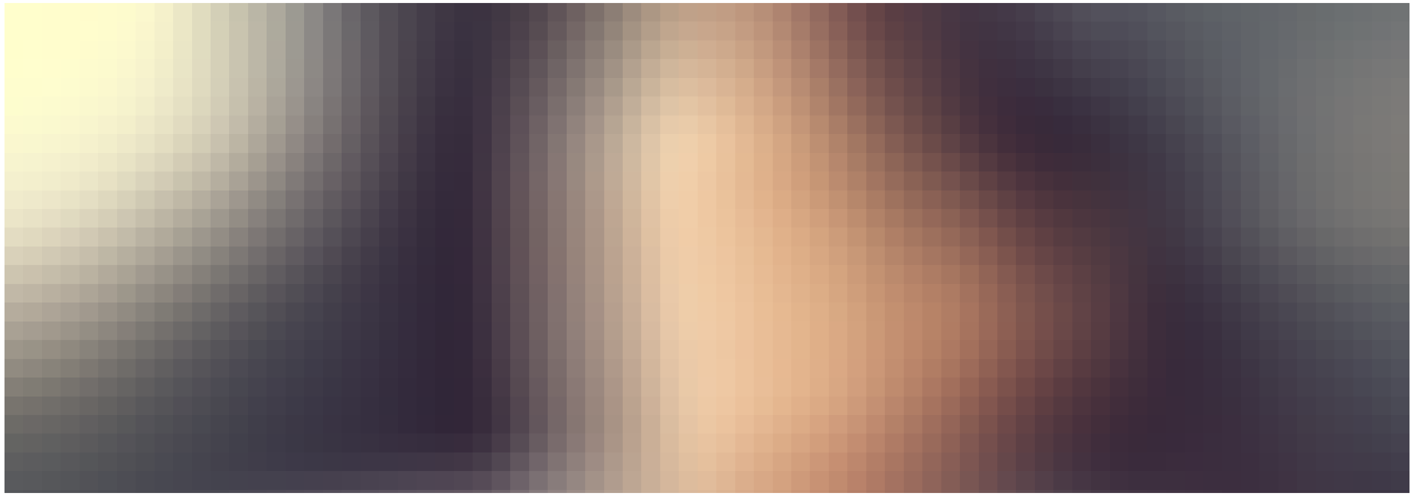
[XSS] Reflected XSS Bypass Filter

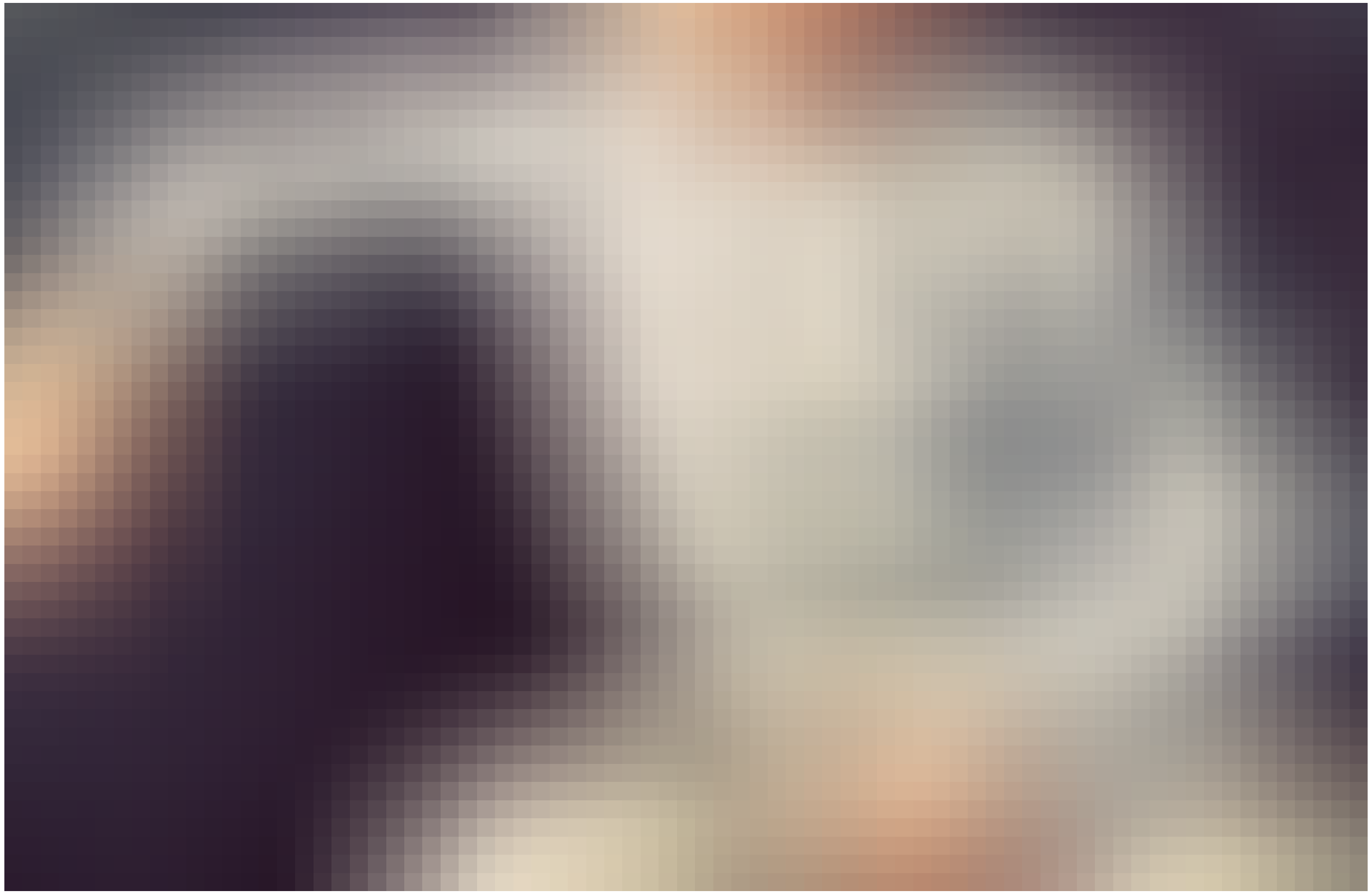
Mohamed Sayed Follow
Apr 22 · 2 min read

