Sri Lanka Institute of Information Technology

IT21299902 (ZAKEY M.S.M.A)

Bug bounty Report 05.

Domain: Inmobi.com

Web security – IE2062

B.Sc. (Hons) in Information Technology Specialization in cyber security.

Declaration:

- I hereby certify that no part of this assignment has been copied from any other work or any other source. No part of this assignment has been written/produced for me by another person.

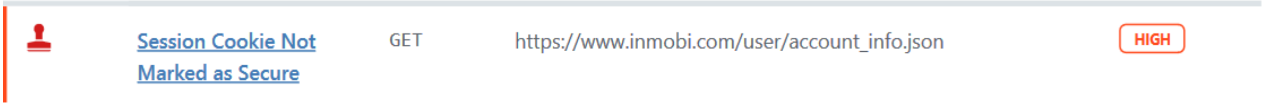
- I hold a copy of this assignment that I can produce if the original is lost or damaged.

1. Sensitive Data exposure.

- **Session cookie not marked as secure (MIMT XSS attack).**

I have identified many vulnerabilities in under domain www.inmboi.com/. I figured out it has vulnerabilities that listed by OWSAP Top 10. And the overall website risk level is **high**. I used net sparker to identify vulnerabilities in the following domain.

I hope this message finds you well. I am writing to report a vulnerability I discovered under the domain of **https://www.inmobi.com/user/account_info.jsonjs** during my participation in the bug bounty program. Please find below the details of the vulnerability for your review and further action.



Session Cookie Not Marked as Secure GET https://www.inmobi.com/user/account_info.json HIGH

Vulnerability title: Session cookie not marked as secure (MIMT possible)

Severity: High

OWASP classification 2013: A3

CVSS 3.0 score: - 5.3

CVSS 3.1 score: - 5.3

CVSS string: - CVSS:3.1/AV: A/AC: H/PR: N/UI: N/S: U/C: H/I: N/A: N

Effected components: User accounts.

Privacy of users

Date of Discovery: 2023/05/10

Date of Report: 2023/05/12

2. Vulnerability Description.

Session cookie is the most important part of when client establishing connection with the server with session cookies will keep track of the user.in this case session cookie is still visible in https transmission. I have identified a possibility of MIMT attack, session hijacking, and session fixation etc. within the affected system. If this attack succeeds in the system it will lead to data leakage, session hijacking, confidentiality breach, and data manipulation.

3. Impact assessment.

Under this OWSAP category I have identified many vulnerabilities like sensitive data exposure that can occur due to bad implementation of security implementations under domain of **https://www.inmobi.com/user/account_info.json**

I have identified while scanning the target domain it is sending the session cookie over a HTTPS enabled connection without marking session cookie as secure.

1. The session cookie can be transmitted through unencrypted HTTP connections rather than HTTPS connections if the "secure" tag is not set. This makes it possible for attackers using MitM attacks to intercept the cookie. Attackers may listen in on the conversation and take the session cookie to access the user's session without authorization.

2. An attacker can obtain the user's session identifier using an unsecured session cookie by taking advantage of flaws like session sniffing or session high jacking. Once the attacker has the session identifier, they can use it to assume the user's identity, log into their account, and take actions on their behalf.

3. Insecure session cookies may not meet regulatory compliance standards like the General Data Protection Regulation (GDPR) or Payment Card Industry Data Security Standard (PCI DSS). The absence of the "secure" characteristic may be flagged as non-compliant by security audits as a vulnerability.

4. Failure to declare the session cookie as secure can reduce user confidence in the security of the online application. Users might be reluctant to conduct sensitive acts or transactions on the website, which could harm the app's credibility and reputation.

Because of this vulnerability marked as High It’s a must to address it with a good solution.

4. Steps to Reproduce.

This attack needs some social engineering as well as attacker should be able to intercept the communication at precisely manner in order to do such a attack.

1. Start by configuring two unique browsers, Chrome and Firefox, or browser profiles, or by using two distinct devices.

2. Make sure you are logged into your user account in one of the browsers or devices before opening the web application in both.

3. To record the network traffic between the browser and the web server, use a network analysis program like Wireshark.

4. Use a proxy tool like Burp Suite to intercept the login request in the second browser or device when you are not logged in.

5. alter the obtained login request such that the session cookie is obtained. You can accomplish this by copying the session ID value from the "Set-Cookie" header.

