



SecureDapp

Your Cybersecurity Edge

VAPT SECURITY AUDIT of ARVO



VAPT Security Audit of ARVO

June 13th, 2025 | v. 1.1



TABLE OF CONTENT

AUDIT INTRODUCTION	3
AUDIT DOCUMENT	4
AUDIT SCOPE	4
AUDIT SUMMARY	8
AUDIT METHODOLOGY	9
FINDINGS SUMMARY:	10
DETAILED FINDINGS:	12
CONCLUSION:	36
DISCLAIMER	37
ABOUT SECURE DAPP	39



AUDIT INTRODUCTION

Auditing Firm	SecureDApp Auditors
Audit Architecture	Secure DApp Auditing Standard
Client Firm	ARVO
Website	https://onearvoventures.com/
Linkedin	https://www.linkedin.com/company/onearvoventures/
Twitter	https://x.com/one_ARVO

About SecureDApp

SecureDApp is a leader in security audits, offering advanced audits and run-time security solutions for projects.

SecureDApp is a Startup recognized by the Department For Promotion Of Industry And Internal Trade, Ministry of Commerce and Industry, Government of India. Powered by Vettedcode Technologies India Pvt. Ltd.



AUDIT DOCUMENT

Name	VAPT Security Audit Report for ARVO
Approved By	Himanshu Gautam CTO and Co-Founder @SecureDApp
Type	VAPT

AUDIT SCOPE

The Vulnerability Assessment and Penetration Testing (VAPT) for ARVO Services was conducted by SecureDApp with the following defined scope:

In-Scope Components:

The assessment focused on the following areas of ARVO Services:

Web Application Security Testing:

- Authentication & Authorization mechanisms (login, session management, role-based access).
- Input validation and business logic flaws (e.g., IDOR, account bypass).
- Security misconfigurations (headers, CORS, file uploads).
- API security (excessive data exposure, rate limiting).
- Frontend vulnerabilities (React Router issues, clickjacking).

Security Headers & Configurations:

- Missing or misconfigured headers (CSP, X-Frame-Options, HSTS, Referrer-Policy).
- Transport security (HTTPS enforcement, TLS weaknesses).
- Session Management:
- Session fixation, logout functionality, and token handling.



Data Exposure Risks:

- Unintended information leakage (server headers, API responses, error messages).

Limitations:

The VAPT assessment conducted for ARVO Services by SecureDApp was comprehensive, but it had certain limitations that may affect the scope and completeness of the findings:

Scope Restrictions:

- Only predefined systems, applications, and endpoints were tested. Any out-of-scope components (e.g., third-party integrations or internal backend systems) were not assessed.
- Testing was limited to the provided test environment, which may not fully replicate production conditions.

Testing Methodology:

- Automated tools were used for initial scanning, but manual validation was required for critical findings. Some vulnerabilities (e.g., logic flaws or business logic bypasses) may require deeper manual analysis.

Tools:

- **Burp Suite:**

Burp Suite is a powerful web vulnerability scanner and penetration testing tool used to identify and exploit security flaws in web applications. It includes features like a proxy server, scanner, repeater, and intruder for comprehensive testing.

- **Wappalyzer:**

Wappalyzer is a browser extension and online tool that identifies the technologies used by websites, such as content management systems, web servers, JavaScript frameworks, and analytics tools.

- **Security Headers:**



Security Headers is a web-based tool that analyzes a website's HTTP response headers and scores them based on their implementation of security-related headers like Content-Security-Policy, Strict-Transport-Security, and X-Frame-Options.

- **Nmap**

Nmap, short known for Network Mapper, is a free and open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify active devices on their networks, discovering hosts that are available and the services they offer, finding open ports and detecting security risks. 7.94 (Open Source)

- **Metasploit**

The Metasploit framework is a very powerful tool that can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. pentesting team can use ready-made or custom code and introduce it into a network to probe for weak spots. Version 6.4.x (Open Source)

- **Kali Linux**

Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. It preloaded with lot of web app security tools to do security assessment. 2024.1 (Open Source)



Review Scope

Application URL(s)	https://arvo.services/
--------------------	------------------------

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to asset loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions.
Medium	Medium-level vulnerabilities are important to fix; however, they cannot lead to asset loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that cannot have a significant impact on execution.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.



AUDIT SUMMARY

The SecureDApp team has performed a line-by-line manual analysis and automated review of the ARVO system. The system was analyzed mainly for common vulnerabilities, exploits, and manipulation hacks. According to the audit:

Status	Critical	High	Medium	Low
Open	0	0	4	3
Acknowledged	0	1	0	1
Resolved	2	1	4	1



AUDIT METHODOLOGY

SecureDApp performs Website VAPT to identify security weaknesses, validate exploitability, and recommend remediations. Below are the systematic steps used by SecureDApp to audit websites:

a. Information Gathering (Reconnaissance):

Understanding the target and collecting as much data as possible.

- i. WHOIS and DNS enumeration
- ii. Identifying technologies in use (CMS, frameworks, servers)
- iii. Subdomain enumeration and URL discovery
- iv. OSINT (Open Source Intelligence) for exposed information

b. Threat Modeling:

Analyzing gathered information to map the attack surface.

- i. Identifying entry points
- ii. Mapping user roles and access levels
- iii. Assessing business logic and sensitive functions

c. Vulnerability Scanning:

Using automated tools to detect known vulnerabilities.

Testing for:

- i. SQL Injection
- ii. Cross-Site Scripting (XSS)
- iii. Command Injection
- iv. Insecure Direct Object References (IDOR)
- v. Security Misconfigurations
- vi. Outdated components

d. Manual Testing:

Deep-dive testing to uncover logic flaws and vulnerabilities that scanners may miss.

- i. logic bypass
- ii. File upload/test bypass
- iii. Authentication and session management flaws
- iv. Custom script exploitation



FINDINGS SUMMARY:

SI.NO	Finding Title	Severity	Status
01	IDOR	Critical (C)	Closed
02	Account Bypass	Critical (C)	Closed
03	IDOR	High (H)	Closed
04	Excessive Data Exposure	High (H)	Acknowledged
05	Cross-origin resource sharing (CORS)	Medium (M)	Closed
06	Vulnerable React Router version	Medium (M)	Open
07	X-Frame-options header not enforced	Medium (M)	Closed
08	Referrer-policy not enforced	Medium (M)	Open
09	Clickjacking	Medium (M)	Closed
10	X-Content-type-options not enforced	Medium (M)	Open
11	Content security policy not enforced	Medium (M)	Open
12	No Rate Limit	Medium (M)	Closed
13	Strict transport security not enforced	Low (L)	Open



14	Permissions-Policy not enforced	Low (L)	Open
15	Unrestricted File Upload	Low (L)	Open
16	Improper session management	Low (L)	Closed
17	Excessive Server Information Exposure	Low(L)	Acknowledged



DETAILED FINDINGS:

Web-01: Insecure Direct Object Reference (IDOR)

