No Rate limiting

Application has Sign up form

↓

click on forget password

↓

server will send otp on your phone

↓

intercept it and make 1000 requests

↓

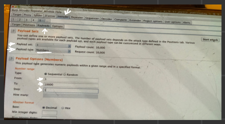
You will recieve 1000 SMS.

↓

Vulnerable

* Steps to Hunt No Rate Limiting:

1. Capture forgot password or any event request into burpsuite.
2. Send to intruder or sequencer. *
3. Make Same request 1000 times.
4. if app will perform same action 1000 times then there is a vulnerability.



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 5 ...
Target Positions Payloads Options
Start attack

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 payload type can be customized in different ways.

Payload set: 1 Payload count: 10,000
Payload type: Numbers Request count: 10,000

Payload Options [Numbers]

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

Number range
Type: ● Sequential ○ Random
From: 1
To: 10000
Step: 1
How many:

Number format
Base: ● Decimal ○ Hex
Min integer digits:

* Send to sequencer → start live capture.

* if you recieve more then 10 emails, then this is vulnerability.

Reporting

Vulnerable name : No Rate limiting

Vulnerability description :

This is a logical flaw in the app not DoS Attack.
By replaying forgot password request. It will send you huge emails.
There should be some rate limite.

Vulnerable URL :

Impact :

How to reproduce this issue :

1. capture forgot password into Burpsuit.
2. Send to intruder
3. Select a position
4. Set payloads to numbers and numbers will be from 1 to 1000 .

Recommendation :

PoC :