API Security Testing

Introduction: API Security testing has been done by Kfintech CISO Team for **SmartAPI used for investor site and kfinkart App** and found below vulnerabilities as part of this assessment.

Scope: **SIP Save** - end point -
https://clientwebsitesuat3.kfintech.com/MiraeUat/Smartservice.svc/**SIPSave**?Adminusername=c21hcnRzZXJ2aWNl&Adminpassword=a2FydnkxMjM0JTI0&Reqsource=VjBWQ1NVeEY%3D&APKVer=TWk0dw%3D%3D&OS=V2luZG93c19OVA%3D%3D&IMEI=MTI3LjAuMC4x&i_euinDeclaration=WQ%3D%3D&i_InvDistFlag=TQ%3D%3D&Option=Rw%3D%3D&i_PerpetialSIP=QQ%3D%3D&i_Amount=MTAwMA%3D%3D&i_frequency=TW9udGhseQ%3D%3D&i_fund=MTE3&customfund=MTE3&i_SchemeCode=R1BDRg%3D%3D&i_brokercode=QVJOLTAwMTg%3D&i_SIPday=MTU%3D&i_euinno=RTAwNTY2OQ%3D%3D&i_id=MQ%3D%3D&EntDt=MDcvMTMvMjAyMQ%3D%3D&i_ModeofPayment=SVNJUA%3D%3D&i_EntBy=ZGVtb3VzZXI%3D&i_folio=Nzk5MzI3NTcxMzI%3D&i_SIPEndDate=MTIvMTUvMjAyMQ%3D%3D&i_SIPStartDate=MDgvMTUvMjAyMQ%3D%3D&i_NoofInstalment=NQ%3D%3D&Requid=ZGVtb3VzZXI

Tools used: Postman and Burp Suite.`

References: OWASP Top10.

Vulnerabilities found:

Issue 1: Missing Security Headers

Severity: Medium.

Description:

- Http Strict Transport Security enforces the connections in https disregarding any scripts called to load any resource in that domain over Http.
- X-XXS protection header helps in enabling the cross site scripting (XXS) filter built on browser.
- Setting this header will prevent the browser from MIME-sniffing a response away from the declared content type.
- In the web server didn't return an x frame option header which means that this website could be at risk of a click jacking attack.
- The response header allows website administration to control resources the user agent is allowed to load for given page. With a few exceptions, policies mostly involve specifying sever origin and script end points. These helps guard again cross site scripting attacks (XXS).

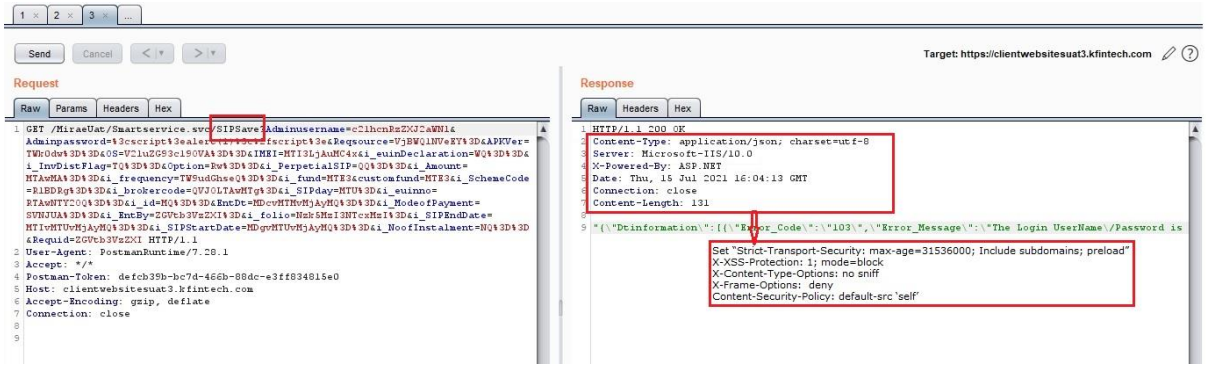
Impact:
It was observed security headers like
- HTTP Strict Transport Security
- X-XSS-Protection
- X-Content-Type-Options
- X-Frame-Options
- Content-Security-Policy

Are missing in the Response Headers.

Remediation:
Configure all the security headers:

- Set "Strict-Transport-Security: max-age=31536000; Include subdomains; preload"
- X-XSS-Protection: 1; mode=block
- X-Content-Type-Options: no sniff
- X-Frame-Options: deny
- Content-Security-Policy: default-src 'self'

POC:



Issue 2: Server Information Disclosure – Microsoft-IIS/10.0.

Severity: Low.

Description: Information exposure through query strings in URL or API occurs when arbitrary values are passed to parameters in the URL or API. This allows attackers to obtain sensitive data such as user names, Passwords, Tokens, Database details and any other potentially sensitive data.

Impact: Sensitive Information disclosure.

Remediation: Remove server banner details from response.

POC: