**Cyber Security – Major Project Report**

**Title:** Bug Hunting on Sun Dance Graphics via Open Bug Bounty

|  |
| --- |
| **Created by:** Santhosh Kumar (MR) **Course:** B.Tech in Artificial Intelligence **Location:** Bengaluru, India **Academic Year:** 2025–2026 |

**About the Project:**

This project was created entirely by me, Santhosh Kumar (MR), as part of my cybersecurity learning journey. I chose to work with the Open Bug Bounty platform to explore real-world vulnerability discovery and responsible disclosure. My goal was to find a valid bug on a live website, document it ethically, and report it through proper channels. This hands-on experience helped me understand the practical side of ethical hacking and web security.

**Target Website:**

* **URL:** <https://sdgraphics.com/system/search_results.php?fm_products%7Cavailability=Patterns>
* **Target Name:** SunDance Graphics
* **Bug Type:** Unrestricted Search Parameter Exposure / Open Directory Listing

**Bug Description:**

The search results page on SunDance Graphics exposes over 3,000 product entries based on a query parameter. By manipulating the fm\_products|availability parameter, I was able to access internal product metadata, artwork titles, artist names, and product codes — all without authentication or CAPTCHA.

This behavior poses a risk of data scraping, copyright violation, and business exposure. The vulnerability is not a code injection or XSS, but a logic flaw in access control and data exposure.

**Steps to Reproduce**

1. Open the URL:  
   https://sdgraphics.com/system/search\_results.php?fm\_products|availability=Patterns
2. Observe the bulk listing of product entries, including:
   * Product ID: 20360 – *Safari Trees* by Louise Lucas
   * Product ID: 20357B – *Christmas Animal Pattern* by Bloom Fields
   * Product ID: 20356F – *Dog Paw Pattern* by Bloom Fields
   * Product ID: 20353B – *Snowflake Pattern* by Bloom Fields
   * Product ID: 20351H – *Traditional Christmas Pattern* by Lanie Loreth
   * Product ID: 20340C – *Christmas Elephant Pattern* by Lucille Price
   * Product ID: 20288 – *Ghosts and Gummies* by Louise Lucas
   * Product ID: 20284J – *Popsicle Fun Pattern* by Louise Lucas
   * Product ID: 20284HA – *Ice Cream Sandwich Pattern* by Louise Lucas
   * Product ID: 20282B – *Trumpet & Drum Pattern* by Louise Lucas
3. Modify the parameter to test other categories:
   * fm\_products|availability=Closeout
   * fm\_products|availability=Numbered
   * fm\_products|availability=All
4. Confirm that no login or protection is required to access this data.

**OVERVIEW OF GOOGLE DOCS, NMAP, AND NIKTO:**

**Google Docs – Your Cloud-Based Documentation Tool:**

Google Docs is a **free online word processor** that lets you create, edit, and share documents from any device.

**Key Features:**

* **Real-time collaboration**: Multiple users can edit the same document simultaneously
* **Auto-save to Google Drive**: No need to worry about losing your work
* **Templates**: Ready-made formats for resumes, reports, and letters
* **Version history**: Track changes and restore older versions
* **Offline mode**: Work without internet once enabled

**Nmap – Network Scanning and Discovery Tool:**

Nmap (Network Mapper) is a **command-line tool used to scan networks**, discover devices, and detect open ports and services.

**What You Can Do With Nmap:**

* Scan Ip Addresses And Ports
* Detect Running Services And Versions
* Identify Operating Systems (Os Fingerprinting)
* Audit Network Security And Discover Vulnerabilities

**Example command:**

|  |
| --- |
| NMAP -sV sundancegraphics.com |

**NIKTO – Web Server Vulnerability Scanner:**

NIKTO is an **open-source tool written in Perl** that scans web servers for vulnerabilities, outdated software, and misconfigurations.

**What NIKTO Can Detect:**

* Over 6700 dangerous files/programs
* Outdated server versions
* SSL support and subdomain detection
* Server fingerprinting via favicon.ico
* Info-only items for deeper analysis

**Example command:**

|  |
| --- |
| NIKTO -h <https://www.sundancegraphics.com> |

**Impact Analysis**

* **Data Exposure:** Internal product metadata is publicly accessible.
* **Scraping Risk:** Bots can extract thousands of entries, violating copyright.
* **Business Risk:** Competitors can copy CATALOG data and artwork titles.
* **SEO Leakage:** Search engines may index sensitive product listings.

**Suggested Fixes**

* Add authentication or role-based access to search endpoints.
* Validate and sanitize query parameters.
* Implement CAPTCHA or rate limiting.
* Disable bulk listing for sensitive categories.