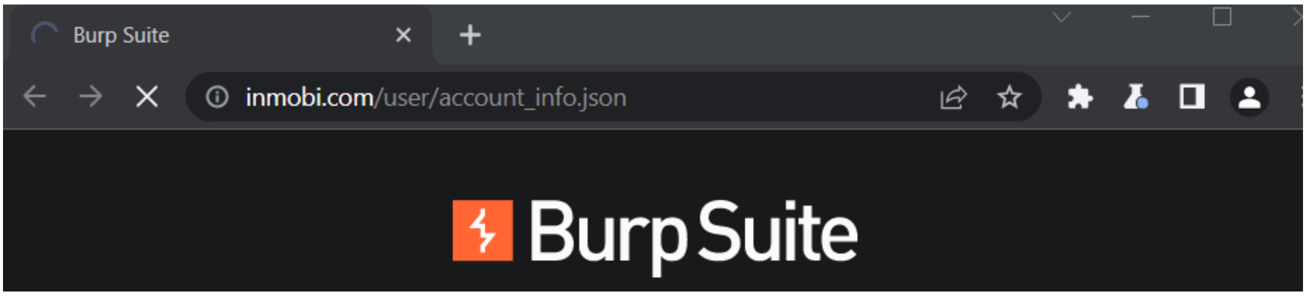
6. To set the value of the session cookie that was captured, open the developer tools on the second browser or device and run the JavaScript script.

7. Use the second browser or device to reload the page or move to a different page inside the online application.

8. If the session hijacking is successful, the web application might acknowledge the session cookie as legitimate and provide you access to the user account without requesting a login.

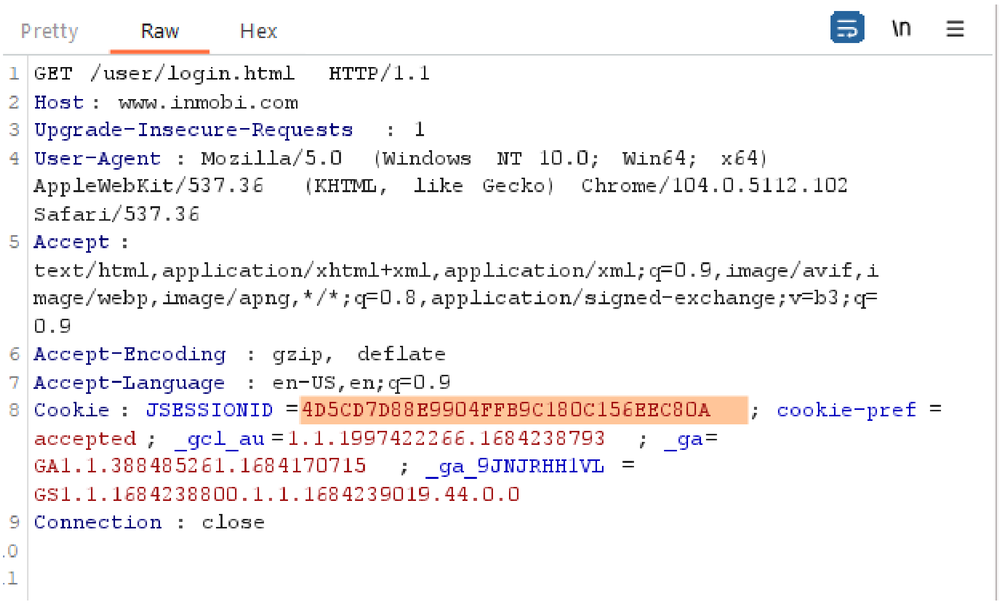
5. Proof of concept.

Loging to the web application using legitimate credentials.



