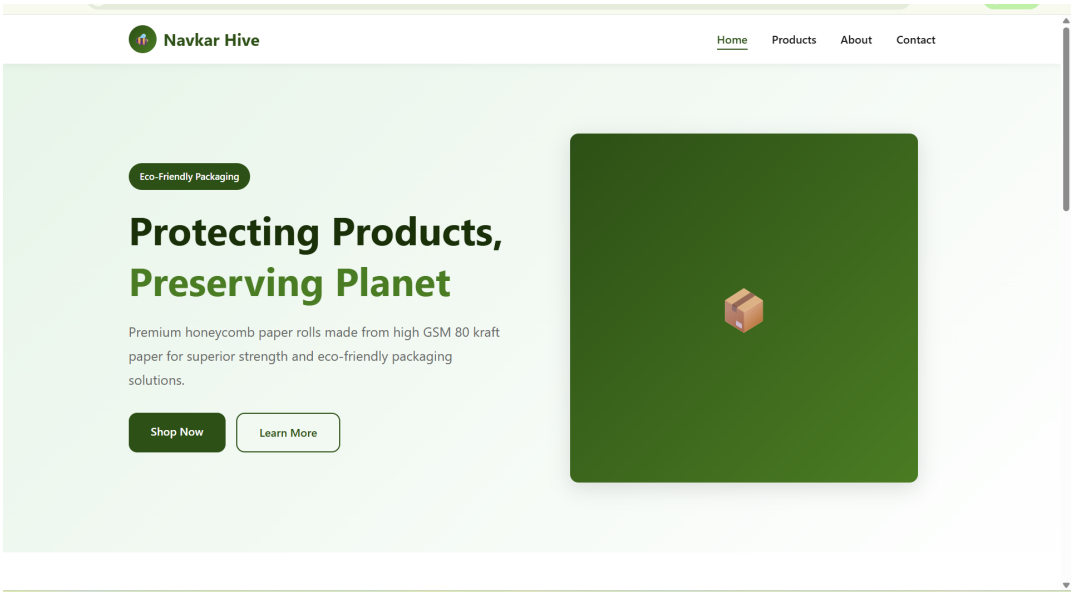
Navkar Hive – LFI Challenge Writeup

Navkar Hive is a web exploitation challenge based on a Local File Inclusion (LFI) vulnerability. The application dynamically includes files using a request parameter without proper validation. By abusing this behavior, sensitive server-side files can be accessed to retrieve the flag.

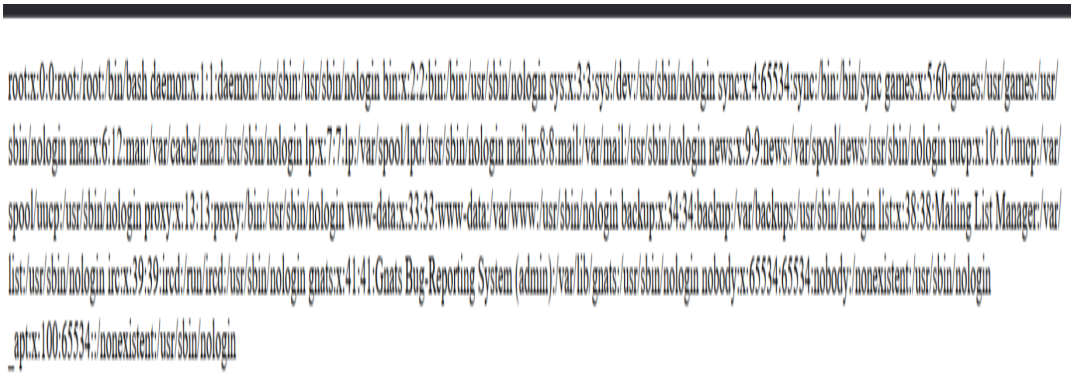


Step 1: Identify the Vulnerable Page

All available pages of the website are tested for file inclusion vulnerabilities. After testing multiple parameters, the vulnerability is discovered on the Contact page.

Step 2: Confirm Local File Inclusion

The vulnerability is confirmed by attempting to include sensitive local files such as */etc/passwd*. The successful output confirms that arbitrary local files can be read.



Step 3: Craft an LFI Payload

To safely read the flag file, a PHP filter wrapper can be used. The following command is provided as an example payload. **Players may use different payloads or techniques** as long as they achieve Base64-encoded file inclusion:

echo -n "php://filter/convert.base64-encode/resource=/flag/flag.txt" | base64

Step 4: Exploit the Live Application

The generated Base64 payload is supplied to the vulnerable parameter on the Contact page. **The target URL and parameter should be adjusted based on the live server configuration** used during the challenge. An example format is shown below:

http://localhost:8080/contact.php?page=PASTE_BASE64_HERE

The server responds with Base64-encoded contents of the flag file.

Step 5: Decode the Flag

The Base64 output returned by the application is decoded to reveal the final flag.

Flag

LNMHACKS{Srd_is_the_future}