INDUSFACE™ WAS

Web Application Audit Report

Draup

https://draup.com/

Confidential

Scan Date: 2024-09-30

INDUSFACE™ WAS

Scope

Application Audit for URL https://draup.com/

1. The entire test by automated scan was carried out with no prior knowledge of the systems and applications.
2. Indusface WAS does not carry out any DOS attacks and makes best effort to not run any exploits which can affect system vulnerability.
3. Indusface has conducted Application scan on web application using valid credentials.
4. Scope of Manual Penetration testing is to report single instance of an individual type of vulnerability required implementing global mitigation.

Confidentiality

This document contains sensitive and/or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained with in this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, Indusface WAS, assumes no liability for the completeness, use of, or conclusions drawn from such data.

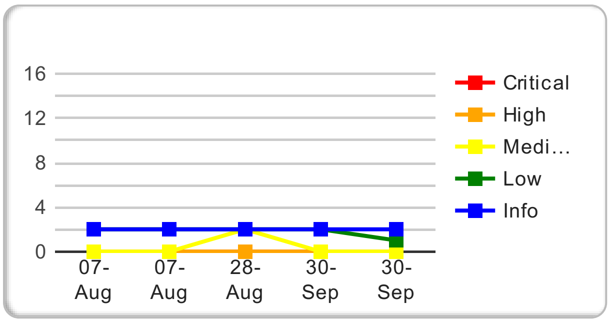
Disclaimer

This, or any other, Security Audit cannot and does not guarantee security. Indusface WAS makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that Indusface WAS shall be held harmless in any event. Indusface WAS makes this information available solely under its Terms of Service Agreement published at was.indusface.com.

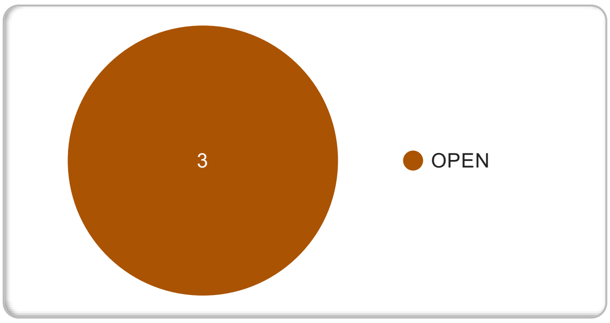
Executive Summary

Total type of vulnerabilities found	3
Total Places found to be vulnerable	3
Total number of instances of vulnerabilities identified	3

Vulnerability Trend



Open Vulnerabilities By Source



Vulnerability Instances

Severity	No of Places Found	No of Instances
Critical	0	0
High	0	0
Medium	0	0
Low	1	1
Info	2	2

Vulnerability Details

Manual Audit Summary

Title	No of Places Found	No of Instances
HTTP Verb Tampering	1	1
Running Service(Open Port)	1	1
Predictable Resource Location	1	1

Note : P tag in details section denotes vulnerability found through manual audit. These alerts won't be updated daily and will be updated only during next manual audit/re-audit.

OWASP Summary:

OWASP Category	Vulnerability Title	No of Places Found	No of Instances	Severity
A5: Security Misconfiguration	HTTP Verb Tampering	1	1	**Low**
A5: Security Misconfiguration	Running Service(Open Port)	1	1	**Info**
A5: Security Misconfiguration	Predictable Resource Location	1	1	**Info**

Detailed Report:

A5: Security Misconfiguration

1 :: HTTP Verb Tampering

Vul Type:	HTTP Verb Tampering	**No of Places Found:**	1
CVSS Score:	3.7	**No of Instances Reported:**	1
CVSS Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N		
CWE :	CWE-285: Improper Authorization		
Severity:	Low		
Reference:	<reference source="URL">https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/03-Testing_for_HTTP_Verb_Tampering</reference>		

Vulnerability Details:

HTTP Verb Tampering found in https://draup.com/

		Unique Alert ID	First Found Date	Last Reopened Date	URI
P	1	4145991	30th October 2023	-	https://draup.com/

