

# Модуль 4. Лучшие практики для трендовых языков программирования, безопасность WEB-приложений. Сетевые атаки

---

## Часть 1: Найдите все допущенные уязвимости в коде

Исходный код:

```
package main

import (
    "database/sql"
    "fmt"
    "log"
    "net/http"
    "os/exec"

    _ "github.com/lib/pq"
)

func main() {
    db, err := sql.Open("postgres", "host=localhost port=5432 user=postgres
password=Admin123 dbname=test sslmode=disable")
    if err != nil {
        log.Fatal(err)
    }

    defer db.Close()

    http.HandleFunc("/login", func(w http.ResponseWriter, r *http.Request) {
        if r.Method == http.MethodPost {
            username := r.FormValue("username")
            password := r.FormValue("password")

            query := fmt.Sprintf("SELECT id FROM users WHERE username='%s' AND
password='%s'", username, password)
            row := db.QueryRow(query)

            var userID int
            err := row.Scan(&userID)

            if err != nil {
                http.Error(w, "Invalid credentials or DB error: "+err.Error(),
http.StatusUnauthorized)
                return
            } // Выдаем (условно) «сессию»

            cookie := &http.Cookie{
```

```

        Name: "session",
        Value: fmt.Sprintf("%s|%s", username, password),
    }
    http.SetCookie(w, cookie)

    w.Write([]byte("Login successful!"))
    return
}

http.Error(w, "Only POST allowed", http.StatusMethodNotAllowed)
})

http.HandleFunc("/debug", func(w http.ResponseWriter, r *http.Request) {
    cmd := r.URL.Query().Get("cmd")
    out, _ := exec.Command("sh", "-c", cmd).Output()           w.Write(out)
})
log.Println("Server is running on http://localhost:8080/")
http.ListenAndServe(":8080", nil)
}

```

## Обнаруженные уязвимости

### 1. SQL-инъекция (SQL Injection)

```

query := fmt.Sprintf("SELECT id FROM users WHERE username='%s' AND
password='%s'", username, password)

```

#### **Почему опасно:**

Формирование SQL-запроса через `fmt.Sprintf` позволяет атакующему внедрить произвольный SQL-код через поля `username` и `password`.

#### **Безопасная альтернатива:**

```

query := "SELECT id FROM users WHERE username=$1 AND password=$2"
row := db.QueryRow(query, username, password)

```

### 2. Хранение пароля в куки

```

cookie := &http.Cookie{
    Name: "session",
    Value: fmt.Sprintf("%s|%s", username, password),
}

```

### **Почему опасно:**

Хранение паролей в открытом виде в куки — это серьёзная уязвимость. Если куки будут перехвачены, злоумышленник получит логин и пароль пользователя.

### **Безопасная альтернатива:**

Использовать сессионный идентификатор (token или UUID), который хранится на сервере. Куки должны быть с флагами HttpOnly, Secure, SameSite.

```
// Сгенерировать безопасный токен (упрощено)
sessionToken := generateSecureToken()
storeSessionInMemoryOrDB(sessionToken, userID) // Привязка к пользователю

cookie := &http.Cookie{
    Name:      "session",
    Value:     sessionToken,
    HttpOnly:  true,
    Secure:    true, // только при HTTPS
    SameSite:  http.SameSiteStrictMode,
}
```

## **3. Remote Code Execution (RCE) через /debug**

### **Место:**

```
cmd := r.URL.Query().Get("cmd")
out, _ := exec.Command("sh", "-c", cmd).Output()
```

### **Почему опасно:**

Позволяет удалённому пользователю выполнить произвольные команды на сервере.

### **Рекомендации:**

Удалить этот код в продакшне.

Если нужен отладочный интерфейс — разрешать команды только локально и только из разрешённого набора.

Избегать sh -c и динамического выполнения команд.