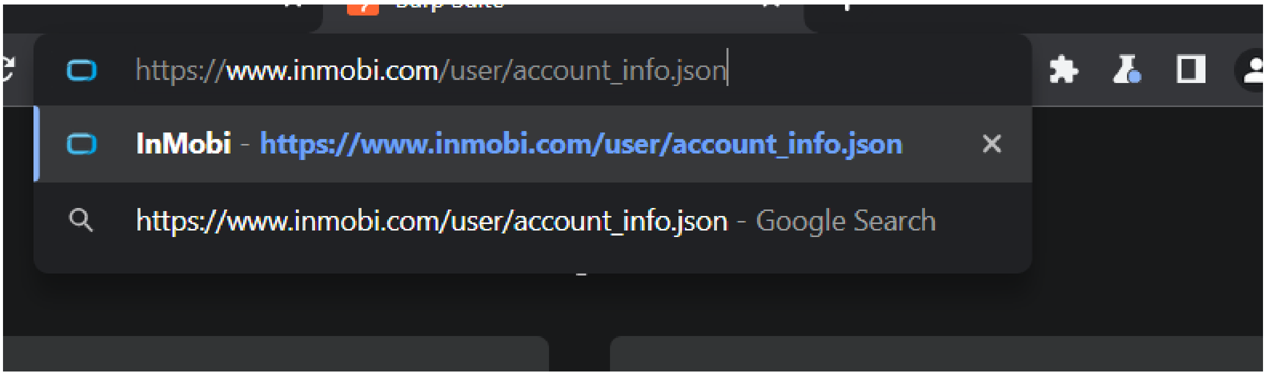
inmobi.com/user/account_info.json

Getting the session cookie to hi jack the session for legitimate user.



```
GET /user/login.html  HTTP/1.1
Host : www.inmobi.com
Upgrade-Insecure-Requests  : 1
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)
AppleWebKit/537.36   (KHTML,  like  Gecko)  Chrome/104.0.5112.102
Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Accept-Encoding  : gzip,  deflate
Accept-Language  : en-US,en;q=0.9
Cookie : JSESSIONID =4D5CD7D88E9904FFB9C180C156EEC80A   ; cookie-pref =
accepted ; _gcl_au =1.1.1997422266.1684238793   ; _ga=
GA1.1.388485261.1684170715   ; _ga_9JNJRHH1VL  =
GS1.1.1684238800.1.1.1684239019.44.0.0
Connection : close
```

Opening the login page using another tab with stolen session cookie.

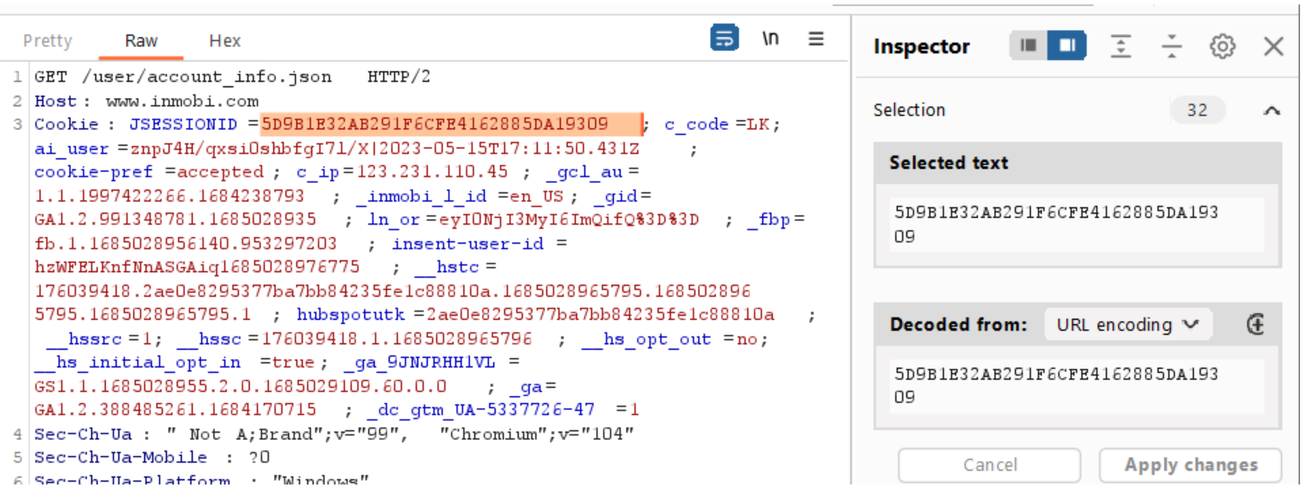


https://www.inmobi.com/user/account_info.json

InMobi - https://www.inmobi.com/user/account_info.json

https://www.inmobi.com/user/account_info.json - Google Search

Replacing session cookie with solen one.



```
GET /user/account_info.json   HTTP/2
Host : www.inmobi.com
Cookie : JSESSIONID =5D9B1E32AB291F6CFE4162885DA19309 ; c_code =LK;
ai_user =znpJ4H/qxsi0shbfgI71/X|2023-05-15T17:11:50.431Z    ;
cookie-pref =accepted ; c_ip=123.231.110.45 ; _gcl_au =
1.1.1997422266.1684238793  ; _inmobi_l_id =en_US ; _gid=
GA1.2.991348781.1685028935  ; ln_or =eyI0NjI3MyI6ImQifQ%3D%3D  ; _fbp=
fb.1.1685028956140.953297203  ; insent-user-id =
hzWFELKnfNnASGAiq1685028976775  ; __hstc =
176039418.2ae0e8295377ba7bb84235fe1c88810a.1685028965795.168502896
5795.1685028965795.1  ; hubspotutk =2ae0e8295377ba7bb84235fe1c88810a  ;
 __hssrc =1; __hssc =176039418.1.1685028965796  ; __hs_opt_out =no;
__hs_initial_opt_in  =true ; _ga_9JNJRHH1VL  =
GS1.1.1685028955.2.0.1685029109.60.0.0   ; _ga=
GA1.2.388485261.1684170715  ; _dc_gtm_UA-5337726-47  =1
Sec-Ch-Ua : " Not A;Brand";v="99",  "Chromium";v="104"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
```