Injected URL:
https://draup.com/

Vector:
INDUSFACE

Request:

```
INDUSFACE / HTTP/2
Host: draup.com
Cookie: accessible-products=sales,talent; _delighted_web={%224EkTbvvUpLAm1MRH%22:{%22_delighted_fst%22:{%22t%22:%221698635923729%22}}}; _gid=GA1.2.662666708.1698635929; _gat_gtag_UA_116543690_1=1; _ga=GA1.1.447542600.1698635929; _ga_YC0VFFTSBC=GS1.1.1698635929.1.1.1698641256.55.0.0
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="118", "Google Chrome";v="118", "Not=A?Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
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=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

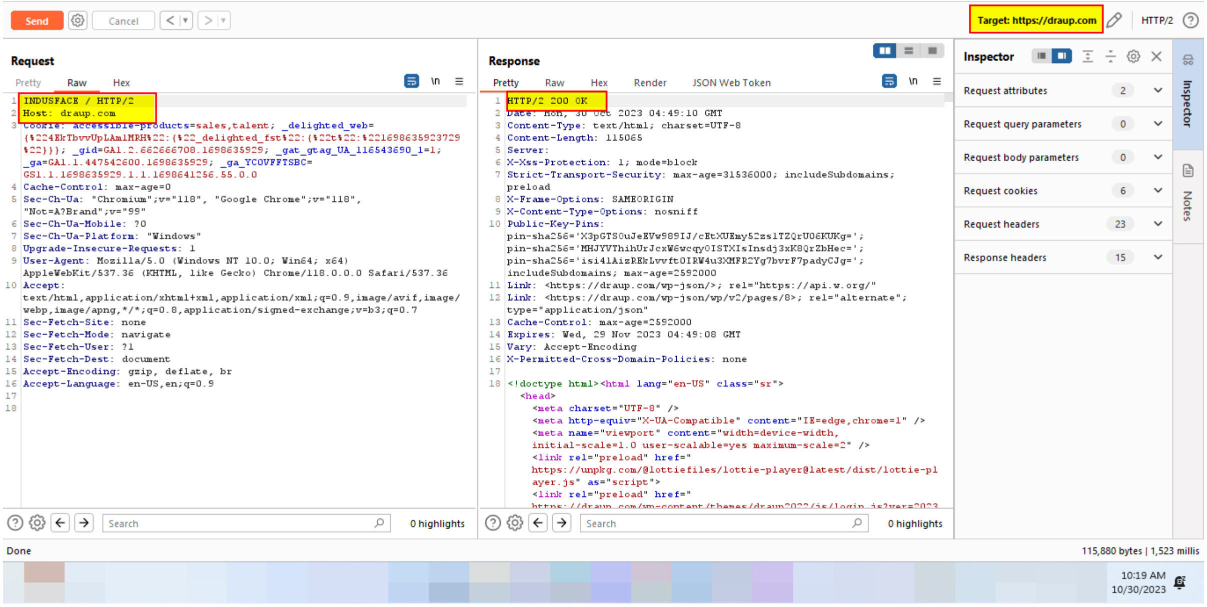
Response:
HTTP/2 200 OK
Date: Mon, 30 Oct 2023 04:49:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 115065
Server:
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Public-Key-Pins: pin-sha256='X3pGTSOuJeEVw989IJ/cEtXUEmy52zs1TZQrU06KUKg='; pin-sha256='MHJYVThihUrJcxW6wcqyOISTXIsInsdj3xK8QrZbHec='; pin-sha256='isi41AizREkLvvft0IRW4u3XMFR2Yg7bvrF7padyCJg='; includeSubdomains; max-age=2592000
Link: <https://draup.com/wp-json/>; rel="https://api.w.org/"
Link: <https://draup.com/wp-json/wp/v2/pages/8>; rel="alternate"; type="application/json"
Cache-Control: max-age=2592000
Expires: Wed, 29 Nov 2023 04:49:08 GMT
Vary: Accept-Encoding
X-Permitted-Cross-Domain-Policies: none

Result:
Arbitrary Methods enabled on server.

Business risk:
An attacker can use this information to craft further attacks.

POC Details :

POC 1: Observe the screenshot, Arbitrary method is enabled on server.