Path/pointer/location: Login Page Packet

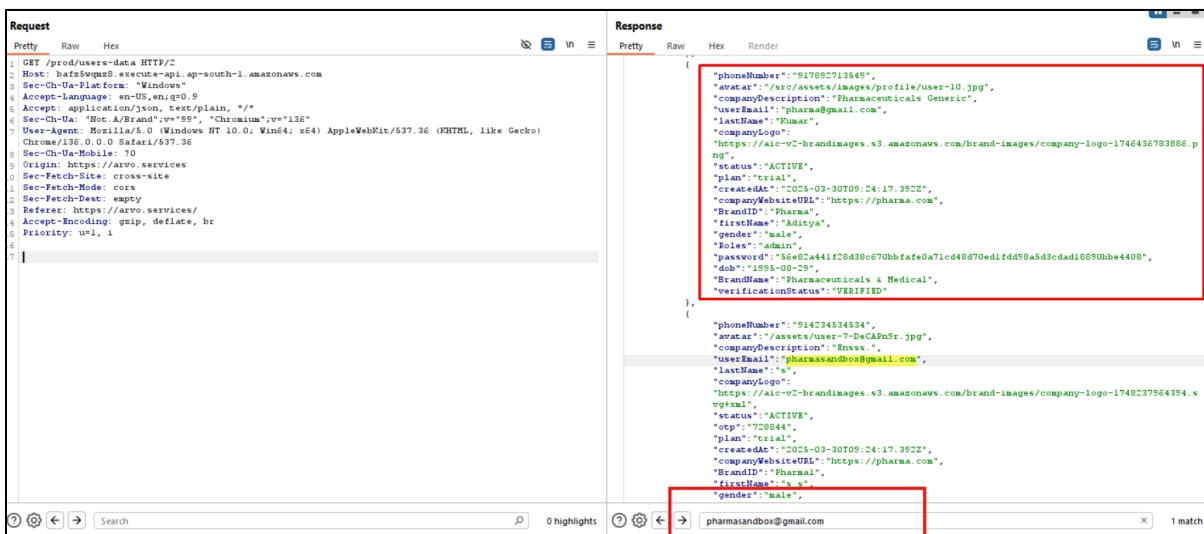
Severity: CRITICAL

CVSS: 9.1

Observation:

- It was observed that the application returns session or user data for all users during the authentication process without requiring any parameter manipulation by the attacker. Simply intercepting the authentication response reveals sensitive information about multiple users.
- This indicates a serious flaw in the application's access control mechanisms, where sensitive data is exposed globally rather than being restricted to the authenticated user only.

Proof of Concept:



The screenshot shows a network traffic analysis tool with two panes: 'Request' and 'Response'. The 'Request' pane shows a GET /prod/users-data HTTP/2 request with various headers, including Host, Sec-Ch-Ua-Platform, Accept-Language, Accept, User-Agent, and Sec-Ch-Ua-Mobile. The 'Response' pane shows a JSON object representing user data. Two user profiles are visible, both with the same sensitive information (phone number, avatar URL, company description, user email, last name, first name, gender, password, and birth date) repeated. The entire JSON object is highlighted with a red box.

```
Request
Pretty Raw Hex
GET /prod/users-data HTTP/2
Host: bat2wqgn8.execute-api.ap-south-1.amazonaws.com
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Device-Platform: "Windows", "Chromium": "136"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://arvo.services
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://arvo.services/
Accept-Encoding: gzip, deflate, br
Priority: u=1

Response
Pretty Raw Hex Render
{
  "phoneNumber": "917092713349",
  "avatar": "/src/assets/images/profile/user-10.jpg",
  "companyDescription": "Pharmaceuticals Generic",
  "userEmail": "pharma@gmail.com",
  "lastName": "Kumar",
  "firstName": "Ranu",
  "companyLogo": "https://s3-v2-brandimages.s3.amazonaws.com/brand-images/company-logo-1746436783086.png",
  "status": "ACTIVE",
  "plan": "trial",
  "createdAt": "2025-03-30T09:24:17.392Z",
  "companyWebsiteURL": "https://pharma.com",
  "BrandID": "Pharma",
  "firstName": "Aditya",
  "gender": "male",
  "lastName": "Aditya",
  "password": "56e02a41f28d38c670bfafe0a71cd48d70ed1fdd59a5d3cdad10050bfe4400",
  "dob": "1995-06-25",
  "BrandName": "Pharmaceuticals & Medical",
  "verificationStatus": "VERIFIED"
},
{
  "phoneNumber": "914234534534",
  "avatar": "/assets/user-7-DeCapnSr.jpg",
  "companyDescription": "Enss",
  "userEmail": "pharmasandbox@gmail.com",
  "lastName": "A",
  "firstName": "A",
  "companyLogo": "https://s3-v2-brandimages.s3.amazonaws.com/brand-images/company-logo-174037564394.svg",
  "status": "ACTIVE",
  "plan": "trial",
  "createdAt": "2025-03-30T09:24:17.392Z",
  "companyWebsiteURL": "https://pharma.com",
  "BrandID": "Pharma",
  "firstName": "A",
  "gender": "male",
  "lastName": "A"
}
```

**Impact:**

Attackers can intercept the authentication request and exploit an IDOR vulnerability to access session data of other users. This results in unauthorized disclosure of sensitive information.

Remediation:

Implement strict session isolation to ensure each user session is uniquely and securely scoped. Avoid exposing user identifiers or session metadata in client-side responses. Additionally, validate and sanitize all session-related data server-side, and use secure, short-lived session tokens with proper access controls to prevent unauthorized access.



Web-02: Account Bypass

Path/pointer/location: My Profile → Edit Page Packet

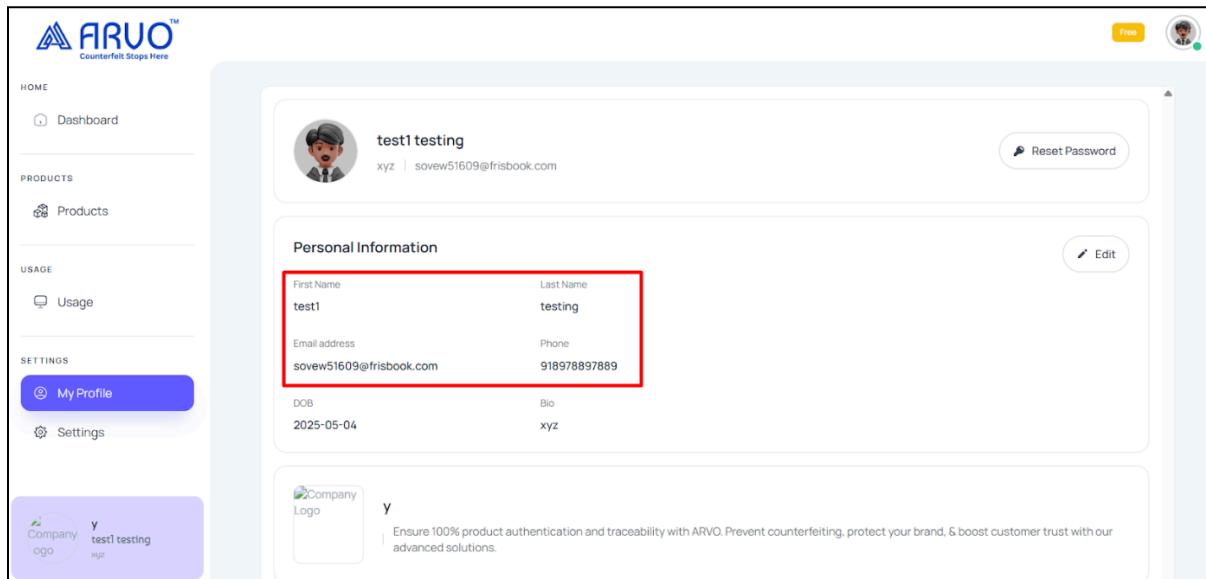
Severity: CRITICAL

Observation:

- It was observed that the application does not properly validate user authorization when updating profile information. By intercepting the profile update request and changing the user identifier (e.g., user ID), an attacker can successfully modify another user's profile details.
- This indicates a lack of proper access control on sensitive update operations.

Proof of Concept:

1) Before Modifying



Personal Information

First Name	Last Name
test1	testing
Email address	Phone
sovew51609@frisbook.com	918978897889



AIC - ARVO Integrated Cloud test1 testing

<https://arvo.services/profile>

Personal Information
Please provide your personal information to keep your profile up-to-date.

First Name: test1

Last Name: testing

Email: sovew51609@frisbook.com

Phone: 918978897889

Company Description:
Ensure 100% product authentication and traceability with ARVO. Prevent counterfeiting.

