

Create a secure Web Application and Generated Report as PDF

¹Murdan Sianturi, ²Mochamad Wahyudi

¹Program Pascasarjana Magister Ilmu Komputer STMIK Nusa Mandiri, Jurusan Manajemen STIE Mulia Pratama

²Program Pascasarjana Magister Ilmu Komputer STMIK Nusa Mandiri, Program Studi Teknik Komputer AMIK BSI

murdan.sianturi@gmail.com

wahyudi@nusamandiri.ac.id

Abstract

Web Base Application this moment has consider by company, specifically for company who having more than one branch or more. With presence application web bases, data can save as centrally. The other thing become consideration for company is the expense belong to cheap, because we can hire the server at provider. There are many Internet Service Provider in Indonesia, with the result they are competing within thing price. However there are cause of why they afraid that is to say complication data safety.

Key words

Web Application, Security, SQL Injection, PDF Report

1. Introduction

In software engineering, a web application is an application that is accessed via a web browser over a network such as the Internet or an intranet. It is also a computer software application that is coded in a browser-supported language (such as HTML, JavaScript, Java, etc.) and reliant on a common web browser to render the application executable.

Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client, sometimes called a thin client. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications include webmail, online retail sales, online auctions, wikis and many other functions.

2. The Most Important Focus To Develop A Web Application

There are four most important focus :

1. Is it application was secure ?
2. Is it application User friendly or easy to use ?
3. Is it application's accessibility good?. And how fast it to find a data using search facility ?
4. Is it application can generated a good report ?

2.1. Is it application was secure ?

In develop an application, be sure to create a secure system, such as :

1. Using Strong Password for User (min. 8 character).
2. Create a Secure in Login System.
3. Create a secure system while send DATA trough browser.

a. Using Strong Password for User

To overcome reconnaissance password (S'to, 2009). The hacker gathering stage about all information user has.

b. Create a Secure in Login System

To create a secure in login system, there is two version. The first version, using session register (Hakim, 2008). Usually a programmer use this method.

If success login :

```
Session_register("namauser");  
Session_register("passw");  
$_session(namauser) = $r[id_user];  
$_session(passw)=$r[passw];
```

For logout :

```
Session_start();  
Session_destroy;
```

The second version, using MD5 command to encrypt username and password.

Algorithm :

1. Open form FormLogin.php, input User_Name and Passw
2. Klik Login Button and directly open CekLogin page. (Locate username & password at table member). Implemented Cek Login in PHP:

```
<?php  
$uname = $_POST["uname"];
```

```

$pas = $_POST["pas"];

include "db.inc.php";
//protect MySQL injection
$username = stripslashes($username);
$password = stripslashes($password);
$username = mysql_real_escape_string($username);
$password = mysql_real_escape_string($password);
$sql="select user,password from operator where
user='$username' and password='$password'";
if (!$res=mysql_query($sql,$dbh)) {
    echo "err1 ".mysql_error();
}
exit;
}
}
$nu = 0;
if ($row=mysql_fetch_row($res)) {
    $nu = 1;
    $user = $row[0];
    $pass = $row[1];
    $combiKey[1]="srah117";
    $combiKey[2]="jonth65";
    $combiKey[3]="mrlun23";
    $combiKey[4]="dgko32";
    $combiKey[5]="gterww31";
    $combiKey[6]="gerardus45";
    $combiKey[7]="sanamra97";
    $combiKey[8]="tansye84";
    $combiKey[9]="rassye443";
    $combiKey[10]="prangs99";
    $n=rand(1,10);
    $encrypt = $user.$pass.$combiKey[$n];
    $vSessionID = md5($encrypt);
}
else {
    echo
    "<script>location.href='index.php?hasilLogin=A
nda+Salah+Password'</script>";
}
exit;
}

?>

```

Why use stripslashes and mysql_real_escape_string?
The function is to add the slash before character ' or '.

