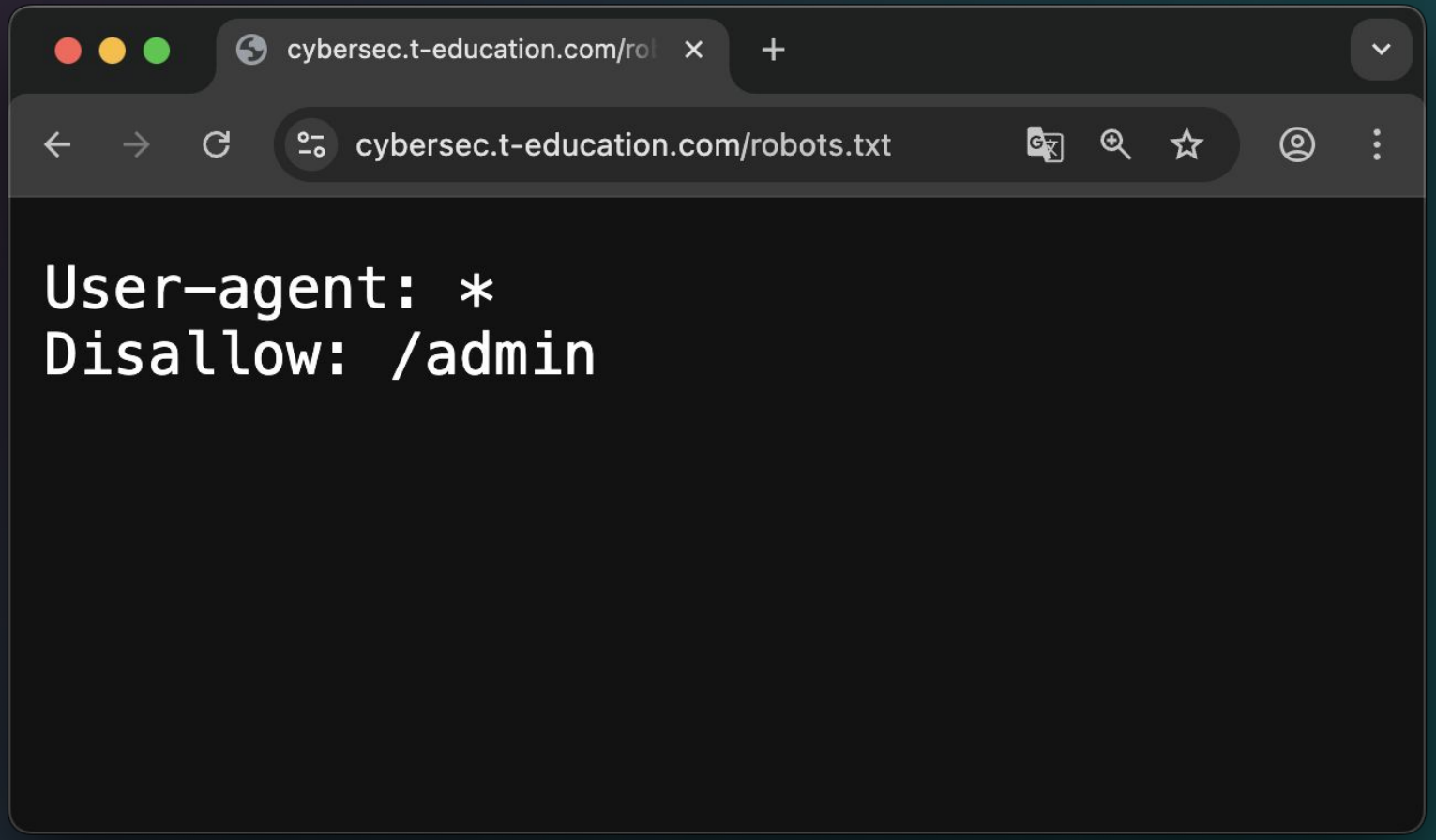
Отсутствие контроля доступа

Как искать?

