

28 :: HTTP OPTIONS Method Enabled

Vul Type:	HTTP OPTIONS Method Enabled	No of Places Found:	1
CVSS Score:	3.1	No of Instances Reported:	1
CVSS Vector:	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N		
CWE :	CWE-16: Configuration		
Severity:	Low		
Description:	The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI. It may expose sensitive information that may help an malicious user to prepare more advanced attacks.		
Solution:	Disable OPTIONS Method on the web server.		

Vulnerability Details:

	Unique Alert ID	First Found Date	Last Reopened Date	Parameter	URI
1	3918370	29th April 2023	24th June 2023	method	http://demo1.indussecure.com/my%20documents?content=personal_deposit.htm

Injected URL:

http://demo1.indussecure.com/my%20documents?content=personal_deposit.htm

Vector:

OPTIONS

Request:

OPTIONS /my%20documents?content=personal_deposit.htm HTTP/1.1
 Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 Accept-Encoding:gzip, deflate
 Accept-Language:en-US
 Cookie:JSESSIONID=4C43F781647CE893253B355A42181398
 Upgrade-Insecure-Requests:1
 User-Agent:Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Electron/11.3.0 Safari/537.36
 Host:demo1.indussecure.com

Response:

HTTP/1.1 200 OK
 server:Apache-Coyote/1.1
 allow:GET, HEAD, POST, PUT, DELETE, OPTIONS
 content-length:0
 date:Tue, 26 Sep 2023 10:44:48 GMT
 connection:close

Result:

The following methods are enabled: GET, HEAD, POST, PUT, DELETE, OPTIONS