

X Cyber Squad Module Documentation

Module: AIOSEO WordPress API Enumeration Script

Objective:

To identify and enumerate AIOSEO plugin REST API endpoints on WordPress websites to check for public data leakage or protected access controls.

Script Name:

xcs-aioseo-enum.sh

Dependencies:

- curl
- jq
- Tested on: Kali Linux, Parrot OS, Ubuntu 20+

Usage:

`./xcs-aioseo-enum.sh https://target-wordpress-site.com`

What It Does:

1. Fetches all available REST API endpoints from /wp-json
2. Filters aioseo/v1/* endpoints
3. Sends requests to each endpoint using browser headers
4. Categorizes response as Public / Unauthorized / Forbidden
5. Saves results to timestamped output file

Use Cases:

- Bug bounty recon
- WordPress plugin misconfig checks
- Classroom demos for API recon
- Pre-engagement passive intelligence

Sample Output:

[200] https://site.com/wp-json/aioseo/v1/seo-analysis/homerresults -> 200 OK

[401] https://site.com/wp-json/aioseo/v1/pagespeed -> 401 Unauthorized

Output File:

xcs_aioseo_results_YYYYMMDD_HHMMSS.txt

Author:

Neerav Patel

Cyber Expert and Forensic Investigator and Crime Investigator

Generated On: 2025-07-26 06:04:13