Subject: Serial Hashing, How Secure?
Posted by a000clown on Sun, 22 Feb 2009 02:50:55 GMT
View Forum Message <> Reply to Message

If I tell someone what my password is under a salted md5 hash chances are pretty much nil they'll be able to get the original password using rainbow tables, so I'd like to know how secure the method is on our Renegade serials.

Reason I'm asking is I want to enable automatic moderator logins, but to keep things safe I will be restricting their nickname to their specific serial hash.
Since other servers can easily find their hash if they play there, I want to know if it's possible to generate that same exact hash value without knowing the original serial. In other words, is what I plan to do secure or not?

Subject: Re: Serial Hashing, How Secure?
Posted by raven on Sun, 22 Feb 2009 05:09:34 GMT
View Forum Message <> Reply to Message

It's fairly secure. From what I recall, the serial hash is generated by the original serial being hashed twice via md5.

I'd say its pretty damn secure.

Edit: However.. RoShamBo does bring up a good point. Someone could send a fake string containing the hash to the server.. so you wouldn't need to reverse the hash cos you could send it directly

Subject: Re: Serial Hashing, How Secure?
Posted by jnz on Sun, 22 Feb 2009 07:48:41 GMT
View Forum Message <> Reply to Message

raven wrote on Sun, 22 February 2009 05:09It's fairly secure. From what I recall, the serial hash is generated by the original serial being hashed twice via md5.

I'd say its pretty damn secure.

No, it's not secure at all. It's extremely trivial to fake a serial.

EDIT: Although it would be fairly difficult to retrieve the original, I suppose.

Subject: Re: Serial Hashing, How Secure?
Posted by raven on Sun, 22 Feb 2009 08:26:42 GMT
View Forum Message <> Reply to Message

Aye, that's what I was talking about.. reversing the hash to get the actual serial.

Subject: Re: Serial Hashing, How Secure?
Posted by a000clown on Mon, 23 Feb 2009 06:07:11 GMT
View Forum Message <> Reply to Message

RoShamBo wrote on Sun, 22 February 2009 02:48raven wrote on Sun, 22 February 2009 05:09It's fairly secure. From what I recall, the serial hash is generated by the original serial being hashed twice via md5.

I'd say its pretty damn secure.

No, it's not secure at all. It's extremely trivial to fake a serial.

EDIT: Although it would be fairly difficult to retrieve the original, I suppose.
So you're saying if the hashed version of my serial was 1234 and someone knew this, it would be easy for them to tell the server 1234, but not easy for them to figure out the original. That right?

Subject: Re: Serial Hashing, How Secure?
Posted by reborn on Mon, 23 Feb 2009 07:34:30 GMT
View Forum Message <> Reply to Message

Yeah, I'm sure that's what he's saying. So if they played in other servers and that server owner decided to retrieve there serial hash, that person could potentially spoof it.
Pretty unlikely to happen I guess. I don't know many server owners that would care enough to do this, but I suppose it could happen.

Subject: Re: Serial Hashing, How Secure?
Posted by jnz on Mon, 23 Feb 2009 12:29:32 GMT
View Forum Message <> Reply to Message

reborn wrote on Mon, 23 February 2009 07:34Yeah, I'm sure that's what he's saying. So if they played in other servers and that server owner decided to retrieve there serial hash, that person could potentially spoof it.
Pretty unlikely to happen I guess. I don't know many server owners that would care enough to do this, but I suppose it could happen.

If a server owner decided to ban on some one's serial, that banned person could send a random serial to the server. Wol or not.