Close Save Changes

xyz

Edit

Company

Interception Forward Drop Open browser

Time Type Method URL Status code

Request

Pretty Raw Hex

```
1 PUT /prod/profile-edit HTTP/2
2 Host: j1txgtnvcva.execute-api.ap-south-1.amazonaws.com
3 Content-Length: 438
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="136"
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/136.0.0.0 Safari/537.36
11 Accept: */*
12 Origin: https://arvo.services
13 Sec-Fetch-Site: cross-site
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://arvo.services/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u1, i
19
20 {
21   "userEmail": "sovew51609@frisbook.com",
22   "firstName": "test1",
23   "lastName": "testing",
24   "phoneNumber": "918978897889",
25   "companyDescription": "Ensure 100% product authentication and traceability with ARVO. Prevent counterfeiting, protect your brand, & boost customer trust with our advanced solutions.",
26   "companyLogo": "https://aic-v2-brandimages.s3.amazonaws.com/brand-images/company-logo-1748252760126.svg+xml",
27   "avatar": "/assets/user-7-DeCAPn9r.jpg"
28 }
```

Interceptor
Notes



2) After Modifying

Target: <https://j1txgtnx.com>

Request	Response
<pre>Pretty Raw Hex PUT /prod/profile-edit HTTP/2 Host: j1txgtnx.com.execute-api.ap-south-1.amazonaws.com Content-Length: 439 Sec-Ch-Ua-Platform: "Windows" Accept-Language: en-US,en;q=0.9 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="136" Content-Type: application/json Sec-Ch-Ua-Mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Accept: */* Origin: https://arvo.services Sec-Fetch-Site: same-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://arvo.services/ Accept-Encoding: gzip, deflate, br Priority: u=1, i ("userEmail": "sovew51609@frisbook.com", "firstName": "Sovew", "lastName": "frisbook", "phoneNumber": "918978897623", "companyDescription": "Ensure 100% product authentication and traceability with ARVO. Prevent counterfeiting, protect your brand, & boost customer trust with our advanced solutions.", "companyLogo": "https://alc-v2-brandimages.s3.amazonaws.com/brand-images/company-logo-1748252760126.svg+xml", "avatar": "/assets/user-7-DeCPnSr.jpg")</pre>	<pre>Pretty Raw Hex Render X-Amzn-Requestid: d298063c-0bcc-4080-995b-0083bb420504 Access-Control-Allow-Origin: * Access-Control-Allow-Headers: Content-Type X-Amz-Apigv-Id: LQ4JGKXhvECIA= Access-Control-Allow-Methods: OPTIONS,PUT X-Amzn-Trace-Id: Root=1-6036a05a-6a6b2af31ee59dc38a51a5;Parent=388a0300cc62dced;Sampled=0;Lineage=1;fd60a9e3:0 { "message": "User updated successfully", "updatedAttributes": ["phoneNumber": "918978897623", "avatar": "/assets/user-7-DeCPnSr.jpg", "companyDescription": "Ensure 100% product authentication and traceability with ARVO. Prevent counterfeiting, protect your brand, & boost customer trust with our advanced solutions.", "userEmail": "sovew51609@frisbook.com", "lastName": "frisbook", "companyLogo": "https://alc-v2-brandimages.s3.amazonaws.com/brand-images/company-logo-1748252760126.svg+xml", "status": "ACTIVE", "otp": "116975", "createdAt": "2025-05-26T09:59:13.119Z", "companyWebsiteURL": "https://arvo.services/", "DPI": "100x100px", "firstName": "Sovew", "gender": "male", "Role": "sys", "password": "fileaf53cfc7fa09674be856ce4d10ec8d0b4cbf80ace81a5e75ab9f042950d9", "dob": "2025-05-04", "otpExpires": "2025-05-27T08:00:26.885Z", "BrandName": "y", "verificationStatus": "VERIFIED"] }</pre>

The screenshot shows the ARVO user profile page for 'Sovew frisbook'. The 'Personal Information' section is highlighted with a red box, showing the following fields: First Name (Sovew), Last Name (frisbook), Email address (sovew51609@frisbook.com), and Phone (918978897623). The 'DOB' field shows 2025-05-04. The 'Bio' field is empty (xyz). The 'Company Logo' field shows a placeholder image. A note at the bottom of the page reads: 'Ensure 100% product authentication and traceability with ARVO. Prevent counterfeiting, protect your brand, & boost customer trust with our advanced solutions.'

Impact:

An attacker can modify another user's profile details by intercepting and altering the request, leading to unauthorized account manipulation, data integrity issues, and potential account takeover.

Remediation:

Enforce strong server-side authorization checks to ensure users can only update their own profiles, validating the authenticated user's identity against the profile being modified before applying changes.



Web-03: Insecure Direct Object Reference (IDOR)

Path/pointer/location: Login Page Packet

Severity: HIGH

CVSS: 7.1

Observation:

- It was observed that the application does not enforce proper access controls on product data linked to brand identifiers. By manipulating the brand_id parameter in the request, an attacker can enumerate and access product information belonging to other brands, including unpublished or internal data.
- This indicates an Insecure Direct Object Reference (IDOR) vulnerability in the product lookup functionality.

Proof of Concept:

1) Before Modifying

Request	Response
<pre>Pretty Raw Hex GET /prod/all?brandId=Pharma1 HTTP/2 Host: xjehsfu59x.execute-api.ap-south-1.amazonaws.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Sec-Ch-Ua-Mobile: ?0 Accept: application/json, text/javascript, */*; q=0.01 Sec-Ch-Ua: "Not I/Brave";v="55";"Chromium";v="136" User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Sec-Ch-Ua-Mobile: ?0 Accept: application/json, text/javascript, */*; q=0.01 Sec-Ch-Ua: "Not I/Brave";v="55";"Chromium";v="136" Accept-Language: en-US,en;q=0.9 Accept-Encoding: gzip, deflate, br Priority: u4, i</pre>	<pre>Pretty Raw Hex Render 1: HTTP/2 200 OK 2: Date: Mon, 02 Jun 2025 07:04:52 GMT 3: Content-Type: application/json 4: Content-Length: 76 5: X-Amzn-TraceId: ha3957a-e07b-4b27-0d96-29493c89251b 6: Access-Control-Allow-Origin: * 7: Access-Control-Allow-Headers: Content-Type 8: X-Amz-ApiGateway-Id: Lhj7BHypBcvEFAw 9: Access-Control-Allow-Methods: OPTIONS,POST,GET,PUT 10: X-Amzn-TraceId: Root=1-683d4d12-715b0cb804f5e6c036362d3b;Parent=5a715f10522c3597;Sampled=0;Lineage=1:5d21b0ac:0 1: "message": "Orders for brandId='Pharma1' retrieved successfully", "items": [] }</pre>

2) After Modifying



Impact:

An attacker can enumerate and access product information by manipulating the brand_id, potentially exposing unpublished or internal data not intended for public view, leading to information leakage and unauthorized access.

Remediation:

Implement strict server-side access controls to validate user permissions and ensure only authorized, published product data is returned based on user roles and brand ownership.



Web-04: Excessive Data Exposure

Path/pointer/location: Login Page Packet

Severity: HIGH

CVSS: 7.5

Observation:

- It was observed that the login API response includes full user details such as name, email, phone number, and date of birth in plaintext.
- This sensitive information is exposed immediately upon successful authentication, enabling attackers to harvest user data through automated or replayed login attempts.

