

scan-it-to-stay-safe

Description

None

Category

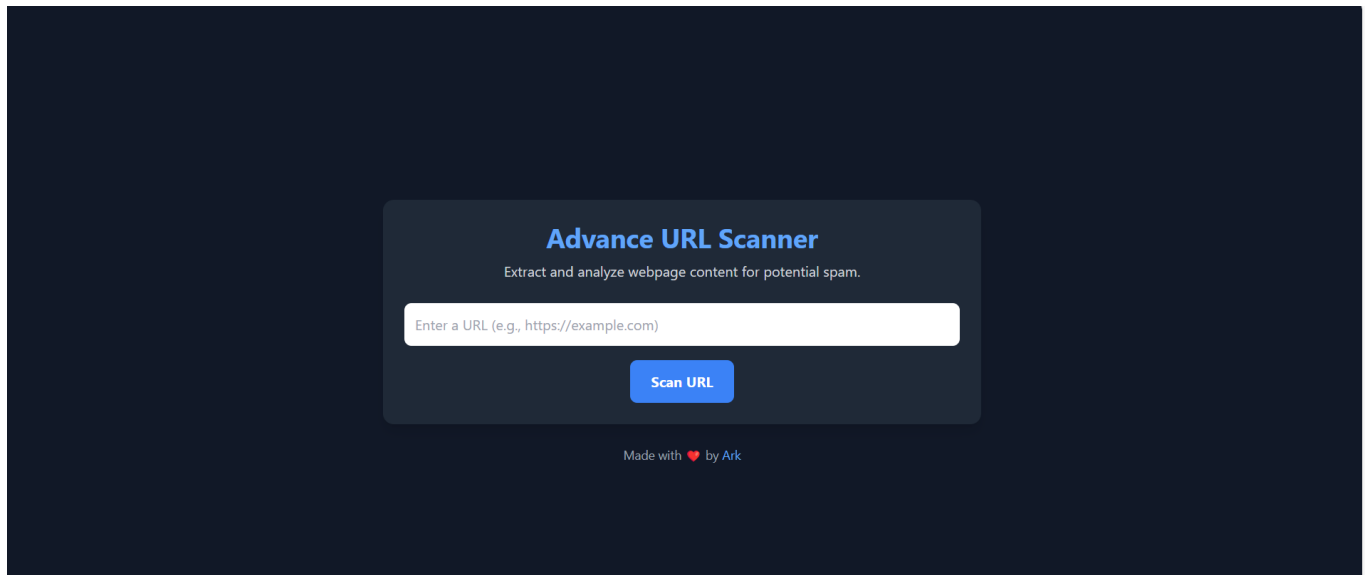
#web

Solution

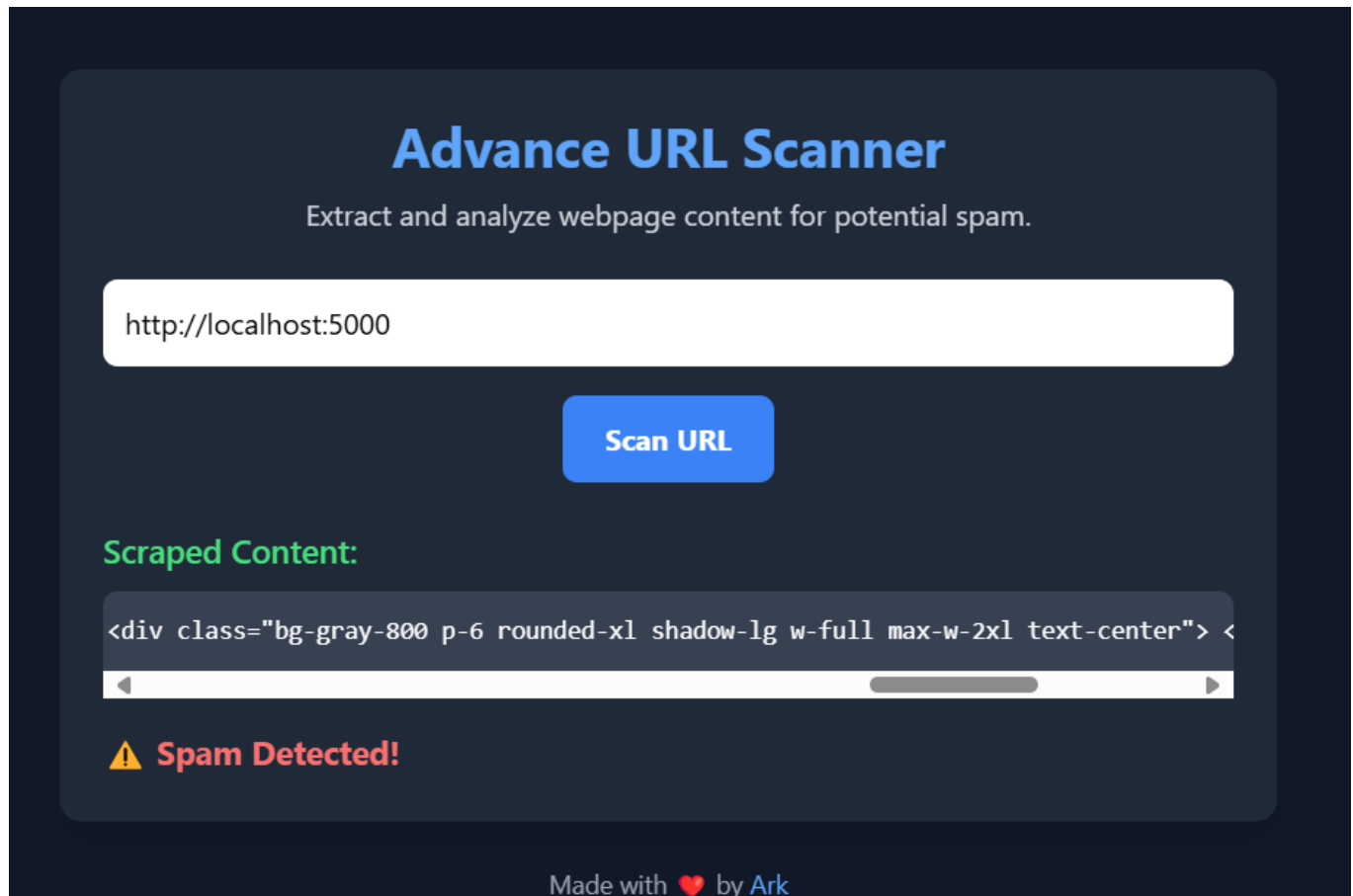
Note: This was a very, very, very confusing web exploitation. There's literally no exploitation in this problem. So feel free to skip.

