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		

VIETNAMESE SECURITY NETWORK JSC

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

Table of content

VIETNAMESE SECURITY NETWORK JSC

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

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).

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

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

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

- 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=5ZlEqFyVD4XMnxJsSFZf2Yra1k3m44o1E59v
		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**

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

		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**
2	**DHFI-2022-40001**	**Vulnerability name**	**Denial of Service (CWE-400)**
		Module	POST /api/auth/send-code
		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 Vector String	**7.5 - 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 Vector String	**5.3 - 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 Vector String	**5.3 - 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 Vector String	**6.7 - 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: https://pay.dhfi.online/api/auth/reAuth?token={{token}}
		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

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

		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 Vector String	**6.5 - 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 Vector String	**5.3 - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N**
		Severity	**Medium**
		Recommendation	Proper configuration of cross-origin requests Only allow trusted sites Avoid whitelisting null Avoid wildcards in internal networks CORS is not a substitute for server-side security policies Refer: https://www.comparitech.com/blog/information-security/cors-attacks-prevent/#How_to_prevent_CORS-based_attacks https://portswigger.net/web-security/cors
		Status	**Resolved**
9	**DHFI-2022-2001**	**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

			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-pay-back/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 -**

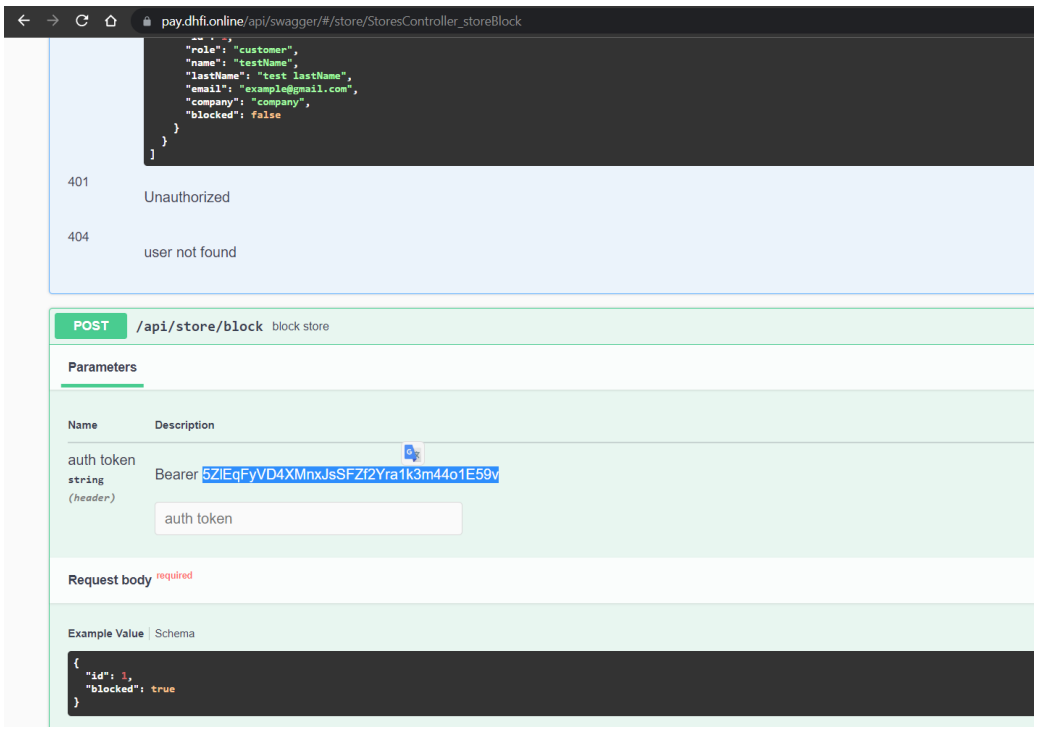
HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

		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 Vector String	**3.7 - 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**