Proof of Concept:

Request	Response
<pre>1 POST /prod/auth HTTP/2 2 Host: wgn02rj8e.execute-api.ap-south-1.amazonaws.com 3 Content-Length: 84 4 Sec-Ch-Ua-Platform: "Windows" 5 Accept-Language: en-US,en;q=0.9 6 Accept: application/json, text/plain, */* 7 Sec-Ch-Ua-Mobile: no 8 Sec-Ch-Ua-Brand: "Android",v="55", "Chromium",v="136" 9 Content-Type: application/json 10 Sec-Ch-Ua-Mobile: 70 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 12 Chrome/120.0.0.0 Safari/537.36 13 Origin: https://arvo.services 14 Sec-Fetch-Site: cross-site 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Dest: empty 17 Referer: https://arvo.services/ 18 Accept-Encoding: gzip, deflate, br 19 Priority: u4, i 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 279 280 281 282 283 284 285 286 287 288 289 289 290 291 292 293 294 295 296 297 298 299 299 300 301 302 303 304 305 306 307 308 309 309 310 311 312 313 314 315 316 317 318 319 319 320 321 322 323 324 325 326 327 328 329 329 330 331 332 333 334 335 336 337 338 339 339 340 341 342 343 344 345 346 347 348 349 349 350 351 352 353 354 355 356 357 358 359 359 360 361 362 363 364 365 366 367 368 369 369 370 371 372 373 374 375 376 377 378 379 379 380 381 382 383 384 385 386 387 388 389 389 390 391 392 393 394 395 396 397 398 399 399 400 401 402 403 404 405 406 407 408 409 409 410 411 412 413 414 415 416 417 418 419 419 420 421 422 423 424 425 426 427 428 429 429 430 431 432 433 434 435 436 437 438 439 439 440 441 442 443 444 445 446 447 448 449 449 450 451 452 453 454 455 456 457 458 459 459 460 461 462 463 464 465 466 467 468 469 469 470 471 472 473 474 475 476 477 478 479 479 480 481 482 483 484 485 486 487 488 489 489 490 491 492 493 494 495 496 497 498 499 499 500 501 502 503 504 505 506 507 508 509 509 510 511 512 513 514 515 516 517 518 519 519 520 521 522 523 524 525 526 527 528 529 529 530 531 532 533 534 535 536 537 538 539 539 540 541 542 543 544 545 546 547 548 549 549 550 551 552 553 554 555 556 557 558 559 559 560 561 562 563 564 565 566 567 568 569 569 570 571 572 573 574 575 576 577 578 579 579 580 581 582 583 584 585 586 587 588 589 589 590 591 592 593 594 595 596 597 597 598 599 599 600 601 602 603 604 605 606 607 608 609 609 610 611 612 613 614 615 616 617 618 619 619 620 621 622 623 624 625 626 627 628 629 629 630 631 632 633 634 635 636 637 638 639 639 640 641 642 643 644 645 646 647 648 649 649 650 651 652 653 654 655 656 657 658 659 659 660 661 662 663 664 665 666 667 668 669 669 670 671 672 673 674 675 676 677 678 679 679 680 681 682 683 684 685 686 687 688 688 689 689 690 691 692 693 694 695 696 697 698 698 699 699 700 701 702 703 704 705 706 707 708 709 709 710 711 712 713 714 715 716 717 718 719 719 720 721 722 723 724 725 726 727 728 729 729 730 731 732 733 734 735 736 737 738 739 739 740 741 742 743 744 745 746 747 748 749 749 750 751 752 753 754 755 756 757 758 759 759 760 761 762 763 764 765 766 767 768 769 769 770 771 772 773 774 775 776 777 778 779 779 780 781 782 783 784 785 786 787 788 788 789 789 790 791 792 793 794 795 796 797 797 798 799 799 800 801 802 803 804 805 806 807 808 809 809 810 811 812 813 814 815 816 817 818 819 819 820 821 822 823 824 825 826 827 828 829 829 830 831 832 833 834 835 836 837 838 839 839 840 841 842 843 844 845 846 847 848 849 849 850 851 852 853 854 855 856 857 858 859 859 860 861 862 863 864 865 866 867 868 869 869 870 871 872 873 874 875 876 877 878 879 879 880 881 882 883 884 885 886 887 888 888 889 889 890 891 892 893 894 895 896 897 897 898 899 899 900 901 902 903 904 905 906 907 908 909 909 910 911 912 913 914 915 916 917 918 919 919 920 921 922 923 924 925 926 927 928 929 929 930 931 932 933 934 935 936 937 938 939 939 940 941 942 943 944 945 946 947 948 949 949 950 951 952 953 954 955 956 957 958 959 959 960 961 962 963 964 965 966 967 968 969 969 970 971 972 973 974 975 976 977 978 979 979 980 981 982 983 984 985 986 987 987 988 989 989 990 991 992 993 994 995 996 997 997 998 999 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1088 1089 1089 1090 1091 1092 1093 1094 1095 1096 1097 1097 1098 1099 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1188 1189 1189 1190 1191 1192 1193 1194 1195 1196 1197 1197 1198 1199 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1288 1289 1289 1290 1291 1292 1293 1294 1295 1296 1297 1297 1298 1299 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1388 1389 1389 1390 1391 1392 1393 1394 1395 1396 1397 1397 1398 1399 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1488 1489 1489 1490 1491 1492 1493 1494 1495 1496 1497 1497 1498 1499 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1588 1589 1589 1590 1591 1592 1593 1594 1595 1596 1597 1597 1598 1599 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1688 1689 1689 1690 1691 1692 1693 1694 1695 1696 1697 1697 1698 1699 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1788 1789 1789 1790 1791 1792 1793 1794 1795 1796 1797 1797 1798 1799 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1888 1889 1889 1890 1891 1892 1893 1894 1895 1896 1897 1897 1898 1899 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1988 1989 1989 1990 1991 1992 1993 1994 1995 1996 1997 1997 1998 1999 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2088 2089 2089 2090 2091 2092 2093 2094 2095 2096 2097 2097 2098 2099 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2149 </pre>	



Request	Response
<pre>1 POST /pre-prod/auth HTTP/2 2 Host: sed08fpf1.execute-api.ap-south-1.amazonaws.com 3 Content-Length: 113 4 Content-Type: application/json 5 Accept: application/json, text/plain, */* 6 Accept-Language: en-US,en;q=0.9 7 Sec-Ch-Ua: "Chromium";v="137", "Not/A Brand";v="24" 8 Content-Type: application/json 9 Content-Length: 113 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 11 Origin: https://arvo.services 12 Sec-Fetch-Site: cross-site 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Storage-Access: active 16 Referer: https://arvo.services/ 17 Accept-Encoding: gzip, deflate, br 18 Priority: u4, i 19 20 { "operation": "signin", "payload": { "userEmail": "pharmasandbox@gmail.com", "password": "Text@123" } }</pre>	<pre>1 HTTP/2 200 OK 2 Date: Fri, 13 Jun 2025 05:19:14 GMT 3 Content-Type: application/json 4 Content-Length: 113 5 X-Amzn-Requestid: d741dc0b-52d8-4740-a8f5-fe967817d20c 6 Access-Control-Allow-Origin: https://arvo.services 7 Access-Control-Allow-Headers: Content-Type, x-csrf-token 8 Set-Cookie: JSESSIONID=415f629343e40cd5e8faba3dd41cc6e208d0b3e793f14406eb6a; Path=/; Max-Age=604800; SameSite=None; Secure, csrfToken=d741dc0b-52d8-4740-a8f5-fe967817d20c; Path=/; Max-Age=604800; SameSite=None; Secure 9 X-Amz-Api-Inv-Id: MfvcvFNBcvWevgw 10 Access-Control-Allow-Methods: OPTIONS,POST,GET,DELETE,PUT 11 X-Amzn-Trace-Id: Root=1-604b4d1-77399bac6c59735665004520;Parent=0e382022f720b650;Sampled=0;Lineage=1:c5b3c21:0 12 Access-Control-Allow-Credentials: true 13 14 { "message": "Sign in successful", "csrfToken": "d741dc0b-52d8-4740-a8f5-fe967817d20c; Path=/; Max-Age=604800; SameSite=None; Secure", "user": { "email": "pharmasandbox@gmail.com", "firstName": "s", "lastName": "s", "role": "user", "avatar": "/assets/user-7-DeCAPn9r.jpg", "companyLogo": "https://a1c-v2.brandimages.s3.amazonaws.com/brand-images/company-logo-1740237864394.svg+xml", "brandId": "Pharma" } }</pre>

Impact:

The login API response exposes full user details (name, email, phone, DOB, etc.) in plaintext, allowing attackers to harvest sensitive data by replaying or automating login attempts.

• (CVE-2023-40662)

Remediation:

Limit API responses to minimal authentication tokens only; never expose user profile data during login. Implement strict access control and sanitize responses to avoid unnecessary data leakage.



