Interim Report

Email Subject:	Re: PG Integration Nagar Nigam Jhansi MID: ObZ4A4ISRViQmh
Merchant Name-	Nagar Nigam Jhansi
Audit Start -	23-Aug-2024
Vulnerability Reported -	27-Aug-2024

We have performed an audit for the following merchant.

The test found Two high-risk vulnerability (i.e. Parameter Manipulation (Fail to success) (open) & Parameter Manipulation (Response Drop) (open) per the test cases. PFA screenshots and update us.

Audit Log:

1st Audit-24-Aug -2024: Replay Attack (close).

2nd Audit: 27-Aug-2024: Parameter Manipulation (Fail to success) (open) & Parameter Manipulation (Response Drop) (open).

1-Description of Vulnerability for Failure to Success:

The parameter manipulation is caused between the Page/Response after the payment information is processed. An adversary could edit failed payment responses from the bank to that of a successful payment.

1. We select 'No' on 3d secure page to failed a transaction

2. The failure response parameter was captured and was swapped with the successful response parameter.

3. This the manipulated response was sent back to the merchant after that which we got a failed receipt also but after comparing with the databases details it shows us success transaction.

Impact:

An adversary can manipulate transactions made through a payment gateway by replacing the failure parameters with the previous response of a successful transaction which might result in huge financial loss.

Solution/Mitigation:

1. Request the developer to calculate the reverse hash correctly and also update the receipt on basis of database entry whether it is a failure or a success.

2. Developers also need to validate the amount along with transaction ids in response to the database.

2-Parameter Manipulation (Response Drop Handling) (open)

Description of Vulnerability: The response handling is caused between the Page/Response after the payment information is processed. An adversary could edit failed payment responses from the bank to that of a successful payment. In which the higher amount got paid with the success response of the lower amount.

Impact:

An adversary can manipulate transactions made through a payment gateway by swapping the failure response with the dropped response of the successful transaction.

Solution/Mitigation:

Request the developer to validate all the response/response parameters with the database and the same need to be stored in the database and reflect on the browser.