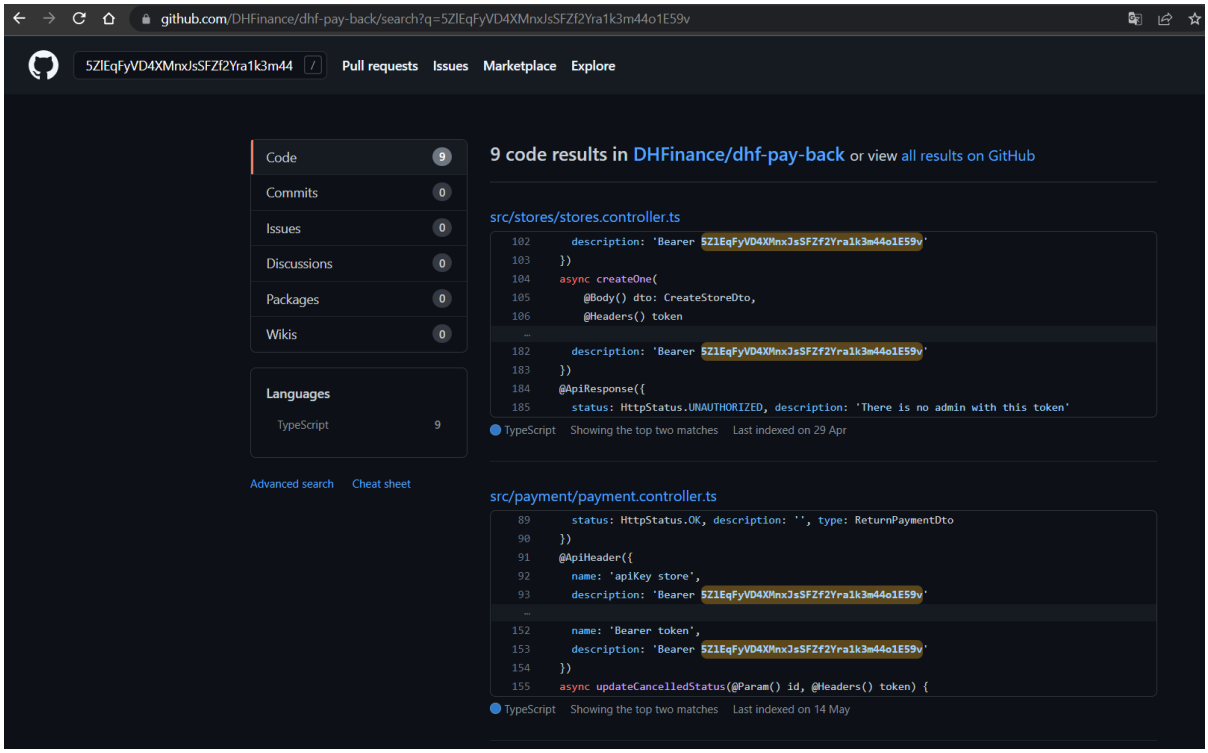
7. Proof of Concept

7.1 DHFI-2022-52201

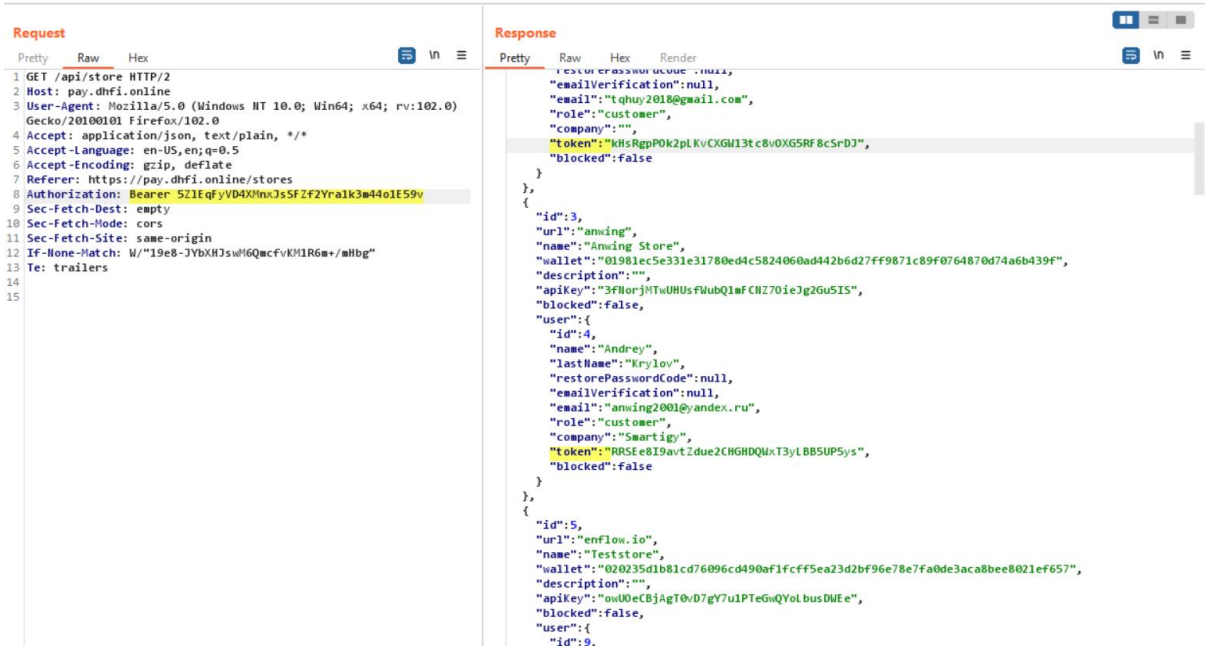
Swagger



Github



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



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

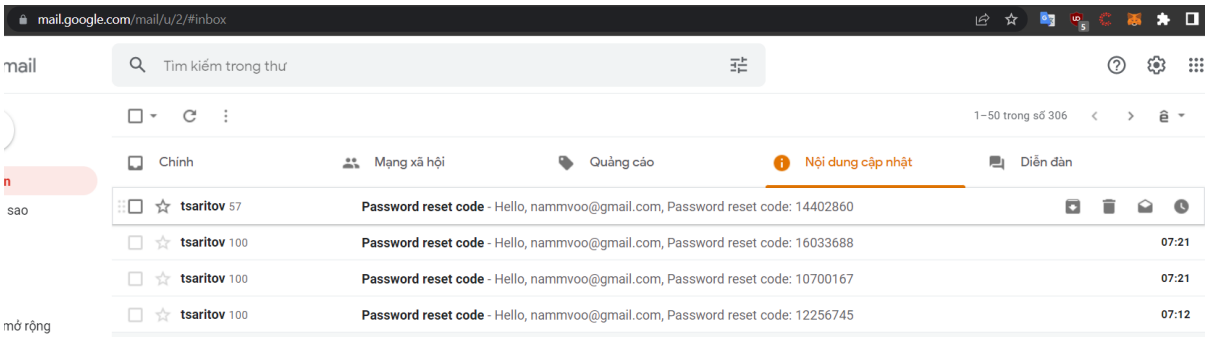
An attacker can access the password reset code in the email by reading in the application's database

Retest:

Admin tokens have been removed from public sources

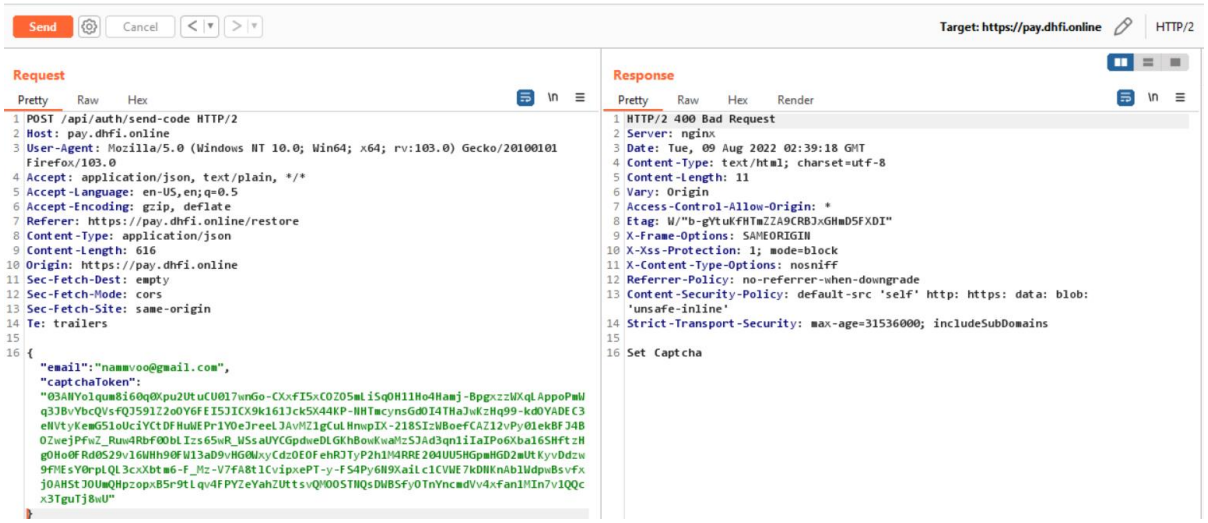
7.2 DHFI-2022-40001

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

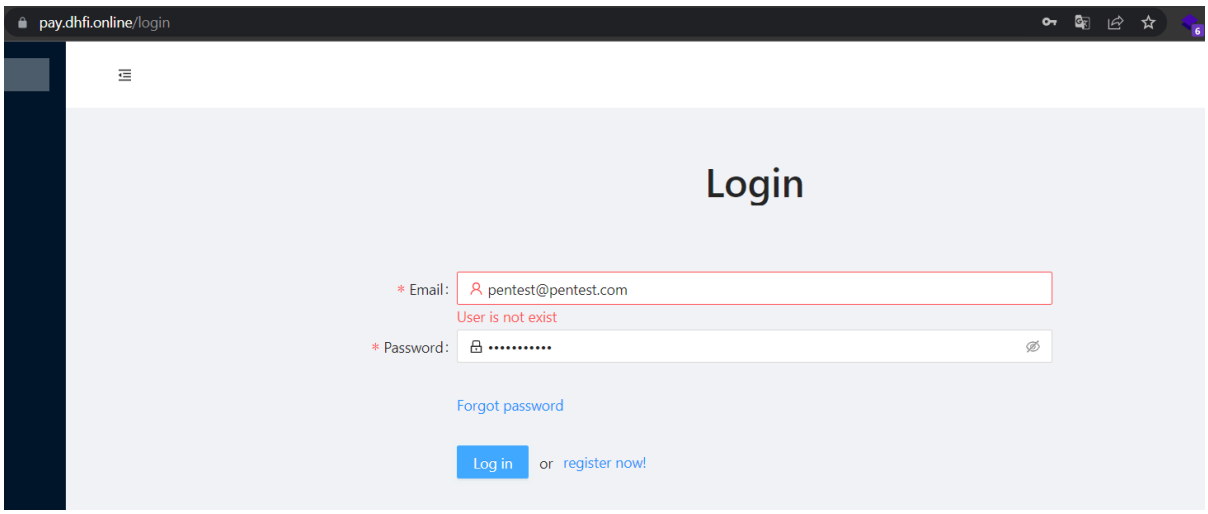


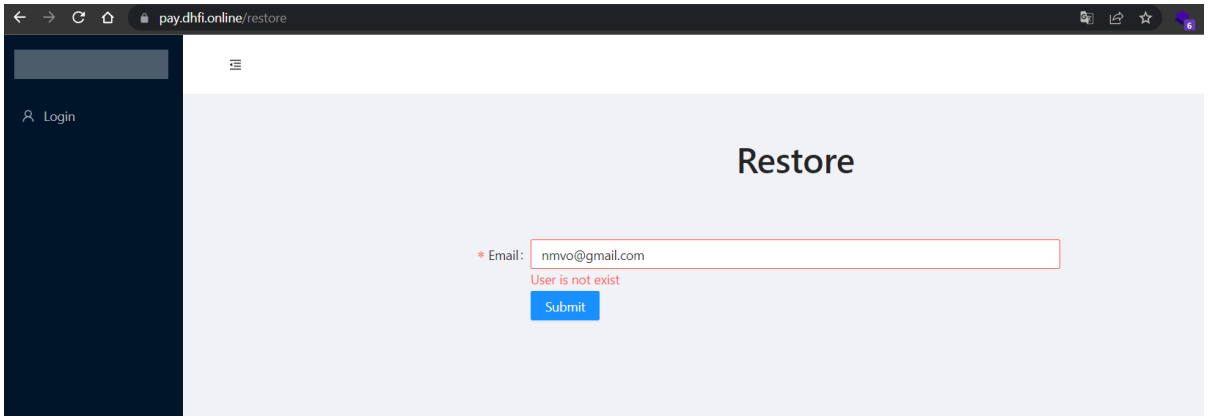
Retest:

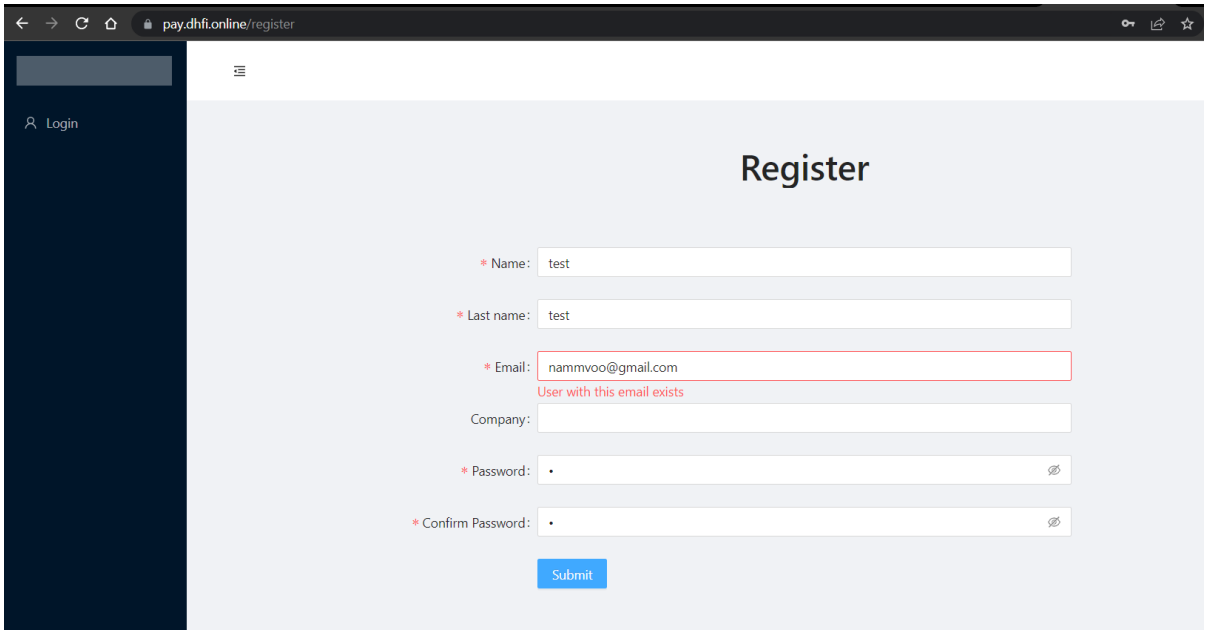
ReCaptcha has been implemented



7.3 DHFI-2022-20901

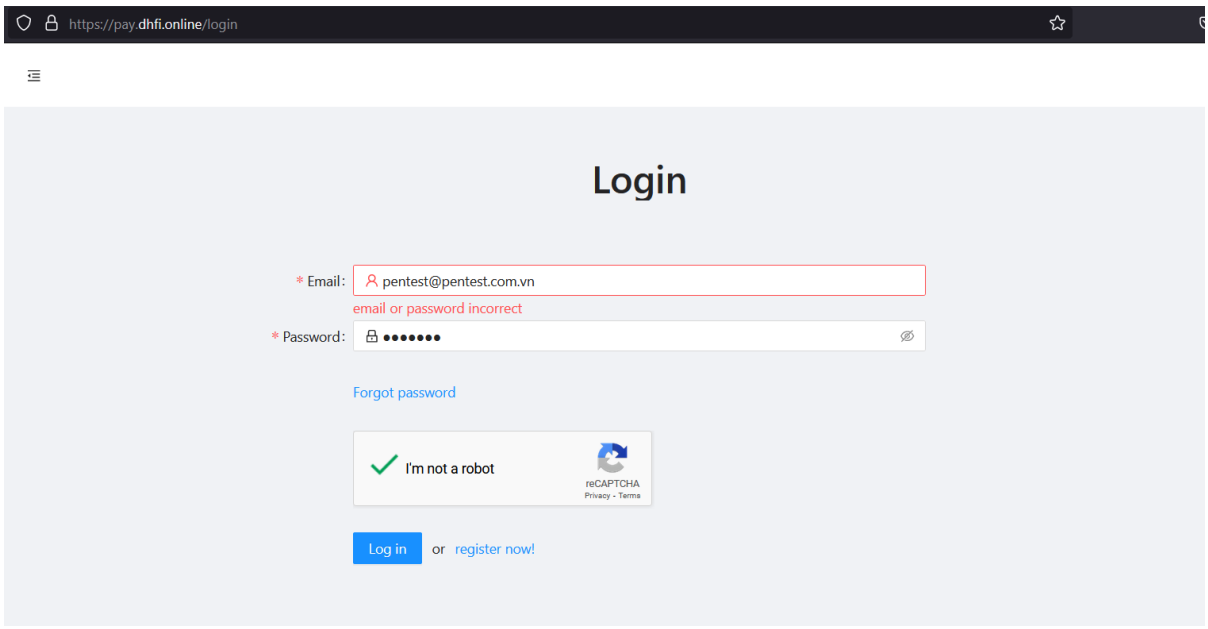

pay.dhfi.online/login
Login
* Email: pentest@pentest.com
User is not exist
* Password:
Forgot password
Log in
or register now!


pay.dhfi.online/restore
Login
Restore
* Email: nmvo@gmail.com
User is not exist
Submit


pay.dhfi.online/register
Login
Register
* Name: test
* Last name: test
* Email: nammvoo@gmail.com
User with this email exists
Company:
* Password:
* Confirm Password:
Submit

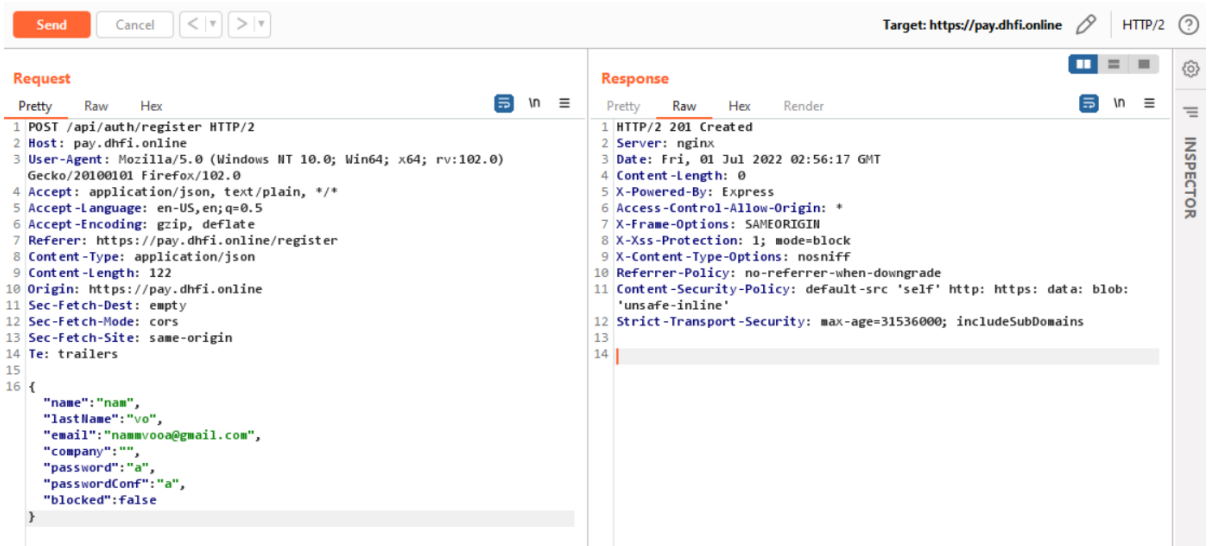
Retest:

Error description has been replaced

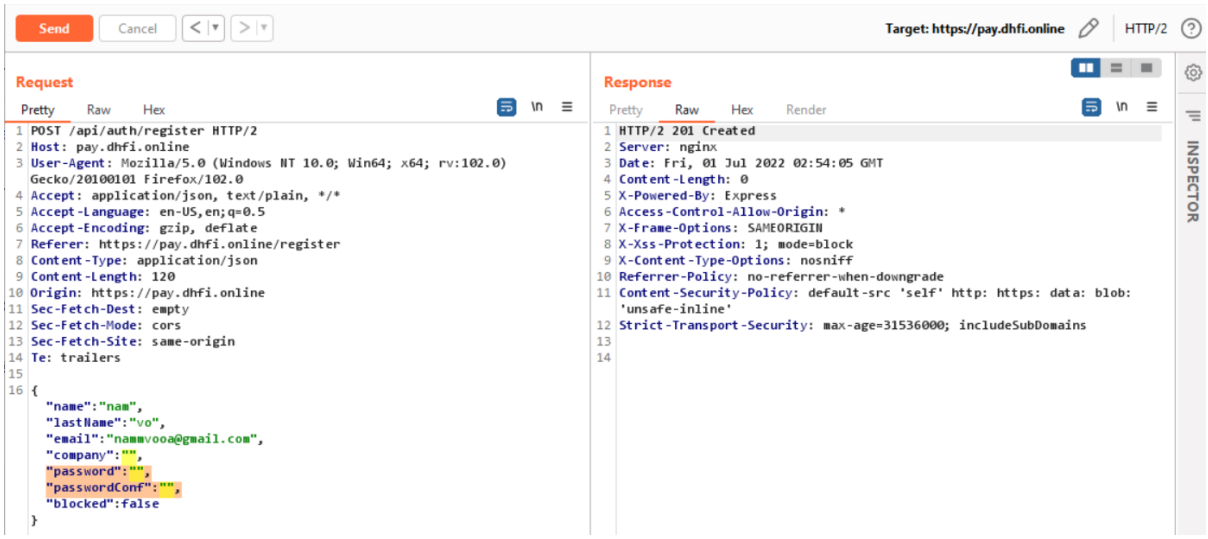


7.4 DHFI-2022-52101

Set password with 1 character

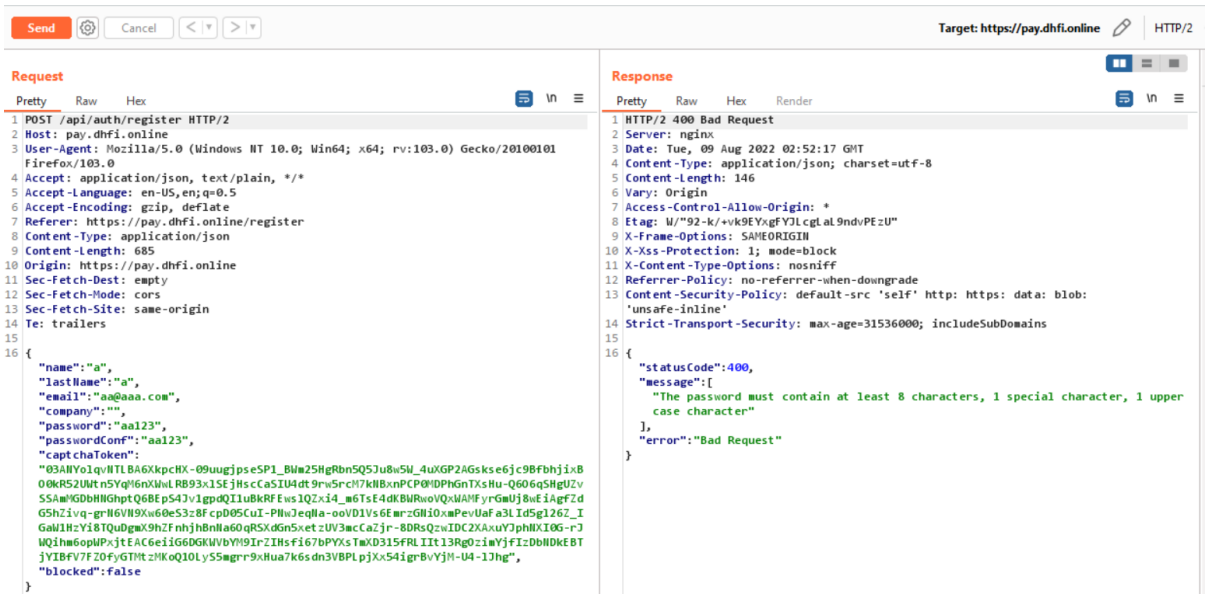


Even if the password is blank, the app still accepts it



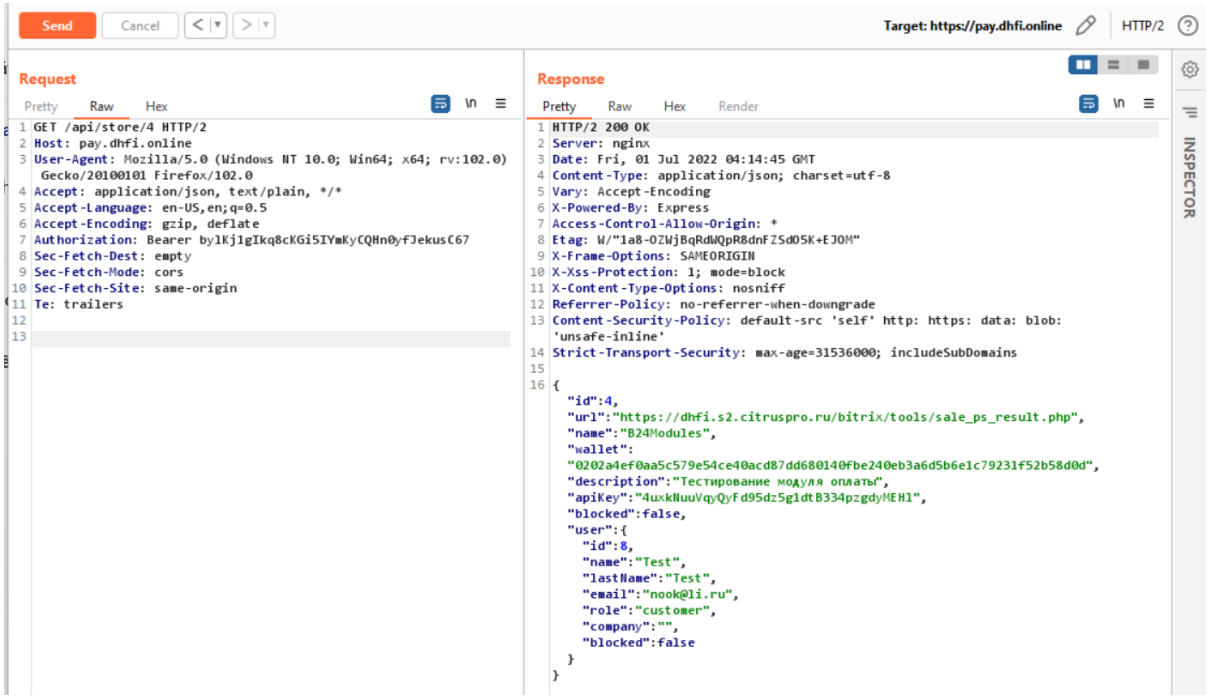
Retest:

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



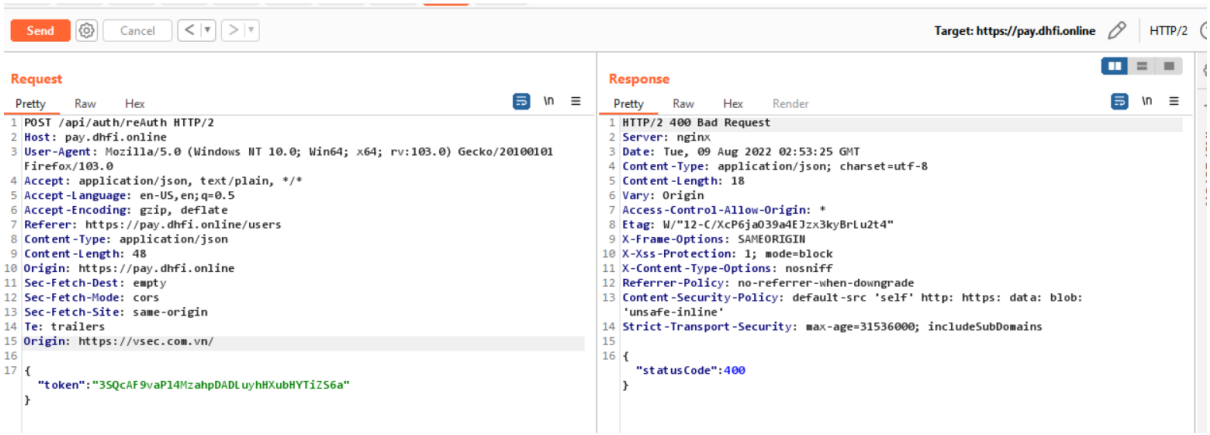
7.5 DHFI-2022-61301

Tokens can still be used after the user logs out

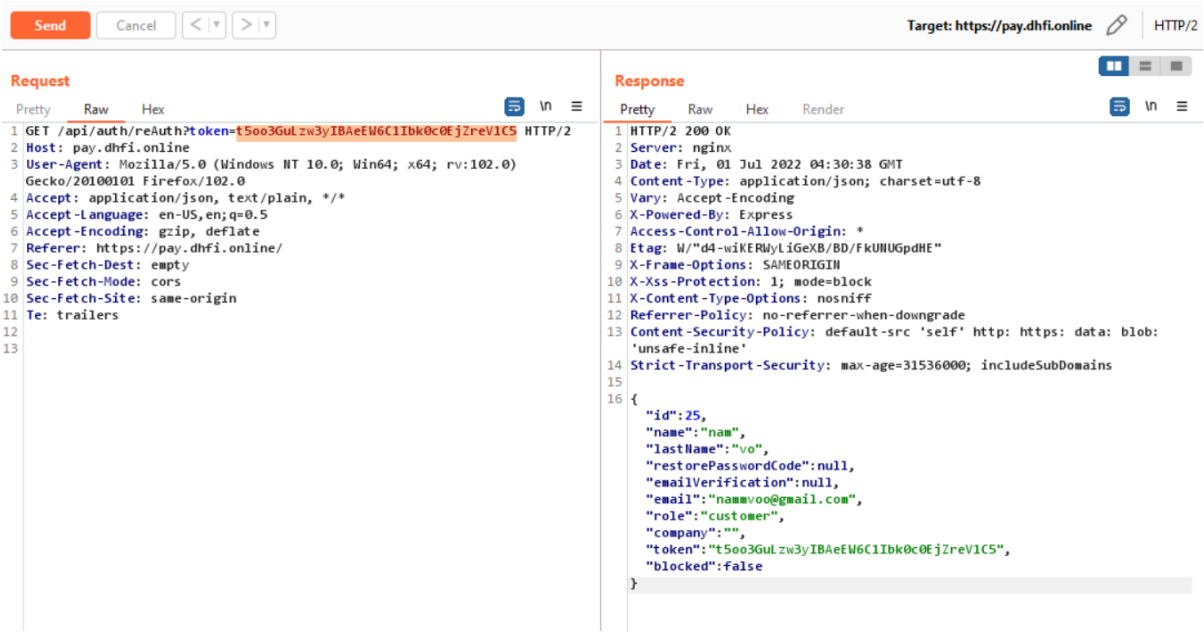


Retest:

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

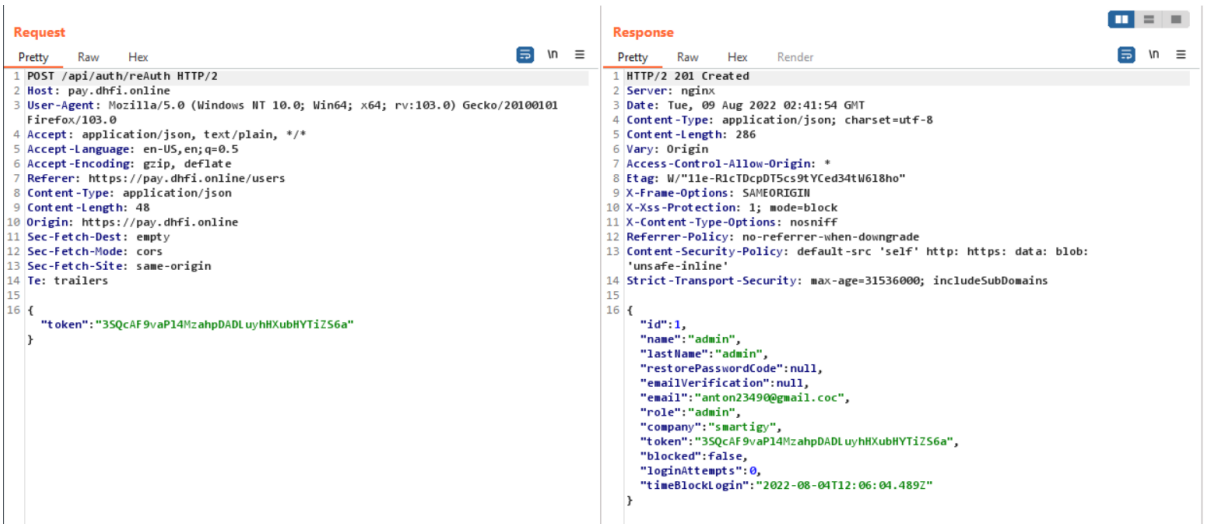


7.6 DHFI-2022-59801



Retest:

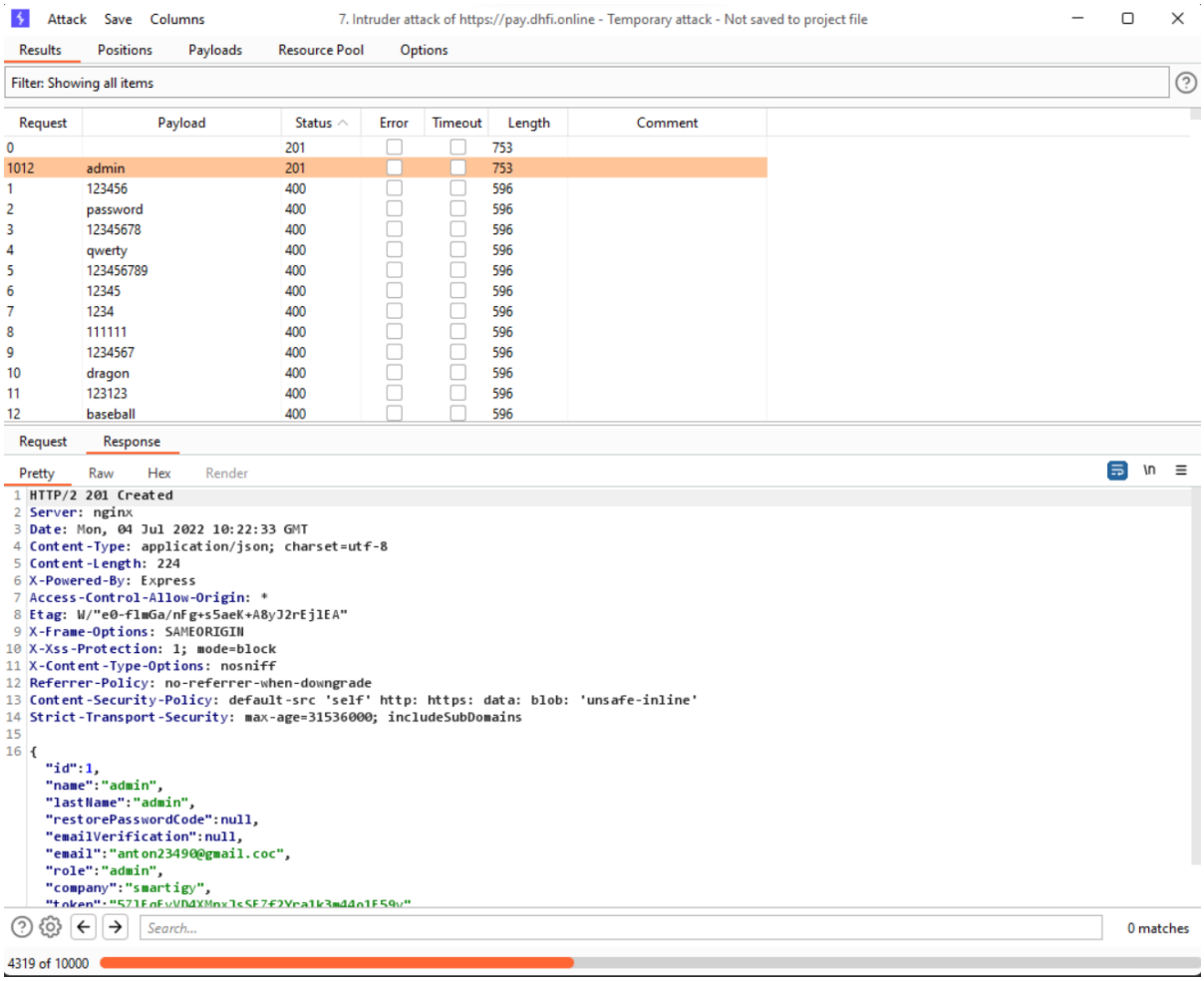
Used POST instead of GET and used body instead of param



