nova + DataQ Penetration Test Report - September 2025

Report generated on Oct 29 2025

Prepared for Power Digital Marketing by Cobalt. This report is for informational purposes, not for any other purpose, and may only be shared with third-parties by Power Digital Marketing. Cobalt disclaims all liability to any third-party arising from this report. Usage of this report by shall be subject to Cobalt's terms, available at https://cobalt.io/terms/.

Targets

app.novapower.io

app.dataq.ai

Test period

Aug 17, 2025 Sep 2, 2025

Status

Final

Test performed by

 Ahmad Shuja Lead

 Bernardo Diaz Pentester

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Contents

Executive Summary 4

Scope of Work 7

Approach 8

Risk Factors 9

Severity Definitions 9

Summary of Findings 11

Recommendations 16

Post-Test Remediation 17

Terms 20

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Executive Summary

Cobalt conducted a pentest of the nova + DataQ application and API to assess the risk posture and identify security issues that could negatively affect Power Digital Marketing's data, systems, or reputation. The scope of the assessment covered nova + DataQ and included credentials for various levels of privilege within the scope. A Cobalt pentest team of 2 conducted this engagement between Aug 18, 2025 and Sep 3, 2025.

This pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the Open Web Application Security Project (OWASP) Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

During this engagement, Cobalt's testers reported their findings and rated them based on the following severities:

	CRITICAL	HIGH	MEDIUM	LOW	INFO
Open	0	0	3	3	1
Resolved	2	4	0	0	0
Total	2	4	3	3	1

During the assessment, Cobalt identified a critical vulnerability related to privilege escalation via client-side role manipulation. This issue allowed a standard user to elevate privileges to "Super Admin" by modifying role parameters client-side. Such an escalation grants unrestricted access across the platform, enabling complete control over all user accounts, data, and administrative functionalities. This represents a direct compromise of confidentiality, integrity, and availability of

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

the application.

Cobalt also identified another critical vulnerability in the GraphQL layer: broken access control in the `deleteUser` mutation. This flaw enabled arbitrary deletion of user accounts through direct API requests without the proper authorization checks. The ability to delete any user, including administrators, could cause significant disruption to business operations, denial of service to clients, and potential permanent loss of critical account data.

High-severity vulnerabilities were identified across multiple GraphQL queries and mutations. The `users`, `contacts`, and `partners` queries exposed complete datasets without enforcing tenant-level authorization, resulting in unauthorized disclosure of sensitive records. In addition, testers confirmed site-wide unauthorized CRUD operations through GraphQL mutations such as `createPulse`, `updateContact`, `createPartner`, and `deletePartner`. These exposed internal-only functionalities to regular users, enabling actions that should not be available through the user interface. The combination of these flaws directly aligned with the client's concerns expressed prior to testing: unauthorized data access, exposure of internal features, and risk of large-scale API abuse.

Medium-severity issues included insecure direct object references (IDOR) in the data integration module, allowing cross-client access to sensitive client details, and stored client-side template injection that led to persistent cross-site scripting (XSS) in both the Profile and Audience modules. These vulnerabilities pose risks of data leakage, client impersonation, and malicious code execution in a victim's browser.

Low-severity findings included a weak password policy that permitted reuse of old or current passwords, verbose GraphQL error messages that disclosed internal schema information, and predictable user ID enumeration through insecure endpoints. Additionally, an informational issue was noted regarding weak SSL ciphers, which may reduce the overall security posture but does not pose an immediate exploitation path.

On the positive side, no vulnerabilities were observed in areas such as SQL injection (SQLi), remote code execution (RCE), server-side request forgery (SSRF), XML external entity injection (XXE), JSON

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

injection, CRLF injection, cache poisoning, host header injection, or JWT (JSON Web Token) implementation. The application also demonstrated good separation of certain tenant boundaries in non-GraphQL modules, and core authentication mechanisms were resistant to common bypass attempts.

Overall, the assessment highlighted systemic flaws in the GraphQL authorization model, with critical and high findings posing an immediate risk of full platform compromise. Addressing these issues should be the highest priority to prevent abuse of exposed APIs, unauthorized role escalation, and unrestricted data access.

The following findings were reported during the pentest:

- Privilege Escalation to Super-Admin via Client-Side Role Manipulation
- Critical Broken Access Control in GraphQL `deleteUser` Mutation Allowing Arbitrary User Deletion
- Site-Wide Unauthorized CRUD Access via GraphQL Mutations
- Authorization Bypass in GraphQL `users` Query Leading to Disclosure of All User Data
- Authorization Bypass in GraphQL `partners` Query Leading to Disclosure of All Partner Records
- Authorization Bypass in GraphQL `contacts` Query Leading to Disclosure of All Contact Records
- Insecure Direct Object Reference (IDOR) - External User Can Access Data Integration Module and Client Details for Another User
- Stored Client-Side Template Injection → Stored XSS in "Audience" module
- Stored Client-Side Template Injection → Stored XSS in Profile
- Information Disclosure via Verbose GraphQL Error Messages
- IDOR at app.novapower.io/users/`<user-id>`
- New Password can be the Same as the Current or Old Password
- SSL - Weak Ciphers in use

Specific recommendations were provided for each finding. As a whole, the recommendations indicate gaps that Power Digital Marketing can address by implementing secure input validation and making improvements to different misconfigurations and access control on the web application. These improvements include recommendations and security best practices that the Power Digital Marketing team should address to increase the overall security posture of the organization.

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Scope of Work

Target description

Application:

- nova + DataQ

Environment:

- Production

In-scope testing methodologies

Web application

Cobalt performed web application penetration testing according to our Web Application testing methodology. This methodology included a manual assessment of the security of the in-scope asset functionality and business logic, as well as testing for documented vulnerabilities, such as those listed in the OWASP API Top 10 or Common Vulnerabilities and Exposures (CVE) databases.

API

Cobalt performed API penetration testing according to our API testing methodology. This methodology included a manual assessment of the security of the in-scope asset functionality and business logic, as well as testing for documented vulnerabilities, such as those listed in the OWASP API Top 10 or Common Vulnerabilities and Exposures (CVE) databases.

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Approach

The engagement was done according to industry best practices. The following outlines the process from start to finish.

Pre Engagement

- Scoping
- Customer documentation
- Access

Engagement

- Reconnaissance
- Tool assisted assessment
- Manual assessment
- Vulnerability identification and/or exploitation
- Risk analysis
- Reporting

Post Engagement

- Prioritized remediation
- Recommendations
- Retesting (if applicable)

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Risk Factors

Each finding is assigned two factors to measure its risk. Factors are measured on a scale of 1 (very low) through 5 (very high).

Impact

This indicates the finding's effect on technical and business operations. It covers aspects such as the confidentiality, integrity, and availability of data or systems; and financial or reputational loss.

Likelihood

This indicates the finding's potential for exploitation. It takes into account aspects such as skill level required of an attacker and relative ease of exploitation.

Severity Definitions

When our pentesters find vulnerabilities, they use the standard OWASP Risk Rating Methodology, and then classify them into one of the following risk levels, based on their business impact and likelihood: `risk = impact * likelihood`

CRITICAL

Includes vulnerabilities that require immediate attention. Risk score of 25.

HIGH

Impacts the security of your application/platform/hardware, including supported systems. Includes high probability vulnerabilities with a high business impact. Risk score range: 16 through 24.

MEDIUM

Includes vulnerabilities that are: medium risk, medium impact; low risk, high impact; high risk, low impact. Risk score range: 5 through 15.

LOW

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Specifies common vulnerabilities with minimal impact. Risk score range: 2 through 4.

INFORMATIONAL

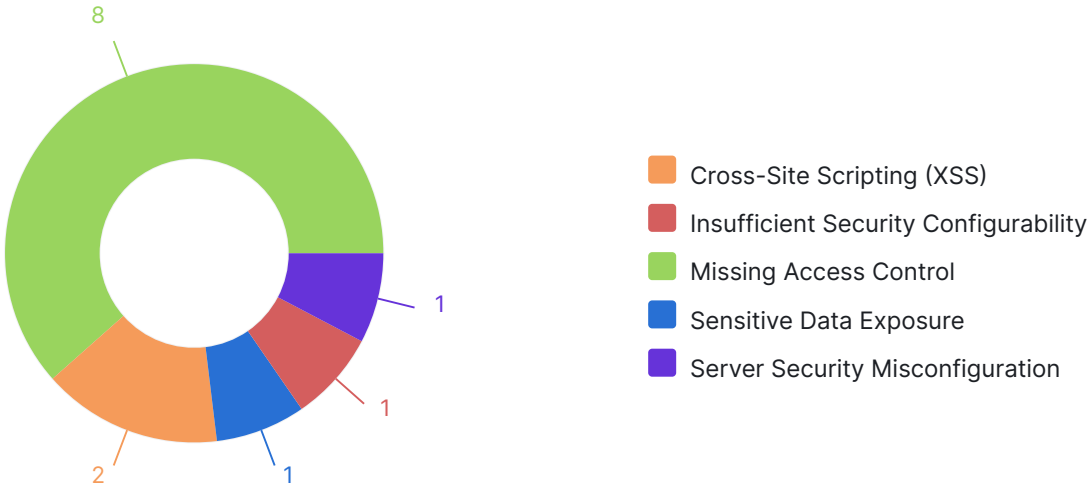
Notes vulnerabilities of minimal risk to your business. Risk score of 1.

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Summary of Findings

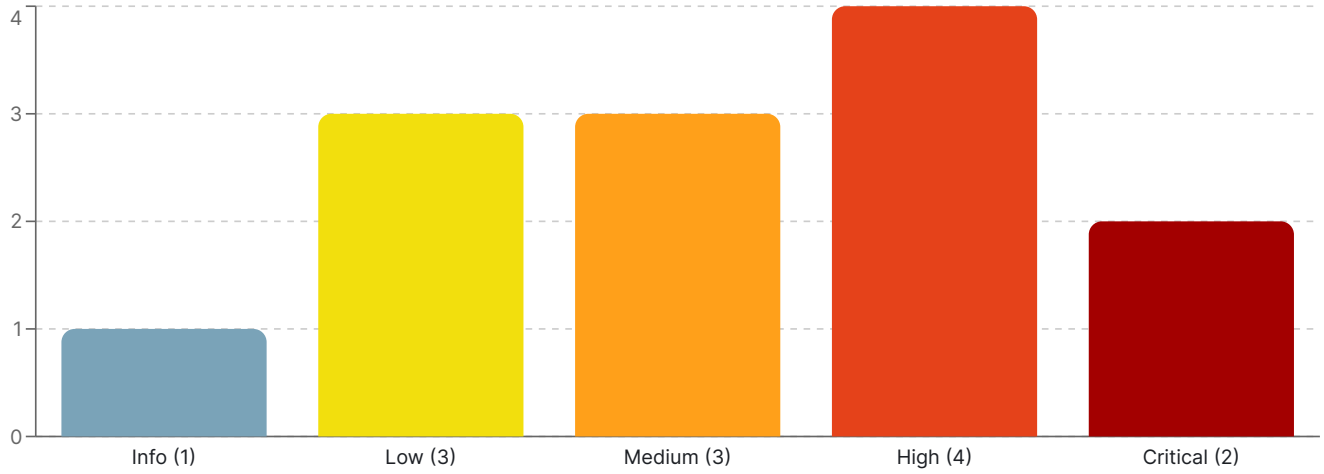
The following charts categorize the findings based on the type of finding and the estimated severity.

Findings by Type



© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Findings by Severity



Analysis

After vulnerability analysis, Cobalt reported the following findings:

Critical-risk findings:

- **Privilege Escalation to Super-Admin via Client-Side Role Manipulation**: The application relies on client-side role values without proper server-side enforcement, allowing an attacker to manipulate the response and escalate their privileges to Super Admin. (#PT32389_10)
- **Critical Broken Access Control in GraphQL `deleteUser` Mutation Allowing Arbitrary User Deletion**: The GraphQL API exposes a `deleteUser` mutation without proper authorization checks, allowing a low-privileged account to delete arbitrary users from the database. (#PT32389_9)

High-risk findings:

- **Site-Wide Unauthorized CRUD Access via GraphQL Mutations**: Multiple GraphQL mutations

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

and queries provide full Create, Read, Update, and Delete (CRUD) access to sensitive objects without enforcing proper authorization controls, allowing any authenticated low-privileged user to perform sensitive actions across the platform. (#PT32389_11)

- **Authorization Bypass in GraphQL `users` Query Leading to Disclosure of All User Data**: The application enforces access control at the UI level, but the underlying GraphQL requests can be directly queried to retrieve sensitive user data, disclosing all details despite the UI explicitly restricting access. (#PT32389_6)
- **Authorization Bypass in GraphQL `partners` Query Leading to Disclosure of All Partner Records**: The application enforces access control at the UI level, but the underlying GraphQL API fails to enforce the same restriction, allowing enumeration and download of sensitive data on all partner records. (#PT32389_7)
- **Authorization Bypass in GraphQL `contacts` Query Leading to Disclosure of All Contact Records**: The application enforces access control at the UI level, but the underlying GraphQL API fails to enforce the same restriction, allowing enumeration and download of all contact records from the system. (#PT32389_8)

Medium-risk findings:

- **Insecure Direct Object Reference (IDOR) - External User Can Access Data Integration Module and Client Details for Another User**: External users can manipulate the client ID in the GraphQL query to access another user's data, leading to wide exposure of sensitive data for multiple clients. (#PT32389_4)
- **Stored Client-Side Template Injection → Stored XSS in "Audience" module**: The application is vulnerable to stored cross-site scripting (XSS) in the "Audience" module due to a client-side template injection vulnerability. (#PT32389_2)
- **Stored Client-Side Template Injection → Stored XSS in Profile**: The application is vulnerable to stored cross-site scripting (XSS) in the profile section due to a client-side template injection vulnerability. (#PT32389_3)

Low-risk findings:

- **Information Disclosure via Verbose GraphQL Error Messages**: Although GraphQL introspection queries were disabled, the API still leaked valid schema details through verbose error messages. (#PT32389_5)

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

- **IDOR at app.novapower.io/users/<user-id>**: The application is vulnerable to Insecure Direct Object Reference (IDOR), allowing attackers to bypass authorization and directly access the names of all users. (#PT32389_1)
- **New Password can be the same as Current/Old password**: The application allows users to set a new password identical to their current or previously used password, undermining the purpose of a password change feature. (#PT32389_12)

Informational findings

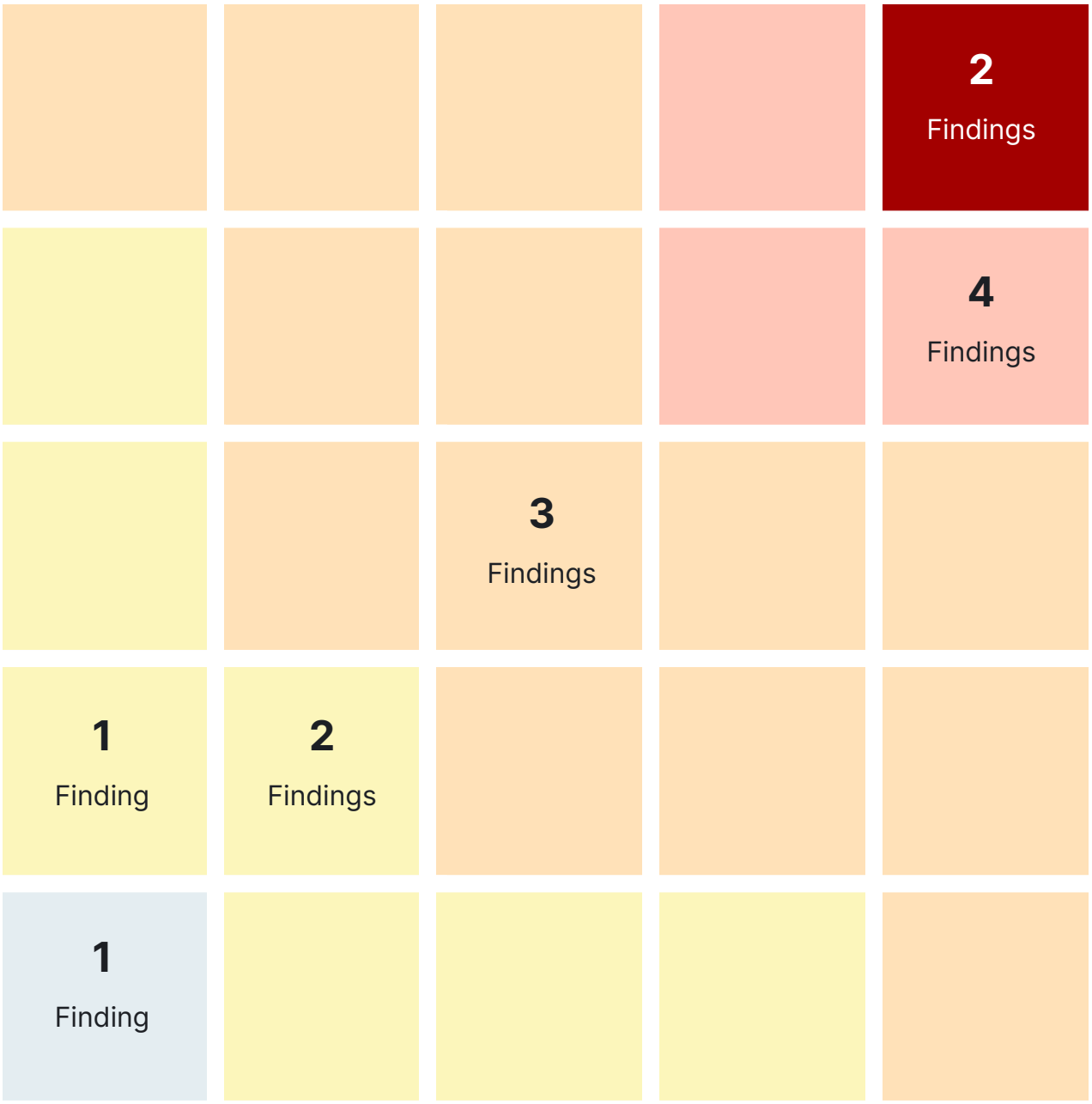
- **SSL - Weak Ciphers in use**: The software stores or transmits sensitive data using an encryption scheme that is theoretically sound but not strong enough for the level of protection required. (#PT32389_13)

