

# Myanmar Security Forum

[HOME](#)
[MEMBERS](#)
[HELP DOCS](#)
[UPGRADE](#)
[AWARDS](#)
[BLACKLIST](#)
[GROUPS](#)
[NEW POSTS](#)
[Hacking](#) > [Cryptography](#) > [Hash Types \[GhostArea\]](#)

[Myanmar Security Forum - MSF](#)

[TODAY'S POSTS](#)
[Thread Rating:](#)
[New Reply](#)
[Hash Types \[GhostArea\]](#)
[Thread Modes](#)

**DaiChinLay**

Code Breakers


 Posts:  
1,173  
Threads:  
0  
Thanks  
Received:  
474 in  
261 posts  
Thanks  
Given:  
380  
Joined:  
Oct 2013  
Reputatio  
n: **56**


02-13-2016, 12:03 AM (This post was last modified: 02-13-2016, 12:04 AM by DaiChinLay.)

#1

ပထမဦးဆုံး Hash ဆိုတာ ဘာလဲပြောရအောင်။ ကျွန်တော်တို့ Forum တစ်ခုထဲကို ပင်တုံအခါ Password ရိုက်သွင်းလိုက်ရင် ဒဲ့ဒဲ့ Password ဟာ Web Server ကသတ်မှတ်ထားတဲ့ Table တစ်ခုထဲ

ကို ပင်သွားပြီး အဲဒီ Password ဟာ Table ထဲက Alogrithum အလိုက် အသွင်ပြောင်းလဲသွားပါတယ်။ ဒီလိုပေါ့ f5d1278e8109edd94e1e4197e04873b9 ဟာ သာမန် ကျွန်တော်တို့ရိုက်လိုက်တဲ့ ရိုးရိုး Password ကို Plain Text လို့ ခေါ်ပြီး Hash Table က ထွက်လာတဲ့ ဟာကိုတော့ Hash လို့ခေါ်ပါတယ်။ ဥပမာ Plain Text ဟာ tester ဖြစ်ရင် Hash ကတော့ လူဖတ်မရတဲ့ f5d1278e8109edd94e1e4197e04873b9 ပေါ့ Hash ကို ဘယ်သောအခါမှာ Plain Text အဖြစ်ပြောင်းလဲလို့မရတော့ပါဘူး။ Hash ကို Decrypt လုပ်နိုင်တယ်ဆိုတာ တစ်ကယ်တော့လုံးမဟုတ်ပါဘူး။ Plain Text အဖြစ်ပြောင်းတာဟာလည်း Decrypt လုပ်တာမဟုတ်ဘဲ Brute Force လုပ်တာပါ။ နောက်မှ အဲဒီ အပိုင်းကို သေချာရှင်းပြပါမယ်။

tgဒါဆို ဘယ်လို Access Gratiended ဖြစ်သလဲဆိုတော့ ကျွန်တော်တို့ Plain Text အဖြစ်ရိုက်သွင်းလိုက်တဲ့ Pass ဟာ Hash Table ကို ဖြတ်ပြီး Hash ဖြစ်သွားပါတယ်။ အဲဒီ Hash နဲ့ နဂို Password ကိုသတ်မှတ်တုန်းက Data Base ထဲမှာ သိမ်းထားတဲ့ Hash တိုက်စစ်လို့တူတဲ့ အခါမှာ Access Gratiended ဖြစ်ပြီး မတူညီတဲ့အခါမှာတော့ Access Denied ပေါ့ဗျာ။ (တကယ်လို့ ခင်ဗျားသာ Web Server ထဲက Password တွေကို Hijack လုပ်ယူနိုင်တယ်ဆိုရင် Plain Text နဲ့ ထွက်ပေါ်လာဖို့ ခဲယဉ်းပါတယ်။ Web Server အများစုက Hash Table မှားနဲ့ Crypt ထားတဲ့အတွက် Hash တွေပဲ ထွက်လာမှာဖြစ်ပါတယ်။ ဒီလို Hash တွေကိုဖြည့်ဖို့ Hash Type တွေကို သိဖို့လိုလိမ့်မယ် )

