Description

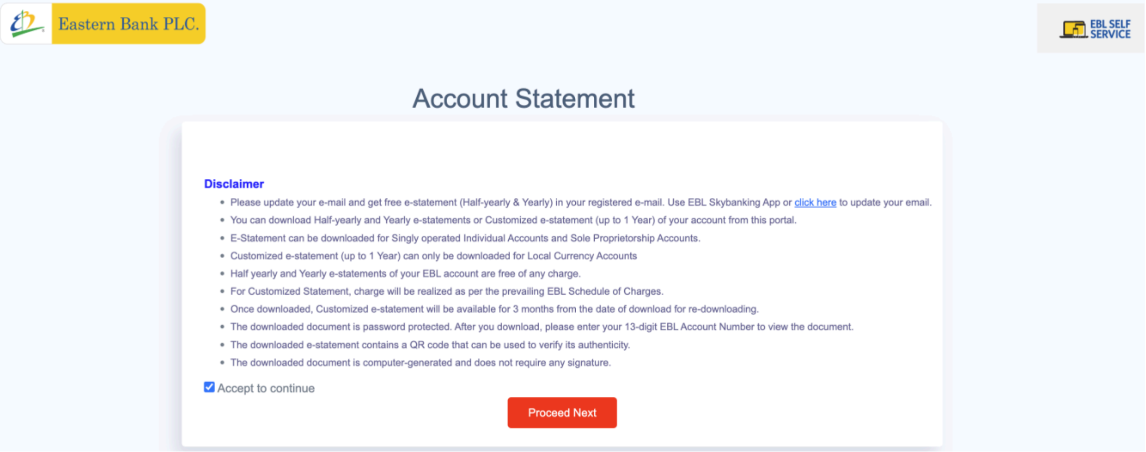
There is a critical security vulnerability discovered in one of Eastern Bank Limited's online portals whereby it's possible for an attacker to acquire important account information and bank statements for an account armed with nothing more than an account number and the associated mobile phone number.

The vulnerability is effectively a Client-Side Validation issue where a critical OTP validation check can be easily bypassed by manipulating the value of a single variable in the client-side Javascript code. The variable is used in a branching condition responsible for either showing an OTP validation error to the user OR to proceed with running the necessary code for taking the user to the next page where account statements can be downloaded.

Shockingly, all the necessary information for entering the "success" branch is embedded in the client side code where this OTP validation check is performed, allowing the attacker to use a common browser inspector tool such as Chrome DevTools to manipulate the variable value to enter the desired execution path in an `if/else` condition.