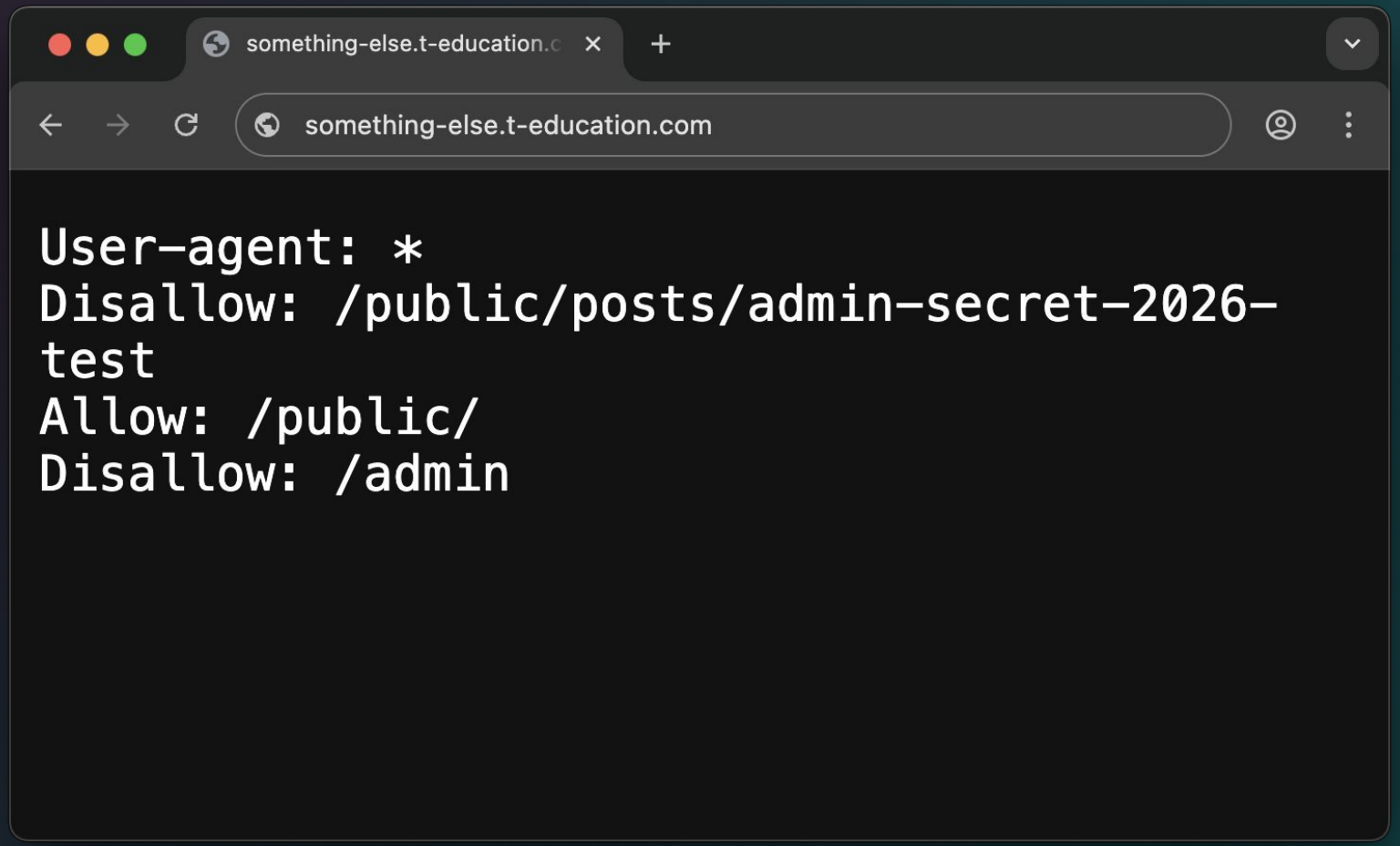
```
# Базовый перебор директорий и файлов с расширениями
dirsearch -u https://example.com -w wordlist.txt \
  -e php,asp,aspx,js,txt -t 50 --random-agent \
  -x 404,400 --exclude-size 0 --exclude-text "Not Found"

# Добавление заголовков/куки (если авторизация обязательна)
dirsearch -u https://example.com -w wordlist.txt \
  -H "Authorization: Bearer <token>" --cookie "SID=..." -t 50
```

```
# Перебор директорий (FUZZ заменяется словом из списка)
ffuf -u https://example.com/FUZZ/ -w wordlist.txt \
  -t 50 -mc 200,204,301,302,307,403 -fc 404 -fs 0

# Перебор файлов с расширениями
ffuf -u https://example.com/FUZZ -w wordlist.txt \
  -e .php,.txt,.zip,.bak -t 50 -mc 200,301,302 -fc 404
```