```
INDUSFACE / HTTP/2
Host: draup.com
Cookie: accessible-products=sales,talent; _delighted_web=
{%224EkTbvvUpLAmlMRH%22:{%22_delighted_fst%22:{%22t%22:%221698635923729
%22}}}; _gid=GA1.2.662666708.1698635929; _gat_gtag_UA_116543690_1=1;
_ga=GA1.1.447542600.1698635929; _ga_YCOVFFTSBC=
GS1.1.1698635929.1.1.1698641256.55.0.0
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="118", "Google Chrome";v="118",
"Not=A?Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
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=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
HTTP/2 200 OK
Date: Mon, 30 Oct 2023 04:49:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 115065
Server:
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubdomains;
preload
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Public-Key-Pins:
pin-sha256='X3pGTSOuJeEVw989IJ/cEtXUEmy52zs1TZQrU06KUKg=';
pin-sha256='MHJYVThihUrJcxW6wcqyOISTXIsInsdj3xK8QrZbHec=';
pin-sha256='isi41AizREkLvvft0IRW4u3XMFR2Yg7bvrF7padyCJg=';
includeSubdomains; max-age=2592000
Link: <https://draup.com/wp-json/>; rel="https://api.w.org/"
Link: <https://draup.com/wp-json/wp/v2/pages/8>; rel="alternate";
type="application/json"
Cache-Control: max-age=2592000
Expires: Wed, 29 Nov 2023 04:49:08 GMT
Vary: Accept-Encoding
X-Permitted-Cross-Domain-Policies: none

<!doctype html><html lang="en-US" class="sr">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <meta name="viewport" content="width=device-width,
    initial-scale=1.0 user-scalable=yes maximum-scale=2" />
    <link rel="preload" href="
    https://unpkg.com/@lottiefiles/lottie-player@latest/dist/lottie-pl
    ayer.js" as="script">
    <link rel="preload" href="
    https://draup.com/wp-content/themes/draup2022/js/login.js?ver=2023
```

2 :: Running Service(Open Port)

Vul Type:	Running Service(Open Port)	**No of Places Found:**	1
CVSS Score:	0	**No of Instances Reported:**	1
CWE :	CWE-16: Configuration		
Severity:	**Info**		
Description:	An open port is possible leading to data loss, DOS attack and other vulnerabilities.		
Solution:	Close unwanted port.		

Vulnerability Details:

Running Service(Open Port) found in https://draup.com

		Unique Alert ID	First Found Date	Last Reopened Date	URI
P	1	3479765	5th April 2022	-	https://draup.com

Injected URL:
https://draup.com

Vector:
NA

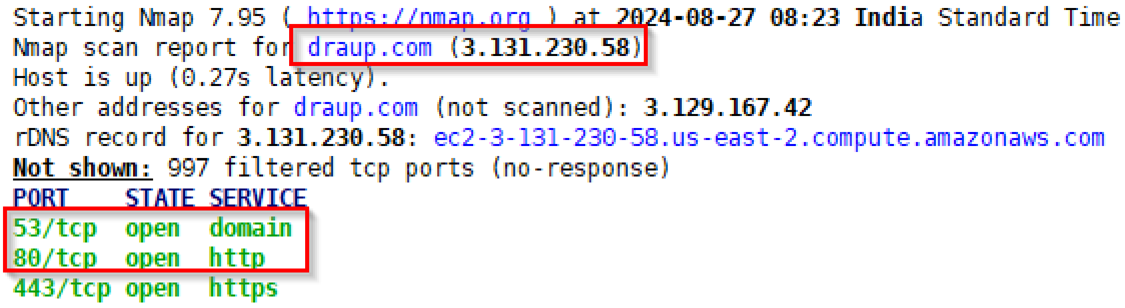
Request:
NA

Response:
NA

Result:
Unnecessary or unwanted ports are open and exposed. Step unnecessary services and close ports which are not required. Restrict the access of the ports which are required or filter such ports.

POC Details :

POC 1: Observe the screenshot, Port 53 & 80 are found to be open



