Vulnerability Assessment & Penetration Testing Report

India Infoline Finance Limited

Smart link

Version 1.0

07 June 2021

Disclaimer

This document contains proprietary & confidential information and is intended for the private use of IIFL. Reproduction or distribution without the express written permission of IIFL is strictly prohibited. This report is valid for the mentioned version of the application only. Any updation or modification beyond this version will invalidate this report.

Document Control

Application Detail

Application Name	SmartLink
Application Environment	UAT
Application URL	https://uat.iifl.com/smartlink/
Application Type	Web Application
Version	1.0

Distribution List

The following people hold authorized copies of this report.

Title	Name of Holder
CISO	Shanker Ramrakhiani
Action Requester (Spoke)	Nikhil Tembkar

Document History

Version	Report Date	Prepared & Tested by	Approved by	Remark
1.0	07-June-2021	Sonu Chaudhary	Kailash Gaonkar	

Index

Table to Content

1. Vulnerability Findings

In Scope	https://uat.iifl.com/smartlink/

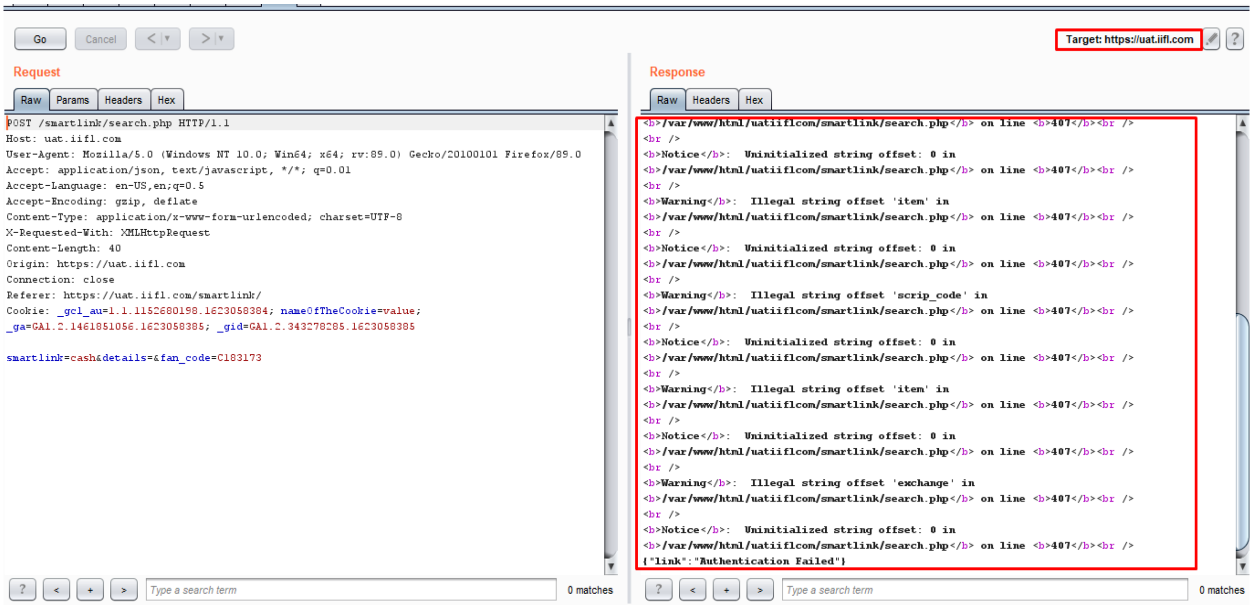
Sr No.	Severity	Vulnerability Name
1	**Low**	Internal URL Disclosure
2	**Low**	Cookie without secure flag

Out of Scope	

2. Comprehensive Vulnerability Details

1	Vulnerability Name	Internal URL Path Disclosure
	Vulnerable URL	https://uat.iifl.com/smartlink/
	Vulnerable Parameter	URL
	Severity	Low
	Description	Possible Internal Path Disclosure in the webpage. This can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.
	Impact	This information might help an attacker gain more information to see the full path of record and the exploiter can utilize this data for misusing some different vulnerability like Local File Inclusion. Information about the generated exception and possibly source code, SQL queries, etc.
	Recommendations	Apply the changes to your web.config file to prevent information leakage by using custom error pages.
	Reference	https://www.valencynetworks.com/kb/internal-path-disclosure.html https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/internal-path-disclosure-windows/

Proof of Concept (POC)