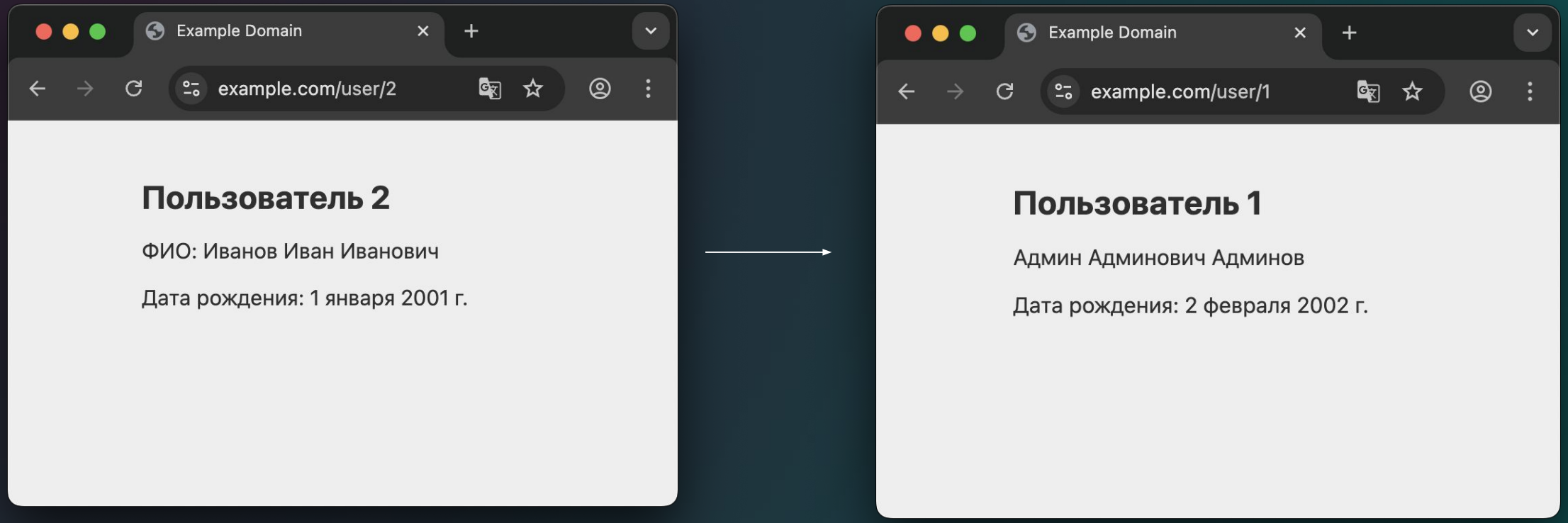
robots.txt


cybersec.t-education.com/rol
cybersec.t-education.com/robots.txt
User-agent: *
Disallow: /admin

robots.txt


something-else.t-education.c
something-else.t-education.com
User-agent: *
Disallow: /public/posts/admin-secret-2026-test
Allow: /public/
Disallow: /admin

IDOR – небезопасная прямая ссылка



Path Traversal

```python
def serve_file():
    filename = request.args.get('image_name')
    try:
        return send_file(filename)
    except Exception:
        abort(404)
```

```
GET /get_image?image_name=image.png HTTP/1.1
Host: example.com
...


HTTP/1.1 200 OK
Content-Type: image/png
Content-Length: 1234

<binary data...>
```

Path Traversal

```
GET /get_image?image_name=../../../etc/passwd
Host: example.com
...


HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 1234

nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
...
```

