



Application Penetration Testing Report

Base URL: mopng.gov.in

Report Date: 15-04-26 01:02 pm

Application Security and Audit Division
(Application Security Group)
National Informatics Centre
A – Block, CGO Complex, Lodhi Road, New Delhi - 110003.

Contributions

S. No.	Name	Role
1.	Shaikh Sarfraj	Auditor
2.	Saksham Jain	Reviewer

Key Findings

Vulnerability List

Assign Number: A20260305006		
Base URL: mopng.gov.in		
S. No.	Incident URL	Vulnerability Name
1.	https://mopng.gov.in/en/pdc	Email Harvesting
2.	https://mopng.gov.in/en	Duplicate Cookie Header

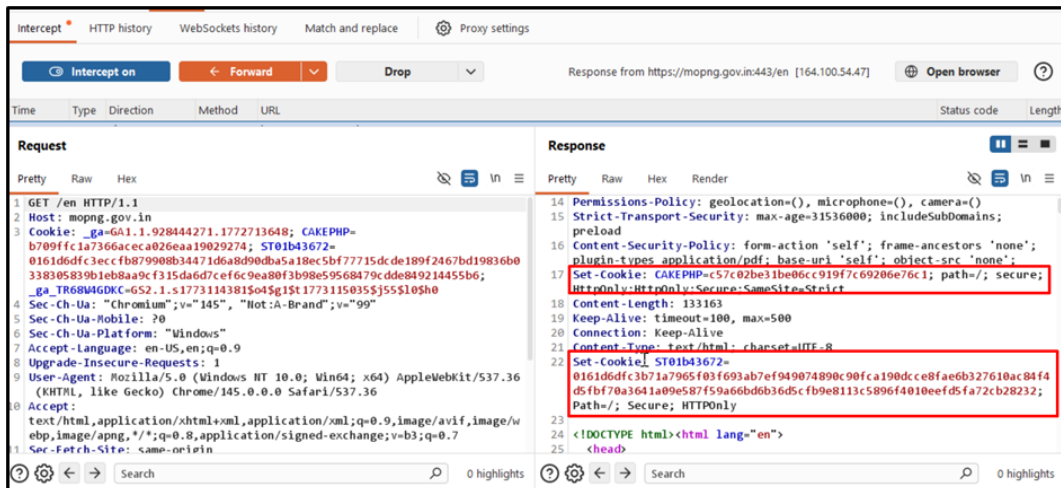
2. Vulnerability Name: Duplicate Cookie Header

Severity:

Low

Proof of Concept:

Step I: From the screenshot below, it is observed that the application has two set-cookie, as shown below:



Description:

the application has implemented duplicate cookie header in the application.

Impact:

the application sets multiple set-cookie headers in the response, which may leak internal information and introduce security management complexity.

Recommendations:

if multiple session cookies are required, validate their necessity and lifecycle, and document their purpose clearly. minimize cookie scope by setting a restrictive domain and path where appropriate.

Other Links: