

Forum: [Hack Forums](#)

Thread: [Need help reverse engineering websocket messages](#)

rarebone - September 25, 2019, 2:34 am

Hey guys, I play a game which uses a websocket to send data between the browser and the server.

Now I want to know, which message the browser sends, if I recruit troops for example, but all I see in Chromes DevTools is this binary data:

Base64: AAAAILcGjaFCX0K1T1KSgMsK+ijC0tT4WUGvAxthMLHWqAMt

I took a look at the source code and found this:

and that:

which may be interesting functions.

You can find the full script here: <https://file.io/lmx0LB>

It is not the full game, just the script that initiates the websocket.

Also good to know: It seems to be a Unity3D WebGL game.

Would be awesome if someone could help me to "decrypt" the messages. Thank you!

Nachfolger - September 25, 2019, 5:00 am

If you're paying, go to the marketplace. Otherwise, post the script url, not just screenshots.

n0s1leep - September 25, 2019, 7:51 am

The send and receive functions wont help you much, try and find the code that calls these functions instead and look for any code that packs/unpacks the data.

rarebone - September 25, 2019, 10:25 am

(Sep 25, 2019 07:51 AM)n0s1leep Wrote: [\[CITE\]](#) The send and receive functions wont help you much, try and find the code that calls these functions instead and look for any code that packs/unpacks the data.

Sounds like a good idea.

I tried to track down what happens after I click a button using Chrome Devtools Performance tab as you can see here:

but I have a hard time finding something websocket related.

Do you have an idea of what would be a good approach on that?

Traffic Solutions - September 25, 2019, 11:05 am

You can replace the script with editing windows hosts file or any network monitor(MiTM proxy, Charles, Fiddler)

Check console and you should have objects/strings printed, you can inspect objects and find it's properties and methods.

If it's encrypted/decrypted, find the encryption function and Console.Log() the input, find the decryption function and Console.Log() at the output.

_socketSend - Anywhere in function place

Console.Log("Socket Send: " + ptr)

_socketRecv - End of function try

Console.Log("Socket Recieve: " + socket.messages)

Traffic Solutions

rarebone - September 25, 2019, 11:26 am

(Sep 25, 2019 11:05 AM)Traffic Solutions Wrote: [\[CITE\]](#) You can replace the script with editing windows hosts file or any network monitor(MiTM proxy, Charles, Fiddler)

Check console and you should have objects/strings printed, you can inspect objects and find it's properties and methods.

If it's encrypted/decrypted, find the encryption function and Console.Log() the input, find the decryption function and Console.Log() at the output.

_socketSend - Anywhere in function place

Console.Log("Socket Send: " + ptr)

_socketRecv - End of function try

Console.Log("Socket Recieve: " + socket.messages)

Traffic Solutions

I see, so everytime the game sends or receives a message, the content gets logged.

How exactly can I replace the script? Because as far as I can see, the script has a different name on every page reload.

I also tried tracking the function calls and got that:

So the send function gets called by many wasm-functions, which look like that:

Traffic Solutions - September 25, 2019, 11:37 am

(Sep 25, 2019 11:26 AM)rarebone Wrote: [\[CITE\]](#) I see, so everytime the game sends or receives a message, the content gets logged.

How exactly can I replace the script? Because as far as I can see, the script has a different name on every page reload.

I also tried tracking the function calls and got that:

So the send function gets called by many wasm-functions, which look like that:

Feature name "auto replacing"/"auto responder" or something like this, you can regex page name to replace.

n0s1eep - September 25, 2019, 11:53 am

This is WebAssembly code, meaning that it is a lot more difficult to read than pure JavaScript. I know there are some wasm disassembler tools that can convert it back to C, google for "wasm disassembler".

I have no personal experience with this though, maybe someone else can help.

rarebone - September 26, 2019, 2:48 am

(Sep 25, 2019 11:05 AM)Traffic Solutions Wrote: [\[CITE\]](#) You can replace the script with editing windows hosts file or any network monitor(MiTM proxy, Charles, Fiddler)

Check console and you should have objects/strings printed, you can inspect objects and find it's properties and methods.

If it's encrypted/decrypted, find the encryption function and Console.Log() the input, find the decryption function and Console.Log() at the output.

_socketSend - Anywhere in function place

Console.Log("Socket Send: " + ptr)

_socketRecv - End of function try

Console.Log("Socket Recieve: " + socket.messages)

Traffic Solutions

I tried editing the script in Chrome Dev Tools Sources tab but that didn't work. Also I can't replace the script with mine in the first place, because its name changes on each reload and I have no idea where this name is generated. Anyone has an idea?