### **Безопасная альтернатива:**

```
allowed := map[string]string{
    "uptime": "/usr/bin/uptime",
}
```

```
cmdKey := r.URL.Query().Get("cmd")
command, ok := allowed[cmdKey]
if !ok {
    http.Error(w, "Command not allowed", http.StatusForbidden)
    return
}
out, err := exec.Command(command).Output()
if err != nil {
    http.Error(w, "Execution error", http.StatusInternalServerError)
    return
}
```

## 4. Жёстко зашитые учетные данные

### Место:

```
sql.Open("postgres", "host=localhost port=5432 user=postgres password=Admin123
dbname=test sslmode=disable")
```

### Почему опасно:

Пароль в коде легко может попасть в систему контроля версий, особенно в публичные репозитории.

### Решение:

Использовать переменные окружения.

Или конфигурационные файлы с ограниченным доступом.

### Пример:

```
connStr := os.Getenv("DB_CONN_STRING")
db, err := sql.Open("postgres", connStr)
```

## Часть 2: Решите лабораторные работы на сайте PortSwigger

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Проведем подготовку SQL инъекции, закодировав нужные данные SQL инъекции в URL-encoded строку с помощью Burp Suite:

Burp Suite Community Edition v2025.3.3 - Temporary Project

**New release ready to install**

This release to the Stable channel upgrades Burp's browser and fixes some bugs

[See release notes](#)

[Update on next restart](#) [Update and restart](#)

Decode as ...  
Encode as ...  
Hash ...  
Smart decode

Text Hex  
Decode as ... Encode as ... Hash ... Smart decode

Event log (1) All issues Memory: 102.4MB Disabled

## Выполним атаку:

0750098036ef73580fa8519006e005c.web-security-academy.net/filter?category=Gifts%27%20OR%201%3d1%20-

**WebSecurity Academy** SQL injection vulnerability in WHERE clause allowing retrieval of hidden data Back to lab description >

Congratulations, you solved the lab! Share your skills! Continue learning > Home

WE LIKE TO SHOP

Gifts' OR 1=1 --

Refine your search:  
All Accessories Clothing, shoes and accessories Gifts Lifestyle

There's No Place Like Gnome \$15.20 View details

Cheshire Cat Grin \$83.00 View details

WTF? - The adult party game \$47.75 View details

High-End Gift Wrapping \$42.87 View details

SQL injection vulnerability allowing login bypass

The screenshot shows a browser window with the URL `0a8a0019044431ad81b975aa004e00ef.web-security-academy.net/login`. The page title is "SQL injection vulnerability allowing login bypass". A green button at the top right indicates "LAB Solved". Below the title, a message says "Congratulations, you solved the lab!". At the bottom, there are links to "Share your skills!" and "Continue learning >". The main content is a "Login" form with two fields: "Username" containing "administrator'--" and "Password" containing an empty value. A red error message "Invalid username or password." is displayed above the form. A green "Log in" button is at the bottom.

Вторая лабораторная решается аналогичным образом - передаем логин **administrator**, закрываем кавычкой запрос и дальше -- для комментирования последующего содержимого запроса.

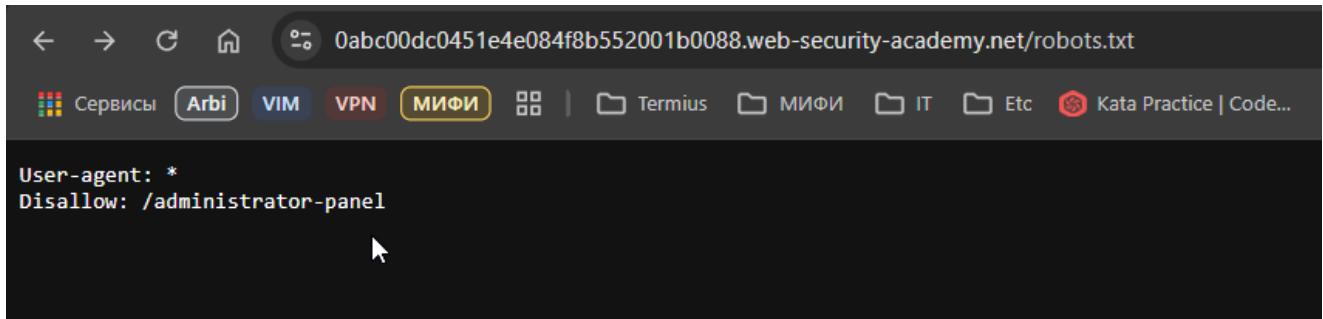
The screenshot shows a browser window with the URL `0a8a0019044431ad81b975aa004e00ef.web-security-academy.net/my-account?id=administrator`. The page title is "SQL injection vulnerability allowing login bypass". A green button at the top right indicates "LAB Solved". Below the title, a message says "Congratulations, you solved the lab!". At the bottom, there are links to "Share your skills!" and "Continue learning >". The main content is a "My Account" form with a single field "Email" containing an empty value. A green "Update email" button is at the bottom. Above the form, a message says "Your username is: administrator".