Path Traversal

```
GET /get_image?image_name=../../../etc/passwd HTTP/1.1
Host: example.com
...


HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 1234

nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
...
```

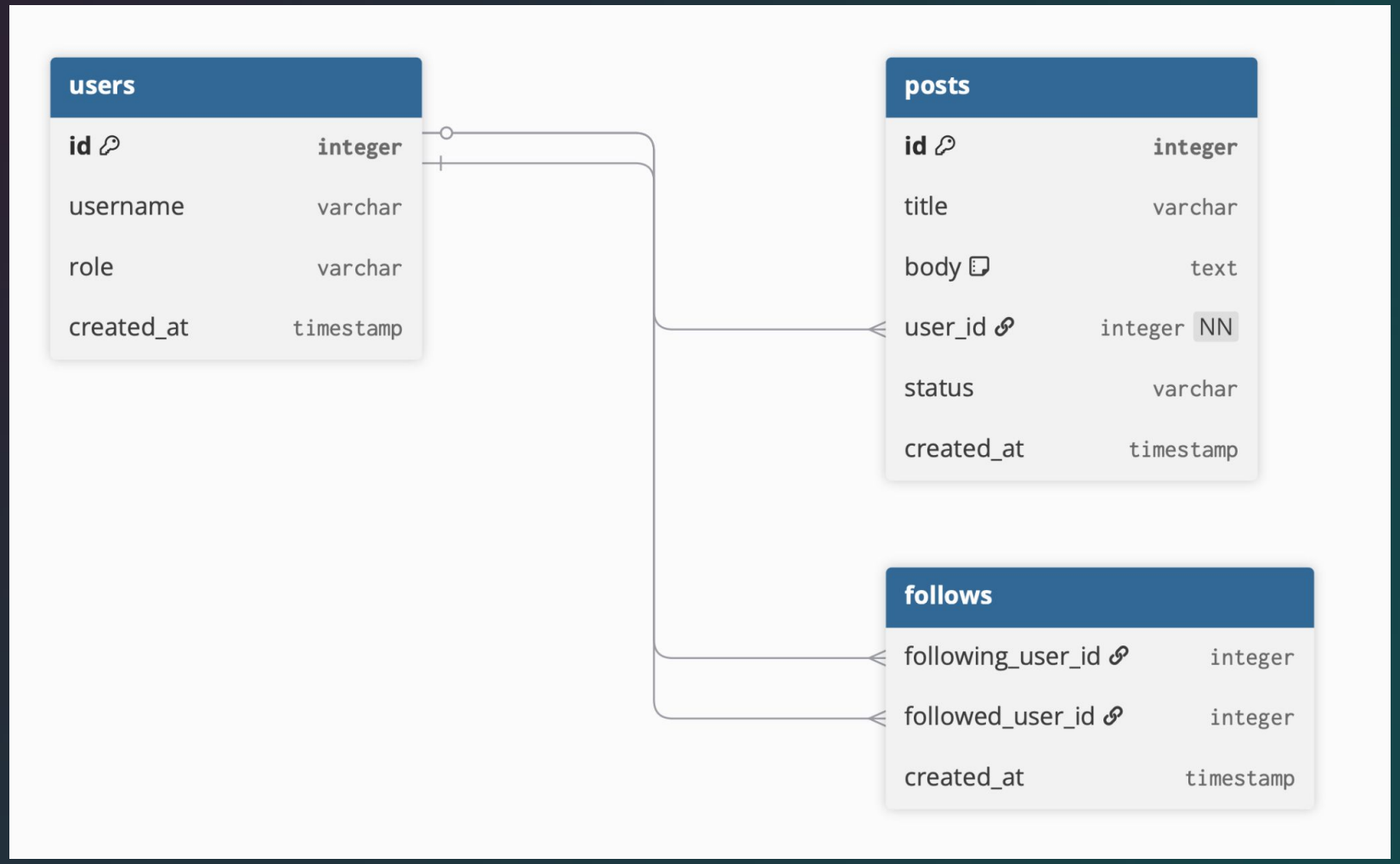
Path Traversal

```
GET /get_image?image_name=../../../proc/self/environ HTTP/1.1
Host: example.com
...


HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 1234

USER=daemon

...
```

