VALKYRIE

Security Assessment Report

Low miles no miles test #2

Target:	https://www.lowmilesnomiles.com
Test Date:	2026-01-13 11:02:03
Status:	COMPLETED
Report Generated:	2026-01-13 23:44:27

CONFIDENTIAL
This report contains sensitive security information and should be handled accordingly. Distribution should be limited to authorized personnel only.

Executive Summary

This security assessment was conducted on **https://www.lowmilesnomiles.com** on 2026-01-13 11:02:03. The assessment identified **100 security findings** across various severity levels.

Severity	Count	Risk Level
Critical	**20**	Immediate action required
High	**49**	Urgent remediation needed
Medium	**27**	Should be addressed
Low	**4**	Minor improvements

Key Findings:

1. Missing Security Header: Strict-Transport-Security [HIGH]
HSTS header missing - site is vulnerable to SSL stripping attacks

2. Missing Security Header: Content-Security-Policy [HIGH]
Content-Security-Policy header missing - site is vulnerable to XSS

3. Unrestricted HTTP Method: PUT [HIGH]
PUT method is accessible without proper restrictions on /category-sitemap.xml

Test Configuration

Test Name:	Low miles no miles test #2
Target URL:	https://www.lowmilesnomiles.com
Authentication:	NONE
Test Started:	2026-01-13 11:02:03
Test Completed:	2026-01-13 11:12:30
Test Status:	COMPLETED

Vulnerability Summary

Vulnerability Type	Count	Highest Severity
Broken Authentication	20	CRITICAL
Exposed Admin Panel	3	MEDIUM
Missing Authentication	19	HIGH
Missing Security Header	5	HIGH
No Rate Limiting	20	MEDIUM
Unencrypted Service	2	MEDIUM
Unrestricted Http Method	28	HIGH
Verbose Error	3	LOW

Detailed Findings

Finding 1: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/category-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/category-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 2: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET https://www.lowmilesnomiles.com/listing-sitemap.xml
Authorization: Bearer invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 3: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_category-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_category-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 4: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_color-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_color-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 5: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_condition-sitemap.xml`
Method:	`GET`

Vulnerability Type:	Broken Authentication
CVSS Score:	9.8

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_condition-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 6: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	https://www.lowmilesnomiles.com/listing_cylinder-sitemap.xml
Method:	GET
Vulnerability Type:	Broken Authentication
CVSS Score:	9.8

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_cylinder-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 7: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	https://www.lowmilesnomiles.com/listing_drive_type-sitemap.xml
Method:	GET
Vulnerability Type:	Broken Authentication
CVSS Score:	9.8

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_drive_type-sitemap.xml Authorization:
Bearer invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 8: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_feature-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_feature-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 9: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_fuel_type-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_fuel_type-sitemap.xml Authorization: Bearer
```

```
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 10: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_location-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_location-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 11: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_make-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_make-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 12: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_model-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_model-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 13: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_transmission-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_transmission-sitemap.xml Authorization:
Bearer invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 14: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/listing_type-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/listing_type-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 15: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/page-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET https://www.lowmilesnomiles.com/page-sitemap.xml
Authorization: Bearer invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 16: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/post-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET https://www.lowmilesnomiles.com/post-sitemap.xml
Authorization: Bearer invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 17: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/post_tag-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/post_tag-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 18: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/product_cat-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/product_cat-sitemap.xml Authorization: Bearer
```

```
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 19: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/product_tag-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/product_tag-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 20: Broken Authentication

SEVERITY: CRITICAL

Endpoint:	`https://www.lowmilesnomiles.com/wtb-listing-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Broken Authentication`
CVSS Score:	`9.8`

Description:

The endpoint accepts invalid authentication tokens.

Proof of Concept:

```
Request with invalid token: GET
https://www.lowmilesnomiles.com/wtb-listing-sitemap.xml Authorization: Bearer
invalid_token_12345 Response: 200
```

Remediation:

Properly validate all authentication tokens. Reject invalid tokens with 401 Unauthorized.

Finding 21: Missing Security Header: Strict-Transport-Security

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`GET`
Vulnerability Type:	`Missing Security Header`

Description:

HSTS header missing - site is vulnerable to SSL stripping attacks

Proof of Concept:

```
Request to https://www.lowmilesnomiles.com does not include
Strict-Transport-Security header
```

Remediation:

Add "Strict-Transport-Security: max-age=31536000; includeSubDomains" header

Finding 22: Missing Security Header: Content-Security-Policy

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`GET`
Vulnerability Type:	`Missing Security Header`

Description:

Content-Security-Policy header missing - site is vulnerable to XSS

Proof of Concept:

```
Request to https://www.lowmilesnomiles.com does not include Content-Security-Policy
header
```

Remediation:

Implement a Content-Security-Policy that restricts resource loading

Finding 23: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/category-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`

CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /category-sitemap.xml

Proof of Concept:

```
PUT /category-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 24: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/category-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /category-sitemap.xml

Proof of Concept:

```
DELETE /category-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 25: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing-sitemap.xml

Proof of Concept:

```
PUT /listing-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 26: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing-sitemap.xml

Proof of Concept:

```
DELETE /listing-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 27: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_category-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_category-sitemap.xml

Proof of Concept:

```
PUT /listing_category-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 28: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_category-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_category-sitemap.xml

Proof of Concept:

```
DELETE /listing_category-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 29: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_color-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_color-sitemap.xml

Proof of Concept:

```
PUT /listing_color-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 30: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_color-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_color-sitemap.xml

Proof of Concept:

```
DELETE /listing_color-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 31: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_condition-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_condition-sitemap.xml

Proof of Concept:

```
PUT /listing_condition-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 32: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_condition-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_condition-sitemap.xml

Proof of Concept:

```
DELETE /listing_condition-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 33: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_cylinder-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_cylinder-sitemap.xml

Proof of Concept:

```
PUT /listing_cylinder-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 34: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_cylinder-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_cylinder-sitemap.xml

Proof of Concept:

```
DELETE /listing_cylinder-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 35: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_drive_type-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_drive_type-sitemap.xml

Proof of Concept:

```
PUT /listing_drive_type-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 36: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_drive_type-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_drive_type-sitemap.xml

Proof of Concept:

```
DELETE /listing_drive_type-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 37: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_feature-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_feature-sitemap.xml

Proof of Concept:

```
PUT /listing_feature-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 38: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_feature-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_feature-sitemap.xml

Proof of Concept:

```
DELETE /listing_feature-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 39: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_fuel_type-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_fuel_type-sitemap.xml

Proof of Concept:

```
PUT /listing_fuel_type-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 40: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_fuel_type-sitemap.xml`

Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_fuel_type-sitemap.xml

Proof of Concept:

```
DELETE /listing_fuel_type-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 41: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_location-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_location-sitemap.xml

Proof of Concept:

```
PUT /listing_location-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 42: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_location-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_location-sitemap.xml

Proof of Concept:

```
DELETE /listing_location-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 43: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_make-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_make-sitemap.xml

Proof of Concept:

```
PUT /listing_make-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 44: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_make-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_make-sitemap.xml

Proof of Concept:

```
DELETE /listing_make-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 45: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_model-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_model-sitemap.xml

Proof of Concept:

```
PUT /listing_model-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 46: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_model-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_model-sitemap.xml

Proof of Concept:

```
DELETE /listing_model-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 47: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_transmission-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_transmission-sitemap.xml

Proof of Concept:

```
PUT /listing_transmission-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 48: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_transmission-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_transmission-sitemap.xml

Proof of Concept:

```
DELETE /listing_transmission-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 49: Unrestricted HTTP Method: PUT

SEVERITY: HIGH

Endpoint:	`/listing_type-sitemap.xml`
Method:	`PUT`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

PUT method is accessible without proper restrictions on /listing_type-sitemap.xml

Proof of Concept:

```
PUT /listing_type-sitemap.xml returns 200
```

Remediation:

Restrict PUT method to authenticated and authorized users only

Finding 50: Unrestricted HTTP Method: DELETE

SEVERITY: HIGH

Endpoint:	`/listing_type-sitemap.xml`
Method:	`DELETE`
Vulnerability Type:	`Unrestricted Http Method`
CVSS Score:	`7.5`

Description:

DELETE method is accessible without proper restrictions on /listing_type-sitemap.xml

Proof of Concept:

```
DELETE /listing_type-sitemap.xml returns 200
```

Remediation:

Restrict DELETE method to authenticated and authorized users only

Finding 51: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/category-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/category-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 52: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing-sitemap.xml`
Method:	`GET`

Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 53: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_category-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_category-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 54: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_color-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_color-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 55: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_condition-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_condition-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 56: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_cylinder-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_cylinder-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 57: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_drive_type-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_drive_type-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 58: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_feature-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_feature-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 59: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_fuel_type-sitemap.xml`

Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_fuel_type-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 60: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_location-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_location-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 61: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_make-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_make-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 62: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_model-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_model-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 63: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_transmission-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_transmission-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 64: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/listing_type-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/listing_type-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 65: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/page-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/page-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 66: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/post-sitemap.xml`

Method:	GET
Vulnerability Type:	Missing Authentication
CVSS Score:	7.5

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/post-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 67: Missing Authentication

SEVERITY: HIGH

Endpoint:	https://www.lowmilesnomiles.com/post_tag-sitemap.xml
Method:	GET
Vulnerability Type:	Missing Authentication
CVSS Score:	7.5

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/post_tag-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 68: Missing Authentication

SEVERITY: HIGH

Endpoint:	https://www.lowmilesnomiles.com/product_cat-sitemap.xml
Method:	GET
Vulnerability Type:	Missing Authentication
CVSS Score:	7.5

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/product_cat-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 69: Missing Authentication

SEVERITY: HIGH

Endpoint:	`https://www.lowmilesnomiles.com/product_tag-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`Missing Authentication`
CVSS Score:	`7.5`

Description:

The endpoint is accessible without any authentication.

