

# Myanmar Security Forum

HOME   MEMBERS   HELP DOCS   UPGRADE

AWARDS   BLACKLIST   GROUPS   Myanmar Security Forum - MSF NEW POSTS

Hacking > Cryptography > Hashing  
အကြောင်း


Search Poly...

Search

TODAY'S POSTS


Thread Rating:   New Reply


Hashing အကြောင်း   Thread Modes



133720

~I love Coding~ Fuck Girl.





Posts: 2,521

Threads: 0

Thanks Received: 1,375 in 951 posts

Thanks Given: 758

Joined: Jun 2013

Reputation: 272



📅 06-28-2013, 02:03 AM

#1

hashing လုပ်တယ်ဆိုတာ data တွေကို အပိုင်းပိုင်းလေးတွေခွဲထုတ်လိုက်တာပါပဲ။ String or Integer အဖြစ်ပြောင်းလဲသွားပါတယ်။  
web developer တွေအသုံးများတဲ့ function တစ်ခုကတော့ md5 ဆိုတာပါ။  
မတူညီတဲ့ languages and systems တွေမှာအတော်လေးအသုံးများတာကိုလည်းတွေ့ရပါတယ်။

#### Code:

```
$name="cyberoot";  
$hash= md5($name);  
echo $hash; //691da7f884a723202cc16371b69b678c
```

md5() function သုံးပြီးလုပ်တဲ့ data တွေဟာဆိုရင် အမြဲတမ်း 32 character string အဖြစ်ပြောင်းလဲသွားပါတယ်။

ဒါပေမယ့် ဒါက hexadecimal character(0 – F) တွေသာ ပါဝင်တာပါ။ 128-bit (16byte) ကိုလည်းကိုယ်စားပြုပါတယ်။ တူတူပဲပေါ့ဗျာ။

hashing ကိုဘယ်မှာသုံးလဲဆိုရင်တော့

user registering လုပ်တဲ့ password field တွေမှာသုံးပါတယ်။

ပြီးတော့ password insert လုပ်တဲ့အခါ password ကို md5 အဖြစ်ပြောင်းပြီး သုံးကြတာများပါတယ်။

ဒါကြောင့် ကျွန်တော်တို့ admin password တွေကိုရှာတဲ့အခါ password ကို hashing အဖြစ်တွေ့ရပါတယ်။

ဒါက မလုံခြုံပါဘူး။ ဘာကြောင့်လဲဆိုတော့ ကျွန်တော်တို့ ပြန်ပြီး decrypt ပြန်လုပ်လို့ရလို့ပါပဲ။

အရင်တုန်းက Crc32 ဆိုတဲ့ hash script ကိုလည်းတော်တော်လေးသုံးခဲ့ပါသေးတယ်။

သူကတော့ နောက်ပိုင်းလူသိနည်းလာတယ်။ နည်းနည်းလည်းကြာပြီးဆိုတော့

**လေ့လာကြည့်ရအောင်**

#### Code:

```
echo crc32('cyberoot_hash');  
  
// output is 4ab4649b
```

အခုဆိုရင် ကျွန်တော် database လေးခိုးခံထိတယ်ဆိုပါစို့ database မှာစောစောတုန်းက hashing လုပ်ထားတဲ့ value လေးရှိတယ်ဗျာ။

အဲဒီ hash လေး 4ab4649b ကို cyberoot\_hash လို့ပြောင်းလို့မရနိုင်ပါဘူး။ ဒါပေမယ့် အခြား password

အဖြစ် နဲ့ တူညီတဲ့ hash value ကိုပြောင်းလဲနိုင်ပါတယ်

decrypt ပြန်လုပ်တဲ့ သဘောပါပဲ အောက်မှာပါ

[View Spoiler](#)

အပေါ်က code ကို run လိုက်တဲ့အခါမှာတော့ hash ကို string အဖြစ်ပြန်လည်ပြောင်းလဲပေးမှာဖြစ်ပါတယ်

ဒါဆိုရင်စောစောက ကျွန်တော်တို့ သုံးခဲ့တဲ့ cyberoot\_hash ဆိုတဲ့ အစား decrypt လုပ်တဲ့ string ကိုပြန်ပြီးအသုံးပြုနိုင်ပါတယ်

ဒါက login page ထဲကို အဆင်ပြေအောင် ပြန်ပြီးဝင်ရောက်နိုင်ပါတယ်

ကျွန်တော်တို့ script ကို run လိုက်တဲ့အခါ မှာ output အနေနဲ့ BZIXMjY50TAwCk== လို့ ထုတ်ပေးတယ်ဆိုပါစို့

ဒီလိုပါ

#### Code:

```
echo crc32('cyberoot_hash'); //outputs :4ab4649b

echo crc32('BZIXMjY50TAwCk=='); //outputs :4ab4649b
```

အဖြေက တူတူပဲထွက်ပါတယ်

စိတ်ပူသွားပြီလား သင့်ရဲ့ security လေးကို ဟီး ဆက်ရှင်းမယ်ဗျာ ကြောက်နဲ့ (အပူရှိရင်အအေးရှိရမယ် တွ)