ကဲ ဒါဆို Hash ဆိုတာ ဘာလဲ သိလောက်ပါပြီ။ Type of Hash ဆိုတာလေးစရအောင် 🤖

ပထမဆုံး အသုံးအများဆုံး Hash ဖြစ်တဲ့ MD5 Hash အကြောင်းစပျာမယ်။

### MD5 Hash

MD5 Hash မှာ အလုံးပေါင်း သုံးဆယ့်နှစ်လုံးပါဝင်ပါတယ် ( 128 Bit Encryption ပေါ့ဗျာ ) a-z နဲ့ 0-9 ပါဝင်ပါတယ်။

Code:

ဥပမာ - f5d1278e8109edd94e1e4197e04873b9

တကယ်လို့ အထက်က အချက် တစ်ခုခုနဲ့မတူရင် MD 5 Hash မဟုတ်ပါဘူး။

### SHA1

SHA1 Hash ဟာလည်း အသုံးများတဲ့ Hash Type တွေထဲမှာပါဝင်ပြီး ပိုမို လုံခြုံမှုရှိပါတယ်။ SHA1 Hash မှာ အလုံးပေါင်းလေးဆယ်ပါဝင်ပါတယ် ( 160 Bit ပေါ့ ) အရင်အတိုင်းပဲ a-z , 0-9 ပါဝင်ပါတယ်။

Code:

ဥပမာ - ab4d8d2a5f480a137067da17100271cd176607a1

### MySQL < 4.1

ဒီ Hash Type ကတော့ MySQL Version 4.1 အောက်က Server တွေမှာ အသုံးများပြီးတော့ ဒီ Type ကို မြင်တာနဲ့ Defacer ပေါက်စတွေဟာ မှာယာ ခပ်တတ်ကြပါတယ်။ သူ့မှာ Character 16 လုံးပဲရှိပါတယ် ( 64 bits ရှိပါတယ် )။ ထုံးစံအတိုင်း a - z , 0 - 9 ရှိပါတယ်။

Code:

ဥပမာ - 606727496645bcba

### MySQL5

အရင်တုန်းက ကျွန်တော်ကို ဒုက္ခ အပေးဆုံး Type တစ်ခုပါ။ အဲဒီတုန်းက Hash Type တွေကိုလည်း သိရသိ Skill ကလည်းနာသေး ( ခုလည်းနာတာပဲ 🙄 ) တော့ ဟိုလူကယ်ပါ ဒီလူကုပါပေါ့ဗျာ ဟီး သူကတော့ နောက်ထွက်တဲ့ MySQL Version တွေမှာ အသုံးပြုပါတယ်။  
သူက ပိုဆိုးတယ်ဗျာ Character ၄၁ လုံးရှိတယ်။  
အားလုံးက Capital Letter တွေရည်း။  
ပြီးတော့ ခရပွင့် Star ( \* ) နဲ့ စသဗျာ။

**Code:**

ဥပမာ - \*C8EB599B8E8EE7BE9F1A5691B7BC9ECCB8DE1C75

**MD 5 ( WordPress )**

ကျွန်တော် အကြောက်ဆုံး Hash ပါ။ ဘယ်လောက်ထိလဲဆို SQL Injection လုပ်လို့ Pass ကို ဒီ Hash ထွက်ရင် လှည့်ကိုမကြည့်တော့ဘူး။ အဲဒီ ဆိုဒ်ကို လက်လျှော့ပစ်တယ် ။ အဲဒီအထိဆိုးပါတယ် ဟီး 🙄  
သူ့မှာ \$P\$ နဲ့စပါတယ်။  
0-9 A-Z a-z အစုံကိုပါပါတယ်။  
သုံးဆယ့်လေးလုံးရှိပါတယ်။  
ကြည့်လိုက်ပါ

**Code:**

\$P\$9QGU5R07ob2qNMbmSCRh3Moi6ehJZR1

**MD 5 (phpBB3 )**

phpBB3 နဲ့ဆောက်ထားတဲ့ Forum တွေမှာအသုံးပြုပါတယ်။  
\$H\$ နဲ့စပါတယ်။  
MD 5 WordPress လိုပဲ အစုံပါပါတယ်။  
Character သုံးဆယ့်လေးလုံးရှိပါတယ်။