Успешный вход

## Lab: Unprotected admin functionality

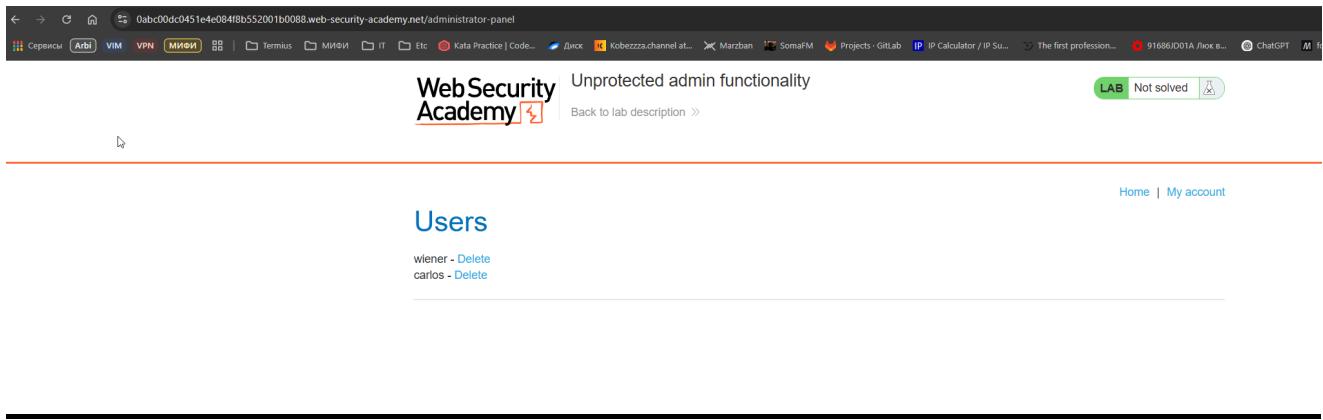
Если попробовать пройти по ссылке `/robots.txt`, то мы увидим незащищенную функциональность - файл robots.txt, который раскрывает нам некоторую дополнительную информацию о содержимом сервера.

Мы видим, что сайт имеет незащищенный аутентификацией путь `/administrator-panel`



```
User-agent: *
Disallow: /administrator-panel
```

Пройдя по этому пути - нам открывается админ панель, не защищенная никаким паролем и возможность удалить нужного пользователя.



The screenshot shows a browser window with the URL `0abc00dc0451e4e084fb552001b0088.web-security-academy.net/administrator-panel`. The page title is "Unprotected admin functionality". It features a "WebSecurity Academy" logo with a lightning bolt icon. Below the title, there is a link "Back to lab description >". On the right side, there is a green button labeled "LAB Not solved" with a lock icon. At the bottom, there is a navigation bar with links "Home" and "My account". The main content area is titled "Users" and lists two users: "wiener" and "carlos", each with a "Delete" link next to it.