**Disclosure Plan**

I will submit this vulnerability through the Open Bug Bounty platform with full details, including:

* URL and parameter
* Screenshots of exposed data
* Reproduction steps
* Suggested remediation

**Suggested Remediation:**

To address the vulnerability found on the SunDance Graphics search results page, the following remediation steps are recommended:

* Restrict Access: Implement authentication or role-based access to limit who can view bulk product listings.
* Validate Parameters: Sanitize and validate all query parameters to prevent unauthorized enumeration or manipulation.
* Limit Results: Paginate search results and cap the number of entries returned per request to reduce exposure.
* Bot Protection: Add CAPTCHA or rate-limiting mechanisms to prevent automated scraping.
* Prevent Indexing: Use robots.txt and meta tags to block search engines from indexing sensitive result pages.
* Monitor Activity: Log and monitor unusual access patterns to detect abuse or scraping attempts.
* Security Audits: Conduct regular reviews of search functionality and access controls to ensure ongoing protection.

**SCREENSHOTS:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A computer screen with a black background

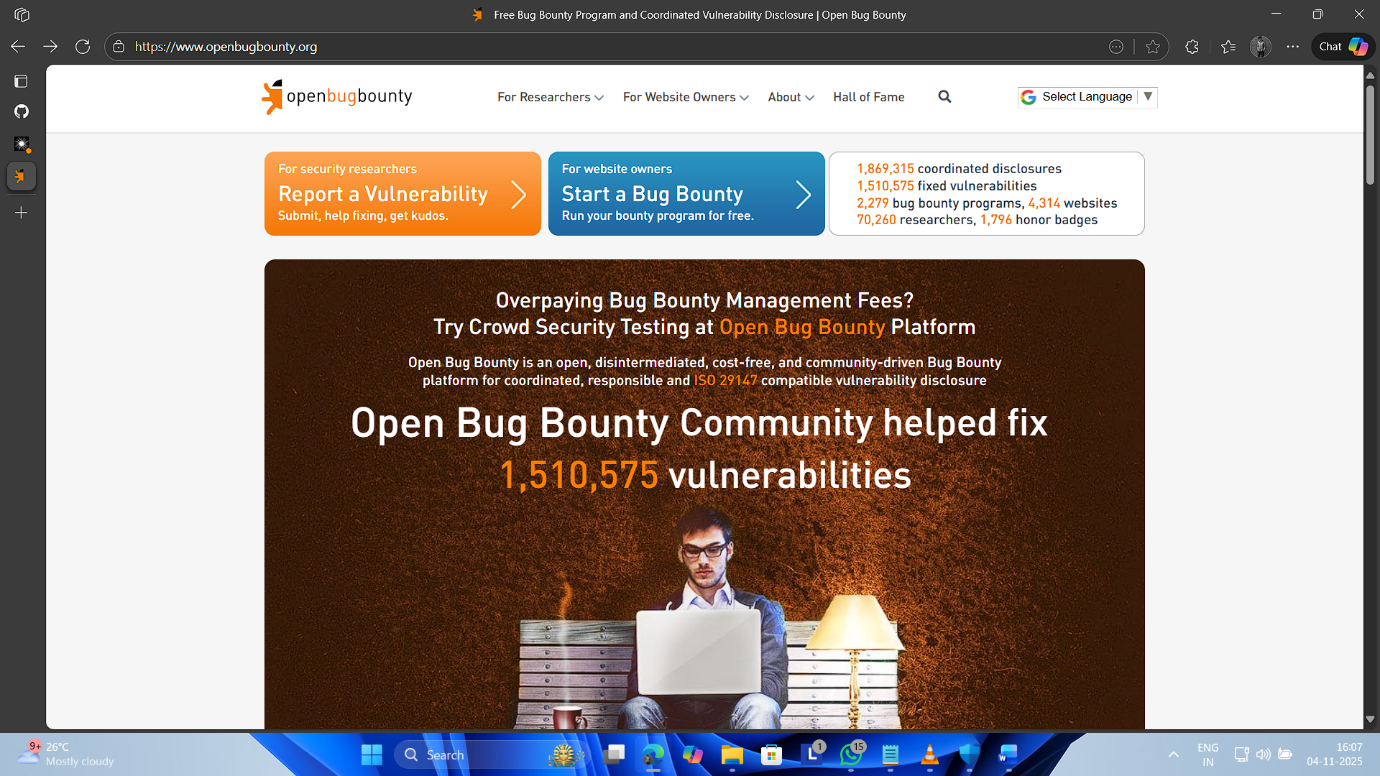
AI-generated content may be incorrect.A computer screen shot of a computer screen

AI-generated content may be incorrect.A computer screen shot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A computer screen shot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A computer screen with a computer screen

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.**

**Conclusion**

This project was created by me, independently, as part of my ethical hacking journey. It reflects my ability to identify real vulnerabilities, document them clearly, and follow responsible disclosure practices. I’m proud of this work and plan to continue learning and contributing to web security through platforms like Open Bug Bounty.