

Bash Shell Scripting by Examples



Welcome to Bashguru

Linux is one of popular version of UNIX operating System. It is open source as its source code is freely available. It is free to use. Linux was designed considering UNIX compatibility. It's functionality list is quite similar to that of UNIX and become very popular over the last several years. Our Basic motive is to provide latest information about Linux Operating system.

POSTED BY VENU K

67 COMMENTS | 10:51 AM

UNIX/Linux Advanced File Permissions - SUID,SGID and Sticky Bit

After you have worked for a while with Linux you discover probably that there is much more to file permissions than just the "rwx" bits. When you look around in your file system you will see "s" and "t"

```
$ ls -ld /tmp
drwxrwxrwt 29 root root 36864 Mar 21 19:49 /tmp

$ which passwd
/usr/bin/passwd

$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 22984 Jan 6 2007 /usr/bin/passwd
```

What is this "s" and "t" bit? The vector of permission bits is really 4 * 3 bits long. Yes there are 12 permission bits,not just 9.The first three bits are special and are frequently zero. And you almost always learn about the trailing 9 bits first.Some people stop there and never learn those first three bits.

The forth permission bit is used only when a special mode of a file needs to be set. It has the value 4 for SUID, 2 for SGID and 1 for the sticky bit. The other 3 bits have their usual significance.

Here we will discuss about the 3 special attributes other than the common read/write/execute:

- 1.Set-User-Id (SUID)
- 2.Set-Group-Id (SGID)
- 3.Sticky Bit

Set-User_Id (SUID): Power for a Moment:

By default, when a user executes a file, the process which results in this execution has the same permissions as those of the user. In fact, the process inherits his default group and user identification.

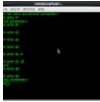
MOST VIEWED

[How to Pass Arguments to Shell Script](#)



[How to Read a File Line by Line in a Shell Script](#)

[Math in Shell Scripts](#)



[Shell Colors: colorizing shell scripts](#)

[Shell Script to Find Prime Number](#)

[Shell Script to Generate Fibonacci Series](#)

FOLLOWERS

Người theo dõi (155) [Tiếp theo](#)



[Theo dõi](#)

COUNTER

1330046

BLOG ARCHIVE

- ▶ 2011 (9)
- ▼ 2010 (19)
 - ▶ December (7)
 - ▶ July (4)
 - ▶ May (1)
 - ▶ April (2)
 - ▼ March (3)

[Creating a User Group and Shared Directory](#)

[UNIX/Linux Advanced File Permissions - SUID,SGID a...](#)

If you set the SUID attribute on an executable file, the process resulting in its execution doesn't use the user's identification but the user identification of the file owner.

The SUID mechanism, invented by Dennis Ritchie, is a potential security hazard. It lets a user acquire hidden powers by running such a file owned by root.

```
$ ls -l /etc/passwd /etc/shadow /usr/bin/passwd
-rw-r--r-- 1 root root 2232 Mar 15 00:26 /etc/passwd
-r----- 1 root root 1447 Mar 19 19:01 /etc/shadow
```

The listing shows that passwd is readable by all, but shadow is unreadable by group and others. When a user running the program belongs to one of these two categories (probably, others), so access fails in the read test on shadow. Suppose normal user wants to change his password, how can he do that? He can do that by running /usr/bin/passwd. Many UNIX/Linux programs have a special permission mode that lets users update sensitive system files - like /etc/shadow -- something they can't do directly with an editor. This is true of the passwd program.

```
$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 22984 Jan 6 2007 /usr/bin/passwd
```

The s letter in the user category of the permission field represents a special mode known as the set-user-id (SUID). This mode lets a process have the privileges of the owner of the file during the instance of the program. Thus when a non-privileged user executes passwd, the effective UID of the process is not the user's, but of root's - the owner of the program. This SUID privilege is then used by passwd to edit /etc/shadow.

What is effective user-id:

Every process really has two user IDs: the effective user ID and the real user ID. (Of course, there's also an effective group ID and real group ID. Just about everything that's true about user IDs is also true about group IDs.) Most of the time, the kernel checks only the effective user ID. For example, if a process tries to open a file, the kernel checks the effective user ID when deciding whether to let the process access the file.

