Vishal Bharad Follow

Feb 3, 2020 · 2 min read · Listen

(Improper Access Control) Vulnerability In Prototype 1.6.0.1 Framework.

Introduction :

Hello, I am **Vishal Bharad** & I am **Mechanical Engineer :**D and working as Penetration Tester. I'm here to share about my findings on **Prototype 1.6.0.1 Framework Which is Used in Many Websites.**

About the Vulnerability :

I have got the url like https://support.target.com. So I have got the **Improper Access Control** Vulnerability. which is Similar like to **Insecure Direct Object Reference.**

For Discovering the bug I have tested many tricks on the various websites. After Deep Research I have got the **Prototype 1.6.0.1 Framework** which is Used in Many Websites for Support. Lets Assume https://support.target.com

So then I have Search for various websites which using **Prototype 1.6.0.1 Framework.**

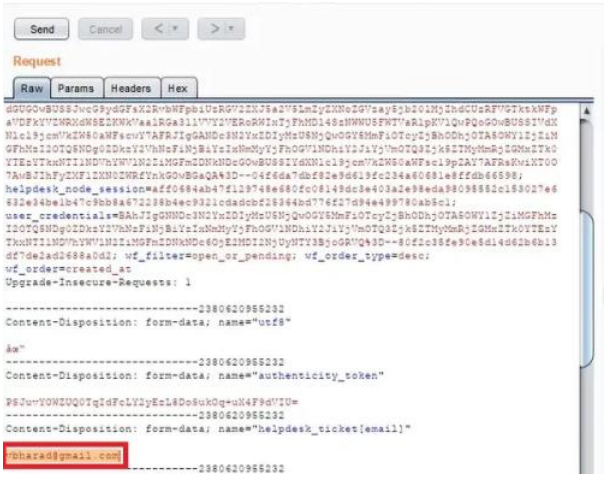
Prototype 1.6.0.1, as used in Many products, allows remote authenticated users to forge ticket creation (on behalf of other user accounts) > via a modified email ID field.

Tools Used for this Vulnerability:

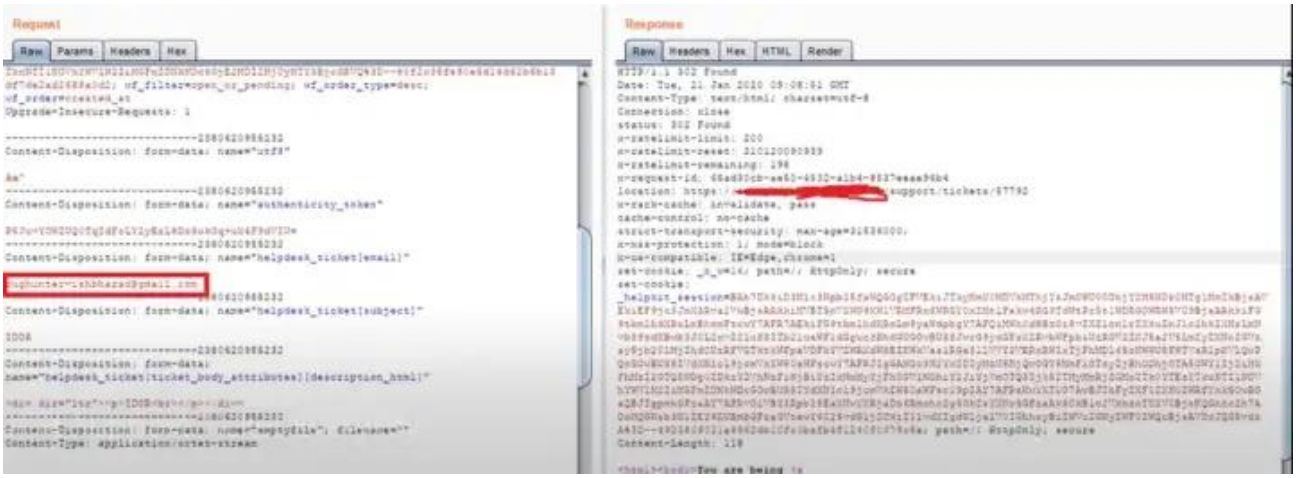
1. ***BurpSuite***

Steps to Reproduce:

1. Open two browser one is Firefox and other is Chrome and login for an 2 accounts.
2. Then go to the attackers account and go to create ticket.
3. In attackers account fill the form of create account and Capture the request in Burp Suite.
4. You can see in the Request there are attackers email id present to create an ticket. So replace the email id with Victims email id and forward the request.



5. Now go to Victims account which is log in on another browser and refresh it. You can see that the Ticket is generated without any authentication.



Thank You

Looking forward to share more blogs

Best Regards

Vishal Bharad

Linkedin Profile : https://www.linkedin.com/in/vishal-bharad-b476b388/