General Risk Profile

The chart below summarizes vulnerabilities according to business impact and likelihood, increasing to the top right.

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Severity of Business Impact



Likelihood of Occurrence

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Recommendations

We recommend running regular security assessments to identify any vulnerabilities that are introduced after Power Digital Marketing makes configuration changes or implements new features. Based on the findings, Cobalt recommends the following remediation actions:

- Enforce server-side role validation and ignore client-supplied role parameters. (**#PT32389_10**)
- Implement strict authorization checks on all GraphQL mutations before execution. (**#PT32389_9**)
- Restrict access to GraphQL mutations with role-based access control and remove internal-only functions from the public schema. (**#PT32389_11**)
- Limit user enumeration and data exposure of users by enforcing least-privilege access controls. (**#PT32389_6**)
- Ensure only authorized and scoped users can access partner-related data in GraphQL queries. (**#PT32389_7**)
- Apply tenant-level access control checks on all GraphQL queries returning sensitive data. (**#PT32389_8**)
- Validate user ownership of requested objects and enforce proper authorization checks at the server. (**#PT32389_4**)
- Implement strict input validation and use safe templating methods to prevent XSS. (**#PT32389_2**)
- Sanitize and encode all template-rendered user inputs before storing or rendering. (**#PT32389_3**)
- Return generic error messages to users and log detailed errors only on the server side. (**#PT32389_5**)
- Restrict direct object access by validating user authorization against requested resources. (**#PT32389_1**)
- Disallow reuse of current or previous passwords by enforcing strong password history policies. (**#PT32389_12**)
- Disable weak SSL/TLS ciphers and enforce strong, modern encryption protocols. (**#PT32389_13**)

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Post-Test Remediation

All identified findings are below with their mitigation status.

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Finding	Type	Severity	State	Resolved
#PT32389_9	Missing Access Control	CRITICAL	Fixed	28 Oct 2025
#PT32389_10	Missing Access Control	CRITICAL	Fixed	28 Oct 2025
#PT32389_11	Missing Access Control	HIGH	Fixed	28 Oct 2025
#PT32389_8	Missing Access Control	HIGH	Fixed	28 Oct 2025
#PT32389_6	Missing Access Control	HIGH	Fixed	28 Oct 2025
#PT32389_7	Missing Access Control	HIGH	Fixed	28 Oct 2025
#PT32389_3	Cross-Site Scripting (XSS)	MEDIUM	Pending Fix	
#PT32389_4	Missing Access Control	MEDIUM	Pending Fix	
#PT32389_2	Cross-Site Scripting (XSS)	MEDIUM	Pending Fix	
#PT32389_1	Missing Access Control	LOW	Pending Fix	
#PT32389_5	Sensitive Data Exposure	LOW	Pending Fix	

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Finding	Type	Severity	State	Resolved
#PT32389_12	Insufficient Security Configurability	LOW	Pending Fix	
#PT32389_13	Server Security Misconfiguration	INFO	Pending Fix	

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Terms

PLEASE NOTE: It is impossible to test networks, information systems, and people for every potential security vulnerability. This report does not form a guarantee that your assets/targets are secured from any and all threats. All assessments performed, and their results, are only from the point-of-view of Cobalt, at the time of the engagement. Cobalt is unable to ensure or guarantee that your assets/targets are or will be completely safe from every form of attack now or in the future. With the ever-changing environment of information technology, any assessment performed by Cobalt will necessarily exclude vulnerabilities in software or systems that are unknown at the time of the engagement. For a full list of terms governing the services of Cobalt, this report, and the usage thereof, please consult the Terms of your Agreement with Cobalt or www.cobalt.io/terms.

© 2025 Cobalt Labs, Inc. | All Rights Reserved.