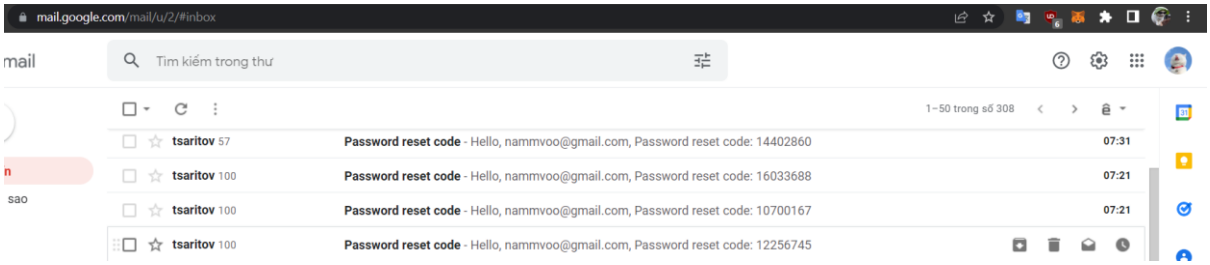
7.7 DHFI-2022-30701

Brute force successfully the Admin account through the login feature

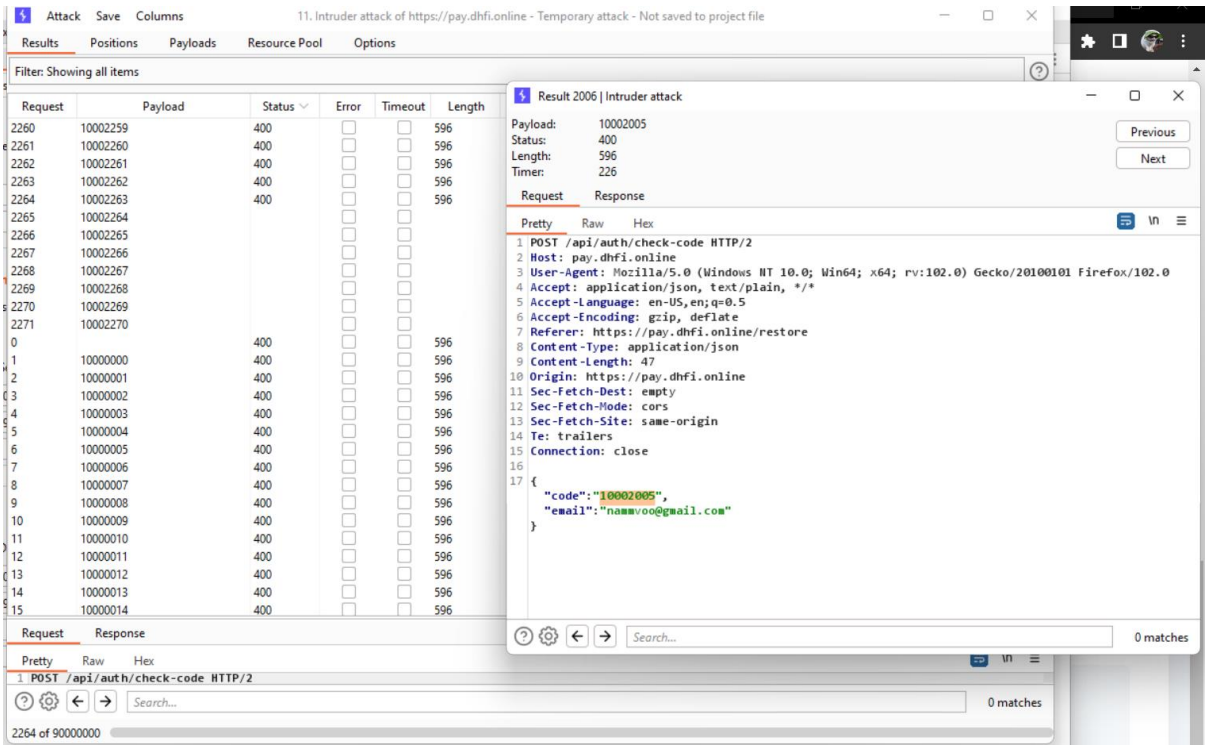
HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn



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



The OTP confirmation feature is also affected

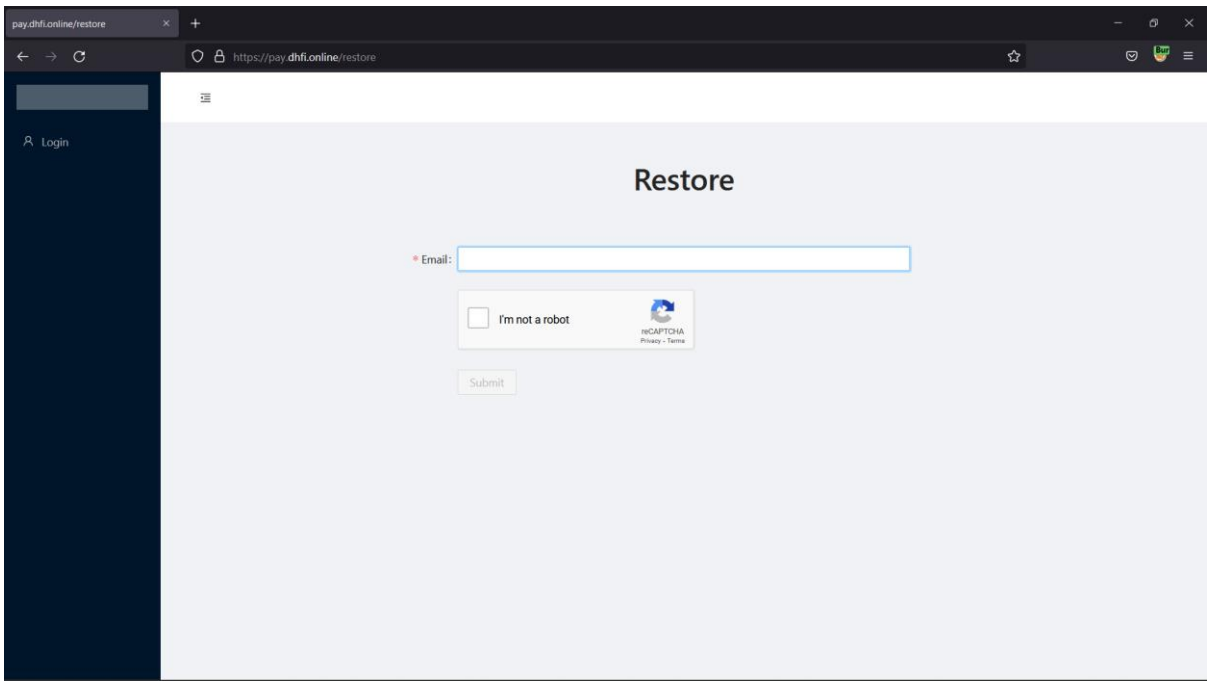


Retest:

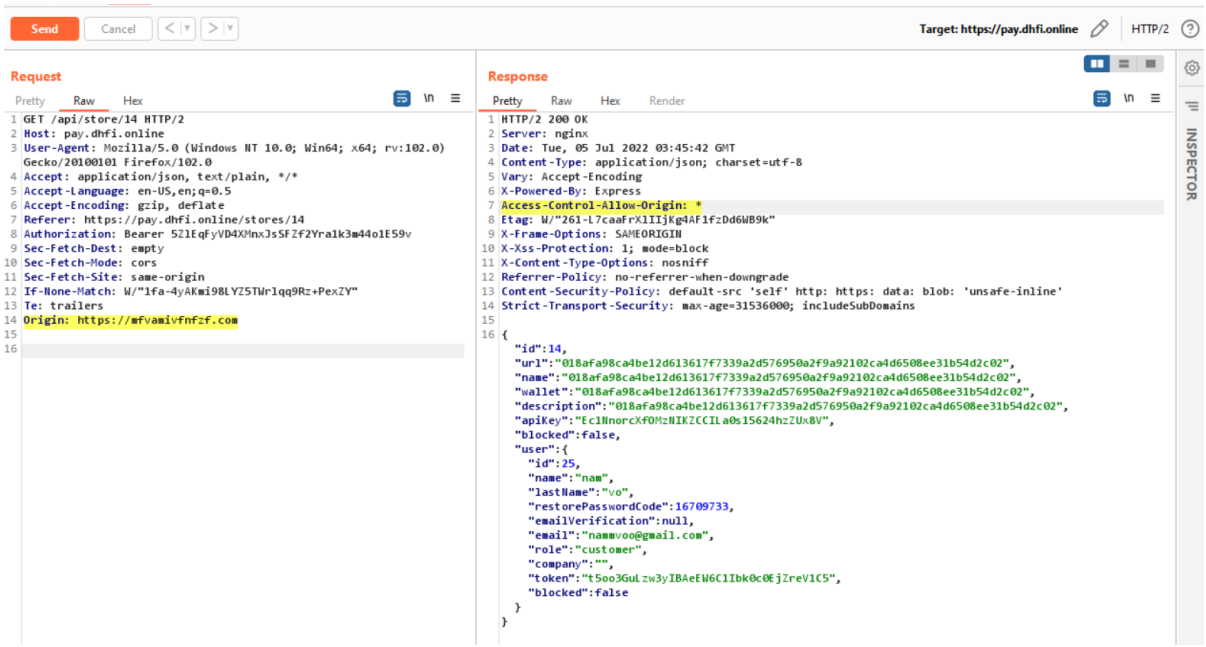
POST /api/auth/login
POST /api/auth/send-code