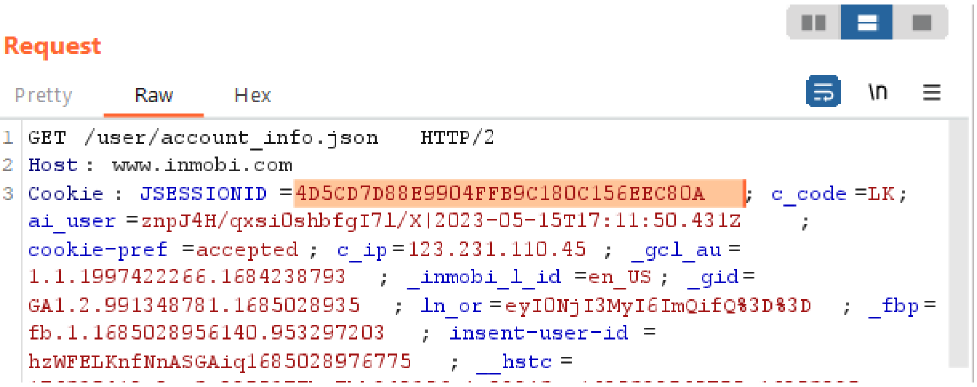
Selection 32

Selected text

```
5D9B1E32AB291F6CFE4162885DA193
09
```

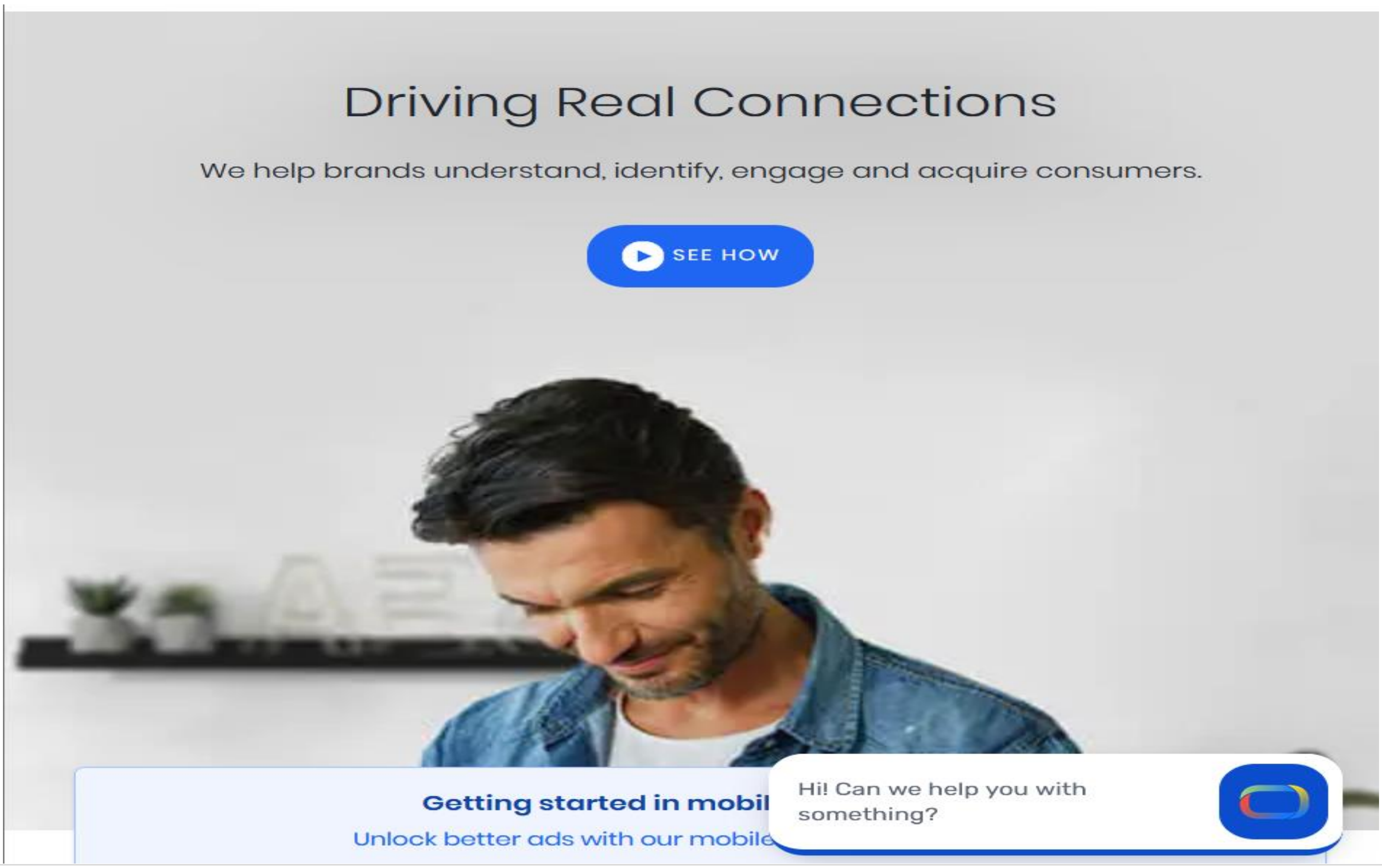
Decoded from: URL encoding

```
5D9B1E32AB291F6CFE4162885DA193
09
```



```
GET /user/account_info.json   HTTP/2
Host : www.inmobi.com
Cookie : JSESSIONID =4D5CD7D88E9904FFB9C180C156EEC80A  ; c_code =LK;
ai_user =znpJ4H/qxsi0shbfgI71/X|2023-05-15T17:11:50.431Z    ;
cookie-pref =accepted ; c_ip=123.231.110.45 ; _gcl_au =
1.1.1997422266.1684238793  ; _inmobi_l_id =en_US ; _gid=
GA1.2.991348781.1685028935  ; ln_or =eyI0NjI3MyI6ImQifQ%3D%3D  ; _fbp=
fb.1.1685028956140.953297203  ; insent-user-id =
hzWFELKnfNnASGAiq1685028976775  ; __hstc =
```

