Security Assessment Report

Target:
Type: Internal Educational Assessment
Author: Josh Sullivan
Date: May 09, 2025
Version: 2.0

Executive Summary

This assessment evaluates the security posture of various [redacted] web assets from both authenticated and unauthenticated user perspectives. The focus was on identifying misconfigurations, access control flaws, and IDOR vulnerabilities that could be leveraged in real-world attack scenarios.

Scope

The assessment covered the following assets under the *.[redacted].com namespace:

dev.[redacted].com

[redacted].com

www.[redacted].com

Additional assets noted for future or partial testing:

autoupdate.[redacted].com

download2.[redacted].com

download.[redacted].com

live.[redacted].com

static2.[redacted].com

static.[redacted].com

www.live.[redacted].com

Vulnerability Summary Table

Vulnerability	Risk Level	Exploit Chain?	Notes
Host-based access control bypass via direct ip access on dev.[redacted].com	Medium	Yes	A suspected dev mirror of the main company website
Insecure Direct Object Reference on User Profile Pages	Low	Yes	Predictable user id allowing for profile enumeration

Vulnerability Details

Host-based access control bypass via direct ip access on dev domain.

Asset:

dev.[redacted].com

(also testable at https://<IP>/users/)

Issue Summary:

A misconfiguration in host-based access control allows unauthenticated users to access restricted resources on dev.[redacted].com by using the servers ip address instead of the domain name. This bypasses authentication checks and exposes internal or privileged endpoints.

Steps to Reproduce:

1. Navigate to dev.[redacted].com/users/
2. Here is where a restricted area login panel appears
3. Replace the url with ip address https://192.0.0.220/users/
4. Here you will see the dev mirror users page without the login restriction

Impact:

- Authentication or access control mechanisms are **bypassed** when accessing via IP.
- **Internal or restricted pages** intended only for authenticated users or developers become publicly accessible.

Supporting Evidence:

- figure 1: 03_dns_resolution.sh results
- figure 2: restricted area login page
- figure 3: restricted area bypass

Insecure Direct Object Reference on User Profile Pages

Asset:

https://[redacted].com/user/user5206/index.html
https://[redacted].com/user/user5205/index.html

Issue Summary:

The application allows direct access to user profile pages by manipulating the user ID in the URL. This results in **unauthenticated access to other users' profile pages**, exposing potentially sensitive data and enabling user enumeration.

Steps to Reproduce:

1. Login and navigate to your own profile at:
   https://[redacted].com/user/user5206/index.html
2. In Burp Suite (or any proxy), modify the URL to:
   https://[redacted].com/user/user5205/index.html
3. Observe that another user's profile page is returned **without authentication or authorization checks**.
4. Repeat the process by incrementing/decrementing the user ID to enumerate other users.

Impact:

1. **User Enumeration**: Attackers can cycle through user IDs to discover valid accounts.
2. **Information Disclosure**: If profile pages expose emails, usernames, or social data, this aids in social engineering or credential stuffing attacks.
3. **Potential Account Manipulation**: If similar numeric ID access is allowed for sensitive actions (e.g., POST/PATCH to /user/<id>/edit), this could escalate into **account takeover** or **privilege escalation**.

Supporting Evidence:

- figure 5: account 1 title
- figure 6: account 2 title

Recommendations

1. **Host-Based Access Control Bypass via Direct IP**
    a. NGINX: Use server_name directives and a default block that returns an error for unmatched IP-based requests.
    b. Add IP whitelisting where appropriate.
    c. Add logging and alerting for raw IP-based access to sensitive dev endpoints.
2. **Insecure Direct Object Reference (IDOR) on Profile Pages**
    a. Add rate limiting or behaviour analytics to detect rapid ID scanning.
    b. Consider using unguessable UUIDs or usernames in URLS rather than incremental ID's.

Appendix

figure 1: 03_dns_resolution.sh results (redacted)

figure 2: restricted area login page (redacted)

figure 3: restricted area bypass (redacted)

figure 5: account 1 title (redacted)

figure 6: account 2 title (redacted)