Web-05: Cross-origin resource sharing (CORS)

Path/pointer/location: Login Page Packet

Severity: MEDIUM

CVSS: 6.8

Observation:

- It was observed that the server is configured to allow cross-origin requests from arbitrary or untrusted origins while Access-Control-Allow-Credentials is set to true.
- This insecure CORS configuration can allow attackers to perform unauthorized actions or access sensitive user data from another origin, potentially leading to privilege escalation and data leakage.

Proof of Concept:

Request	Response
<pre>1 GET /prod/ui-config?brandId=b0ed3c HTTP/2 2 Host: rdnh7dhuua.execute-api.ap-south-1.amazonaws.com 3 Sec-Ch-Ua-Platform: "Windows" 4 Accept-Language: en-US,en;q=0.9 5 Sec-Ch-Ua: "Not A/Brand";v="99", "Chromium";v="136" 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 7 Sec-Ch-Ua-Mobile: ?0 8 Accept: /* 9 Origin: https://arvo.services 10 Sec-Fetch-Site: cross-site 11 Sec-Fetch-Mode: cors 12 Sec-Fetch-Dest: empty 13 Referer: https://arvo.services/ 14 Accept-Encoding: gzip, deflate, br 15 Priority: u=1, i 16 17</pre>	<pre>1 HTTP/2 200 OK 2 Date: Mon, 02 Jun 2025 05:31:41 GMT 3 Content-Type: application/json 4 Content-Length: 561 5 Vary: X-Forwarded-For 6 X-Amzn-Request-Id: da7a163a-fd31-41d8-a7a7-08404039b3fb 7 Access-Control-Allow-Origin: * 8 Access-Control-Allow-Headers: Content-Type 9 X-Amz-Apigw-Id: LNWRDEKOBcvEfg= 10 Access-Control-Allow-Methods: OPTIONS,GET 11 X-Amzn-Trace-Id: Root=1-683d373c-2d440ce77c539dd31c996c40;Parent=243389c015b9c9a5;Sampled=0;Line age=1;3a734c4c:0 12 { 13 "qrTypes": [14 "QR_Codes" 15], 16 "updatedAt": "5/26/2025, 9:58:13 AM", 17 "cards": [18 "scans", 19 "batchdata", 20 "traceability" 21], 22 "usageMetrics": [23 "codes": 100, 24 "products": 4 25], 26 "tier": "Free", 27 "brandId": "b0ed3c", 28 "sh": "UI#CONFIG", 29 "subscriptionExpiry": "2035-05-26T09:59:13.184Z", 30 "sidebarNav": [31 { 32 "url": "/", 33 "label": "Dashboard" 34 }, 35 { 36 "url": "/Settings", 37 "label": "Settings" 38 } 39] 40 }</pre>

Impact:

Cross-origin resource sharing (CORS) enables browsers to perform cross domain requests in a controlled manner. This request has an Origin header that identifies the domain that is making the initial request and defines the protocol between a browser and server to see if the request is allowed.



An attacker can take advantage of this and possibly carry out privileged actions and access sensitive information when the Access-Control-Allow Credentials is enabled.

- **(CVE-2021-27786)**

Remediation:

Disable Access-Control-Allow-Credentials unless necessary, validate Origin headers and limit cross-origin sharing to trusted domains to mitigate risks.



Web-06: Vulnerable React Router version

Path/pointer/location: Login Page

Severity: MEDIUM

Observation:

- The application is using React Router version 7.5.0, which is a relatively recent release (as of early 2025), but may still contain unpatched or undiscovered security issues.
- Lack of updates increases the attack surface and risk of compromise.

Proof of Concept:

The screenshot shows the Wappalyzer tool interface. At the top, the URL 'arlo.services/auth/login' is displayed in a browser-like address bar. Below the address bar, the Wappalyzer logo is visible. The main content area is divided into sections: 'TECHNOLOGIES' (selected), 'MORE INFO', and 'Export' (with a download icon). The 'TECHNOLOGIES' section lists the following technologies:

JavaScript frameworks	CDN
React	Amazon S3
React Router 7.5.0	Amazon CloudFront

Below this, there are sections for 'Font scripts' (Google Font API) and 'PaaS' (Amazon Web Services). A link 'Something wrong or missing?' is also present at the bottom of the list.

Impact:



React-Router (Framework mode) processes the `X-React-Router-SPA-Mode` header, forcing Server-Side Rendering (SSR) pages into Single-Page Application (SPA) mode. This triggers an unhandled error, corrupting the page response. If cached, the poisoned response serves the error to all users, causing a denial-of-service (DoS) via cache poisoning. The attack requires a page using a `loader` function and a misconfigured cache layer storing error responses.

Remediation:

Upgrade to React-Router's latest version and make sure that all the headers must be sanitized.



Web-07: X-Frame-options header not enforced

Path/pointer/location: Security Header → X-Frame-options header not enforced

Severity: MEDIUM

CVSS: 6.3

Observation:

- The application does not enforce the X-Frame-Options header, which leaves it vulnerable to clickjacking attacks.
- In the absence of this header, the site can be embedded within a <frame> or <iframe> on a malicious site, potentially tricking users into performing unintended actions (e.g., clicking buttons or links without realizing it).
- This can lead to unauthorized actions, data leakage, or session hijacking under certain conditions.

Proof of Concept:

Security Report Summary	
	Site: https://arvo.services/
	IP Address: 3.162.140.129
	Report Time: 26 May 2025 06:41:09 UTC
Headers:	✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy

Impact:

Clickjacking, session hijacking, data exposure, and trust issues pose security and compliance threats. Implement header for protection.

- **(CVE-2022-3260)**

Remediation:

Implement X-Frame-Options header, use frame-busting scripts, and ensure strict iframe management to prevent these attacks effectively.



Web-08: Referrer-policy not enforced

Path/pointer/location: Security Header → Referrer-policy not enforced

Severity: MEDIUM

CVSS: 5.3

Observation:

- The application does not enforce the Referrer-Policy HTTP header, which may lead to unintended leakage of sensitive information (such as full URLs, query parameters, or paths) to third-party websites via the Referrer header.
- Absence of this header weakens user privacy and increases the risk of information disclosure in cross-origin requests.

Proof of Concept:

Security Report Summary	
	Site: https://arvo.services/
	IP Address: 3.162.140.129
	Report Time: 26 May 2025 06:41:09 UTC
Headers:	✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy

Impact:

If a document's Referrer Policy attribute is set to "no-referrer" sometimes two network requests are made for elements instead of one. One of these requests includes the referrer instead of respecting the set policy to not include a referrer on requests.

- (CVE-2017-7842)

Remediation:

Implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.



Web-09: Clickjacking

Path/pointer/location: Login Page

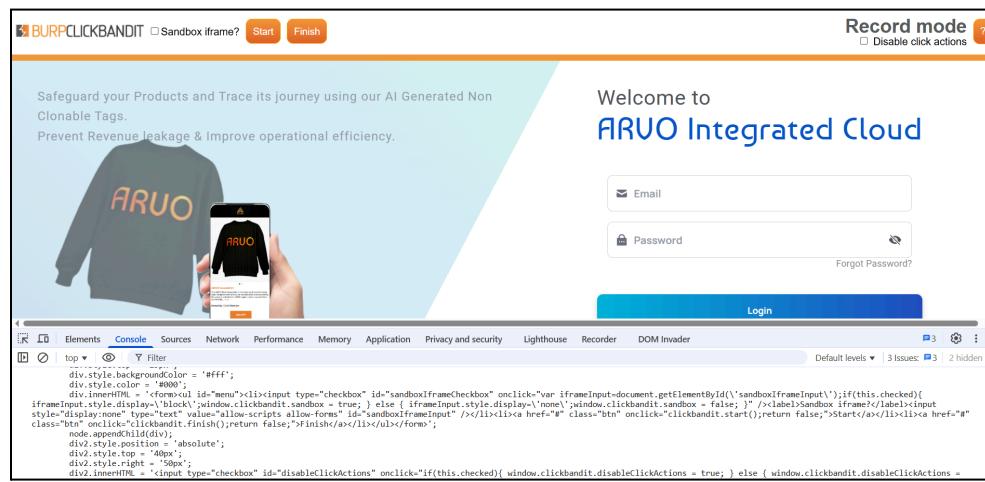
Severity: MEDIUM

CVSS: 5.0

Observation:

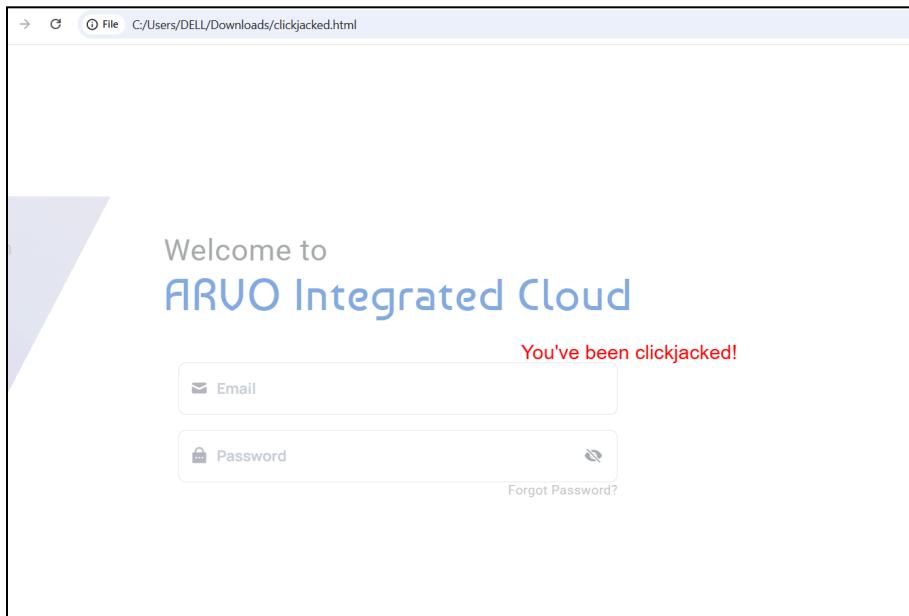
- The application is vulnerable to clickjacking if it does not implement proper framing protections using security headers like X-Frame-Options or Content-Security-Policy (frame-ancestors).
- This attack can lead to unauthorized actions, such as changing settings, making transactions, or revealing sensitive information.

Proof of Concept:



The screenshot shows a Burp Suite interface with the following details:

- Record mode:** Enabled (indicated by the orange button).
- Console Tab:** Shows the raw HTML code of the page, which includes a checkbox for enabling Clickjacking protection.
- Page Content:**
 - Header:** Welcome to **ARVO Integrated Cloud**
 - Form:** Email, Password, and Login button.
 - Background Image:** A person holding a smartphone displaying the ARVO logo.
 - Text:** Safeguard your Products and Trace its journey using our AI Generated Non Clonable Tags. Prevent Revenue leakage & Improve operational efficiency.



Impact:

Clickjacking is an attack that occurs when an attacker uses a transparent iframe in a window to trick a user into clicking on an actionable item, such as a button or link, to another server in which they have an identical webpage.

- **(CVE-2021-35237)**

Remediation:

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.



Web-10: X-Content-type-options not enforced

Path/pointer/location: Security Header → X-Content-type-options not enforced

Severity: MEDIUM

Observation:

- The application does not enforce the X-Content-Type-Options header, which can allow browsers to perform MIME type sniffing on responses.
- Without this header, a browser may attempt to guess the content type of a resource, even if the Content-Type is incorrectly declared.

Proof of Concept:

Security Report Summary	
	Site: https://arvo.services/
	IP Address: 3.162.140.129
	Report Time: 26 May 2025 06:41:09 UTC
Headers:	✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy

Impact:

Risks content misinterpretation, increasing vulnerabilities like content spoofing and potential security breaches.

Remediation:

Set 'X-Content-Type-Options' to 'nosniff' in the HTTP response headers to prevent MIME-type sniffing vulnerabilities. X-Content-Type-Options.



Web-11: Content security policy not enforced

Path/pointer/location: Security Header → Content security policy not enforced

Severity: MEDIUM

CVSS: 6.3

Observation:

- The application does not enforce a Content-Security-Policy (CSP) header, which significantly weakens its defence against cross-site scripting (XSS), data injection, and content hijacking attacks.
- Without a CSP, browsers will accept and execute content from any source by default, which could lead to the execution of malicious code if an attacker injects a payload.

Proof of Concept:

Security Report Summary	
	Site: https://arvo.services/
	IP Address: 3.162.140.129
	Report Time: 26 May 2025 06:41:09 UTC
	Headers: ✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy

Impact:

Content Security Policy (CSP) is not applied correctly to all parts of multipart content sent with the "multipart/x-mixed-replace" MIME type. This could allow for script to run where CSP should block it, allowing for cross-site scripting (XSS) and other attacks. This vulnerability affects Firefox < 60.

- **(CVE-2018-5164)**

Remediation:

By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.



Web-12: No Rate Limit

Path/pointer/location: My Profile page → Reset password

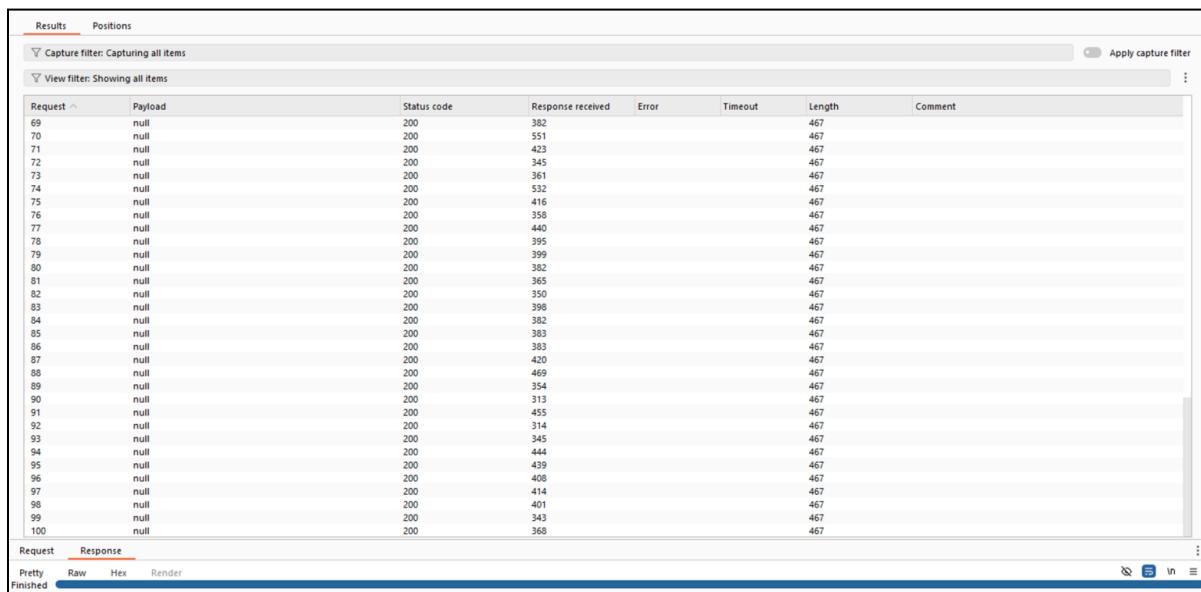
Severity: MEDIUM

Observation:

- It was observed that the application does not implement rate limiting on critical endpoints such as login or form submissions.
- As a result, attackers can send an unlimited number of requests without being blocked or throttled, enabling brute force attacks, spam, and abuse of functionality.