Steps to reproduce

1. Go to https://selfservicehub.ebl-bd.com/online_statement
2. Accept the disclaimer shown below



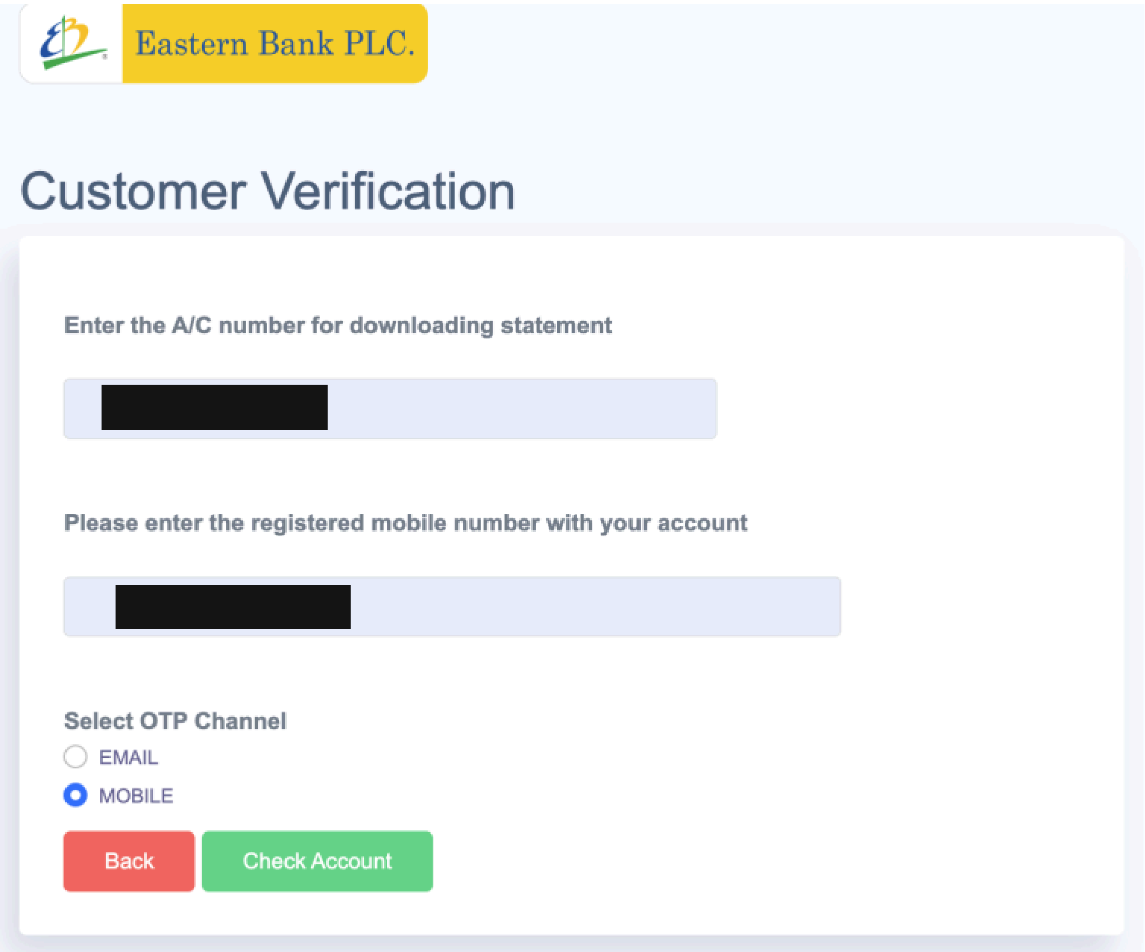
Account Statement

Disclaimer

- Please update your e-mail and get free e-statement (Half-yearly & Yearly) in your registered e-mail. Use EBL Skybanking App or click here to update your email.
- You can download Half-yearly and Yearly e-statements or Customized e-statement (up to 1 Year) of your account from this portal.
- E-Statement can be downloaded for Singly operated Individual Accounts and Sole Proprietorship Accounts.
- Customized e-statement (up to 1 Year) can only be downloaded for Local Currency Accounts
- Half yearly and Yearly e-statements of your EBL account are free of any charge.
- For Customized Statement, charge will be realized as per the prevailing EBL Schedule of Charges.
- Once downloaded, Customized e-statement will be available for 3 months from the date of download for re-downloading.
- The downloaded document is password protected. After you download, please enter your 13-digit EBL Account Number to view the document.
- The downloaded e-statement contains a QR code that can be used to verify its authenticity.
- The downloaded document is computer-generated and does not require any signature.

☑ Accept to continue

3. Enter the EBL account number and the associated mobile phone number in the next screen and hit "Check Account" (must select "MOBILE" as OTP Channel here)



Eastern Bank PLC.

Customer Verification

Enter the A/C number for downloading statement

[redacted]

Please enter the registered mobile number with your account

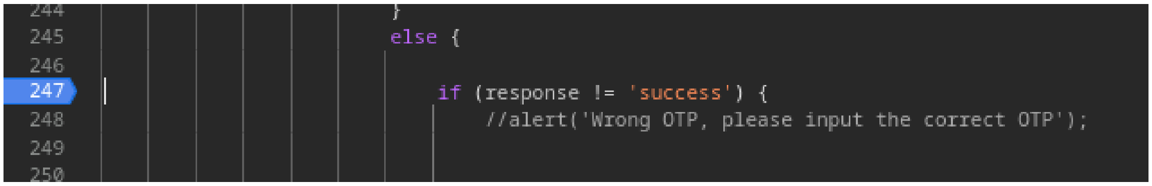
[redacted]