Save the following script under the name reids.pl and make it executable (chmod 755 reids.pl).

```
#!/usr/bin/perl
# print real UID
print "Real UID: $<\n";
# print real GID
print "Real GID: $(\n";
# print effective UID
print "Effective UID: $>\n";
# print effective GID
print "Effective GID: $)\n";
```

check file permissions:

```
$ ls -l reids.pl
-rwxr-xr-x 1 venu venu 203 Mar 24 10:40 reids.pl
```

Linux File and Directory Permissions

- February (1)
- January (1)
- 2009 (24)
- 2008 (8)

CATEGORIES

- [Article](#) (15)
- [Beginners Scripts](#) (17)
- [HowTo's](#) (3)
- [Linux Fun](#) (1)
- [Shell Scripts](#) (24)

Note: For security reasons the s-bit works only when used on binaries (compiled code) and not on scripts (an exception are perl scripts). Scripts, i.e. programs that cannot be executed by the kernel directly but need an interpreter such as the Bourne shell or Java, can have their setuid bit set, but it doesn't have any effect. There are some platforms that honor the s bits even on scripts (some System V variants, for example), but most systems don't because it has proven such a security headache - most interpreters simply aren't written with much security in mind. Set the SUID bit on shell script is useless, that's why I am using perl script here.

When you run the script you will see that the process that runs it gets your user-ID and your group-ID:

```
$ ./reids.pl
Real UID: 500
Real GID: 500 500
Effective UID: 500
Effective GID: 500 500
```

Note: If you get an error like this:
Can't do setuid (cannot exec perl)

In Debian install perl-suid using following command:
apt-get install perl-suid

In Centos install perl-suidperl using following command:
yum install perl-suidperl

Now change ownership to another user (Do it as an administrator).

```
# chown king /home/venu/reids.pl
# ls -l /home/venu/reids.pl
-rwxr-xr-x 1 king venu 203 Mar 24 10:40 /home/venu/reids.pl
```

Now run the script again.

```
$ ./reids.pl
Real UID: 500
Real GID: 500 500
Effective UID: 500
Effective GID: 500 500
```

What you observed, the output of the program depends only on the user that runs it and not the one who owns the file.

How to assign SUID permission:

The SUID for any file can be set (mostly by the superuser) with a special syntax of the chmod command. This syntax uses the character s as the permission. Now add SUID permission to the script reids.pl :

```
# chmod u+s /home/venu/reids.pl      (Do it from root account)
```

Now return from the super user mode to the usual non privileged mode.

```
$ ls -l reids.pl
-rwsr-xr-x 1 king venu 203 Mar 24 10:40 reids.pl
```

To assign SUID in an absolute manner, simply prefix 4 to whatever octal string you would otherwise use (like 4755 instead of 755).

The file reids.pl is owned by king and has the s-bit set where normally the x is for the owner of the file. This causes the file to be executed under the user-ID of the user that owns the file rather than the user that executes the file. If venu runs the program then this looks as follows:

```
$ perl reids.pl
Real UID: 500
Real GID: 500 500
Effective UID: 503
Effective GID: 500 500
```

Effective user id of process is 503, this is not the venu's , but of king's - the owner of the program. As you can see this is a very powerful feature especially if root owns the file with s-bit set. Any user can then do things that normally only root can do.

Caution: When you write a SUID program then you must make sure that it can only be used for the purpose that you intended it to be used. As administrator, you must keep track of all SUID programs owned by root that a user may try to create or copy. The find command easily locate them:

```
# find /home -perm -4000 -print | mail root
```

The extra octal bit (4) signifies the SUID mode, but find treats the "-" before 4000 as representing any other permissions.

Set-Group_Id (SGID) :

The set-group-id (SGID) is similar to SUID except that a program with SGID set allows the user to have the same power as the group which owns the program. The SGID bit is 2, and some typical examples could be `chmod g+s reids.pl` or `chmod 2755 reids.pl`.