**Code:**

ဥပမာ - \$H\$9xAbu5SruQM5WvBldAnS46kQMEw2EQ0

ကဲ ဒါဆို Hash Type အစုံကို သိလောက်ပါပြီ။

အရင်က Ghost Area က အကိုတစ်ယောက်ရေးထားတဲ့ post လေးပါ။ သိမ်းထားတာ... note လေးတွေ မွှေးရင်း တွေ့လို့ share လိုက်တာ။ 🙏

 **The following 2 users say Thank You to DaiChinLay for this post:**

• Bu5t0r, Hacke3erDD

PM Find

Reply Quote Report

**j0hnphy0**

Engineers From Mawlamyine(EFM)



Posts: 119  
 Threads: 0  
 Thanks Received: 61 in 21 posts  
 Thanks Given: 14  
 Joined: Jan 2016  
 Reputation: **49**

02-13-2016, 12:37 AM

#2

အရမ်းအကိုးရှိတဲ့ ပိုက်လေးပါ ဗတ်မှတ်လေ့လာသွားပါတယ် ကျေးဇူးတင်ပါတယ်... : nose :

PM Find

Add Thank You

Reply

Quote

Report

**abcd**

Junior Member



Posts: 22  
 Threads: 0  
 Thanks Received: 5 in 3 posts  
 Thanks Given: 5  
 Joined: Feb 2016  
 Reputation: **5**

02-13-2016, 01:50 AM (This post was last modified: 02-13-2016, 01:50 AM by abcd.)

#3

MD5 (phpbb3) ဆိုတာ Custom MD5 ဖြစ်ပုံရပါတယ်။ ဖိုရမ် admin က experienced programmer တစ်ယောက်ဖြစ်ခဲ့ရင် ထပ်ပြင်လို့ရပါသေးတယ်။ ဒီ hash ကို ပြန်ဖော်ဖို့က Main value ၄ ခုကို သိရပါမယ်။ ဒီတော့ login.php က hash algorithm ကို အရင်ဆုံးသိအောင်လုပ်ပြီး rainbow table ဖန်တီးမှပဲ ရလုံးနဲ့အောက် password တွေကို ဖော်နိုင်မှာပါ။ Ready-made tool, table တွေကတော့ အလုပ်ဖြစ်မှာ မဟုတ်ပါဘူး။

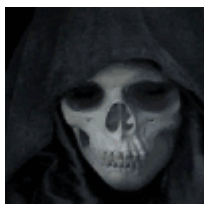
PM Find

Add Thank You

Reply

Quote

Report

**133720**

~I love Coding~ Fuck Girl.



Posts: 2,521  
 Threads: 0  
 Thanks Received:

1,375 in  
951 posts  
Thanks  
Given:  
758  
Joined:  
Jun 2013  
Reputatio  
n: **272**



02-13-2016, 01:56 AM

#4

mybb မှာ Hash value and salt နှစ်ခုသိရင်လည်းမောလိုရပါတယ်ဘရို

## WEB DEVELOPMENT & SECURITY

PM Find

Add Thank You

Reply

Quote

Report



abcd ●

Junior Member



Posts: 22  
Threads:  
0  
Thanks  
Received:  
5 in 3  
posts  
Thanks  
Given: 5  
Joined:  
Feb 2016  
Reputatio  
n: **5**



02-13-2016, 02:06 AM (This post was last modified: 02-13-2016, 02:11 AM by abcd.)

#5

**133720 Wrote:**

(02-13-2016, 01:56 AM)

mybb မှာ Hash value and salt နှစ်ခုသိရင်လည်းမောလိုရပါတယ်ဘရို

I meant that we can decrypt ready-made mybb and other boards scripts only. Can't decrypt admin-modified custom MD5 coz we need to know 4 initialized hex values and other info. Am I wrong? :-)

U can see my Reversing Challenge 10 program.

It is similar SHA512. But I modified final password. :-) :-) :-)

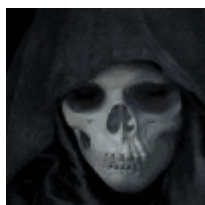
PM Find

Add Thank You

Reply

Quote

Report



**133720**

~I love Coding~ Fuck Girl.