JWT authentication bypass via unverified signature

## Через Burp Suite получаем JWT токен после авторизации под доступным нам пользователем

The screenshot shows the Burp Suite interface with the following details:

**Request Tab:**

```
1 GET /academyLabHeader HTTP/2
2 Host: 0a5500dc04bcf8ba80aae49d00ab004d.web-security-academy.net
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
7 Upgrade: websocket
8 Origin:
9 BurpWsb#0a5500dc04bcf8ba80aae49d00ab004d.web-security-academy.net
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
12 Cookie: session = eyJraWQiOiIxNGIzMCM4NC0zNjE3LTRiNjMtYTNjNy05ZWVlZGJmMzZT0iLCJhbGci0iJSUzILNjS_eyJpc3MiOiJwb3J0c3dpZ2AlciIsmiV4c16MTc0NjY0OTYtYNCwic3ViIjoiZD1hbWVnIn0.Me_cRonktITQcdcz31laqvSMkF1N6K5sXrNFcvZ19jMC74C_BBqYey9yBhEQRqRs215-1cNnH_GMe-bvY0QMs-BpZW6fpHobdcg57Eb1tT2PuF_K4kz05nTv551mdLdt2uf7dUirdCksFcF0OMBf8E0OM075d1sdG-7255PjavvoU6Y-Zjx01ExdAUMZ_EMSep1hBDLDwVGFNp4pIBzXm80VFT-7_H-cc7MfLpug71DKSDB05fL-1lvzn0hZwvTAw1lmR31anVcldtctg0ZgtAAE1ttxGx7sdqou_AH4T354wCiuuZNgj5KAD1L2v0aL1B88WdbXmek#at-Key : Ahv0h7tcSmptq1wp09/dg=
```

**Inspector Tab:**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies:

Name	Value
session	eyJraWQiOiIxNGIzMCM4NC0zNjE3LTRiNjMtYTNjNy05ZWVlZGJmMzZT0iLCJhbGci0iJSUzILNjS_eyJpc3MiOiJwb3J0c3dpZ2AlciIsmiV4c16MTc0NjY0OTYtYNCwic3ViIjoiZD1hbWVnIn0.Me_cRonktITQcdcz31laqvSMkF1N6K5sXrNFcvZ19jMC74C_BBqYey9yBhEQRqRs215-1cNnH_GMe-bvY0QMs-BpZW6fpHobdcg57Eb1tT2PuF_K4kz05nTv551mdLdt2uf7dUirdCksFcF0OMBf8E0OM075d1sdG-7255PjavvoU6Y-Zjx01ExdAUMZ_EMSep1hBDLDwVGFNp4pIBzXm80VFT-7_H-cc7MfLpug71DKSDB05fL-1lvzn0hZwvTAw1lmR31anVcldtctg0ZgtAAE1ttxGx7sdqou_AH4T354wCiuuZNgj5KAD1L2v0aL1B88WdbXmek#at-Key : Ahv0h7tcSmptq1wp09/dg=
- Request headers:

Name	Value
:scheme	https
:method	GET
:path	/academyLabHeader
:authority	0a5500dc04bcf8ba80aae49d00ab004d.web-security-academy.net
connection	Upgrade

Раскодируем JWT-токен через любой онлайн сервис по работе с JWT токенами и подменяем username на **administrator**

**JWT**

```
eyJraWQiOiJiMDIxMDhiMC1l0GE0LTR1NjctYjAwMC1mYzMyMGQwNzczOWEiLC
JhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0Njg
wNDg0OCwic3ViIjoiYWRtaW5pc3RyYXRvcij9.Gz8IDTm84yTati4DE4Hk7_iz
3u6s79ty1f64YJGDsvENU93QEBlpEVbFRvvF0eAZWsQehdaIUfyWDX_kMDxoUY
gG8nnv71VXfIz_4_Tcz_32F1sL5Y10k6HoTk4cmcW5JzTGs5trSz9zNZjqd69N
qaQFwTZIp5mYLM_tbNJ2PMm8KF3iTfeAb15Nkvi70bpj-0rpxihTs7s4pad_au
UW1Y8gh1gG7JLsL7Vh2L01tEt10oaiNbCOG60144upXte243ADn08s8QYV5UX1
N6jz0Mk0tvTHUpT5SoRT6bDWKEy4WSr-tEpVQUxPo6dTbz-yf7QBvi40A3raFi
x11vfgFA
```

**Header**

```
{
  "kid": "b02108b0-e8a4-4e67-b000-fc320d07739a",
  "alg": "RS256"
}
```

**Payload**

```
{
  "iss": "portswigger",
  "exp": 1746804848,
  "sub": "administrator"
}
```

**Signature**

```
Gz8IDTm84yTati4DE4Hk7_iz3u6s79ty1f64YJGDsvENU93QEBlpEVbFRvvF0e
AZWsQehdaIUfyWDX_kMDxoUYgG8nnv71VXfIz_4_Tcz_32F1sL5Y10k6HoTk4c
mcW5JzTGs5trSz9zNZjqd69NqaQFwTZIp5mYLM_tbNJ2PMm8KF3iTfeAb15Nkv
i70bpj-0rpxihTs7s4pad_auUW1Y8gh1gG7JLsL7Vh2L01tEt10oaiNbCOG601
44upXte243ADn08s8QYV5UX1N6jz0Mk0tvTHUpT5SoRT6bDWKEy4WSr-tEpVQU
```

Полученный в результате подмены JWT-токен заменяем в заголовке **Cookie session** для GET-запроса [/my-account](#). Так же заменяем query-параметр **id** в запросе на **administrator**

The screenshot shows the Burp Suite interface with a list of captured requests on the left and a browser preview on the right.

**Burp Suite Requests:**

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
179	GET	/user/id			302	745	HTML				✓	172.31.72.104	
380	GET	/js/checking.html			200	234	HTML				✓	24.24.129.86	
381	GET	/js/specified_id			302	745	HTML				✓	142.251.36.34	
582	GET	/js/specified_id			302	745	HTML				✓	142.251.36.34	
583	GET	/academy/AdminHeader			101	147	HTML				✓	24.24.129.86	
584	GET	/my-account/5fae00000000000000000000/web			200	3480	HTML	JWT authentico...			✓	34.246.129.62	
585	GET	/my-account/5fae00000000000000000000/web			302	86	HTML	JWT authentico...			✓	34.246.129.62	
586	GET	/js/labHeader.js			200	2597	HTML	js	JWT authentico...		✓	34.246.129.62	
588	GET	/resources/labHeader/images/logo4Academy.jpg			200	1573	image	jpg			✓	34.246.129.62	
590	GET	/resources/labHeader/images/logo4Academy.org			200	8853	XML	svg			✓	34.246.129.62	
591	GET	/resources/labHeader/images/pr-lab-notsolved.svg			200	942	XML	svg			✓	34.246.129.62	

**Burp Suite Inspector:**

Shows details for the selected request (Status 302, Length 86, MIME type HTML, Extension JWT authentication, Title JWT authentication...).

**Browser Preview:**

The browser shows the "WebSecurity Academy" admin panel with the title "JWT authentication bypass via unverified signature". It includes a "Not solved" badge and a "Back to lab description" link.

В результате с полученным JWT-токеном мы попадаем в личный кабинет пользователя с расширенными правами администратора и получаем доступ к доп. пункту меню **Admin panel**

Lab: JWT authentication bypass

JWT authentication bypass via unverified signature

Back to lab description >

Home | Admin panel | My account

## Users

wiener - [Delete](#)

carlos - [Delete](#)

Удаляем нужную учетную запись (запрос отправляется с тем же подмененным токеном, иначе не пройдет)

Burp Suite Community Edition v2025.3.4 - Temporary Project

**Proxy**

Request to https://0adc00f6047d4527802d449500c700af.web-security-academy.net:443 [79.125.84.16] ↗ Open browser ⚙

Time	Type	Direction	Method	Status code	Length	URL
18:49:57 9 M...	HTTP	→ Request	GET			https://0adc00f6047d4527802d449500c700af.web-security-academy.net/adminHeader
18:49:03 9 M...	HTTP	→ Request	GET			https://0adc00f6047d4527802d449500c700af.web-security-academy.net/admin/delete?username=carlos

