

Forum:[Hack Forums](#)

Thread: [An Old, Long Story - Runescape Private Server Exploit](#)

SIM-2501407 - January 24, 2022, 6:00 pm

Wrote this up a long time ago, but I felt like sharing it here. Maybe someone will find the story interesting.

There's no tldr. Read it or don't.

Quote:During my prime of bug abuse, I was extremely dedicated into finding exploits. This story is about finding a smuggle on a once popular server, SoulPlay. Now, prior to this finding there were many other smuggles of dungeoneering. Some of these include using the bank interface and the bank pin interface. However, this is by far the most extensive and complex smuggle I, and probably anyone, has done in the Runescape Private Server Community.

To begin the story, I will start off by stating that I was using Cheat Engine to find various interfaces on SoulPlay. After a few hours of trial and error of dozens interfaces, I came across a single interface that went unchecked. Only one chat interface out of the entire server was able to be forced and interacted with. If I spoke to a NPC or had some form of dialogue occurring and the dialogue ended abruptly (e.g. walking away using the minimap), I could use that interface to continue the interaction. As to why it was only this one interface, I cannot say for certain the reason for this case. Knowing this information, I went around the entire server, speaking to every NPC that existed, in hopes that one of them would allow to teleport. Unfortunately, none of the NPC dialogues with this given interface ID had an option to teleport.

However, I was not one to give up on my mission to find a use-case (exploit) of this bug. Me, being autistic in this scenario, ran around the whole map, interacting with everything. With luck, I came across the lumbridge gate to the desert, and just so happened it was using the very interface that I was looking for! Using the dialogue, you would be teleported to the other side of the gate. Perfect for my purposes!

My brain immediately thought "what if i use this 1 block force teleport to get outside duel arena or castle wars?" I took this theory and ran with it, quite literally (more on this soon). Alas, I quickly came to realize that a single block teleport would not get me out of duel arena. Knowing this information, I tried my luck from castle wars. Using the same strategy, I forced the single interface to teleport outside of the castle wars arena (thanks to jagex for having the observation wall). With excitement, I ran to dungeoneering, entered the lobby, then into the dungeon. My high hopes came crashing down after the castle wars game ended. My character was not force teleported out. They seemed to have blocked teleports, including forced ones (meaning an admin would not even be able to do a ;;teletome command) while I am in the dungeon.

Again, at this point, I was not going to accept defeat. My solution: adding duel arena into the mix. So again, we waited for castle wars to begin; used our 1 time use and 1 block force teleport to get outside of castle wars. From there, I ran all the way to the duel arena. On my second account, I offered a summoning scroll and tabs alongside it. Duel arena did not have the same check as dungeoneering. Meaning once the castle wars game ended, I was sent back to outside the minigame. Due to lack of area checks, I was now in a duel without being in the restricted area. I then ran back to the dungeoneering lobby and entered dungeon. Knowing the previous information, I made my second account forfeit the duel, giving my main character the tools of destruction. I was able to spawn the familiar within the dungeoneering area and also was able store items. Finally,

after hours and hours of hunting and trying everything, I was able to smuggle items out.

Funny story, the first time I did this, I summoned the NPC inside the dungeoneering lobby and I found out the hard way there was an additional check when talking to the NPC to enter for spawned familiars (and pouches), so it did not work. Also, if I recall correctly, it did not work with the lower level storing familiars; only the higher ones. Again, not able explain this either.

Hope you enjoyed my story about SoulPlay. It certainly was one of, if not the most, complex and niche bug abuse stories I have ever done. Let this be a lesson to always have area checks, even if you believe there is no way of packet or interface exploitation. It is always better be safe than sorry.

neightworks. - February 4, 2022, 2:51 pm

Seems like a lot of work to smuggle items out of an RSPS but I'm sure it felt rewarding. Did they have alch value?

SIM-2501407 - February 4, 2022, 10:27 pm

(Feb 4, 2022 03:51 PM)neightworks. Wrote: [\[CITE\]](#) Seems like a lot of work to smuggle items out of an RSPS but I'm sure it felt rewarding. Did they have alch value?

None of which i can remember, ahaha.

Though, thanks to the devs at ultimatescape2 back in the day for having custom castle wars capes that were worth 10m a pop. Had a script automatically smuggling it (via bank pin interface IIRC)

But it was about beating the challenge. Smuggles we're always my favorite. No impact to the economy, but still required quite of bit of knowledge and skill. It was a super fun challenge to me.

That's honestly why i enjoyed exploiting on RSPS. While it was easy to pick up, I had to have a great understanding of the game mechanics, and I was live pen-testing with instant results 99% of the time.

Oh this didn't work? Let me try this... hmmm, okay, i see maybe this exploit will be possible, and let me go try playing around with this too. Always trying to find a loophole with something. Was great for my ADHD mind

Obviously at times i was strictly going for duplications. Wasn't the most friendly of players back in the day either; I'd drop gold and whatnot. But on the flip side, i also sold exploits or gave methods of patching (if it was a Oday) to some in the community.

Spoiler [\(Click to View\)](#) i really should get into pentesting and security as a full time job

jcole - February 5, 2022, 12:06 pm

I never remember a popular server called Soulplay I do remember Soulsplit.

Edit: I watched a few videos from SohanRS and saw that the owners remade the server after it shutdown as "Forgotten Paradise".