Posts:

2,521

Threads:

0

Thanks

Received:

1,375 in

951 posts

Thanks

Given:

758

Joined:

Jun 2013

Reputatio

n: **272**



02-13-2016, 02:13 AM

#6

#### Quote:

ဒီ hash ကို ပြန်ဖော်ဖို့က Main value ငှ ခုကို သိရပါမယ်

I mean this bro. Yes we can change the hash type in mybb by edit the socure code. but if attacker get the source. it also can decrpyt. i think it little more safe. better way to use is 2 step verification in mybb.

**WEB DEVELOPMENT & SECURITY**

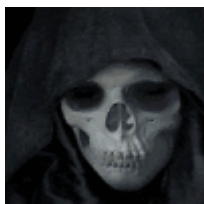
PM Find

Add Thank You

Reply

Quote

Report

**133720**

~I love Coding~ Fuck Girl.



Posts:

2,521

Threads:

0

Thanks

Received:

1,375 in

951 posts

Thanks

Given:

758

Joined:

Jun 2013

Reputatio

n: **272**

02-13-2016, 02:15 AM

#7

**abcd Wrote:**

(02-13-2016, 02:06 AM)

U can see my Reversing Challenge 10 program.

It is similar SHA512. But I modified final password. :-) :-) :-)

I not good at reversing. and don't understand C# and vb.net. That why i can't solve your challenge.

**WEB DEVELOPMENT & SECURITY**

PM Find

Add Thank You

Reply

Quote

Report

**KpZ**

MSF VIP Member

Posts:

241

Threads:

0



Thanks  
Received:  
39 in 32  
posts  
Thanks  
Given: 73  
Joined:  
Aug 2015  
Reputatio  
n: **15**



02-13-2016, 07:36 AM

#8

Nice Thread Bro ..note အဖြစ်မှတ်ထားရမယ်.



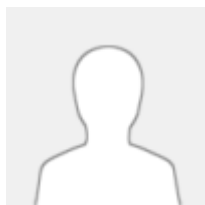
PM Find

Add Thank You

Reply

Quote

Report

**Talphax** ●

Newbie



Posts: 5  
Threads:  
0  
Thanks  
Received:  
0 in 0  
posts  
Thanks  
Given: 0  
Joined:  
Mar 2016  
Reputatio  
n: **-2**

03-22-2016, 07:05 PM

#9

Covered a few hashes that weren't familiar, thanks.

PM Find

Add Thank You

Reply

Quote

Report

**banana** ●

Junior Member




Posts: 17  
Threads:  
0  
Thanks  
Received:  
1 in 1  
posts  
Thanks  
Given: 28  
Joined:  
Jun 2016  
Reputatio  
n: **0**

07-09-2016, 02:56 AM

#10




Quick Reply 

PM Find **Add Thank You** Reply Quote Report

« **Next Oldest** | **Next Newest** »

Enter Keywords Search Thread

New Reply

Quick Reply 

**Message**  
Type your reply to this message here.

☐ **Disable Smilies**

Post Reply Preview Post

Possibly Related Threads...				
Thread	Author	Replies	Views	Last Post
Cryptography : Identify Different types of Hashes	Pix3l P0w3r	1	74	11-16-2015, 03:16 PM Last Post: garyz
Hash Types	Lotus Black	7	188	09-21-2015, 09:49 AM Last Post: KpZ
Hash Cracking Online Site Lists [ Big Collections ]	133720	3	74	06-14-2015, 07:21 PM Last Post: 3rr0rL@y
Cracking Hash with MorXCrack [Tut]	Luna	1	67	06-13-2015, 11:44 AM Last Post: Hades.y2k
Hash Decrypter Online tools	Luna	5	111	05-30-2015, 04:21 PM Last Post: th3lolipop

[View a Printable Version](#)

[Subscribe to this thread](#)

Forum Jump:

Go

Users browsing this thread: Hacke3erDD

Myanmar Security Forum (MSF) Powered By MyBB, © 2002-2016 MyBB Group. — Theme by FlatInk LLC.  
© 2013 - 2016 - All Rights Reserved.      [Contact Us](#) — [Return to Top](#) — [Lite \(Archive\) Mode](#) — [RSS Syndication](#) | [Awards](#)