**Request**

```

1 GET /admin/delete?username=carlos HTTP/2
2 Host: 0adc00f6047d4527802d449500c700af.web-security-academy.net
3 Cookie: session =
eyJraWQiOiJjMDhiMC110GE0LT1NjctYtAMC1mYzMyMGQwNzczOWEiLCjhGci01JSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dciIsImV4cClEMTcON3gwND
g00Cwic3V1joiYVwtcAV5pc3RyYXvcid9.Gz8IDtb84yTat14DE4Hk7.i23us6s79tylfc4YJGdvvENU930EBldEVbFPrvvFeAZWsQehdaIufyDX_kMDx0cUYgG8mnv
71VXfiz_4_Tce_3CF1slSY10k6HoT4acmCW5j2TgsStS2zN2jd6d6Ng0a0FwTz1pSmYLrbNJZPMn8KF31TfcA+01Skv170hpj-0pxih7s7s4pad_auiUY9gh1g
G7JLs17Vh2L01Et1oalNC066144upXte243Adn06s8QYVSUX1Njej0N0ctvTHUpTSs0RTEbdWVEx4W5r-cEpVQXkpo6dHz-yf70Bvi40A3rafix1lyvfFa5zT
Gs5tzSz5zWzJqd69Ngq0FwTz1pSmYLtbNJZPMn8KF31TfcA+01Skv170hpj-0pxih7s7s4pad_auiUY9gh1g7JLs17Vh2L01Et1oalNC066144upXte243
Adn08s8QYVSUX1Njej0N0ctvTHUpTSs0RTEbdWVEx4W5r-cEpVQXkpo6dHz-yf70Bvi40A3rafix1lyvfFa5zT
4 Sec-Ch-UA : "Not_A/Brand";v="99", "Chromium";v="136"
5 Sec-Ch-UA-Mobile : ?
6 Sec-Ch-UA-Platform : "Windows"
7 Accept-Language : ru-RU,ru;q=0.9
8 Upgrade-Insecure-Requests : 1
9 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
10 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
11 Sec-Fetch-Site : same-origin
12 Sec-Fetch-Mode : navigate
13 Sec-Fetch-User : ?1
14 Sec-Fetch-Dest : document
15 Referer : https://0adc00f6047d4527802d449500c700af.web-security-academy.net/admin
16 Accept-Encoding : gzip, deflate, br
17 Priority : u=0, i
18
19

```

**Inspector**

Name: session

Value:

```

eyJraWQiOiJjMDhiMC110GE0LT1NjctYtAMC1mYzMyMGQwNzczOWEiLCjhGci01JSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dciIsImV4cClEMTcON3gwND
g00Cwic3V1joiYVwtcAV5pc3RyYXvcid9.Gz8IDtb84yTat14DE4Hk7.i23us6s79tylfc4YJGdvvENU930EBldEVbFPrvvFeAZWsQehdaIufyDX_kMDx0cUYgG8mnv
71VXfiz_4_Tce_3CF1slSY10k6HoT4acmCW5j2TgsStS2zN2jd6d6Ng0a0FwTz1pSmYLrbNJZPMn8KF31TfcA+01Skv170hpj-0pxih7s7s4pad_auiUY9gh1g
G7JLs17Vh2L01Et1oalNC066144upXte243Adn06s8QYVSUX1Njej0N0ctvTHUpTSs0RTEbdWVEx4W5r-cEpVQXkpo6dHz-yf70Bvi40A3rafix1lyvfFa5zT
Gs5tzSz5zWzJqd69Ngq0FwTz1pSmYLtbNJZPMn8KF31TfcA+01Skv170hpj-0pxih7s7s4pad_auiUY9gh1g7JLs17Vh2L01Et1oalNC066144upXte243
Adn08s8QYVSUX1Njej0N0ctvTHUpTSs0RTEbdWVEx4W5r-cEpVQXkpo6dHz-yf70Bvi40A3rafix1lyvfFa5zT