ဒီလိုနည်းလည်းကိုကာကွယ်ဖို့ နည်းလမ်းရှိပါတယ်

md5() function ကိုသုံးတာလည်းကောင်းပါတယ် ဒါက 128 bit hashes အဖြစ် generate လုပ်ပေးပါတယ်

နောက်ပြီး sha1() function က ပိုပြီးတော့ ကောင်းပါတယ် သူကတော့ 160 -bit hash value ပါ

md5 ထက် sha1 က ပိုပြီး ရှည်ပါတယ် ဒါပေမယ့် ဒီလိုရိုးရိုး နည်းတွေကလည်း စိတ်မချရသေးပါဘူး

Rainbow Table သုံးပြီးတိုက်ခိုက်ရင် ထိမှာသေချာပါတယ် ဒီတော့ ပိုကောင်းအောင်ဘယ်လိုလုပ်မလဲဆိုတာကို စဉ်းစားရပါမယ်

အောက်ကရေးထားတာကိုကြည့်ပါ

#### Code:

```
$password = "easypassword"; //password ကို ပုံမှန်အတိုင်းပုံပေးထားတာပါ character အဖြစ်နဲ့ပေါ့

echo sha1($password); //output is : 6c94d3b42518febd4ad747801d50a8972022f956
```

ပြန်ပြီး sha1 () function သုံးပြီး hashing လုပ်ထားတာပါ

ဒီအထိကျွန်တော်တို့ decrypt လုပ်နိုင်ပါတယ်

အဲလိုမျိုးမလုပ်နိုင်အောင် ကျွန်တော်က variable တစ်ခုသတ်မှတ်ပြီး string ကို assign လုပ်လိုက်ပါတယ်

`$salt = "f#@V)Hu^%Hg15fds*";` //ဒါက ကျွန်တော် သတ်မှတ်ထားတဲ့ string တစ်ခုပါ

ဒါကို sha1() function သုံးပြီး စောစောတုန်းက ပုံမှန်ရေးထားတဲ့ \$password နဲ့ ပေါင်းလိုက်တော့ decrypt လုပ်လို့မရတော့ပါဘူး ဟီး ဒါပေမယ့် security ဆိုတာ 99% ပဲ

#### Code:

```
echo sha1($salt . $password); // cd56a16759623378628c0d9336af69b74d9d71a5
```

ဒီတော့ code က ဒီလိုဖြစ်သွားမယ်

#### Code:

```
$salt = "f#@V)Hu^%Hg15fds*";
```

```
echo sha1($salt . $password); //cd56a16759623378628c0d9336af69b74d9d71a5
```

အဲလိုမျိုး hashing ကို decrypt လုပ်လို့မရတော့ပါဘူး

ဘာကြောင့်လဲဆိုတော့ Rainbow Table ကတော့ md5 & sha1 အခြားနည်းတွေအများကြီးကို decrypt လုပ်နိုင်စွမ်းရှိပါတယ်

ကျွန်တော်တို့က string နဲ့ hash နဲ့ပေါင်းလိုက်တော့ ပိုပြီးလုံခြုံသွားပါတယ်

အကြံပေးချင်တာတစ်ခုက သင့် website ရဲ့ admin or member တွေထည့်တဲ့အခါ database ကိုအောက်မှာရေးထားတဲ့ ပုံစံမျိုးထည့်ပေးရင်ပိုပြီးတော့စိတ်ချရပါတယ်

#### Code:

```
$hash = sha1($user_id . $password); သို့မဟုတ် $hash = md5($user_id . $password);
```

```
$hash = md5($_POST['$user_id . $password']);
```

ဒါဆို ok မယ်ထင်ပါတယ်ဗျာ

ကျွန်တော်လည်းအများကြီးမသိပါဘူး နောက်ထပ်နည်းလမ်းတွေလည်းအများကြီးရှိပါတယ်

သိသလောက်လေးမျှပေးပေးလိုက်တာပါ အမှာပါရင်လည်း ဝင်ရောက်ဆွေးနွေးပေးပါလို့ဖိတ်ခေါ်ပါတယ်

**CYBER SECURITY TRAINING**

 The following 23 users say Thank You to **133720** for this post:

• **Anubis**, Asadi, **b4ByPuNkGhOsT**, **BA KONE**, Bu5t0r, DarkAdmiral, **Dr.Jekyll**, Hacke3erDD, JD Exploit kiddie, **KpZ**, **LiquidFoxer**, little, Lotus Black, Lout Ta Yu, Luna, oolushwe, rences, Supernova, The Freak, Thwet, Toke Kway, webk!tz, Z0d!@()

PM Find

Reply Quote Report



**Thwet**

MSF Respected



Posts: 85

Threads:

0

Thanks

Received:

134 in 61

posts

Thanks

Given:

237

Joined:

Jun 2013

Reputatio

n: **63**



06-29-2013, 11:32 PM

#2

ကောင်းတယ် အစ်ကိုရေ အားပေးနေတယ် မျက်စိတော့ ပွင့်သွားပြီ 🤔

PM Find

Add Thank You

Reply

Quote

Report



**The Freak**

Senior Member



Posts:

500

Threads:

0

Thanks

Received:

335 in

226 posts

Thanks

Given:

296

Joined:

Jul 2013

Reputatio

n: **119**



07-19-2013, 04:16 AM

#3

MD5 ဆိုတာ ဒီကြီးကိုး။ :O

PM Find

Add Thank You

Reply

Quote

Report

**b4ByPuNkGhOsT**

Senior Member



Posts: 84

Threads:

0

Thanks

Received:

6 in 12

posts

Thanks

Given: 6

Joined:

Aug 2013

Reputatio

n: 1



08-19-2013, 10:10 AM

#4

Hash တွေ တော်တော်များများ ဖြေလို မရတာတွေ တွေ ဘူးတယ် အာ ဖိုးတွေကို ရအောင်ဖြေဖို့ ဘာတွေ လိုမဲ ဥပမာ အဲလေ ဥပမာပေါ့ Tools ကောင်းကောင်းလေးတွေ ချိရင် မှုပါဦး ဖြစ်နိုင်ရင် Online ရော Offline ရော သုံးနိုင်တဲ့ Tools လေးတွေရရင် ပိုကောင်းမယ် မိခိ 🙏

The following 1 user says Thank You to **b4ByPuNkGhOsT** for this post:

• Bu5t0r

PM Find

Add Thank You

Reply

Quote

Report

**Dr.Jekyll**

MSF Respected



Posts:

461

Threads:

0

Thanks

Received:

236 in

263 posts

Thanks

Given:

251

Joined:

Jun 2013

Reputatio

n: 144



08-19-2013, 01:19 PM

#5

Hash cat is really nice one.

- 1.Hash Cat
- 2.Password Pro
- 3.Cain & Able

PM Find

Add Thank You

Reply

Quote

Report

**DarkAdmiral**

Junior Member



Posts: 43  
 Threads: 0  
 Thanks Received: 20 in 15 posts  
 Thanks Given: 2  
 Joined: Jul 2013  
 Reputation: **30**

09-11-2013, 03:54 AM

#6

ကျေးဇူးပါအပ်ကို....။ အခုလိုရှင်းပြပေးတာ။နောက်ကိုလည်းဆက်ရေးပေးပါဦး။ 🙏

PM Find

Add Thank You

Reply

Quote

Report

**Lout Ta Yu**

SQL Worm



Posts: 451  
 Threads: 0  
 Thanks Received: 133 in 147 posts  
 Thanks Given: 223  
 Joined: Oct 2013  
 Reputation: **55**



01-10-2014, 11:04 PM

#7

ကျေးဇူးကိုရုံရေ နည်းနည်းတော့ နားလည်သွားပြီ...

နောက်ထပ်လဲဆက်ရေးပေးပါဦးခင်ဗျာ.... မျှော်နေပါမယ်... 🙏

PM Find

Add Thank You

Reply

Quote

Report

**wailiux** ●

Newbie



Posts: 6  
 Threads:  
 0  
 Thanks  
 Received:  
 1 in 1  
 posts  
 Thanks  
 Given: 0  
 Joined:  
 Sep 2014  
 Reputatio  
 n: **-1**

09-26-2014, 11:50 PM

#8

ရှေးလူပါဗျာ ... နောက်လည်း ဒါမျိုးတွေ ရေးပေးပါအုံး။ အားပေးပါတယ်

The following 1 user says Thank You to wailiux for this post:

• Demonhset

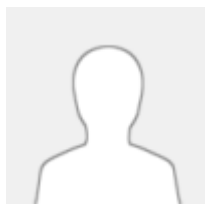
PM Find

Add Thank You

Reply

Quote

Report

**DC!M** ●

Junior Member



Posts: 33  
 Threads:  
 0  
 Thanks  
 Received:  
 0 in 0  
 posts  
 Thanks  
 Given: 0  
 Joined:  
 Dec 2015  
 Reputatio  
 n: **0**

03-13-2016, 04:55 PM

#9

Nice အရမ်းကောင်းတဲ့ hashing အကြောင်းလေးပါ bro အခု လို sharing လုပ်ပေး လို ရှေးလူပါ bro နောက်မဆို သိဖို့ မလွယ်သေးဘူး :p

PM Find

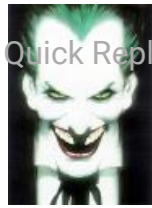
Add Thank You

Reply

Quote

Report





Quick Reply

**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, 03:17 AM

#10

အလင်းပြပေးလိုကူးလူးပဲ ဘဒို သိတာနောက်တစ်ခု ထပ်တိုးသွားပီ...

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

[View a Printable Version](#)[Subscribe to this thread](#)

Forum Jump: -- Cryptography

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](#)

