

Forum:[Hack Forums](#)

Thread: [Found XSS Vulnerabilities](#)

Perica - March 20, 2020, 5:10 am

Hello, I recently found XSS vulnerability on a website but i dont know what to do i mean benefit from it.

I can contact owner of the website and tell them. Or i can benefit from it ??

Here is the picture:

<https://imgur.com/a/yUF81z6>

Sitrep - March 20, 2020, 4:15 pm

The XSS-protection header is missing, but that doesn't mean it's vulnerable by default. Have you actually found an entry point where an XSS is launched?

Also, you can benefit in some cases but it's rare and you need to know how to use a stored XSS where you also receive cookies at your end for example.

But the best thing you can do, is to contact the service owner and report the bug if you find one.(then you might get paid as a thanks).

But an online scan result as in your picture wont due, you need a real PoC (Proof Of Concept).

Hope it helped you a bit.

SIM-4199941 - March 20, 2020, 4:37 pm

(Mar 20, 2020 05:10 AM)Perica Wrote: [\[CITE\]](#) Hello, I recently found XSS vulnerability on a website but i dont know what to do i mean benefit from it.

I can contact owner of the website and tell them. Or i can benefit from it ??

Here is the picture:

<https://imgur.com/a/yUF81z6>

You can use Pixload for hack the website with just an image.. like PNG or JPG

You're a great bug finder ?

Perica - March 20, 2020, 6:49 pm

(Mar 20, 2020 04:15 PM)Sitrep Wrote: [\[CITE\]](#) The XSS-protection header is missing, but that doesn't mean it's vulnerable by default. Have you actually found an entry point where an XSS is launched?

Also, you can benefit in some cases but it's rare and you need to know how to use a stored XSS where you also receive cookies at your end for example.

But the best thing you can do, is to contact the service owner and report the bug if you find one.(then you might get paid as a thanks).

But an online scan result as in your picture wont due, you need a real PoC (Proof Of Concept).

Hope it helped you a bit.

Can i use Burp Suite or smth like that bcs i dont know how to do it manually.

Sitrep - March 20, 2020, 8:17 pm

(Mar 20, 2020 06:49 PM)Perica Wrote: [\[CITE\]](#) Can i use Burp Suite or smth like that bcs i dont know how to do it manually.

You can use burp suite for it yes, but you will have to read about the fundamentals first, to understand what XSS is and how to exploit it.

<https://owasp.org/www-community/attacks/xss/>

Some manual input will be needed most likely.

Perica - March 21, 2020, 2:21 am

(Mar 20, 2020 08:17 PM)Sitrep Wrote: [\[CITE\]](#) You can use burp suite for it yes, but you will have to read about the fundamentals first, to understand what XSS is and how to exploit it.

<https://owasp.org/www-community/attacks/xss/>

Some manual input will be needed most likely.

Thank you, really helped me.