

Forum:[Hack Forums](#)

Thread: [Session Hijacking with Reverse Proxy..](#)

Null - December 31, 2019, 11:29 am

Hey,
It's been a while since i've pose something here, anyway..
I've gotten a reverse proxy set on some PC which i'm trying to steal a session off, is this achievable in any way ?
I don't want to log in with my browser using his IP as that's clearly a different session and it may trigger stuff as mobile verification etc..
Help would be much appreciated <3

RCE - December 31, 2019, 11:32 am

Achieving full session hijacking with only a reverse proxy is not possible,
You can use HVNC to clone the current session and avoid security issues like 2fa.

Mr. Robot - December 31, 2019, 11:33 am

Depends on your full setup really. What site specifically, what country and what browser.

gsxrest8 - January 1, 2020, 7:15 am

hi Im interested to buy plz send me PM

Null - January 1, 2020, 11:39 am

(Dec 31, 2019 12:33 PM)Mr. Robot Wrote: [\[CITE\]](#) Depends on your full setup really. What site specifically, what country and what browser.
chrome and it's twitter.

Mr. Robot - January 1, 2020, 11:49 am

(Jan 1, 2020 12:39 PM)Null Wrote: [\[CITE\]](#) chrome and it's twitter.
Do they have 2auth enabled?

Null - January 1, 2020, 12:07 pm

(Dec 31, 2019 12:32 PM)RCE Wrote: [\[CITE\]](#) Achieving full session hijacking with only a reverse proxy is not possible,
You can use HVNC to clone the current session and avoid security issues like 2fa.
sorry but i don't understand what do you mean by HVNC, is that anything different from remote desktop connection?

(Jan 1, 2020 12:49 PM)Mr. Robot Wrote: [\[CITE\]](#) Do they have 2auth enabled?
SMS verification yeah

Mr. Robot - January 1, 2020, 12:21 pm

(Jan 1, 2020 01:07 PM)Null Wrote: [\[CITE\]](#) sorry but i don't understand what do you mean by HVNC, is that anything different from remote desktop connection?

SMS verification yeah
I don't know the full setup with twitter but what i'd recommend is setting up a twitter with 2fa and see what you can accomplish on your own account for testing.

Null - January 1, 2020, 12:23 pm

(Jan 1, 2020 01:21 PM)Mr. Robot Wrote: [\[CITE\]](#) I don't know the full setup with twitter but what i'd recommend is setting up a twitter with 2fa and see what you can accomplish on your own account for testing.

using just a reverse IP will do nothing, it's like using two browsers on same computer to log on the website so it will treat each browser as a separate session, i need to copy the session somehow.

Mr. Robot - January 1, 2020, 12:24 pm

(Jan 1, 2020 01:23 PM)Null Wrote: [\[CITE\]](#) using just a reverse IP will do nothing, it's like using two browsers on same computer to log on the website so it will treat each browser as a separate session, i need to copy the session somehow.

I don't know if taking a session via something like zANTI or droidsheep would work in this case.

Null - January 1, 2020, 12:27 pm

(Jan 1, 2020 01:24 PM)Mr. Robot Wrote: [\[CITE\]](#) I don't know if taking a session via something like zANTI or droidsheep would work in this case.

I'm not sure if i can use these with a reverse proxy, droidsheep alone fails to steal https sessions anyway iirc, i will do some research now that you mentioned this i kind of totally forgot i could do that lol

Update: I've successfully initiated a HVNC connection with Ozone RAT and it's so freaking awesome, the only problem is that the PC is disgustingly old so it's a pain in the ass to navigate around.

I was using Quasar Initially

Youssef Sherif - January 18, 2020, 4:10 am

Spoiler ([Click to View](#))

M3tktsH en enta mhtag hidden vnc le twitter , enta kan momkn t reverse el proxy we tnzl browser esmo Multi login we t import el cookies bt3et el victim we b3d kda t spoof el user agent fa htdkhol mn gher ay 2FA , cookies we user agent mohmen , bas cookies aham lw 3mltIha convert w import sah s3at momkn tdkhol mngher mt spoof el user agent.