I would like to write about this but it takes some time to bypass the filter and some time to find the right HTML tag to write a payload.

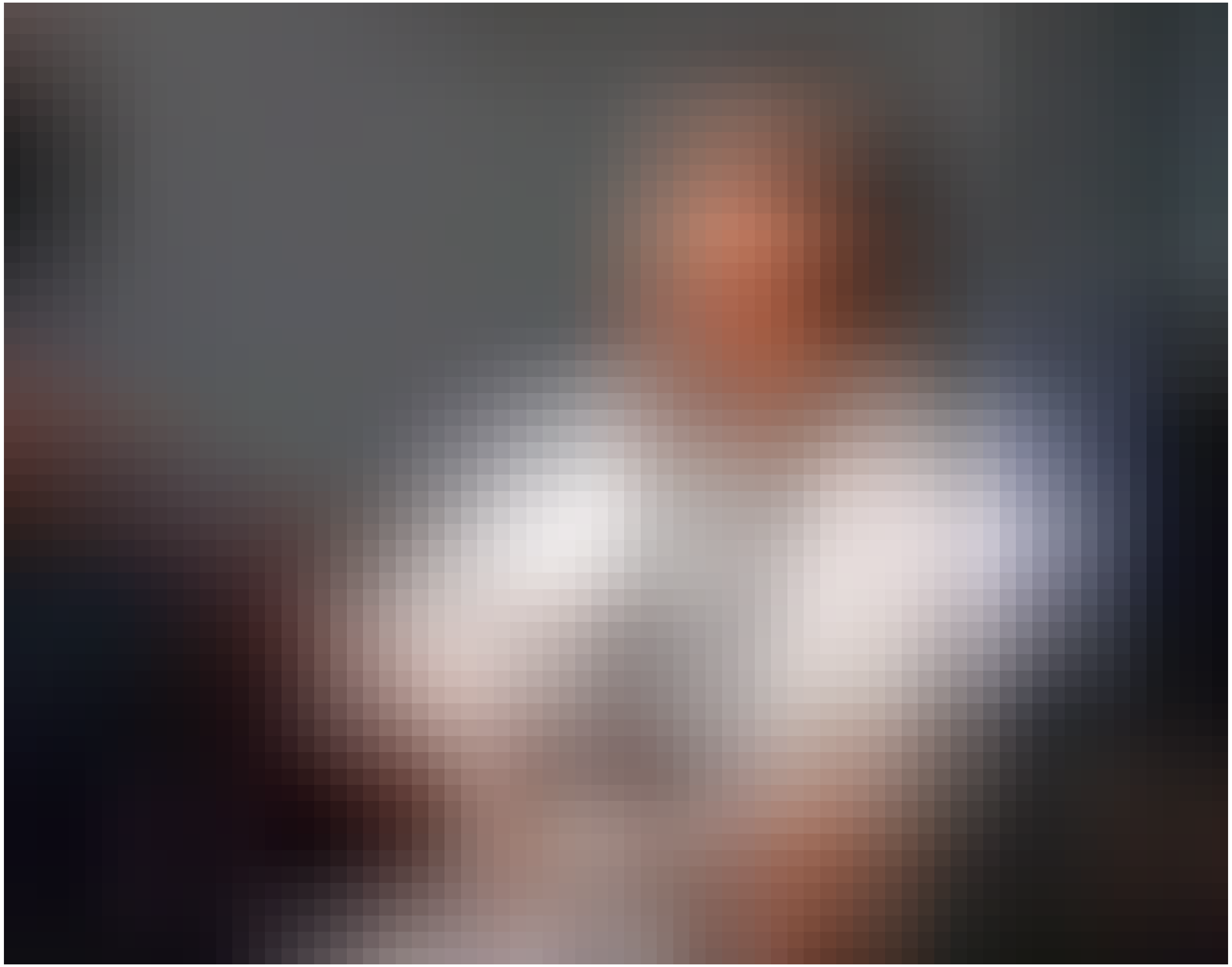
I was testing on a program which is private let’s call it `example.com` I found a search field so I start to test it with my lovely value `'"><` to know what will be blocked I found that the value added to a lot of places on the source code but almost all of them encoded with HTML-Encode but I found my value added on a tag called `dfn` without encoding so there is a hope to find an XSS so I added an XSS payload but It redirects me to block page because of these `< >` values not accepted after a few minutes I understand how the function works the function block the request if this `<` connected to anything like the word `<svg` or special char `<!` and if I write a complete HTML tag the filter will delete all of the tag I tried to bypass it using URL-Encoding but it doesn’t work so I tried double encode and it works to bypass it and I wrote a payload like that `%253Csvg onload=alert0)%253E` this payload added to the source code but there was a problem that the filter delete this `=` I tried a lot to bypass this but I couldn’t `:(` I told to my self `what? after all of this time I couldn’t execute XSS payload`