```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-27 08:23 India Standard Time
Nmap scan report for draup.com (3.131.230.58)
Host is up (0.27s latency).
Other addresses for draup.com (not scanned): 3.129.167.42
rDNS record for 3.131.230.58: ec2-3-131-230-58.us-east-2.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
```

3 :: Predictable Resource Location

Vul Type:	Predictable Resource Location	**No of Places Found:**	1
CVSS Score:	0	**No of Instances Reported:**	1
CWE :	CWE-310: Cryptographic Issues		
Severity:	**Info**		
Reference:	http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location		

Vulnerability Details:

Predictable Resource Location found in https://draup.com/wp-admin/images/

		Unique Alert ID	First Found Date	Last Reopened Date	URI
P	1	4145994	30th October 2023	-	https://draup.com/wp-admin/images/

Injected URL:
https://draup.com/wp-admin/images/

Vector:
None

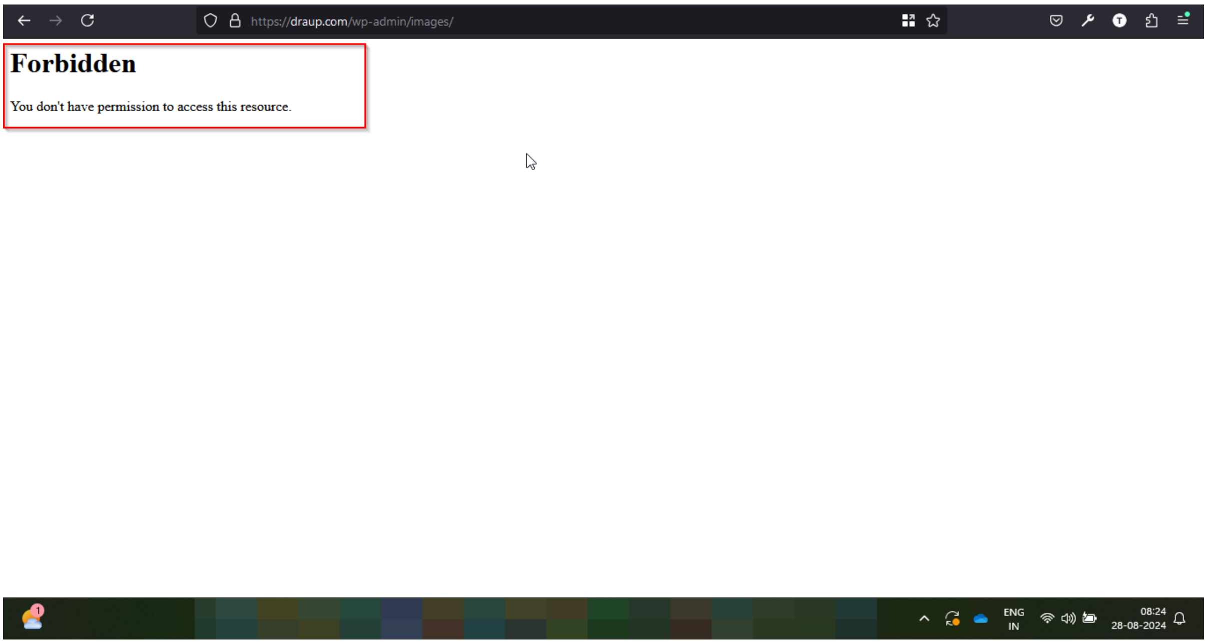
Request:
GET /wp-admin/images/ HTTP/2
Host: draup.com
Cookie: gnta2t25=2kg6ej1n2iz4; 1fgtj40p=e9txqcrdank4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://platform.draup.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-site
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

Response:
HTTP/2 403 Forbidden
Date: Wed, 28 Aug 2024 02:55:40 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 199
Server:
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Public-Key-Pins: pin-sha256='X3pGTSOuJeEVw989IJ/cEtXUEmy52zs1TZQrU06KUKg='; pin-sha256='MHJYVThihUrJcxW6wcqyOISTXIsInsdj3xK8QrZbHec='; pin-sha256='isi41AizREkLvvft0IRW4u3XMFR2Yg7bvrF7padyCJg='; includeSubdomains; max-age=2592000

Result:
Predictable Resource Location is an attack technique used to uncover hidden website content and functionality. By making educated guesses via brute-forcing an attacker can guess file and directory names not intended for public viewing. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc.

POC Details :

POC 1: Observe the screenshot, Resources can be predicted



https://draup.com/wp-admin/images/

Forbidden

You don't have permission to access this resource.