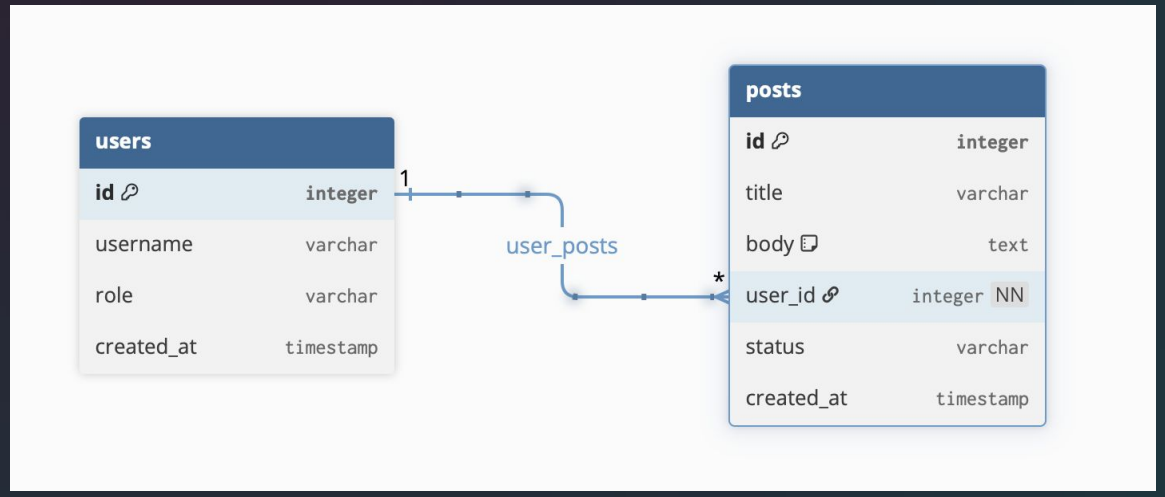
Path Traversal. Защищаемся

```
def serve_file():
    filename = request.args.get('image_name')
    try:
        return send_from_directory('static', filename)
    except Exception:
        abort(404)
```