I asked my friends about payloads without this `=` and I asked Google but I didn't found anything, the problem not here the problem is my mind was sleep and when he wakes up I got it





I forgot the king of XSS payloads `<script>alert(0)</script>` WOW I don’t know how I forgot it but this is our guy so I decoded it and try to execute but there is another problem is these two `( )` so I replaced it with `` ` ` `` and the payload executed I was WoooooooooW



I like this bug and I like you who completed the topic I hope it is helpful to you guys, thanks for reading this, goodbye.

Security Xss Vulnerability Xss Bypass Writeup Infosec

70 claps

1

Mohamed Sayed

Follow

My name is Mohamed my nickname is Flex, I'm a Bug Hunter at HackerOne and Synack Red Team Member.

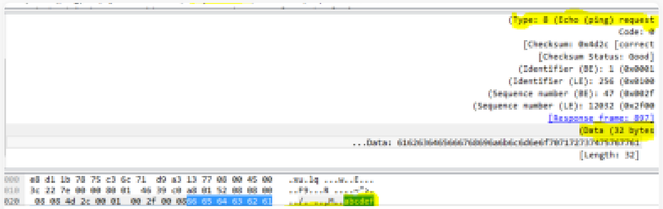
InfoSec Write-ups

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. #sharingiscaring

More from InfoSec Write-ups

Writing a Password Protected Bind Shell (Linux/x64)



```
(Type: 8 (Echo (ping) request
Code: 0
[Checksum: 0x4d2c [correct
[Checksum Status: Good]
(Identifier (BE): 1 (0x0001
(Identifier (LE): 256 (0x0100
(Sequence number (BE): 47 (0x002f
(Sequence number (LE): 12032 (0x2f00
[Response frame: 897]
(Data (32 bytes
...Data: 6162636465666768696a6b6c6d6e6f7071727374757677616
[Length: 32]
```

More from InfoSec Write-ups

Ping Power — ICMP Tunnel

More from InfoSec Write-ups

How to Make a Captive Portal of Death

0x0FFB347
Mar 8 · 5 min read
246

Nir Chako
Dec 17, 2018 · 8 min read
488

Trevor Phillips
Dec 18, 2018 · 6 min read
280

Responses

Write a response…

Conversation between Muhammad Hassoub and Mohamed Sayed.

Muhammad Hassoub
Apr 24

good work bro

1

1 response

Mohamed Sayed
Apr 24

Thank you.