

Forum:[Hack Forums](#)

Thread: [SOL SPIN](#)

sensei1312 - September 5, 2026, 8:10 pm

Thank me later boys ?

[Deleted] delete space

Charlie Sheen - September 5, 2026, 9:18 pm

Well, I looked into this before anyone decided to connect a wallet to it.

This was a scam.

I pulled the source and started going through the JavaScript. The entire “Solana Spin” game is bullshit.

The spin is rigged so everybody wins 5 SOL. It's not random. The code literally places 5 as the target on all three reels and then animates them to it.

The “recent wins” scrolling across the site are fake too. The site generates random Base58-looking wallet addresses in JavaScript, randomly assigns them winnings between 0.5 and 10 SOL, labels them JUST NOW, and continuously adds new fake winners every few seconds.

The 4,827 users online is a hard-coded number that randomly moves up and down.

The 12,483 SOL jackpot is a hard-coded number that JavaScript automatically increases.

The NEXT DROP countdown is just a client-side timer.

Basically every piece of “live activity” you see on the site is fabricated.

So what's the point?

You “win” the guaranteed 5 SOL and then get:

“Your reward is ready. Connect your wallet to continue.”

That's where things get much more interesting.

The wallet functionality is hidden in a separate, heavily obfuscated ~1MB JavaScript bundle. I pulled that apart too.

It contains actual Solana wallet functionality for signTransaction, signAllTransactions, signMessage, SPL/Token-2022 tokens, SOL, USDC, transaction instructions, etc.

More importantly, it enumerates the assets in the wallet you connect and calculates their USD value.

Think about that for a second.

You're supposedly there to receive the 5 SOL you just "won." Why does the website need to find out what tokens you already own and calculate how much they're worth?

I also extracted six Solana addresses hard-coded inside the obfuscated application:

```
6ugBBLhRJqsuB1H4G6rGBMCyMWjdFpvpEUKnp6XCB1t7
9piPeQWJ7wxGmsWieeJhQKJ13DjJLga9j8CE5ydLTHC6
6ARSYR2B1aPWSjK11ZXDPmApgLgar3bCrm2BTYGS2jBK
4qti6FcMybVSLL2k4rqRQ3Ph1a2jGrzPmBN8Wmt4A5wr
HsVYhMDQRf6CkjdUzqNDNRfDwsgw9nAX8feLVC3TAGp
4moJ9mfFDqFgGMp5UJUgcVhAaFtBxiapt9DVJE3LcVao
```

I'm not going to claim those are all confirmed receiving addresses without a victim transaction proving it. But they're deliberately embedded in the wallet code.

Interestingly, the bottom two are currently active, and I found both of them appearing as recipients in the same recent on-chain transaction, so there is an independent blockchain connection between two addresses extracted from the site's code.

The domain itself was only registered July 24, 2026.

So yeah...

Fake casino. Fake jackpot. Fake winners. Fake online users. Guaranteed fake 5 SOL win, followed by an obfuscated wallet application that inventories the value of the wallet you connect and has transaction-signing capabilities.

"Thank me later boys" indeed.

Banned.

CL1B - September 6, 2026, 12:52 am

(Sep 5, 2026 09:18 PM)Charlie Sheen Wrote: [\[CITE\]](#) Well, I looked into this before anyone decided to connect a wallet to it.

This was a scam.

I pulled the source and started going through the JavaScript. The entire "Solana Spin" game is bullshit.

The spin is rigged so everybody wins 5 SOL. It's not random. The code literally places 5 as the target on all three reels and then animates them to it.

The "recent wins" scrolling across the site are fake too. The site generates random Base58-looking wallet addresses in JavaScript, randomly assigns them winnings between 0.5 and 10 SOL, labels them JUST NOW, and continuously adds new fake winners every few seconds.

The 4,827 users online is a hard-coded number that randomly moves up and down.

The 12,483 SOL jackpot is a hard-coded number that JavaScript automatically increases.

The NEXT DROP countdown is just a client-side timer.

Basically every piece of “live activity” you see on the site is fabricated.

So what's the point?

You “win” the guaranteed 5 SOL and then get:

“Your reward is ready. Connect your wallet to continue.”

That's where things get much more interesting.

The wallet functionality is hidden in a separate, heavily obfuscated ~1MB JavaScript bundle. I pulled that apart too.

It contains actual Solana wallet functionality for signTransaction, signAllTransactions, signMessage, SPL/Token-2022 tokens, SOL, USDC, transaction instructions, etc.

More importantly, it enumerates the assets in the wallet you connect and calculates their USD value.

Think about that for a second.

You're supposedly there to receive the 5 SOL you just “won.” Why does the website need to find out what tokens you already own and calculate how much they're worth?

I also extracted six Solana addresses hard-coded inside the obfuscated application:

```
6ugBBLhRJqsuB1H4G6rGBMCyMWjdFpvpEUKnp6XCB1t7
9piPeQWJ7wxGmsWieeJhQKJ13DjJLga9j8CE5ydLTHC6
6ARSYR2B1aPWSjK11ZXDPMagLgar3bCrm2BTYGS2jBK
4qti6FcMybVSLL2k4rqRQ3Ph1a2jGrzPmBN8Wmt4A5wr
HsVYhMDQRf6CkjdUzqNDNRfDwsgw9nAX8feLVC3TAGp
4moJ9mfFDqFgGmp5UJUgcVhAaFtBxiapt9DVJE3LcVao
```

I'm not going to claim those are all confirmed receiving addresses without a victim transaction proving it. But they're deliberately embedded in the wallet code.

Interestingly, the bottom two are currently active, and I found both of them appearing as recipients in the same recent on-chain transaction, so there is an independent blockchain connection between two addresses extracted from the site's code.

The domain itself was only registered July 24, 2026.

So yeah...

Fake casino. Fake jackpot. Fake winners. Fake online users. Guaranteed fake 5 SOL win, followed by an obfuscated wallet application that inventories the value of the wallet you connect and has transaction-signing capabilities.

“Thank me later boys” indeed.

Banned.

Goodjob on this bullshit