Successfully logged in.


Driving Real Connections
We help brands understand, identify, engage and acquire consumers.
SEE HOW
Getting started in mobil
Unlock better ads with our mobile
Hi! Can we help you with something?

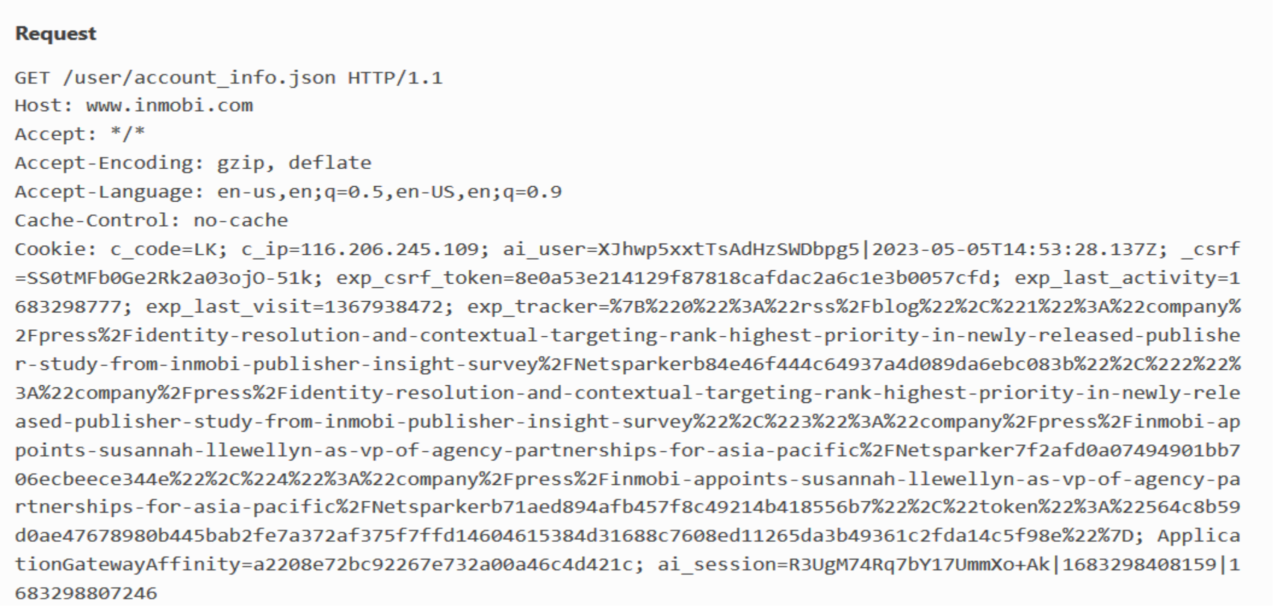
6. Existence of the vulnerability

Identified Cookie(s)