You can remove SGID bit using following commands:

```
$ chmod g-s reids.pl
$ chmod 755 reids.pl      (Absolute manner)
```

It is really useful in case you have a real multi-user setup where users access each others files. As a single homeuser I haven't really found a lot of use for SGID. But the basic concept is the same as the SUID, Similar to SUID, SGID also grants privileges and access rights to the process running the command, but instead of receiving those of the file's owner it receives those of the file's group. In other words, the process group owner will be set to the file's group.

I explain it with an example. I have created two user accounts king and venu with same home directory project. king belongs to king and development groups, venu belongs to venu and development groups.

```
# groups king venu
king : king development
venu : venu development
```

venu's default group is venu and king's default group is king.

Login as king and create reids.pl file again and make it executable (using chmod 755 reids.pl) .

```
$ id
uid=503(king) gid=503(king) groups=501(development),503(king)
$ ls -l reids.pl
-rwxr-xr-x 1 king development 203 Mar 25 19:00 reids.pl
```

Now login as venu and run the program:

```
$ id
uid=501(venu) gid=504(venu) groups=501(development),504(venu)
$ perl reids.pl
Real UID: 501
Real GID: 504 504 501
Effective UID: 501
Effective GID: 504 504 501
```

The effective GID of the process is the venu's, but not of the king's - the owner of the program.

Now login as king and assign SGID bit to reids.pl program:

```
$ chmod 2755 reids.pl; ls -l reids.pl
-rwxr-sr-x 1 king development 203 Mar 25 19:00 reids.pl
```

Now login as venu and run the reids.pl program:

```
$ perl reids.pl
Real UID: 501
Real GID: 504 504 501
Effective UID: 501
Effective GID: 501 504 501
```

Real GID and Effective GID are different, here Effective GID is the king's - the owner of the program.

Set SGID on a directory:

When SGID is set on a directory it has a special meaning. Files created in a directory with SGID set will inherit the same group ownership as the directory itself, not the group of the user who created the file. If the SGID is not set the file's group ownership corresponds to the user's default group.

In order to set the SGID on a directory or to remove it, use the following commands:

```
$ chmod g+s directory    or    $ chmod 2755 directory
$ chmod g-s directory    or    $ chmod 755 directory
```

As I mentioned earlier venu and king's home directory is same that is /home/project. I changed group ownership of /home/project directory to development.

```
# ls -ld /home/project/
drwxrwxr-x 16 root development 4096 Mar 26 00:22 /home/project/
```

Now login as king and create a temp file.

```
$ whoami
king
$ pwd
/home/project/
$ touch temp; ls -l temp
-rw-r--r-- 1 king king 0 Mar 26 12:34 temp
```

You can see from the `ls` output that the group owner for `project` is `development`, and that the SGID bit has not been set on the directory yet. When `king` creates a file in `project`, the group for the file is `king` (king's primary gid).

Set SGID bit on `project` directory. For that login as `administrator` and set SGID bit using following command:

```
# chmod g+s /home/project/
# ls -ld /home/project/
drwxrwsr-x 15 root development 4096 Mar 26 12:34 /home/project/
```

From the `ls` output above, you know the SGID bit is set because of the `s` in the third position of the group permission set, which replaces the `x` in the group permissions.

Now login as `king` and create `temp2` file.

```
$ whoami
king
$ touch temp2; ls -l temp2
-rw-r--r-- 1 king development 0 Mar 26 13:49 temp2
```

Notice the group ownership for `temp2` file. It inherits group permission from the parent directory.

Enabling SGID on a directory is extremely useful when you have a group of users with different primary groups working on the same set of files.

For system security reasons it is not a good idea to set many program's set user or group ID bits any more than necessary, since this can allow an unauthorized user privileges in sensitive system areas. If the program has a flaw that allows the user to break out of the intended use of the program, then the system can be compromised.

Sticky bit:

The sticky bit (also called the saved text bit) is the last permission bit remaining to be discussed. It applies to both regular files and directories. When applied to a regular file, it ensures that the text image of a program with the bit set is permanently kept in the swap area so that it can be reloaded quickly when the program's turn to use the CPU arrives. Previously, it made sense to have this bit set for programs like `vi` and `emacs`. Today, machines with ultra-fast disk drives and lots of cheap memory don't need this bit for ordinary files and that is also useless.