Look at below as example protect MySQL injection:
?php

```

// Query database to check if there are any matchig
users
$query = "SELECT * FROM users WHERE user='{
$_POST['username']}' AND password='{$_POST['p
assword']}'";
mysql_query($query);

```

// We didn't check \$_POST['password'], it could be anything the user wanted! For example:

```

$_POST['username'] = 'murdan';
$_POST['password'] = "' OR '='";

```

// This means the query sent to MySQL would be :
echo \$query;
?>

The query sent to MySQL:
SELECT * FROM users WHERE user='murdan'
AND password="" OR ""

This would allow anyone to log in without a valid password.

But if use stripslashes and mysql_real_escape_string, result should be :

The query sent to MySQL :
SELECT * FROM users WHERE user='murdan'
AND password='\' OR \'=\'

It's mean the condition should be FALSE.

- If username and password found, save \$hexa as cookies
Setcookie("Cid", \$hexa, time() +3600);
/* expire in 1 hour */
- Insert data to tbl_session
include "dbses.inc.php";
\$sql = "insert into tbl_session (cid,user_name)
values ('\$hexa','\$user_name)";
if (!mysql_query(\$sql,\$dbh)) {
 echo mysql_error();
}

Notes:

dbses.inc.php is a script to make connection to database.

```

<?php
//dbses.inc.php
$databse="aplikasi";
$hostname="localhost";
$username="root";
$password="tHe98452est";
if
(!($dbh=mysql_connect($hostname,$username,
$password)) {
    echo mysql_error();
}
exit;
}
mysql_select_db($databse,$dbh);
?>

```

- Call direct INDEX.php
Usually a website consist a header, detail and footer. While index.php called it's should be called header.php, detail.php and footer.php. While header.php called, it's also called cekses.php by Include "cekses.php" command.
- At every page run Cekses.php
Cekses.php is a script which is should be call every time to compare cookies value with data at table session. If found at table, the user_name

should be display on top of pages (header), definite that user is ONLINE.

Look this script :

```
<?php
//cekses.php
//GET COOKIE VALUE First
//and COMPARE it with username at table
$cookies_id = $_COOKIE["cid"];
include " dbses.inc.php";
$sql="select user_name from tbl_session where
id='$cookies_id ' order by id";
if (!$res=mysql_query($sql,$dbh)) {
echo mysql_error();
exit;
}
if ($row=mysql_fetch_row($res)) {
    $userOK = $row[0];
}
?>
```

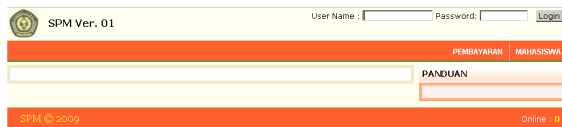


Figure 1. Login Page



Figure 2. After Login

c. Logout

Algorithm Logout for version 2 :

1. Read variabel Cookies. By command `$cookies_id = $_COOKIE["cid"];`
2. Delete id from table `tbl_session`, which is equal with `$cookies_id`
3. Delete Cookies variable. By command `setcookie("cid","",0);`

d. Secure while send DATA to other page trough browser

To send DATA from a Form, usually using POST method. Look at this script FormLogin.php :

```
<FORM name=tform method="POST"
action="login.php" onSubmit="">
User Name : <INPUT name="uname" size="16">
Password: <INPUT type=password name="pas"
size="10">
&nbsp;&nbsp;&nbsp;<input value='Login' type='submit'>
</FORM>
<SCRIPT language=JavaScript>
document.tform.uname.focus() ;
document.tform.uname.select() ;
```

```
</SCRIPT>
```

It's mean, after post User Name and Password and klik Login. The login.php script should be accessed directly. There are two variable bring to page login.php, namely \$uname and \$pas.

