Vulnerability Disclosure Report

4 messages

c███████ <c███████@gmail.com>   Tue, Jul 19, 2022 at 9:48 PM
To: rvdp@nciipc.gov.in

Dear Team,

I'm Chethan Vasthaw Tippani
Security Researcher, Bug Hunter.

Host: https://dharani.telangana.gov.in/gis/
IP address: ████████████
Organisation: Dharani Portal (Revenue Department of Telangana)

I Found a Critical Bug In XSS.

Name: XSS Cross-site scripting

Here I just used a simple XSS Payload,

Cross-site scripting is a type of security vulnerability typically found in web applications. XSS attacks enable
attackers to inject client-side scripts into web pages viewed by other users. Attackers may use a cross-site
scripting vulnerability to bypass access controls like the same-origin policy. In a Cross-site Scripting attack (XSS),
the attacker uses your vulnerable web page to deliver malicious JavaScript to your user. The user's browser
executes this malicious JavaScript on the user's computer. Note that about one in three websites is vulnerable to
Cross-site scripting.

Vulnerable Host: https://dharani.telangana.gov.in/

Vulnerable Url: https://dharani.telangana.gov.in/gis/

Vulnerable Item: Search bar (Survey No)

Payload:
████████████████████████████████

How To Reproduce:

1) Visit https://dharani.telangana.gov.in/gis/
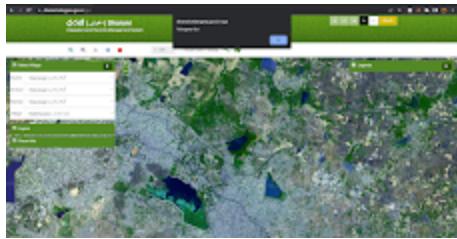2) In the 'Select Village', type all the required information(any of the details to be filled)
3) Now in the search bar which is 'Survey No' type the vulnerability. in this, i just used a simple XSS payload which
is: ██████████████████████████

#So Please Fix it ASAP otherwise some black hats will get the benefit.

POC: The screenshot is attached below.

---

 2 attachments

vulnerable.png
4503K

Vulnerability_Disclosure_Form.pdf
646K

NCIIPC RVDP <rvdp@nciipc.gov.in>   Tue, Jul 19, 2022 at 9:51 PM
To: c████████@gmail.com

Dear Sir/Madam,

Thank you for contacting RVDP, NCIIPC. We have received your email and the concern will be addressed soon.

Please note that this is an auto-generated email.

With Best Regards.
Team RVDP, NCIIPC

NCIIPC RVDP <rvdp@nciipc.gov.in>   Wed, Jul 20, 2022 at 10:03 AM
To: c████████@gmail.com

Dear Researcher,

1. We acknowledge the issue reported by you.

2. We are in the process of verification and remediation in coordination with the respective stakeholder(s) and look forward to your continued contribution.

Thanks & Regards,
Team RVDP, NCIIPC

From: c████████@gmail.com
To: "NCIIPC RVDP" <rvdp@nciipc.gov.in>
Sent: Tuesday, July 19, 2022 9:48:03 PM
Subject: Vulnerability Disclosure Report
[Quoted text hidden]