However, the sticky bit becomes a useful security feature when used with a directory. The UNIX/Linux system allows users to create files in `/tmp`, but none can delete files not owned by him. That's possible

because sticky bit set for /tmp directory.

The /tmp directory is typically world-writable and looks like this in a listing:

```
# ls -ld /tmp
drwxrwxrwt 32 root root 36864 Mar 27 12:38 /tmp
```

Everyone can read,write and access the directory.The t indicates that only the user (root and owner of the directory,of course) that created a file in this directory can delete that file.

In order to set or to remove the sticky bit, use the following commands:

```
$ chmod +t directory      or      $ chmod 1754 directory
$ chmod -t directory      or      $ chmod 754 directory
```

Note: 754 permissions for a directory are powerful enough to guard your directories from intruders with malicious intentions, that's why I used 754 as default,if you want you can change it.

Example:

I logged in as king and created a temp file.

```
$ whoami
king
$ pwd
/home/project/
$ touch temp; ls -l
-rw-r--r-- 1 king king          0 Mar 27 13:44 temp
```

Now logged in as venu and try to delete temp file.

```
$ whoami
venu
$ rm temp
rm: remove write-protected regular empty file `temp'? Y
$ ls temp
ls: temp: No such file or directory
```

So what happened? venu deleted file owned by king.

Assign sticky bit to the project directory.As a owner of the directory or administrator.

```
# chmod +t /home/project
# ls -ld /home/project/
drwxrwxr-t 15 root development 4096 Mar 27 13:46 /home/project/
```

From the ls output above, you know the sticky bit is set because of the t in the third position of the other permission set,which replaces the x in the other permissions.

Now repeat same steps again,then you get the following message:

```
$ whoami
venu
$ ls -l temp
```

```
-rw-r--r-- 1 king king 0 Mar 27 17:36 temp
$ rm temp
rm: remove write-protected regular empty file `temp'? y
rm: cannot remove `temp': Operation not permitted
```

Observation: Login as normal user and create a file.

```
[venu@localhost ~]$ touch sample
[venu@localhost ~]$ ls -l sample
-rw-rw-r-- 1 venu venu 0 Dec 21 03:41 sample
```

Now change permissions to 644

```
[venu@localhost ~]$ chmod 644 sample
[venu@localhost ~]$ ls -l sample
-rw-r--r-- 1 venu venu 0 Dec 21 03:41 sample
```

Now assign SUID permission.

```
[venu@localhost ~]$ chmod u+s sample
[venu@localhost ~]$ ls -l sample
-rwsr--r-- 1 venu venu 0 Dec 21 03:41 sample
```

After setting SUID, if you see 'S' then it means that the file has no executable permissions for that user.

Now remove SUID permission and change permissions to 744. Then assign SUID permission. You should see a smaller 's' in the executable permission position.

```
[venu@localhost ~]$ chmod u-s sample
[venu@localhost ~]$ chmod 744 sample
[venu@localhost ~]$ chmod u+s sample
[venu@localhost ~]$ ls -l sample
-rwsr--r-- 1 venu venu 0 Dec 21 03:41 sample
```

Same is applicable for SGID and Stickybit.



ARTICLE

[Newer Post](#)

[Home](#)

[Older Post](#)

67 comments:



Anonymous April 12, 2010 at 7:47 AM

Perfect explanation! thanks a lot!

[Reply](#)



Anil April 13, 2010 at 11:53 PM

Nice explanation, clears all my doubts, thanks a lot !!!!!!!!

[Reply](#)



Anonymous April 17, 2010 at 2:03 PM

From the ls output above, you know the sticky bit is set because of the s in the third position of the other permission set, which replaces the x in the other permissions.

I think you meant 'because of the t in the third position of the other permission set'

[Reply](#)



venu k [April 18, 2010 at 12:43 AM](#)

Thank you, I modified it.