- JSESSIONID

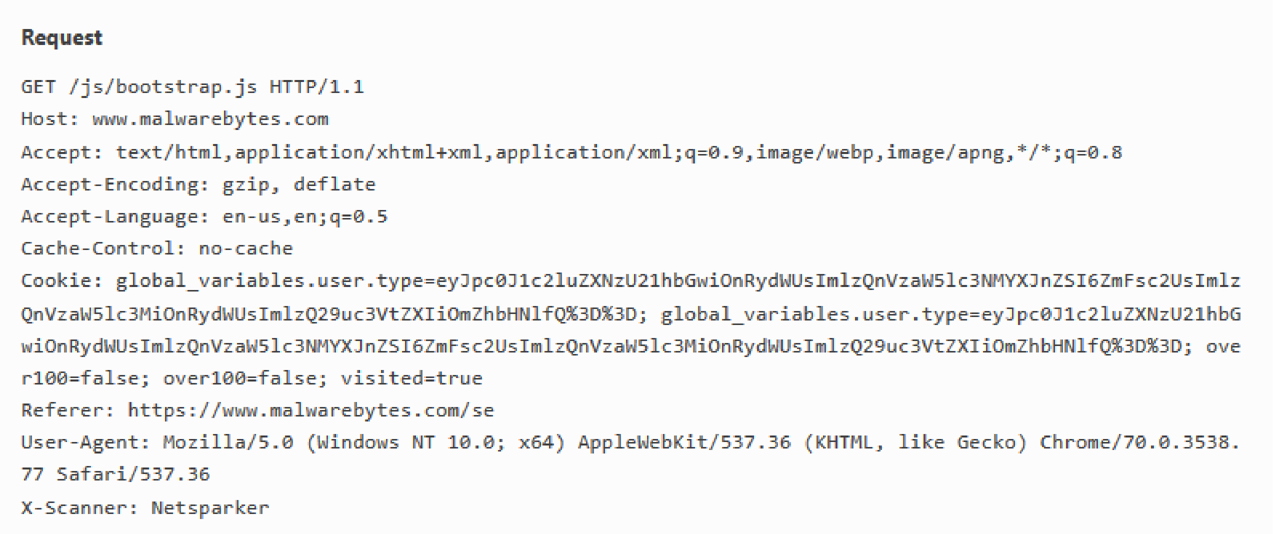
Cookie Source

- HTTP Header



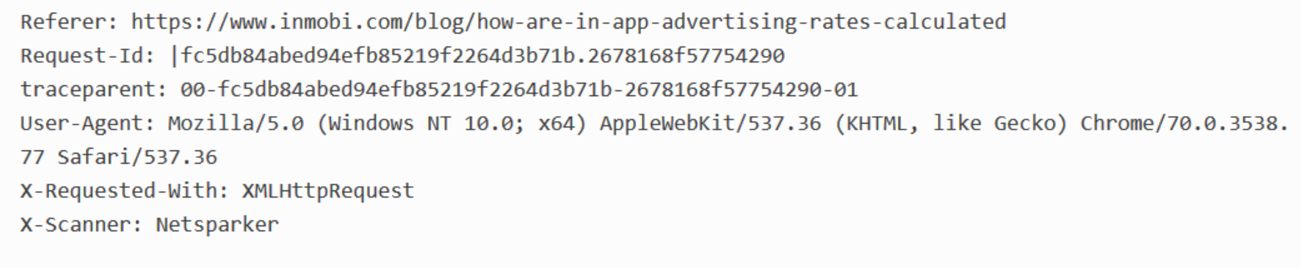
Request

```
GET /user/account_info.json HTTP/1.1
Host: www.inmobi.com
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5,en-US,en;q=0.9
Cache-Control: no-cache
Cookie: c_code=LK; c_ip=116.206.245.109; ai_user=XJhwp5xxtTsAdHzSWDbpg5|2023-05-05T14:53:28.137Z; _csrf
=SS0tMFb0Ge2Rk2a03ojO-51k; exp_csrf_token=8e0a53e214129f87818cafdac2a6c1e3b0057cfd; exp_last_activity=1
683298777; exp_last_visit=1367938472; exp_tracker=%7B%220%22%3A%22rss%2Fblog%22%2C%221%22%3A%22company%
2Fpress%2Fidentity-resolution-and-contextual-targeting-rank-highest-priority-in-newly-released-publishe
r-study-from-inmobi-publisher-insight-survey%2FNetsparkerb84e46f444c64937a4d089da6ebc083b%22%2C%222%22%
3A%22company%2Fpress%2Fidentity-resolution-and-contextual-targeting-rank-highest-priority-in-newly-rele
ased-publisher-study-from-inmobi-publisher-insight-survey%22%2C%223%22%3A%22company%2Fpress%2Finmobi-ap
points-susannah-llewellyn-as-vp-of-agency-partnerships-for-asia-pacific%2FNetsparker7f2afd0a07494901bb7
06ecbeece344e%22%2C%224%22%3A%22company%2Fpress%2Finmobi-appoints-susannah-llewellyn-as-vp-of-agency-pa
rtnerships-for-asia-pacific%2FNetsparkerb71aed894afb457f8c49214b418556b7%22%2C%22token%22%3A%22564c8b59
d0ae47678980b445bab2fe7a372af375f7ffd14604615384d31688c7608ed11265da3b49361c2fda14c5f98e%22%7D; Applica
tionGatewayAffinity=a2208e72bc92267e732a00a46c4d421c; ai_session=R3UgM74Rq7bY17UmmXo+Ak|1683298408159|1
683298807246
```