Proof of Concept:

```
Request without Authorization header: GET
https://www.lowmilesnomiles.com/product_tag-sitemap.xml Response: 200
```

Remediation:

Implement authentication for all sensitive endpoints. Reject requests without valid credentials.

Finding 70: Missing Security Header: X-Frame-Options

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`GET`
Vulnerability Type:	`Missing Security Header`

Description:

X-Frame-Options header missing - site is vulnerable to clickjacking

Proof of Concept:

```
Request to https://www.lowmilesnomiles.com does not include X-Frame-Options header
```

Remediation:

Add "X-Frame-Options: DENY" or "X-Frame-Options: SAMEORIGIN" header

Finding 71: Missing Security Header: X-Content-Type-Options

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`GET`
Vulnerability Type:	`Missing Security Header`

Description:

X-Content-Type-Options header missing - browsers may MIME-sniff responses

Proof of Concept:

```
Request to https://www.lowmilesnomiles.com does not include X-Content-Type-Options
header
```

Remediation:

Add "X-Content-Type-Options: nosniff" header

Finding 72: Exposed Admin Panel: /admin/login

SEVERITY: MEDIUM

Endpoint:	`/admin/login`
Method:	`GET`
Vulnerability Type:	`Exposed Admin Panel`
CVSS Score:	`5.0`

Description:

Admin login panel is publicly accessible at /admin/login

Proof of Concept:

```
GET https://www.lowmilesnomiles.com/admin/login returns login form Page contains:
password, username, login
```

Remediation:

Protect admin panels with IP whitelisting, VPN, or additional authentication layer

Finding 73: Exposed Admin Panel: /user/login

SEVERITY: MEDIUM

Endpoint:	`/user/login`
Method:	`GET`
Vulnerability Type:	`Exposed Admin Panel`
CVSS Score:	`5.0`

Description:

Admin login panel is publicly accessible at /user/login

Proof of Concept:

```
GET https://www.lowmilesnomiles.com/user/login returns login form Page contains:
password, username, login
```

Remediation:

Protect admin panels with IP whitelisting, VPN, or additional authentication layer

Finding 74: Exposed Admin Panel: /admin/login/

SEVERITY: MEDIUM

Endpoint:	`/admin/login/`
Method:	`GET`
Vulnerability Type:	`Exposed Admin Panel`
CVSS Score:	`5.0`

Description:

Admin login panel is publicly accessible at /admin/login/

Proof of Concept:

```
GET https://www.lowmilesnomiles.com/admin/login/ returns login form Page contains:
password, username, login
```

Remediation:

Protect admin panels with IP whitelisting, VPN, or additional authentication layer

Finding 75: Unencrypted Service on Port 80

SEVERITY: MEDIUM

Endpoint:	`www.lowmilesnomiles.com:80`
Method:	`TCP`
Vulnerability Type:	`Unencrypted Service`
CVSS Score:	`5.0`

Description:

Unencrypted HTTP service is accessible on port 80. This may allow traffic interception.

Proof of Concept:

```
Port 80 (HTTP) is open and accessible
```

Remediation:

Redirect HTTP traffic to HTTPS or disable HTTP access

Finding 76: Unencrypted Service on Port 8080

SEVERITY: MEDIUM

Endpoint:	`www.lowmilesnomiles.com:8080`
Method:	`TCP`
Vulnerability Type:	`Unencrypted Service`
CVSS Score:	`5.0`

Description:

Unencrypted HTTP-Alt service is accessible on port 8080. This may allow traffic interception.

Proof of Concept:

```
Port 8080 (HTTP-Alt) is open and accessible
```

Remediation:

Redirect HTTP traffic to HTTPS or disable HTTP access

Finding 77: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/category-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.86 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/category-sitemap.xml All
requests succeeded (200 OK) Time taken: 1.86s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 78: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.79 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/listing-sitemap.xml All
requests succeeded (200 OK) Time taken: 1.79s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 79: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_category-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.67 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_category-sitemap.xml All requests succeeded
(200 OK) Time taken: 1.67s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 80: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_color-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.89 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/listing_color-sitemap.xml
All requests succeeded (200 OK) Time taken: 1.89s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 81: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_condition-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.75 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_condition-sitemap.xml All requests
succeeded (200 OK) Time taken: 1.75s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 82: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_cylinder-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.86 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_cylinder-sitemap.xml All requests succeeded
```

