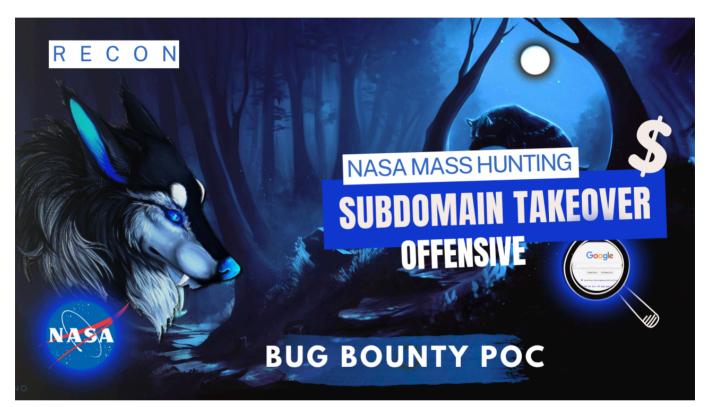


Mass Subdomain Takeover on NASA.gov – Bug Bounty Write-Up

▲ Mann Sapariya ② Month Ago



Disclaimer

This blog is for **educational purposes only**. All tests were performed on assets that are part of **public bug bounty scopes** and were disclosed responsibly under program rules. I do **not encourage or support any unauthorized scanning or hacking**.

What is Subdomain Takeover?

A **subdomain takeover** occurs when a subdomain (like test.nasa.gov) points to a third-party service (e.g., GitHub Pages, AWS S3) but that service is **no longer in use** — allowing an attacker to register it and "take over" the subdomain.

This is a serious issue because it can lead to:

Fake phishing pages hosted on a legit domain

Session hijacking

Data theft

Brand impersonation

99

© Target Scope

The target in this case was:

*.nasa.gov - part of a public program that allows testing for vulnerabilities like subdomain takeovers.



₹ Tools Used

subfinder - For discovering subdomains

subzy - For detecting potential takeover



X Step-by-Step Recon & Exploitation



1. Subdomain Enumeration

I used **recursive and deep search** to find as many valid subdomains as possible.

subfinder -d nasa.gov -all -recursive > subnasa.txt

- -d nasa.gov: target domain
- -all: use all available sources
- -recursive: find subdomains of subdomains

Output saved to: subnasa.txt



🚨 2. Subdomain Takeover Scanning

After collecting the subdomains, I used **Subzy** to scan for takeover possibilities.

```
subzy run --targets subnasa.txt --concurrency 100 --hide_fails --verify_ssl
```

- --targets: file with subdomains
- --concurrency 100: speed up scan
- --hide_fails: cleaner output
- --verify_ssl: check if SSL certs are valid
- After a few minutes of scanning, 10+ subdomains were found vulnerable to takeover.

```
sedupdate.gsfc.nasa.gov [ Uptimerobot ]
                      [Issue #45] (https://github.com/EdOverflow/can-i-take-over-xyz/issues/45)
                          [Uptimerobot-Sub-takeover] (https://exploit.linuxsec.org/uptimerobot-com-custom-domain-sub-
domain-takeover/)
                      spsoservices.gsfc.nasa.gov [ Uptimerobot ]
                      [Issue #45](https://github.com/EdOverflow/can-i-take-over-xyz/issues/45)
- [Uptimerobot-Sub-takeover](https://exploit.linuxsec.org/uptimerobot-com-custom-domain-sub
domain-takeover/)
                      c-ras.cdscc.nasa.gov [ Cargo Collective ]
                      [Issue #152] (https://github.com/EdOverflow/can-i-take-over-xyz/issues/152)
                       - [Cargo Support Page] (https://support.2.cargocollective.com/Using-a-Third-Party-Domain)
                      rsvpify.goes-u-launch.nasa.gov [ Uptimerobot ]
                      [Issue #45] (https://github.com/EdOverflow/can-i-take-over-xyz/issues/45)
- [Uptimerobot-Sub-takeover] (https://exploit.linuxsec.org/uptimerobot-com-custom-domain-sub
domain-takeover/)
```



Impact of These Vulnerabilities

Subdomain takeovers can:

Host malicious scripts under a trusted domain

Trick users into giving away sensitive data

Affect brand reputation and user trust



Responsible Disclosure

All vulnerabilities were reported **responsibly** through the appropriate bug bounty channels. This blog post was published after validation and patching.



Always clean up your DNS records when removing services

Subdomain takeover is still one of the most underrated attack vectors

Automation with tools like subfinder and subzy helps catch low-hanging fruits

Thank You for Reading

If you found this write-up helpful, feel free to share it with others. Have questions or want personal guidance?

Mass Subdomain Takeover on NASA | Bug Bounty POC Maxx_191



Watch on

Reach out to me for Private Session: Bug Bounty & Ethical Hacking & Ethical Hacking.

Let's secure the web − one bug at a time. 🤍

BUGBOUNTY f y ρ in \odot

YOU MAY LIKE THESE POSTS

Mass Subdomain Takeover on NASA.gov – Bug Bounty Write-Up

• June 20, 2025

Deep Dive Into HTTP Request Smuggling – A High-Impact Bug for Bounty Hunters

① June 14, 2025

Jenkins Security Guide:
Common Bugs & Real-World
Exploitation (Beginner to
Advanced)

① May 28, 2025

0 Comments

To leave a comment, click the button below to sign in with Blogger.

SIGN IN WITH BLOGGER

TOTAL PAGEVIEWS



POPULAR POSTS

New Method For Account Takeover In Android Applications

^o July 07, 2023

How to Set Up a Robust Android Testing Environment ^o June 18, 2023

Jenkins Security Guide: Common Bugs & Real-World Exploitation (Beginner to Advanced)

O May 28, 2025

CATEGORIES

^{>} BugBounty	
> Life Lessons	

> Security

TRANSLATE

Select Language		
Powered by Google Translate		
y	:	
9 ©	in	
w	IKIPEDIA	

Submit		
Search results		
Home	About	
Bug Bounty	Advertise	
	TAGS	
BugBounty Life Lessons Security		
Elie Lessons Security		
CONTACT FORM		
Name		
Name	Fine will #	
	Email *	
Message *		

Manan Sapariya 'Ethical Hacker | Security Researcher | Bug Bounty Hunter.

mannsapariya004@gmail.com

Copyright © 2023 MANN SAPARIYA All Right Reserved Blogger Theme