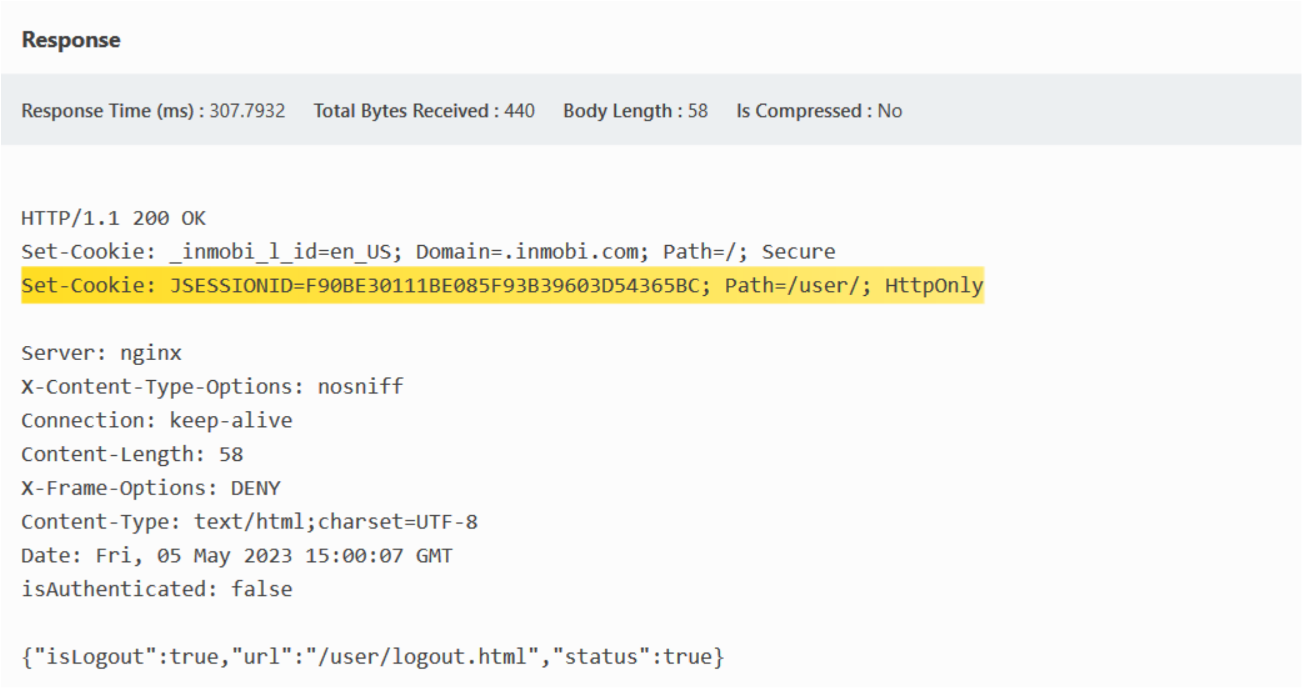


Request

```
GET /js/bootstrap.js HTTP/1.1
Host: www.malwarebytes.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: global_variables.user.type=eyJpc0J1c2luZXNzU21hbGwiOnRydWUsImlzQnVzaW5lc3NMYXJnZSI6ZmFsc2UsImlz
QnVzaW5lc3MiOnRydWUsImlzQ29uc3VtZXIiOmZhbHNlfQ%3D%3D; global_variables.user.type=eyJpc0J1c2luZXNzU21hbG
wiOnRydWUsImlzQnVzaW5lc3NMYXJnZSI6ZmFsc2UsImlzQnVzaW5lc3MiOnRydWUsImlzQ29uc3VtZXIiOmZhbHNlfQ%3D%3D; ove
r100=false; over100=false; visited=true
Referer: https://www.malwarebytes.com/se
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```