Select OTP Channel

○ EMAIL

● MOBILE

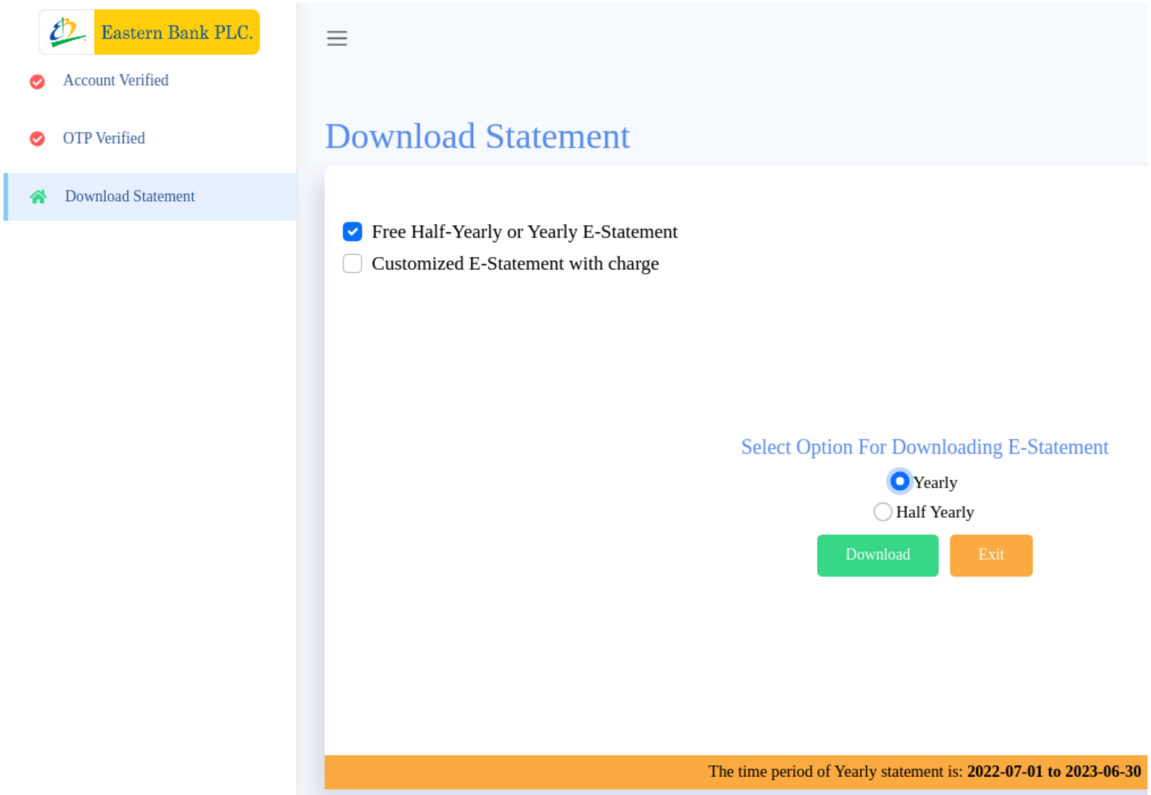
4. If the account number and phone number is correct, on the next page open browser inspector and add a breakpoint in line 247 of customer_verification_page.php



```
244             }
245             else {
246 
247                 if (response != 'success') {
248                     //alert('Wrong OTP, please input the correct OTP');
249 
250 
```

5. Enter any OTP (does not need to be valid) and hit “Submit OTP”
6. The debugger will now stop code execution at the breakpoint. Execute `response = ‘success’` in the console and resume execution

7. You will be successfully validated and enter the next page



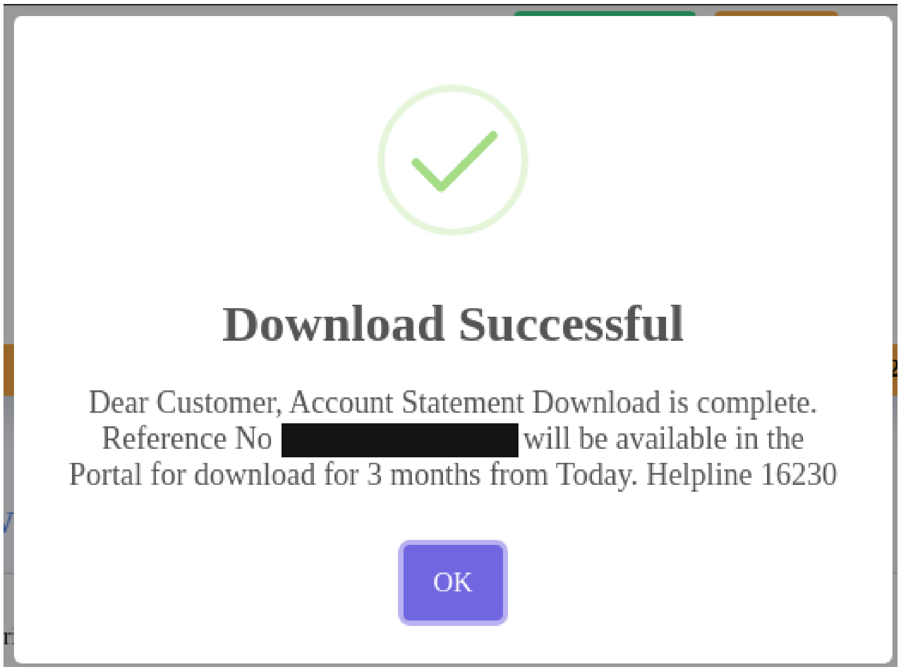
Download Statement

☑ Free Half-Yearly or Yearly E-Statement
□ Customized E-Statement with charge

Select Option For Downloading E-Statement
● Yearly
○ Half Yearly

The time period of Yearly statement is: **2022-07-01 to 2023-06-30**

8. You can download the bank statement without further checks



Download Successful

Dear Customer, Account Statement Download is complete. Reference No [redacted] will be available in the Portal for download for 3 months from Today. Helpline 16230