[Reply](#)



Anonymous [August 2, 2010 at 10:23 AM](#)

Thank you a lot buddy for perfect explanation

[Reply](#)



sandeep [August 23, 2010 at 8:43 AM](#)

thanks buddy, its amazing informaton please keep it up

[Reply](#)



Anonymous [September 6, 2010 at 2:53 AM](#)

The info is amazing!!!!

[Reply](#)



gita [December 2, 2010 at 1:02 AM](#)

Good explanation. Thank u

[Reply](#)



Anonymous [January 9, 2011 at 10:47 PM](#)

Please, make some explanation, why Real GID or Effective GID show 3 numbers, e.g. 504 504 501, and which is which from these numbers, since it is uncelar from tht text.
Thanks!

[Reply](#)



Anonymous [January 9, 2011 at 11:23 PM](#)

Following the example above, what is the purpose of assigning GID to reids.pl under king account, when permissions for others are the same as for the file owner's group? I mean, if you run the reids.pl under venu without the GID set, you will have the same permissions as when inheriting them from group's permissions, when the GID is set, don't you? Please, correct me, if I'm wrong.
Thx.

[Reply](#)



Anonymous [January 12, 2011 at 9:03 AM](#)

I don't think the sticky bit info is relevant.
drw-r-xr-x 2 ivo ivo 1 2011-01-12 18:53 test
\$ whoami
mitko
\$
\$ rm -R test
rm: remove write-protected directory `test'? Y
rm: remove write-protected directory `test'? Y
rm: cannot remove directory `test': Permission denied

[Reply](#)



Anonymous [March 8, 2011 at 2:14 AM](#)

You must have rwx permission (to parent and all recursive if any) to remove a non-empty directory.

[Reply](#)



Gladiator [April 10, 2011 at 11:01 AM](#)

thanks for great explanation....

[Reply](#)




Evader [April 17, 2011 at 10:48 PM](#)

The best article about the matter I have ever read. Thank you very much!

[Reply](#)

[Javin @ unix grep command](#) [July 2, 2011 at 5:41 AM](#)

This is really an amazing article, I have been struggling with this concept but after reading this

 post I have gained lot of knowledge. you have indeed covered the topic well and with examples. great job and keep it up.

Javin

[Secrets of symbolic link or symlink in Unix](#)

[Reply](#)

 **Anonymous** [July 20, 2011 at 9:48 AM](#)

Very good explanation, finally an understandable one.

Congratulations!!

[Reply](#)

 **Anonymous** [August 16, 2011 at 11:24 AM](#)

nice explanation..

Thanks

[Reply](#)

 **Anonymous** [August 20, 2011 at 10:27 AM](#)

Thanks a lot..You explained it in a perfect manner. I appreciate it..Keep doing the good work.:-)

[Reply](#)

 **Anonymous** [October 28, 2011 at 2:10 AM](#)

Thank you very much. It clears all my doubts and saves my time also.

[Reply](#)

 **Anonymous** [October 30, 2011 at 11:02 AM](#)

Thank you very much!! Really clear and complete!

[Reply](#)

 **Unknown** [November 1, 2011 at 3:14 AM](#)

Thank you very much. Your way of explanation is very good. It clears all my doubts. You posted observation block, I didn't observed until I read this article.

[Reply](#)

 **suma** [November 2, 2011 at 8:10 AM](#)

I have many doubts about sticky bit, all are cleared here.

Thank you very much for your way of explanation and effort.

[Reply](#)

 **Anonymous** [November 3, 2011 at 10:27 AM](#)

Thank you very much!! good explanation.

[Reply](#)

 **Srinivas Jupudi** [November 4, 2011 at 3:55 AM](#)

Excellent Article. Thanks.

[Reply](#)

 **shloka** [November 4, 2011 at 7:38 AM](#)

very good explanation, I am learning more here about bash. Thank you for sharing your knowledge.

[Reply](#)

 **suraj patel** [November 6, 2011 at 5:46 AM](#)

Excellent blog, I am following your blog now

[Reply](#)

[Ravi Kumar](#) [November 8, 2011 at 7:18 AM](#)



Excellent way of explanation.