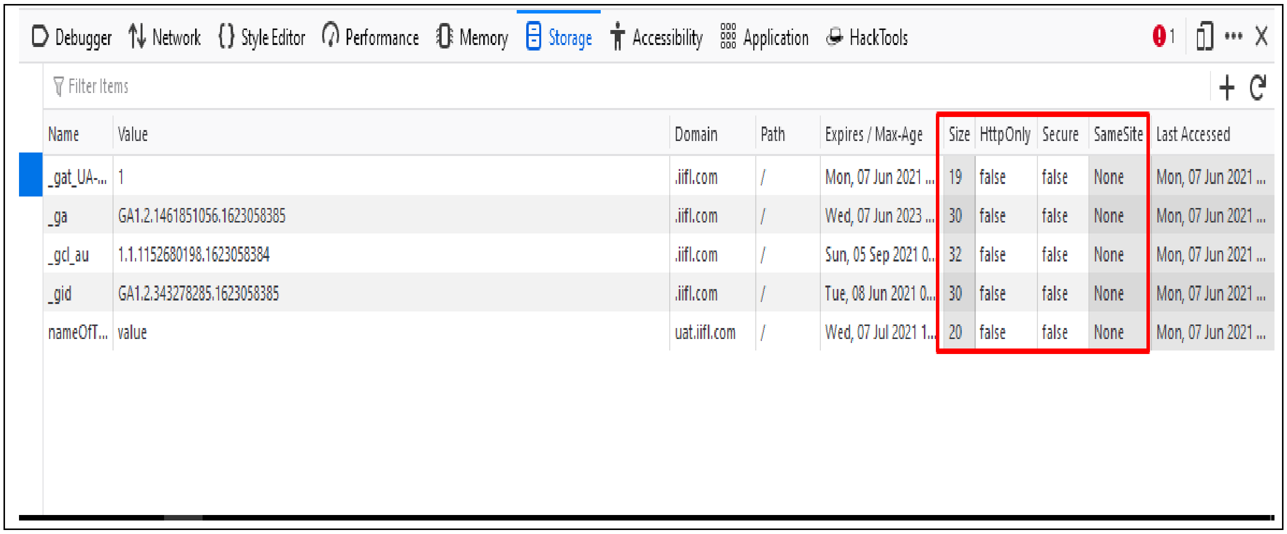
```
POST /smartlink/search.php HTTP/1.1
Host: uat.iifl.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 40
Origin: https://uat.iifl.com
Connection: close
Referer: https://uat.iifl.com/smartlink/
Cookie: _gcl_au=1.1.1152680198.1623058384; nameOfTheCookie=value;
_ga=GA1.2.1461851056.1623058385; _gid=GA1.2.343278285.1623058385

smartlink=cash&details=&fan_code=C183173
```

```
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Notice</b>:  Uninitialized string offset: 0 in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Warning</b>:  Illegal string offset 'item' in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Notice</b>:  Uninitialized string offset: 0 in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Warning</b>:  Illegal string offset 'scrip_code' in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Notice</b>:  Uninitialized string offset: 0 in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Warning</b>:  Illegal string offset 'item' in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Notice</b>:  Uninitialized string offset: 0 in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Warning</b>:  Illegal string offset 'exchange' in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
<br />
<b>Notice</b>:  Uninitialized string offset: 0 in
<b>/var/www/html/uatiiflcom/smartlink/search.php</b> on line <b>407</b><br />
{"link":"Authentication Failed"}
```

1	Vulnerability Name	Cookie without secure flag
	Vulnerable URL	https://uat.iifl.com/smartlink/
	Vulnerable Parameter	URL
	Severity	Low
	Description	For application cookie not marked as Secure, and transmitted over HTTP. This means an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack could potentially steal the cookie.
	Impact	Cookie without Secure flag will be transmitted over a HTTP connection, therefore if this cookie is important (such as a session cookie), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie
	Recommendations	The Secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTP. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTP/ HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.
	Reference	[https://www.netsparker.com/web-vulnerability scanner/vulnerabilities/cookienot-marked-assecure/](https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/cookienot-marked-assecure/) https://odino.org/security-hardening-http-cookies/

Proof of Concept (POC)



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_gat_UA-...	1	.iifl.com	/	Mon, 07 Jun 2021 ...	19	false	false	None	Mon, 07 Jun 2021 ...
_ga	GA1.2.1461851056.1623058385	.iifl.com	/	Wed, 07 Jun 2023 ...	30	false	false	None	Mon, 07 Jun 2021 ...
_gcl_au	1.1.1152680198.1623058384	.iifl.com	/	Sun, 05 Sep 2021 0...	32	false	false	None	Mon, 07 Jun 2021 ...
_gid	GA1.2.343278285.1623058385	.iifl.com	/	Tue, 08 Jun 2021 0...	30	false	false	None	Mon, 07 Jun 2021 ...
nameOfT...	value	uat.iifl.com	/	Wed, 07 Jul 2021 1...	20	false	false	None	Mon, 07 Jun 2021 ...

1. OWASP Top 10

The Application Penetration testing include all the vulnerability in the OWASP Top 10 and the status of the application against those are depicted in the table below.

Category	OWASP Top 10 - 2017	Status
A1	Injection	Safe
A2	Broken Authentication	Safe
A3	Sensitive Data Exposure	Safe
A4	XML External Entities (XXE)	Safe
A5	Broken Access Control	Safe
A6	Security Misconfiguration	Unsafe
A7	Cross Site Scripting (XSS)	Safe
A8	Insecure Deserialization	Safe
A9	Using Components with Known Vulnerability	Safe
A10	Insufficient Logging & Monitoring	Safe
#	Miscellaneous	Safe

Note:- Please make sure Suggested/Recommended vulnerability Fixes need to be apply throughout application.

2. Severity Classification

*Throughout the document, each vulnerability or risk identified has been labeled as a finding and categorized as **High**, **Medium** or **Low**. These terms are defined below:*

Severity	Description
High	• The vulnerability may result in high risk exposure and should be addressed immediately. • The vulnerability may be exploited to compromise the system.
Medium	• The vulnerability may result in medium risk exposure and should be addressed as soon as possible. • The vulnerability may be exploited to compromise the system.
Low	• The vulnerability may result in low risk exposure and may be addressed in due time. • These vulnerabilities cannot compromise the system; these vulnerabilities coupled with other vulnerabilities may be exploited to compromise a part of an IT system.

Level of access required	**Ease of Exploitation**	**Impact**		
		High	**Medium**	**Low**
Internal **(Local Network)**	Easy	Medium	Medium	Low
	Moderate	Medium	Low	Low
	Difficult	Low	Low	Low
External **(Public Facing)**	Easy	High	High	Medium
	Moderate	High	Medium	Low
	Difficult	Medium	Medium	Low