Sagar Sajeev Follow

Aug 12 · 4 min read · Listen

Save

File Upload Bypass to RCE == $$$$

Hello Everyone. My name is Sagar Sajeev .

In this writeup, I'll explain how I was able to bypass a File upload feature on the target and chain it to an RCE. Thus increasing the severity.

The fun thing is that, the target Website Security team had deployed fix 3 times for this same vulnerability, as I had managed to bypass the fix all three times. So I'll also explain all 3 bypass scenarios in this writeup.

Also I was awarded 3 bounties (for 3 bypasses) for the same vulnerability . Thus, this is my first 4 digit bounty $$$$ 🤑

Scenario #1

1. Payload with .php extension is not allowed.
2. Renaming payload from : ‘payload.php’ to ‘payload.pHp5’ . Changing extensions to random upper and lower case bypassed it.
3. But do note that such payloads only work if target has client-side validation only . So sometimes the payload may go through the frontend, but you may not get the callback as it has been blocked by the IDS or backend firewall.
4. In this case, I received the callback and RCE was established.

> *Bounty #1 was awarded*
>
> *The Security team deployed a fix and asked me to confirm it.*
>
> *Well, I was able to bypass it. How? That takes us to Scenario #2.*

Scenario #2

1. Payload with .php extension is not allowed.
2. Renamed the payload from : ‘payload.php’ to ‘payload.php\x00.png’ Appending \x00.png to the end bypassed the restriction(Null Byte).
3. Right click → view image in new tab triggered the script.
4. RCE was achieved.

Note:-

- In some cases .inc , .phps , .phtml can also be used.
- When you are using this, make sure to change content-Type accordingly. P.S : Stored XSS was also possible here.

> *Guess what, I again bypassed it. How? Let's move on to Scenario #3*

Scenario #3

- This time, it took a while to find a valid bypass. They had set up a strict rule to only allow images.
- I was not able to figure out how the target web app was verifying if the data was indeed an image. But after a lot of research, I found that they were checking the magic bytes of the payload to verify it.
- Sometimes applications identify file types based on their first signature bytes. Adding/replacing them in a file might trick the application.

> *Magic byte is nothing but the first few bytes of a file which is used to recognize a file. It is not visible if you open the file. We need special hex editors to view the magic bytes of a file.*
>
> *I use Linux. So I can use inbuilt hex editor and xxd to view and edit the magic bytes. But You can use any hex editor to achieve the same results.*

- I also found out that backend filters and removes certain keywords. For example, it removes the term '.php'. So we can rename a file as 'payload.p.phphp'. So when the filter removes '.php' , the file name would become 'payload.php'. Since the firewall has been bypassed at this stage, script will be executed. One of John Hammonds video helped me with this.

1. 89 50 4e 47 0d 1a 0a → magic bytes of a png file
2. echo "89 50 4e 47 0d 1a 0a" | xxd -p -r >> payload.p.phphp
3. Upload the script and get a full fledged RCE.

> *Bounty #3 was awarded*
>
> *The Sec Team again deployed the fix.*


> *Bonus Tip*
>
> *Once the Sec Team has deployed a fix to the vulnerability you have reported, they will ask you to confirm if the bug has indeed been fixed. So try to check if it's possible to find a bypass to it. If yes, it can even get you more bounty.*

> *Timeline*
>
> *Submitted : 02–08–2022*
>
> *Accepted : 03–08–2022*
>
> *Bounty #1 : 04–08–2022*
>
> *Bounty #2 : 06–08–2022*
>
> *Bounty #3 : 09–08–2022*
>
> *Resolved : 10–08–2022*

I do occasionally share some tips about Bug Bounties and related stuff over at my Twitter and LinkedIn handle. So do follow me there. If you've got any queries, feel free to message me. I will be more than happy to help.

LinkedIn : https://www.linkedin.com/in/sagar-sajeev-663491208/

Twitter : https://twitter.com/Sagar__Sajeev

Thanks for going through my writeup and I hope it was useful to you. I've made 5 other writeups on my Medium handle. Please do check those out as well.

Happy Hunting!