And at login.php, need set up two variabel also to get data. Look at this script :

```
<?php
//login.php
$uname = $_POST["uname"];
$pas = $_POST["pas"];
...
...
?>
```

Notes:

```
<SCRIPT language=JavaScript>
document.tform.uname.focus() ;
document.tform.uname.select() ;
</SCRIPT>
```

It's mean is: Put the cursor automaticly standby in box of field uname. How if from FormLogin.php we also send other variabel, like `$special_member = "1"?` But we don't want this data known by public ?

At above form (FormLogin.php), we can change should be `action="login.php?special_member=1" onSubmit="">`

And login.php become :

```
<?php
//login.php
$uname = $_POST["uname"];
$pas = $_POST["pas"];
$special_member = $_GET["special_member"];
...
...
?>
```

It's no secure. Because at browser we still can see the variabel showing. The solution is making the variabel is hidden. Set it before `</FORM>`, like this:

```
<INPUT type="hidden" name="special_member"
value="1">
```

So the FormLogin.php should be change, like this :

```
<FORM name=tform method="POST"
action="login.php" onSubmit="">
User Name : <INPUT name="uname" size="16">
Password: <INPUT type=password name="pas"
size="10">
&nbsp;&nbsp;&nbsp;<input value='Login' type='submit'>
<INPUT type="hidden" name="special_member"
value="1">
</FORM>
<SCRIPT language=JavaScript>
```

```
document.tform.uname.focus() ;
document.tform.uname.select() ;
</SCRIPT>
```

And at login.php, need set up three variabel to get hidden data was come from the form. Look at this script:

```
<?php
//login.php
$username = $_POST["uname"];
$password = $_POST["pas"];
$special_member=$_POST["special_member"];
```

....

...
 ?>

This is has most secure. If you worry somebody change parameter on browser and may effect to your database.

e. About Cookies

The problem, while use cookies. Hijacking cookie (S'to, 2004). If some body know your cookies code at another computer and set this code at their computer by Opera browser, automaticly they has login as your account.

So, for cekses.php need additional function to check user IP and User Agent. If these attributes not same while user log on, the system need to reject access for user.

2.2. Is it application user friendly or easy to use?

On every page accessed, need some instructions to help the user step by step how to run the application.

Help instructions to find data.



Figure 3.

Help instructions to input data.

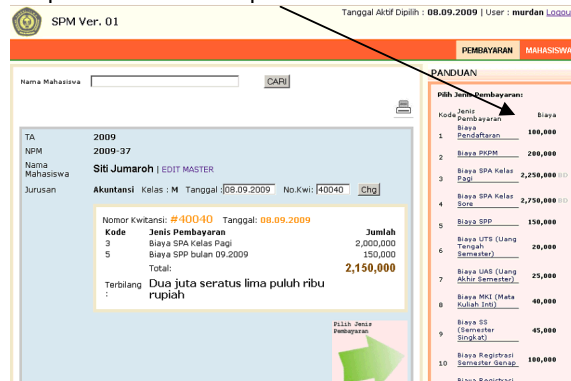


Figure 4.

2.3. Is it application having good accessibility ?

How fast it to find data using search engine facility ? How fast your application ? It's most the important one, if you want to build an application web base.

a. Fast while accessing the web page.

On this cases, be sure to minimize using query command at every page. If necessary don't use query anymore. I mean, be sure that every page would be access by visitor has be a HTML file. So when does the application should execute query database ? The solution is : Query should be done after saving data. And don't forget to save the result as html file.

Algorithm :

- input data
- click submit
- save data to database by insert command
- do query command to read database and generated information page as html file.

How to save data as html or as php file?

```
<?php
//genfile.php
$sv=" "
<?php
$harga = 100;
$jumlah = 20;
$tot = $harga*$jumlah;
Echo "Total :\".$tot;
?>";
$namafile="coba.php";
if (file_exists($namafile)) {
    unlink($namafile);
}
$handle= fopen($namafile,'a');
fputs($handle, $sv);
?>
```

After run genfile.php, you have a file coba.php now, with volume such as :

```
<?php
$harga = 100;
```

\$jumlah = 20; \$tot = \$harga*\$jumlah;
 Echo "Total :".\$tot;
 ?>

b. Fast while Searching Data.