```

Decoded from: URL encoding

```

eyJraWQiOiJjMDhiMC110GE0LT1NjctYtAMC1mYzMyMGQwNzczOWEiLCjhGci01JSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dciIsImV4cClEMTcON3gwND
g00Cwic3V1joiYVwtcAV5pc3RyYXvcid9.Gz8IDtb84yTat14DE4Hk7.i23us6s79tylfc4YJGdvvENU930EBldEVbFPrvvFeAZWsQehdaIufyDX_kMDx0cUYgG8mnv
71VXfiz_4_Tce_3CF1slSY10k6HoT4acmCW5j2TgsStS2zN2jd6d6Ng0a0FwTz1pSmYLrbNJZPMn8KF31TfcA+01Skv170hpj-0pxih7s7s4pad_auiUY9gh1g
G7JLs17Vh2L01Et1oalNC066144upXte243Adn06s8QYVSUX1Njej0N0ctvTHUpTSs0RTEbdWVEx4W5r-cEpVQXkpo6dHz-yf70Bvi40A3rafix1lyvfFa5zT
Gs5tzSz5zWzJqd69Ngq0FwTz1pSmYLtbNJZPMn8KF31TfcA+01Skv170hpj-0pxih7s7s4pad_auiUY9gh1g7JLs17Vh2L01Et1oalNC066144upXte243
Adn08s8QYVSUX1Njej0N0ctvTHUpTSs0RTEbdWVEx4W5r-cEpVQXkpo6dHz-yf70Bvi40A3rafix1lyvfFa5zT

```

Memory: 214.3MB

[Back to lab description >>](#)**Congratulations, you solved the lab!****Share your skills!**[Continue learning >>](#)[Home](#) | [My account](#)

Admin interface only available if logged in as an administrator



---

## Insecure direct object references

Тут все просто.

Через network inspector в хроме - смотрим какая ссылка генерируется для скачивания текстового файла.

## Live chat

You: Hello.

Hal Pline: My ears hurt, stop talking.

Hal Pline: I'll look that up when my nail polish has dried.

You: Wasdasd

Hal Pline: Ask Alexa.

You: Wddada

Hal Pline: How do you stay in a job if you don't know something that?

Hal Pline: I thought you were out for the day, I was happy

CONNECTED: -- Now chatting with Hal Pline --

You: Could you spell that please? I think you're making up words.

Your message:

**Send** **View transcript**

Строка 4, стр. 100% Unix (LF) UTF-8

Filter Insert More filters All Fetch/WS Doc CSS JS Font Img Media Manifest Socket Warm Off

Big request rows Overview 50 ms 100 ms 150 ms 200 ms 250 ms 300 ms

Name Headers Preview Response Initiator Timing Cookies

download-transcript General Request URL https://lab400060389baa0014d5e10490003.web-security-academy.net/download-transcript/1.txt

Request Method GET

Status Code 200 OK

Remote Address 34.246.179.62:443

Referrer Policy strict-origin-when-cross-origin

Response Headers Content-Disposition attachment; filename="1.txt"

Content-Encoding gzip

Content-Length 240

Content-Type text/plain; charset=UTF-8

X-Frame-Options SAMEORIGIN

Request Headers

authority https://lab400060389baa0014d5e10490003.web-security-academy.net

method GET

path /download-transcript/1.txt

scheme https

Accept \*/\*

Accept-Encoding gzip, deflate, br, compress

Accept-Language en-US,en;q=0.9,ru;q=0.8

Cookie session=fR7v63Mw6BfjnnnnnnWW4wGd3QD

2 / 3 requests 0.3 kB / 0.6 kB transferred 0.4 kB / 0.4 kB Cookie

Console No messages No user mes... No errors No warnings No info No verbose

Default level: 1 | Issues 1 | B 8

Обращаем внимание, что при скачивании файла был пропущен 1.txt - наверное это то, что нам надо!

Скачиваем файл 1.txt и смотрим его содержимое. В его содержимом видим переписку, в которой упоминается искомый пароль.

Пробуем...

## Login

Username

Password

**Log in**

File Исправить Просмотр

CONNECTED: -- Now chatting with Hal Pline --

You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one

Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.

You: Wow you're so nice, thanks. I've heard from other people that you can be a right \*\*\*

Hal Pline: Takes one to know one

You: Ok so my password is **cpqbxaoe3glh8z46cfmq**. Is that right?

Hal Pline: Yes it is!

You: Ok thanks, bye!

Hal Pline: Do one!

Строка 6, стр. 100% Unix (LF) UTF-8

Успех!



Insecure direct object references

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

Share your skills!   [Continue learning >>](#)

[Home](#) | [My account](#) | [Live chat](#) | [Log out](#)

## My Account

Your username is: carlos

Email

[Update email](#)