

Forum:[Hack Forums](#)

Thread: [HELP ME TO EXPLOIT CVE-2015-9251 URGENT HELP PLEASE](#)

scannereyefox - July 1, 2023, 6:22 am

I FOUND A VULNERABLE SITE THAT USES OLDER VERSION OF JQUERY(2.2.4) WHICH IS VULNERABLE TO XSS

IN DOCUMENTATION OF CVE-2015-9251 THEY SAID: jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

but i dont know how to exploit it can any one help ? [warn]

naturewizard69 - July 3, 2023, 2:05 pm

I mean, you basically answered your own question but you can exploit it with an XSS attack and use JS to exploit it.

DramaKing - July 3, 2023, 2:21 pm

My preferred XSS scanner is XSSStrike. It will test a site for XSS and provide exploits that are successful.

scannereyefox - July 5, 2023, 12:07 pm

(Jul 3, 2023 02:21 PM)DramaKing Wrote: [\[CITE\]](#) My preferred XSS scanner is XSSStrike. It will test a site for XSS and provide exploits that are successful.

BRO IT WORKS BUT I DONT KNOW HOW TO EXPLOIT THAT AND THIS TOOL IS REALLY GREAT THANKYOU

(Jul 3, 2023 02:05 PM)naturewizard69 Wrote: [\[CITE\]](#) I mean, you basically answered your own question but you can exploit it with an XSS attack and use JS to exploit it.

IAM A NEWBIE BRUH I FOUND THAT BY AUTOMATED SCAN AND I REALLY SEARCHED FOR ITS VULNERABILITY BUT I DON'T KNOW TO EXPLOIT IT IF YOU HAVE ANY RESOURCE GIVE ME PLZ

naturewizard69 - July 5, 2023, 2:07 pm

Just google "how to make a cross-domain Ajax request" And do that for the site you are using.

DramaKing - July 5, 2023, 5:54 pm

(Jul 5, 2023 02:07 PM)naturewizard69 Wrote: [\[CITE\]](#) Just google "how to make a cross-domain Ajax request" And do that for the site you are using.

Agreed. I can't find a POC, so do your own research. Also, make sure you know what you're doing and don't be an idiot.

naturewizard69 - July 5, 2023, 6:52 pm

(Jul 5, 2023 05:54 PM)DramaKing Wrote: [\[CITE\]](#) I can't find a POC, so do your own research. Also, make sure you know what you're doing and don't be an idiot.

Why quote me on this?

DramaKing - July 6, 2023, 6:53 am

Because I was concurring. Sorry for not being clear.

scannereyefox - July 6, 2023, 9:04 am

(Jul 5, 2023 02:07 PM)naturewizard69 Wrote: [\[CITE\]](#) Just google "how to make a cross-domain Ajax request" And do that for the site you are using.

THANK YOU BRO IT HELPED ME A LOT

(Jul 5, 2023 05:54 PM)DramaKing Wrote: [\[CITE\]](#) Agreed. I can't find a POC, so do your own research. Also, make sure you know what you're doing and don't be an idiot.

OK BRUH I GETTHAT FROM YOUR POINT OF YOU THANKS

naturewizard69 - July 6, 2023, 9:37 am

(Jul 6, 2023 09:04 AM)scannereyefox Wrote: [\[CITE\]](#) THANK YOU BRO IT HELPED ME A LOT

OK BRUH I GETTHAT FROM YOUR POINT OF YOU THANKS

No problem hmu if you have any more questions

scannereyefox - July 8, 2023, 12:51 am

(Jul 6, 2023 09:37 AM)naturewizard69 Wrote: [\[CITE\]](#) No problem hmu if you have any more questions

YEAH SURE