In application it's most important to prepare a search facility. Why?. To ascertain user is the data was available or not. Or to find some information about data having.

But if you search data at a big table, it should be influence speed of searching. So before, be sure well set up a small table for search facility. For example the table for searching having only three fields. The field are title varchar(150) and content (text, 800) and url (varchar 100). Data for this table are come from all table, from master file, from transaction file and news file.

Algorithm Store Data to Search Tabel :

1. Read all data from table master
2. Store to search table
3. Read all data from table transaction
4. Store to search table

When doing add data to search table ? Doing it every add new data in the system. Example, after add master file or transaction file. Or doing as manually what script should be called to do this. Algorithm for Searching a Data :

1. Open file "search table".
2. Query Data by condition
3. Display Result.

You can take example Google to do this.

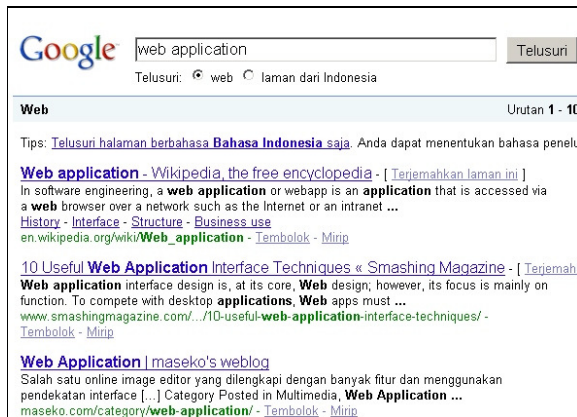


Figure 5.

2.4 Is it application can generated a good report ?

In PHP we can generated a report to PDF using Class. There are two file class needed, to run report. The file is class.ezpdf.php and class.Cpdf.php. Both file, you can download it in www.sinergypro.com/murdan/class.zip. Example : How to print Acquittance for student and Payment Report ?

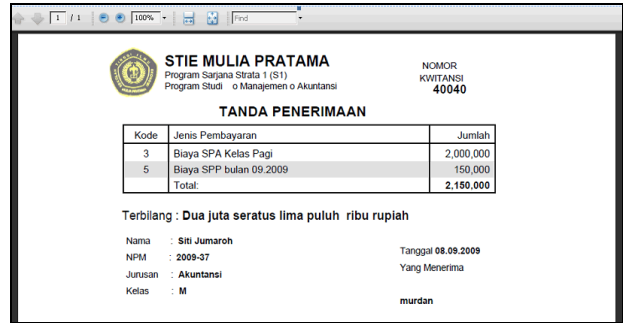


Figure 6.