POST /api/auth/check-code

Implemented ReCaptcha



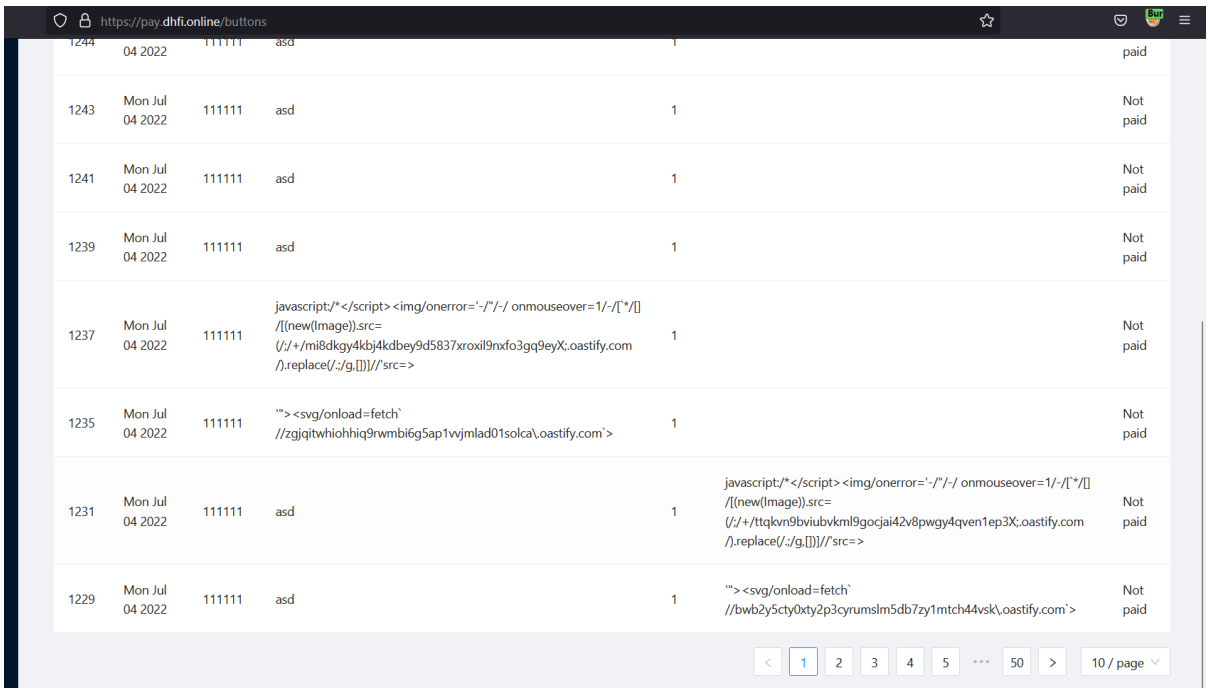
7.8 DHFI-2022-94201



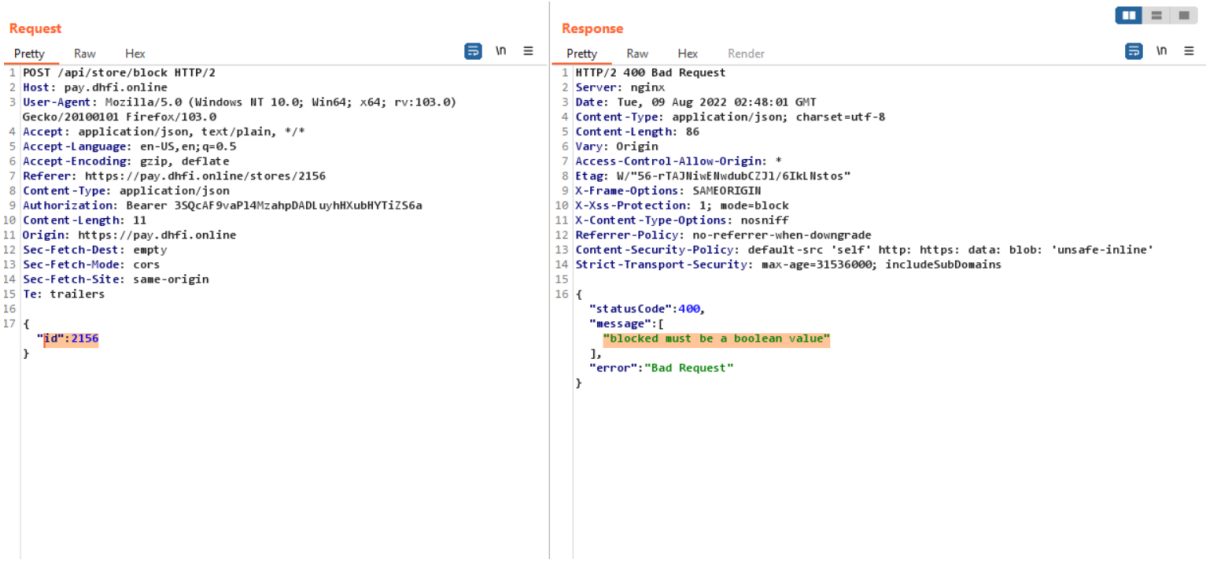
Retest:

Vulnerability currently does not affect the application

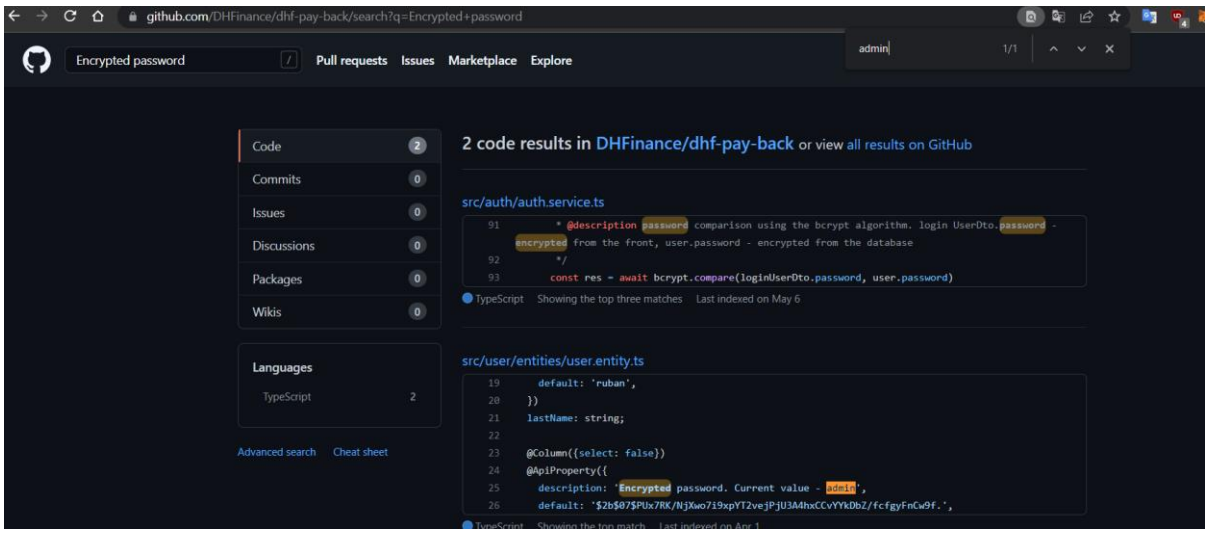
7.9 DHFI-2022-2001



Retest:

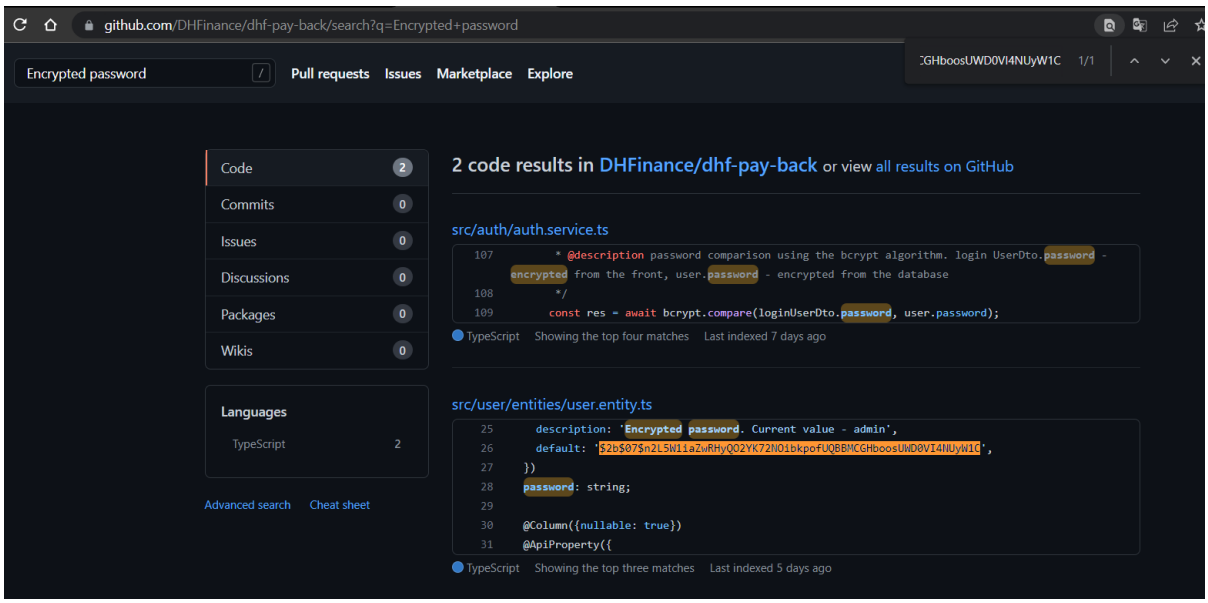


7.10 DHFI-2022-25601



Retest:

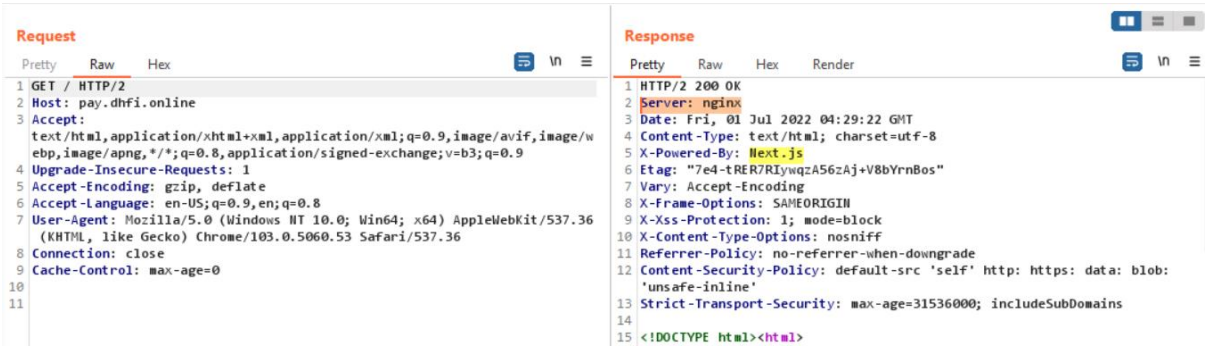
Value has been changed



7.11 DHFI-2022-20001

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

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn



Request

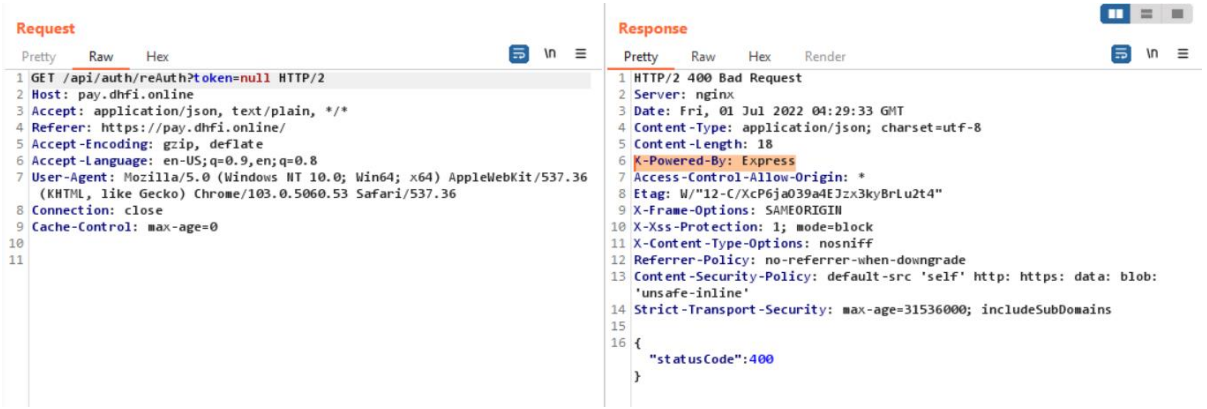
```
GET / HTTP/2
Host: pay.dhfi.online
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/2 200 OK
Server: nginx
Date: Fri, 01 Jul 2022 04:29:22 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Next.js
Etag: "7e4-tRER7RIywqzA56zAj+V8bYrnBos"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer-when-downgrade
Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
Strict-Transport-Security: max-age=31536000; includeSubDomains

<!DOCTYPE html><html>
```

And the backend uses Express



Request

```
GET /api/auth/reAuth?token=null HTTP/2
Host: pay.dhfi.online
Accept: application/json, text/plain, */*
Referer: https://pay.dhfi.online/
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
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
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/2 400 Bad Request
Server: nginx
Date: Fri, 01 Jul 2022 04:29:33 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 18
X-Powered-By: Express
Access-Control-Allow-Origin: *
Etag: W/"12-C/XcP6jaO39a4EJzx3kyBrLu2t4"
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer-when-downgrade
Content-Security-Policy: default-src 'self' http: https: data: blob: 'unsafe-inline'
Strict-Transport-Security: max-age=31536000; includeSubDomains

{
  "statusCode":400
}
```

Default nginx web server error message.

Retest:

HQ: 275 Nguyen Trai St., Thanh Xuan Dist., Ha Noi
HCMC: 412 Nguyen Thi Minh Khai St., District 3, HCM City
H: (+84) 906 831 337
W: www.vsec.com.vn
E: contact@vsec.com.vn

The technology information of the web app has been hidden

Request

Pretty Raw Hex

```
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.coc",
     "password":"admin",
     "captchaToken":
     "03AWYolqvZR786R4_6BcvH6cFbBDtGURQI4QIPd7brhvkK3QKHU1pdAOJ
     kvVGpZnGCwgCyzSYkFNLr51U3qcppbHg71_fKObRsm5X-G4R6BKmb6GmIT
     flZMJkuUnLpAyeu028kw7eEIdrJac6HrEyIygGdPL_ei5ALNJcB6ATeLeS
     3DVftSN-ZN_VOayJMRt-Z-aBueZ9S-CDnRDm_THZa_lH7en34Wgv8-dJLB
     MNDLRK3_PyphAtwd6Ae0mu70pxOJNa6Bfnq5s70aJsyEW-gQCxajpQsGcx
     cyCKM5E8F1jgrHJPjyr-pGXp_iYhaZtNy0E9IZOX1CbQCmLk9qqqyg1yHx
     kEPIKChvg_N_Cdw5_YW0r_vJViDRX09eogN1osuV3eDa4I-VwGAR7LWNFk
     7U2uA_fB8eX6YmcnpXbCjyEDaXKaxkejTJvZWyF-xf8hFV-YaZbU-XM2Mn
     RHhsP0waWgFx96wNez0ozXKa2z1rUNEFM-vQFTKwv4G0pmJQdWmH6tAg8L
     qA8jtHUqBqNuDalVqIS6tp85xog"
   }
```

Response

Pretty Raw Hex Render

```
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-3C3bZ198ntGaX3o7UNjj+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.coc",
     "role":"admin",
     "company":"smartigy",
     "token":"xe6ZwBf8X732LStfB1rYqKkC8D1UR5DwXtaw",
     "blocked":false,
     "loginAttempts":0,
     "timeBlockLogin":"2022-08-04T12:06:04.489Z"
   }
```