Proof of Concept:

1) Sending Request for 100 OTP's



The screenshot shows a network traffic capture interface with the 'Results' tab selected. A capture filter is set to 'Capturing all items'. The table displays 100 requests, each with a 'Request' number (69 to 100), a 'Payload' of 'null', a 'Status code' of '200', and a 'Length' of '467'. The 'Comment' column is empty. The interface includes a 'View filter: Showing all items' dropdown, an 'Apply capture filter' button, and a toolbar with 'Pretty', 'Raw', 'Hex', and 'Render' buttons. The status bar at the bottom shows 'Finished'.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
69	null	200	382			467	
70	null	200	551			467	
71	null	200	423			467	
72	null	200	345			467	
73	null	200	361			467	
74	null	200	532			467	
75	null	200	416			467	
76	null	200	358			467	
77	null	200	440			467	
78	null	200	395			467	
79	null	200	399			467	
80	null	200	382			467	
81	null	200	365			467	
82	null	200	350			467	
83	null	200	398			467	
84	null	200	382			467	
85	null	200	383			467	
86	null	200	383			467	
87	null	200	420			467	
88	null	200	469			467	
89	null	200	354			467	
90	null	200	313			467	
91	null	200	455			467	
92	null	200	314			467	
93	null	200	345			467	
94	null	200	444			467	
95	null	200	439			467	
96	null	200	408			467	
97	null	200	414			467	
98	null	200	401			467	
99	null	200	343			467	
100	null	200	368			467	

2) Receiving 100 OTP's



Impact:

No rate limit vulnerabilities allow attackers to perform brute force, spam, or abuse actions without restriction, leading to account compromise and service disruption.

Remediation:

Implement rate limiting, CAPTCHAs, and monitoring to restrict excessive requests and detect abusive behaviour.



Web-13: Strict transport security not enforced

Path/pointer/location: Security Header → Strict transport security not enforced

Severity: Low

Observation:

- The lack of this header weakens transport layer security and user trust, especially for login forms, sensitive data, and authenticated sessions.

Proof of Concept:

Security Report Summary	
	Site: https://arvo.services/
	IP Address: 3.162.140.129
	Report Time: 26 May 2025 06:41:09 UTC
Headers:	✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy

Impact:

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection.

Remediation:

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.



Web-14: Permissions-Policy not enforced

Path/pointer/location: Security Header → Permissions-Policy not enforced

Severity: Low

Observation:

- Without this policy, all supported features may be available by default, even if they are not required, which increases the attack surface and risks unauthorized access to sensitive device capabilities.
- The absence of this header may lead to privacy issues and unintended behaviours, especially in cross-origin iframes or embedded content.

Proof of Concept:

Security Report Summary	
	Site: https://arvo.services/
	IP Address: 3.162.140.129
	Report Time: 26 May 2025 06:41:09 UTC
Headers:	✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy

Impact:

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Remediation:

Enforce Permissions-Policy headers, limit web features, and enhance website security



Web-15: Unrestricted File Upload

Path/pointer/location: Sign in Page → Register

Severity: Low

Observation:

- It was observed that the application allows file uploads without properly validating file type, content, or extension.
- This lack of restriction enables attackers to upload malicious files, which can be executed on the server, potentially leading to remote code execution and full system compromise.

Proof of Concept:

1) File upload

The screenshot shows a web browser displaying the ARVO registration page at <https://arvo.services/auth/register>. The page has a light blue header with the ARVO logo and a sub-header: "We provide a flexible approach tailored to each brand's unique needs, offering a diverse range of solutions to effectively address authentication challenges." Below this is a "Sustainability" section with a sub-header "Empowering brands to demonstrate sustainability practices directly to consumers through our platform, ensuring transparency and trust." A diagram at the bottom illustrates the "ARVO INTEGRATED CLOUD" architecture, showing various components like "Raw Material Procurement", "Inventory Management", "Quality Audit Inspection", "Production Scheduling", "Logistics", and "Retailer Integration". The main form area is titled "Create an account" and contains "Company info" fields for "Company Name" (value: "xyz") and "Upload Company Logo" (file selected: "newtest.svg", with a note: "SVG, PNG, JPG, or GIF (MAX. 800x400px)."). The "Company Description" field contains the value "uuuu6tflauly8urffdf7fdkfudacydysayc". A "Next" button is located at the bottom right of the form area.

2) File upload successful and moved to the next page



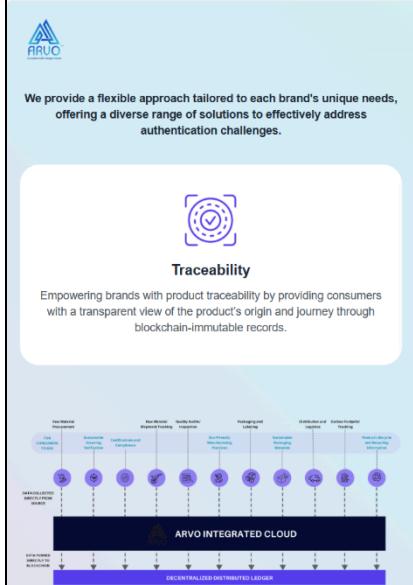
https://arvo.services/auth/register

ARVO

We provide a flexible approach tailored to each brand's unique needs, offering a diverse range of solutions to effectively address authentication challenges.

Traceability

Empowering brands with product traceability by providing consumers with a transparent view of the product's origin and journey through blockchain-immutable records.



Create an account

Person Info

First Name: Last Name:

Phone Number: Role or Position:

Select Gender: Date of Birth:

Choose an Avatar:

Backs **Next**

Impact:

Unrestricted file uploads can lead to severe security breaches, enabling attackers to upload and execute malicious files on the server. This can result in data breaches, remote code execution, and potentially complete compromise of the web application and server.

Remediation:

To mitigate unrestricted file upload risks:

- **Implement File Type Validation:** Restrict allowed file types to a specific whitelist and reject any other file types.
- **Implement File Size Limitations:** Set size limits for uploaded files to prevent denial of service attacks and conserve server resources.
- **Store Uploaded Files Securely:** Save uploaded files outside the web root directory, ensuring they can't be executed.



Web-16: Improper session management

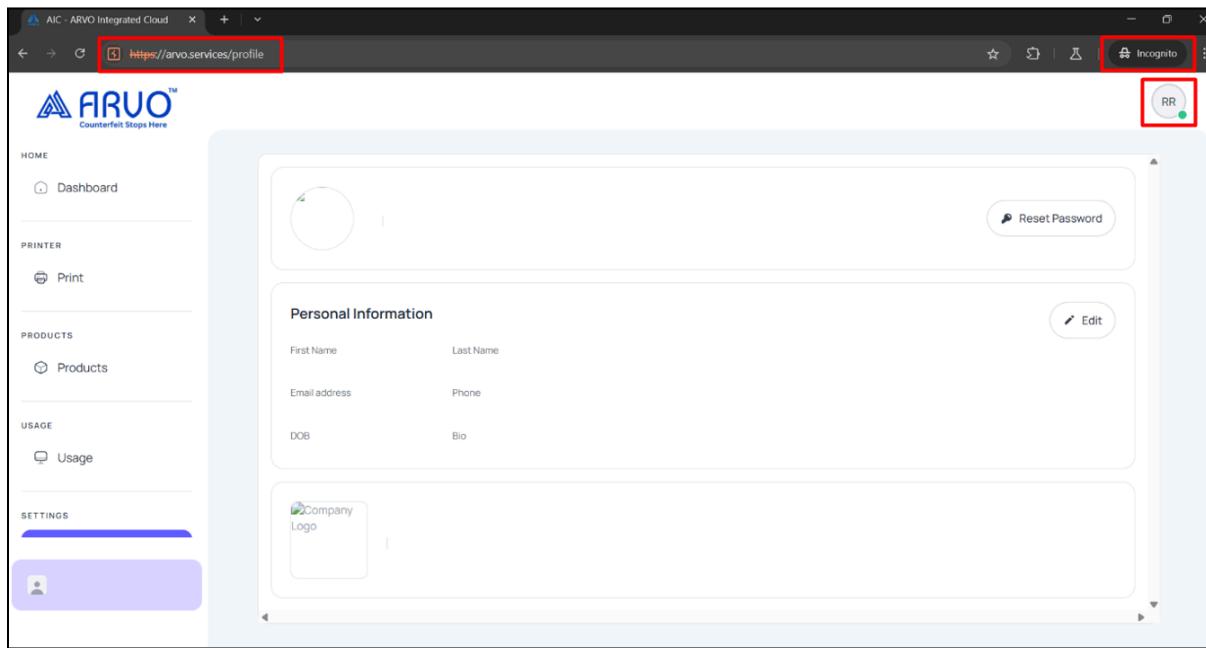
Path/pointer/location: arvo.services/profile

Severity: Low

Observation:

- It was observed that the /profile endpoint is accessible without authentication. Even after logging out, unauthenticated users can still view random user profiles, resulting in unauthorized access to sensitive personal information and serious privacy violations.