```
Referer: https://www.inmobi.com/blog/how-are-in-app-advertising-rates-calculated
Request-Id: |fc5db84abed94efb85219f2264d3b71b.2678168f57754290
traceparent: 00-fc5db84abed94efb85219f2264d3b71b-2678168f57754290-01
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Requested-With: XMLHttpRequest
X-Scanner: Netsparker
```



Response

Response Time (ms) : 307.7932 Total Bytes Received : 440 Body Length : 58 Is Compressed : No

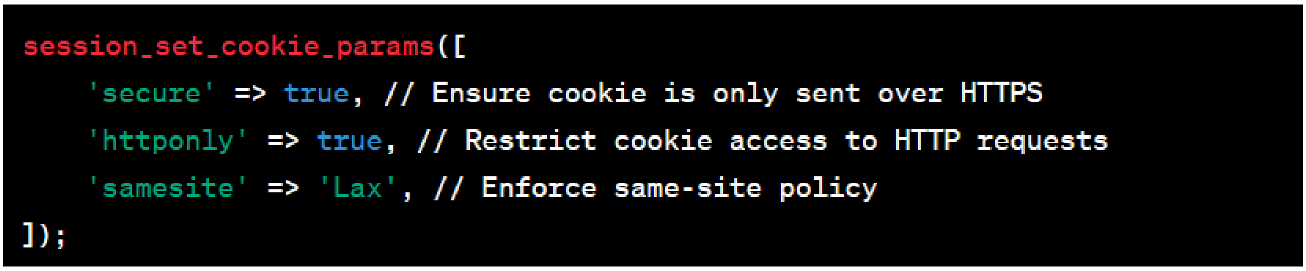
```
HTTP/1.1 200 OK
Set-Cookie: _inmobi_l_id=en_US; Domain=.inmobi.com; Path=/; Secure
Set-Cookie: JSESSIONID=F90BE30111BE085F93B39603D54365BC; Path=/user/; HttpOnly

Server: nginx
X-Content-Type-Options: nosniff
Connection: keep-alive
Content-Length: 58
X-Frame-Options: DENY
Content-Type: text/html;charset=UTF-8
Date: Fri, 05 May 2023 15:00:07 GMT
isAuthenticated: false

{"isLogout":true,"url":"/user/logout.html","status":true}
```

7. Proposed mitigation/fix.

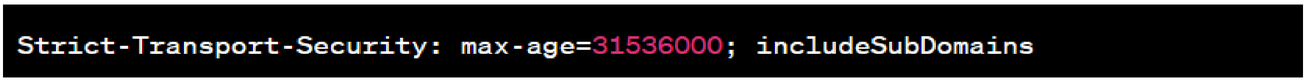
1. Make that the "Secure" attribute is set on the session cookie. This attribute tells the browser to send cookies exclusively over HTTPS-encrypted connections. By setting this attribute, you can reduce the chance of an attacker intercepting the session cookie by preventing its transmission via insecure channels.



```
session_set_cookie_params([
    'secure' => true, // Ensure cookie is only sent over HTTPS
    'httponly' => true, // Restrict cookie access to HTTP requests
    'samesite' => 'Lax', // Enforce same-site policy
]);
```

2. Make sure that HTTPS is being used to deliver your complete web application. This guarantees that all communication, including the transmission of session cookies, is encrypted between the client and server. To enforce secure connections, configure your web server to forward all HTTP requests to HTTPS.

3. Use HSTS to tell the browser to always communicate with your web application via HTTPS. This helps lower the danger of session cookie interception by preventing users from visiting your site using unsecured HTTP connections.



```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

4. If a significant event occurs, such as a successful login, password change, or privilege elevation, implement a way to regenerate the session identification. Even if an attacker succeeds in stealing a session cookie, this helps to lessen the effects of session hijacking.

5. Implement a technique to regularly re-authenticate users by asking them to do so after a specific period of inactivity or at predetermined intervals. Even if an attacker obtains access to a legitimate session cookie, this can lessen the possibility of session hijacking.