Thank you.

[Reply](#)



Anonymous [November 10, 2011 at 6:24 AM](#)

Good article. It clears some of my doubts.

Thank you.

[Reply](#)



Revanth [November 17, 2011 at 6:50 AM](#)

Thanks, I learned a lot from this article.

Now I'm follower of your blog.

[Reply](#)



Anonymous [January 2, 2012 at 9:45 PM](#)

good article..thanks

[Reply](#)



Anonymous [May 9, 2012 at 10:00 PM](#)

It clears all my doubt on this topic. Thank you!

[Reply](#)



Anonymous [July 14, 2012 at 8:16 PM](#)

very nicely explained... Thank You!

[Reply](#)



Anonymous [July 19, 2012 at 6:58 AM](#)

As a long time security professional, I still little value in the "sticky bit" other than it sounds good.

The reality is that a user can simply "cat /dev/nul > filename" and you've esentially erased it anyway. You didn't actual "delete" the file, but it's gone none the less.

[Reply](#)



Anonymous [July 21, 2012 at 6:17 PM](#)

Before "Set SGID on a directory", why effective GID is 501 504 501?
It could be 503, the default king's group...

[Reply](#)



oracle-admin [August 27, 2012 at 6:36 AM](#)

Nice information. Thanks. www.oracle-admin.blogspot.com

[Reply](#)



Alexei [September 10, 2012 at 1:37 PM](#)

Hello there,

I am trying to execute this script but I don't know if I am doing something wrong, because my effective UID is always from the user that executes the script and not the UID from the owner...See below...

Someone can give me a tip about where is my mistake on it???

```
aluno:~$ ls -l suid.pl
-rwsr-xr-x 1 meualuno alun0 200 Set 10 16:53 suid.pl
aluno:~$
aluno:~$ id meualuno
uid=1001(meualuno) gid=1002(meualuno) grupos=1002(meualuno),1011(curso_linux)
aluno:~$
aluno:~$ id alun0
uid=1005(aluno) gid=1009(aluno) grupos=1009(aluno),1012(alunos-dltec)
aluno:~$
aluno:~$ whoami
aluno
aluno:~$ perl suid.pl
Real UID: 1005
Real GID: 1009 1009 1012
```

Effective UID: 1005
Effective GID: 1009 1009 1012
aluno:~\$

[Reply](#)

Udit [December 27, 2012 at 3:57 PM](#)

brilliant explanation with perfect examples.. thanks.. it cleared all my doubts regarding the topics

[Reply](#)

Anonymous [February 27, 2013 at 12:13 PM](#)

cool...explained the concept

[Reply](#)



khaja vali [April 12, 2013 at 3:32 AM](#)

in simple SUID means , when SUID is applied on a file , the file is executing by all users but file thinks that the file is executing by the owner.

SGID- When SGID is applied on a directory , to inherits the group ownership to the consecutive files and directories.

Stickybit- When stickybit is applied on a directory to protect the consecutive files and directories getting deleted from others even though they have full traditional file permissions.

[Reply](#)

Anonymous [September 1, 2013 at 11:52 PM](#)

This really a great article, Please keep doing such a fine work.

Thank you very much, it saved my lot of time.

David

[QuickBooks Hosting](#)

[Reply](#)

david [December 28, 2013 at 11:26 PM](#)

Thanks, I learned a lot from this article. Please also discuss about firewall and security.

Now I'm follower of your blog to get update.

Thanks,

Dav

[QuickBooks Hosting](#)

[Reply](#)

Anonymous [February 2, 2014 at 7:04 AM](#)

very nice explained...
i googled my doubts related to effective uid , sticky bit but finally got answer here...

[Reply](#)

Anonymous [March 30, 2014 at 2:55 AM](#)

Perfect explanation and examples !! Thank you

[Reply](#)

Anonymous [April 25, 2014 at 3:38 AM](#)

erudition...

[Reply](#)

Anonymous [November 27, 2014 at 3:26 AM](#)

Great Work. Cheers ! Great explanation, though little confusing at a point or two but easy understandable with good examples. Keep up. Thanks a lot.