Proof of Concept:



Impact:

Unauthenticated users can access random user profiles via the /profile endpoint after logout, leading to serious data leakage and privacy violations.

Remediation:

Enforce strict authentication checks on protected routes and ensure server-side session tokens are properly invalidated upon logout.



Web-17: Excessive Server Information Exposure

Path/pointer/location: Login Page Packet

Severity: Low

Observation:

- In almost all the packages of ARVO website the sensitive API ID's are Displaying.
- It was observed that the application exposes internal headers such as X-Amzn-RequestId, X-Amz-Apigw-Id, and X-Amzn-Trace-Id in responses. These headers reveal internal system identifiers that could assist attackers in reconnaissance and potentially facilitate targeted attacks.

Proof of Concept:

Request	Response
<pre>Pretty Raw Hex 1 GET /prod/ui-config?brandId=b0ed3c HTTP/2 2 Host: rdnh7dhuua.execute-api.ap-south-1.amazonaws.com 3 Sec-Ch-Ua-Platform: "Windows" 4 Sec-Ch-Ua: "Not/A/Brand";v="99", "Chromium";v="136" 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 6 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 7 Sec-Ch-Ua-Mobile: ?0 8 Accept: */* 9 Origin: https://arvo.services 10 Sec-Fetch-Site: cross-site 11 Sec-Fetch-Mode: cors 12 Sec-Fetch-Dest: empty 13 Referer: https://arvo.services/ 14 Accept-Encoding: gzip, deflate, br 15 Priority: u=1, i 16 17</pre>	<pre>Pretty Raw Hex Render 1 HTTP/2 200 OK 2 Date: Mon, 02 Jun 2025 05:31:41 GMT 3 Content-Type: application/json 4 Content-Length: 551 5 X-Amzn-RequestId: da21192e-fd31-41d8-afe3-0840f039b3f8 6 Access-Control-Allow-Origin: * 7 Access-Control-Allow-Headers: Content-Type 8 X-Amz-Apigw-Id: LhWdAFR0BcwWEfgy 9 Access-Control-Allow-Methods: OPTIONS, GET 10 X-Amzn-Trace-Id: Root=1-03d3d373c-2d448ce77c539dd31c996c40;Parent=243385c01b9c9a5;Sampled=0;LinenAge=1:3a734c4c:0 11 12 { "qrTypes": ["QR Codes"], "updatedAt": "5/26/2025, 9:59:13 AM", "cards": ["scans", "batchdata", "traceability"], "usageMetrics": ["codes": 100, "products": 4], "tier": "Free", "brandId": "b0ed3c", "sh": "UI#CONFIG", "subscriptionExpiry": "2035-05-26T09:59:13.184Z", "sidebarNav": [{ "url": "/", "label": "Dashboard" }, { "url": "/Settings", "label": "Settings" }] }</pre>

After Patch (13/06/2025)



Impact:

Exposing headers like X-Amzn-RequestId, X-Amz-Apigw-Id, and X-Amzn-Trace-Id can provide attackers with internal identifiers that aid in reconnaissance, debugging, or chaining with other vulnerabilities for targeted attacks.

Remediation:

Configure the server or API gateway to suppress unnecessary internal headers in production responses, and ensure only essential information is exposed to end users.



CONCLUSION:

The Vulnerability Assessment and Penetration Testing (VAPT) of the ARVO web application identified a few areas of improvement, mainly concerning configuration settings, component updates, and authentication mechanisms. We are pleased to report that all critical vulnerabilities have been successfully remediated, along with the majority of high, medium, and low-severity findings—demonstrating the team's strong commitment to security. These proactive measures have notably enhanced the overall security posture of the application. To ensure continued protection against evolving threats, we recommend ongoing improvements and regular security assessments.



DISCLAIMER

SecureDApp provides clear and actionable cybersecurity assessments of web applications, APIs, cloud platforms, mobile apps, and enterprise systems. The findings in this report are based on industry-standard vulnerability assessment and penetration testing methodologies. While the report identifies known security risks and configuration issues, it makes no claim of guaranteeing absolute security or the complete absence of vulnerabilities.

This report is intended solely for the client's internal use. SecureDApp does not make any warranties or representations—express or implied—regarding the accuracy, completeness, reliability, or suitability of the information contained herein. The audit is limited to the scope defined at the time of engagement and does not extend to software dependencies, third-party services, user devices, or components outside of the testing environment.

Cybersecurity is inherently complex, and all assessments carry a degree of uncertainty. As such, this report may contain false positives or false negatives and should not be considered exhaustive. The client acknowledges and accepts that use of this report, and any associated materials or services, is at their own risk and on an “as-is,” “where-is,” and “as-available” basis.

CONFIDENTIALITY

This report is confidential and subject to the terms outlined in the service agreement between SecureDApp and the client. Distribution, disclosure, or reliance by any third party is strictly prohibited without prior written authorization from SecureDApp. All content within this report is the intellectual property of SecureDApp and is intended solely for the use of the intended recipient.

NO FINANCIAL OR LEGAL ADVICE

This cybersecurity assessment report is not an endorsement of any product, service, organization, or technology. It is provided purely for informational and technical purposes. It should not be interpreted as financial, legal, investment, or regulatory advice. SecureDApp does not accept liability for decisions made by third parties based on this report.

TECHNICAL DISCLAIMER

SecureDApp disclaims all warranties, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not guarantee that our findings will meet the client's specific goals, be error-free, or detect every potential threat or vulnerability. Compatibility, performance, and behavior of systems outside the testing scope are not covered.



TIMELINESS OF CONTENT

This report reflects the state of the application and infrastructure at the time of testing. SecureDApp does not commit to continuous updates or tracking of changes after delivery of the report. Security is a constantly evolving field, and new threats may arise at any time.

THIRD-PARTY LINKS

This report may reference third-party websites or tools. These links are provided for informational purposes only. SecureDApp is not responsible for the accuracy, functionality, or content of any external site and disclaims all liability for their use.



ABOUT SECURE DAPP

SecureDApp is a cybersecurity solutions provider focused on helping businesses safeguard their digital infrastructure through comprehensive security assessments and proactive threat mitigation. We specialize in identifying vulnerabilities across web applications, mobile apps, APIs, cloud platforms, and enterprise systems.

Our services include Vulnerability Assessments, Penetration Testing (VAPT), Secure Code Reviews, Security Architecture Consulting, DevSecOps integration, and threat modeling. Whether you are a startup or an enterprise, SecureDApp helps you build and maintain a resilient security posture.

Our team consists of seasoned security professionals, ethical hackers, engineers, and compliance experts distributed globally. We combine manual and automated testing methodologies to uncover potential weaknesses, misconfigurations, and security gaps before they can be exploited.

At SecureDApp, our mission is to deliver scalable, high-quality, and easy-to-integrate security services that empower organizations to operate safely and confidently in today's complex digital landscape.

To learn more, visit : <https://securedapp.in/>

To view our audit portfolio, visit : github.securedapp.in

To book an audit, message : securedapp.telegram



Securedapp.in



[Securedapp_Linkedin](https://www.linkedin.com/company/securedapp/)



[Securedapp_Telegram](https://t.me/Securedapp)