To print Acquittance for student :

```
<?php
$gtanggal = $_GET["gtanggal"];
//23.10.2009
$tahunct = substr($gtanggal,6,4);
$bulanct = substr($gtanggal,3,2);
$rec = $_GET["rec"];
$namafile = $_GET["namafile"];
$c = $_GET["c"];
//cari $rec di tabel mahasiswa
include "db.inc.php";
$sql= "select npm,nama,jurusan,ta,kelas
from mahasiswa where rec='$rec'";
if (!$res=mysql_query($sql,$dbh)) {
echo mysql_error(); exit;
}
if ($row=mysql_fetch_row($res)) {
    $vnpm = $row[0];
    $vnama = $row[1];
    $vjurusan = $row[2];
    $vta = $row[3];
    $vkelas = $row[4];
}

include "db.inc.php";
$sql= "select npm,nama,jurusan,
ta,kelas,tanggal,jumlah,terbilang,nomor_kwi,opr
from kwitansi_bayaran where npm='$vnpm' and
tanggal='$gtanggal'";
if (!$res=mysql_query($sql,$dbh)) {
echo mysql_error();
}
exit;
if ($row=mysql_fetch_row($res)) {
    $vnpm = $row[0];
    $vnama = $row[1];
    $vjurusan = $row[2];
    $vta = $row[3];
    $vtanggal = $row[5];
    $vjumlah = $row[6];
    $vterbilang = $row[7];
    $vnomor_kwi = $row[8];
    $vopr = $row[9];
}
////
include "db.inc.php";
```

```

$sql= "select
kode_pembayaran,jenis_pembayaran,keter.jumlah,sk
from tr_bayaran where npm='$vnpm' and
tanggal='$vtanggal' order by kode_pembayaran";
if (!$res=mysql_query($sql,$dbh)) {
    echo mysql_error(); exit; }
$n=0; $tjumlah = 0;
while ($row=mysql_fetch_row($res)) {
    $n++;
    $xkode_pembayaran[$n] = $row[0];
    $xjenis_pembayaran[$n] = $row[1];
    $xketer[$n] = $row[2];
    $xjumlah[$n] = $row[3];
    $xsks[$n] = $row[4];
    $tjumlah = $tjumlah+$xjumlah[$n];
}

$koma_vjumlah = "" .number_format($tjumlah,0,',','');
/////

//$sude="array('Kode'=>','Jenis
Pembayaran'=>','Jumlah'=>"),";
$i = 0;
while ($i<$n) {
    $i++;
    $fiel1 = $xkode_pembayaran[$i];
    $keterangan="";
    if ($xketer[$i]) {
        $keterangan=" $xketer[$i]";
    }
    $fiel2 = $xjenis_pembayaran[$i].$keterangan;
    $fiel3 = $xjumlah[$i];
    $c_fiel3 = "" .number_format($fiel3,0,',','');
    $sude=$sude. "array('Kode'=>'$fiel1','Jenis
Pembayaran'=>'$fiel2','Jumlah'=>'$c_fiel3'),";
}
$sude=$sude. "array('Kode'=>','Jenis
Pembayaran'=>'Total:','Jumlah'=><b>$koma_vjumlah</b>')";

$sude="<?php
$brs=807;
$pdf->addText(400,$brs,9,'NOMOR');
$brs=$brs-12;
$pdf->addText(400,$brs,9,'KWITANSI');
$brs=$brs-12;
$pdf->addText(400,$brs,12,'<b>$vnomor_kwi</b>');
$pdf-
>addJpegFromFile('images/stiemp.jpg',90,780,50);
$brs=810;
$pdf->addText(146,$brs,15,'<b>STIE MULIA
PRATAMA</b>');
$brs=$brs-12;
$pdf->addText(146,$brs,9,'Program Sarjana Strata 1
(S1)');
$brs=$brs-11;
$pdf->addText(146,$brs,9,'Program Studi o
Manajemen o Akuntansi');
$brs=$brs-26;