```
(200 OK) Time taken: 1.86s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 83: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_drive_type-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.80 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_drive_type-sitemap.xml All requests
succeeded (200 OK) Time taken: 1.80s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 84: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_feature-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.66 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_feature-sitemap.xml All requests succeeded
(200 OK) Time taken: 1.66s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 85: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_fuel_type-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.79 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_fuel_type-sitemap.xml All requests
succeeded (200 OK) Time taken: 1.79s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 86: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_location-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.66 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_location-sitemap.xml All requests succeeded
(200 OK) Time taken: 1.66s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 87: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_make-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.72 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/listing_make-sitemap.xml
All requests succeeded (200 OK) Time taken: 1.72s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 88: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_model-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.51 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/listing_model-sitemap.xml
All requests succeeded (200 OK) Time taken: 1.51s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 89: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_transmission-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.54 seconds.

Proof of Concept:

```
Sent 20 rapid requests to
https://www.lowmilesnomiles.com/listing_transmission-sitemap.xml All requests
succeeded (200 OK) Time taken: 1.54s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 90: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/listing_type-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.56 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/listing_type-sitemap.xml
All requests succeeded (200 OK) Time taken: 1.56s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 91: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/page-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.57 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/page-sitemap.xml All
requests succeeded (200 OK) Time taken: 1.57s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 92: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/post-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.50 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/post-sitemap.xml All
requests succeeded (200 OK) Time taken: 1.50s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 93: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/post_tag-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.69 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/post_tag-sitemap.xml All
requests succeeded (200 OK) Time taken: 1.69s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 94: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/product_cat-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.77 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/product_cat-sitemap.xml
All requests succeeded (200 OK) Time taken: 1.77s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 95: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/product_tag-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.68 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/product_tag-sitemap.xml
All requests succeeded (200 OK) Time taken: 1.68s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 96: Missing Rate Limiting

SEVERITY: MEDIUM

Endpoint:	`https://www.lowmilesnomiles.com/wtb-listing-sitemap.xml`
Method:	`GET`
Vulnerability Type:	`No Rate Limiting`
CVSS Score:	`5.3`

Description:

The endpoint has no rate limiting. Successfully made 20 requests in 1.72 seconds.

Proof of Concept:

```
Sent 20 rapid requests to https://www.lowmilesnomiles.com/wtb-listing-sitemap.xml
All requests succeeded (200 OK) Time taken: 1.72s
```

Remediation:

Implement rate limiting to prevent abuse and DoS attacks. Use techniques like token bucket or sliding window.

Finding 97: Missing Security Header: X-XSS-Protection

SEVERITY: LOW

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`GET`
Vulnerability Type:	`Missing Security Header`

Description:

X-XSS-Protection header missing or disabled

Proof of Concept:

```
Request to https://www.lowmilesnomiles.com does not include X-XSS-Protection header
```

Remediation:

Add "X-XSS-Protection: 1; mode=block" header

Finding 98: Verbose Error Messages

SEVERITY: LOW

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`POST`
Vulnerability Type:	`Verbose Error`
CVSS Score:	`3.0`

Description:

Application returns detailed error messages that may reveal system information

Proof of Concept:

```
Malformed request triggers verbose error containing: exception
```

Remediation:

Configure application to return generic error messages in production

Finding 99: Verbose Error Messages

SEVERITY: LOW

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`POST`
Vulnerability Type:	`Verbose Error`
CVSS Score:	`3.0`

Description:

Application returns detailed error messages that may reveal system information

Proof of Concept:

```
Malformed request triggers verbose error containing: exception
```

Remediation:

Configure application to return generic error messages in production

Finding 100: Verbose Error Messages

SEVERITY: LOW

Endpoint:	`https://www.lowmilesnomiles.com`
Method:	`POST`
Vulnerability Type:	`Verbose Error`
CVSS Score:	`3.0`

Description:

Application returns detailed error messages that may reveal system information

Proof of Concept:

```
Malformed request triggers verbose error containing: exception
```

Remediation:

Configure application to return generic error messages in production

Recommendations

Immediate Actions:

- Address all Critical and High severity vulnerabilities immediately
- Implement security fixes in a test environment before production deployment
- Conduct re-testing after remediation to verify fixes

Short-term Improvements:

- Resolve Medium severity vulnerabilities within 30 days
- Implement security monitoring and logging for detected attack patterns
- Review and update security policies and procedures

Long-term Strategy:

- Address Low severity findings during regular maintenance cycles
- Implement security training for development team
- Establish regular security assessment schedule (quarterly recommended)
- Integrate security testing into CI/CD pipeline
- Consider implementing a Web Application Firewall (WAF)

Note: This report reflects the security posture at the time of testing. Security is an ongoing process, and regular assessments are recommended to maintain a strong security posture.