Enumeration

The website gives us a way to scan for URL. Meaning that it might be vulnerable to SSRF.



Which it is. However, this is NOT the solution.



Checking out the cookie gives us two other cookie, 1 is session and 1 is hint. The session can be used for impersonation. However, this is NOT the solution.

^ hint	
Name	hint
Value	"Follow the trail..."
Show Advanced	
^ session	
Name	session
Value	eyJ1c2VyX2lkjjo0OH0.Z8bsPw.wjdMtpC8KdDgcfRxOaWlmF0dinU
Show Advanced	

Exploit

Create a webhook to see all requests information

The screenshot shows the Webhook.site interface. The top navigation bar includes links for Docs & API, Features & Pricing, Terms, Privacy & Security, and Support. The main header has a 'Copy' button, an 'Edit' button, a '+ New' button, and a 'Sign Up Now' button. The left sidebar shows an 'INBOX (1/100)' with a search query and a list of requests. The main content area displays 'Request Details & Headers' for a specific request. The request is a GET method to the URL 'https://webhook.site/1265e435-d94d-4469-9bfc-a375db9b4698'. The headers section lists various request headers such as 'accept-language', 'accept-encoding', 'referer', 'sec-fetch-dest', 'sec-fetch-user', 'sec-fetch-mode', 'sec-fetch-site', 'accept', 'user-agent', 'upgrade-insecure-requests', 'sec-ch-ua-platform', 'sec-ch-ua-mobile', 'sec-ch-ua', and 'host'. The 'Query strings' and 'Form values' sections are both empty. The 'Request Content' section shows 'No content'.

Enter the webhook in the input

The screenshot shows the 'Advance URL Scanner' interface. The main heading is 'Advance URL Scanner' with the subtitle 'Extract and analyze webpage content for potential spam.' Below this is a large input field containing the URL 'https://webhook.site/1265e435-d94d-4469-9bfc-a375db9b4698'. A blue button labeled 'Scan URL' is positioned below the input field. The 'Scraped Content:' section shows a preview of the scraped content, which is a single line of HTML: '<edit/1265e435-d94d-4469-9bfc-a375db9b4698">Change response in Webhook.site.'. Below the preview is a green checkmark icon and the text 'Content Looks Safe'. At the bottom of the interface, it says 'Made with ❤️ by Ark'.

Comes the flag

Request Details & Headers

GET

https://webhook.site/1265e435-d94d-4469-9bfc-a375db9b4698

Host

13.126.47.8

WhoisShodanNetifyCensysVirusTotal

Date

03/04/2025 9:32:08 PM (a few seconds ago)

Size

0 bytes

Time

0.000 sec

ID

8bbd6485-a308-4167-9655-696bbfe0bc63

Note

Add Note

Query strings

(empty)

flag

VishwaCTF{Y0u_7R4c30117_3000_4rK}

accept

/

accept-encoding

gzip, deflate

user-agent

python-requests/2.31.0

host

webhook.site

Form values

(empty)

Request Content

No content