[Reply](#)



Michale Daniel [January 6, 2015 at 9:35 AM](#)

It was very nice article and it is very useful to Linux learners.We also provide [Linux online](#)

[training](#)

[Reply](#)



malik khan November 6, 2015 at 2:02 AM

This comment has been removed by the author.

[Reply](#)



malik khan November 6, 2015 at 2:04 AM

I read your article. it was very nice

[Quickbooks Hosting](#)

[Reply](#)



shariq ansari January 18, 2016 at 1:53 AM

Nice and Excellent topic. It clears all doubt on this topic. Thank you!

[Lacerte Hosting](#)

[Reply](#)



Allen jeley January 23, 2016 at 7:36 AM

I learn many specific information in this article ad now i easily solve my problem thanks for sharing [personal statement midwifery examples](#) .

[Reply](#)



mary Brown June 15, 2016 at 11:45 AM

I have read your blog its very attractive and impressive. I like it your blog.

[Java Training in Chennai](#) [Java Training in Chennai](#) | [Core Java Training in Chennai](#)

[Online Java Training](#) [Online Java Training](#) | [Java J2EE Online Training](#) | [JavaEE Training Institute in Chennai](#)

[Reply](#)



mary Brown June 15, 2016 at 11:47 AM

[Java Training in Chennai](#)
[Online MVC Training India](#) | [Angularjs Training](#) | [javase j2ee javaee interview questions](#) |
[Java Training in Chennai](#) |
[Java Training in CHennai](#)

[Reply](#)



Anonymous July 29, 2016 at 12:11 AM

highlight the difference between S and s. missing in your article.

[Reply](#)



Unknown August 6, 2016 at 5:11 AM

Thank you

[Reply](#)



Tokecash December 8, 2016 at 4:15 AM

Thanks for your marvelous posting! I quite enjoyed reading it, you happen to be a great author. I will remember to bookmark your blog and will eventually come back very soon. Go to best social plan for get more related topic. Have a nice evening!
[Situs BandarQ, Poker, Domino 99 Online Terpercaya](#) - [Situs Judi Bola Online Terbesar dan Terpercaya Indonesia](#)

[Reply](#)



shree priya February 3, 2017 at 2:13 AM

This is my first visit to your blog, your post made productive reading, thank you. [dot net training in chennai](#)

[Reply](#)

tanki online February 20, 2017 at 2:11 AM

Thanks for sharing your info. I really appreciate your efforts and I will be waiting for your further write.
Thanks for sharing !

[Reply](#)

tanki online February 20, 2017 at 2:14 AM

Thanks for sharing your info. I really appreciate your efforts and I will be waiting for your further write.

Thanks for sharing !

[tanki online 2 | 2048 game online](#)

[Reply](#)

cara menggugurkan kandungan March 17, 2017 at 8:48 AM

This blog is so nice to me. I will continue to come here again and again. Visit my link as well.
Good luck

<http://www.jualobataborsiherbal.com/> [obat aborsi](#)

<http://caramenggugurkankandung.info/> [cara menggugurkan kandungan](#)

<http://obataborsi59.com/> [obat aborsi](#)

<http://obataborsi59.com/cara-menggugurkan-kandung-dengan-cepat-dan-aman/> [cara menggugurkan kandungan](#)

<http://obattelatdatangbulan.info/> [obat telat datang bulan](#)

<http://klinikobataborsi.com/> [jual obat aborsi](#)

<http://jualobatpenggugurkandung.net/> [obat penggugur kandungan](#)

<http://tandatandakehamilan.net/> [tanda tanda kehamilan](#)

<http://tandatandakehamilan.net/cara-cepat-dan-selamat-menggugurkan-kandung/> [cara menggugurkan kandungan](#)

[Reply](#)



Shreeja K June 6, 2017 at 4:43 AM

Informative article, just what I was looking for.[seo services chennai](#)

[Reply](#)

agen bandarq online June 12, 2017 at 6:39 AM

this a very nice.. thanks for the article.. its really helped :)

[Agen BandarQ Online](#)

[Agen DominoQQ](#)

[Bandar Qiu Qiu](#)

[Forum DominoQQ](#)

[Situs BandarQ Online](#)

[Reply](#)

acehpoker June 16, 2017 at 3:05 PM

Telah Hadir [Agen Poker](#), [DominoQQ](#), [Capsa Susun](#), [Bandar Ceme](#), [Ceme Keliling](#), & [Live Poker](#) Terbaik dan Terpercaya.