Базы данных

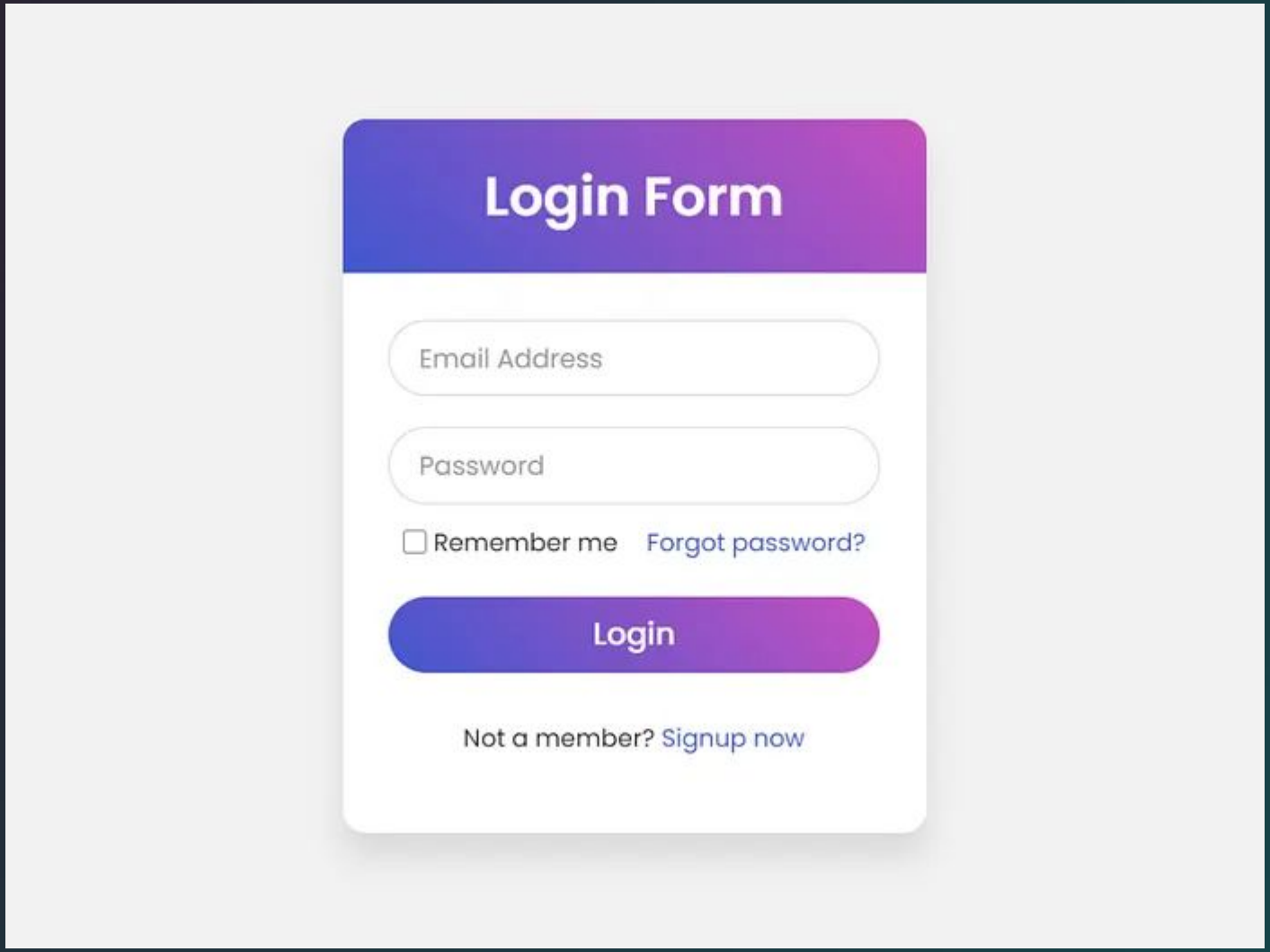

users
id integer
username varchar
role varchar
created_at timestamp
posts
id integer
title varchar
body text
user_id integer NN
status varchar
created_at timestamp
follows
following_user_id integer
followed_user_id integer
created_at timestamp

Базы данных. Язык SQL




```sql
SELECT * FROM users;

SELECT * FROM posts
    WHERE user_id = 1234;

SELECT * FROM posts
    WHERE status = 'published'
    OR user_id = 1234;
```

Базы данных. Уязвимый сайт



Базы данных. Уязвимый сайт

Python

```python
template = "SELECT * FROM users WHERE username='{}' and password_hash='{}'"
cursor = db.cursor()
cursor.execute(template.format(request.username, hash(request.password)))

if cursor.fetchone():
    return True, "Привет, " + request.username
else:
    return False, "Неверный логин или пароль!"
```

Базы данных. Уязвимый сайт

```
SELECT * FROM users
    WHERE username='{}'
    AND password_hash='{}'
```

```
{
    "username": "admin' OR -- ",
    "password": ""
}
```

```
SELECT * FROM users
    WHERE username='admin' OR
    -- AND password_hash='{}'
```

Базы данных. Уязвимый сайт

Python

```python
template = "SELECT * FROM users WHERE username='{}' and password_hash='{}'"
cursor = db.cursor()
cursor.execute(template.format(request.username, hash(request.password)))

if cursor.fetchone():
    return True, "Привет, " + request.username
else:
    return False, "Неверный логин или пароль!"
```

Базы данных. Запрос и параметры

Python

```python
template = "SELECT * FROM users WHERE username=%s and password_hash=%s"
db_connection.query(template, (request.username, request.password))

if db_connection.fetchone():
    return True, "Привет, " + request.username
else:
    return False, "Неверный логин или пароль!"
```

Базы данных. Опасные последствия

```
SELECT * FROM users
    WHERE username='admin';
DROP TABLE users
    -- AND password_hash='{}'
```

```
SELECT * FROM users
    WHERE username='admin';
UPDATE users SET role = 'admin'
    WHERE username='evil'
    -- AND password_hash='{}'
```

Основы защиты Web-приложений

И примеры атак