Hanya dengan Minimal Deposit 10 ribu Bonus 10 ribu dan Minimal Withdraw 25 ribu anda dapat bermain di [Acehpoker](#);

1. Acehpoker memberikan bonus Referral 15% (Seumur Hidup)
2. Sistem keamanan terjamin dan Data pribadi akan aman bersama kami.
3. Player Vs Player (100% No Robot)
4. Dengan Sistem Confirm Deposit terbaru Max 2 menit (Jika semua Nama di Id dan di bank sama)
5. CS yang ramah dan Melayani dengan Professional
6. Online 365 Hari 24 Jam
7. Anda Menang berapapun Kami Bayar tanpa Maksimal Withdraw dan Tidak ada batas maksimal withdraw dalam 1 hari.
8. Dapat bermain 6 permainan hanya dengan 1 Web , yaitu Poker , DominoQQ , Bandar Ceme, Capsa Susun, Ceme Keliling, Live Poker
9. Bisa bermain di Android dan IOS
10. Sistem pembagian Kartu menggunakan teknologi yang mutakhir dengan sistem Random Permanent (acak) , Dan tersedia Ratusan meja untuk tempat anda bermain

Pin BBM : 563AB8CA

yahoo : mahadewi374@yahoo.com

Line: Lilly080615

[Bola](#)

[Agen Bola Terpercaya](#)

[Daftar Judi Bola Maxbet](#)

[Bandar Bola IBCBET](#)

[Daftar Bola BCA](#)

[Cara Bermain Poker](#)
[Agen Poker Terpercaya](#)
[Poker Bonus Deposit](#)
[Cara Daftar Poker](#)
[Bandar Ceme Terpercaya](#)
[Cara Bermain Poker](#)
[Situs Poker Terpercaya](#)
[Judi Bandar Capsa](#)
[Poker Bonus Member Baru](#)
[Panduan Bermain Poker](#)
[Agen Poker Terbaik](#)
[Poker Promo Poker Online](#)
[Poker Online Terpercaya](#)
[Capsa Susun Uang Asli](#)
[Qiu Qiu Uang Asli](#)
[Poker Online Terbaik](#)
[Domino QQ Online](#)
[Bandar Ceme Keliling](#)
[Judi Poker Online](#)
[Agen Ceme Keliling](#)
[qiu qiu](#)
[texas holdem poker](#)
[Poker Online Indonesia](#)

[Reply](#)



[okcupid](#) June 22, 2017 at 2:26 AM

great post

[Reply](#)



[findgirlsdating](#) June 22, 2017 at 10:00 PM

good site and post

[Reply](#)



[Agen Domino 99, BandarQ Online Terpercaya](#) July 22, 2017 at 8:05 PM

good and nice post thank you
[Poker Online Indonesia](#)

[Reply](#)



[gondes ribut](#) August 19, 2017 at 12:31 PM

Use this article to increase your knowledge . [cara menggugurkan kandungan](#)

[Reply](#)



[CERITA SEXUAL](#) September 16, 2017 at 11:25 AM

Bergabung Dan Tunjukkan Cara Bermain Pokermu.
 Bersama GadisPoker Dan Menangkan Hadiah jutaan Rupiah.
<https://goo.gl/iXP5pY>
 Untuk Info Lebih lanjut Silakan hubungi CS (customer Service).
[poker online](#)

[judi poker](#)

<http://www.gadispoker.com/>

[Reply](#)

Comment as:

thandieu_9x (Goo

[Sign out](#)

[Publish](#)

[Preview](#)

☐ [Notify me](#)

Subscribe to: [Post Comments \(Atom\)](#)