```

```

$pdf->addText(200,$brs,14,'<b>TANDA
PENERIMAAN</b>');
$all = $pdf->openObject();
$pdf->saveState();
$pdf->restoreState();
$pdf->closeObject();
$pdf->addObject($all,'all');
$brs=$brs-12;
$pdf->ezSetDy(-60);
$data = array($sude);
$cols = array('Kode'=>'Kode','Jenis
Pembayaran'=>'Jenis
Pembayaran','Jumlah'=>'Jumlah');
$pdf->ezTable($data,$cols,"
array('xPos'=>110,'xOrientation'=>'right','cols'=>array(
'Kode'=>array('width'=>45,'justification'=>'center'),
'Jenis Pembayaran'=>array('width'=>260),
'Jumlah'=>array('width'=>65,'justification'=>'right')
));
$pdf->ezSetDy(-14);
$pdf->ezText('Terbilang : <b>$vterbilang</b>',12);
$pdf->ezSetDy(-14);
$pdf->ezText('Nama : <b>$vnama</b>',9);
$pdf->ezSetDy(-6);
$pdf->ezText('NPM : <b>$vnpm</b>',9);
$pdf->ezSetDy(-6);
$pdf->ezText('Jurusan : <b>$vjurusan</b>',9);
$pdf->ezSetDy(-6);
$pdf->ezText('Kelas : <b>$vkelas</b>',9);
$pdf->ezSetDy(50);
$pdf->ezText('Tanggal <b>$vtanggal</b>',9);
$pdf->ezSetDy(-6);
$pdf->ezText('Yang Menerima',9);
$pdf->ezSetDy(-6);
$pdf->ezText(' ',9);
$pdf->ezSetDy(-6);
$pdf->ezText(' <b>$vopr</b>',9);
?>
";
$namafile="cetak/kwi.php";
if (file_exists($namafile)) {
    unlink($namafile);
}
$handle= fopen($namafile,'a');
fputs($handle, $sude);
unset($sude);
echo
"<script>location.href='gene_report.php?namafile=$na
mafile'</script>";
exit;
?>

Script gene_report.php:
<?php
//gene_report.php
include getcwd().'class.ezpdf.php';
$pdf = & new Cezpdf("a4");
$pdf->selectFont(getcwd().'fonts/Helvetica.afm');
$pdf->openHere('Fit');
$pdf -> ezSetMargins(30,40,20,20);

```

```
include "kwi.php";
$pdf->ezStream();
?>
```

TANGGAL	NPM	KODE PEMBAYARAN	JENIS PEMBAYARAN	SKS	JUMLAH	NO. KWITANSI
27.03.2009	2009-15	1	Biaya Pendaftaran	0	100,000	37596
27.03.2009	2009-15	2	Biaya PKPM	0	200,000	37596
23.03.2009	2009-13	1	Biaya Pendaftaran	0	100,000	37580
23.03.2009	2009-13	2	Biaya PKPM	0	200,000	37580
18.03.2009	2009-12	1	Biaya Pendaftaran	0	100,000	37573
18.03.2009	2009-12	2	Biaya PKPM	0	200,000	37573
06.03.2009	2009-10	1	Biaya Pendaftaran	0	100,000	37385
06.03.2009	2009-10	2	Biaya PKPM	0	200,000	37385
Total:					1,200,000	

Figure 7.

To print Payment Report:

```
//gener_pembayaran.php?bt=08.2009
<?php
//gener_daftar_bayaran.php?bt=
$bt=$_GET["bt"];
```

```
include "db.inc.php";
$sql="select
npm,tanggal,kode_pembayaran,jenis_pembayaran,kete
r,sks,jumlah,nomor_kwi,opr from tr_bayaran where
right(tanggal,7)='$bt' order by nomor_kwi
DESC,kode_pembayaran";
if (!$res=mysql_query($sql,$dbh)) { echo
mysql_error(); exit; }
```

```
$z=0;
while ($row=mysql_fetch_row($res)) {
    $z++;
    $vnpm[$z] = $row[0];
    $vtanggal[$z] = $row[1];
    $vkode_pembayaran[$z] = $row[2];
    $vjenis_pembayaran[$z] = $row[3];
    $vsks[$z] = $row[5];
    $vjumlah[$z] = $row[6];
    $vnomor_kwi[$z] = $row[7];
    //echo "$vnpm[$z]<br>";
}
```

```
$i = 0;
while ($i<$z) {
    $i++;
    $fiel1 = $vnpm[$i];
    $fiel2 = $vtanggal[$i];
    $fiel3 = $vkode_pembayaran[$i];
    $fiel4 = $vjenis_pembayaran[$i];
    $fiel5 = $vsks[$i];
    $fiel6 = $vjumlah[$i];
    $fiel7 = $vnomor_kwi[$i];
    $tjumlah = $tjumlah + $fiel6;
    $c_fiel6 = ".number_format($fiel6,0,',','');
}
```

```
$c_tjumlah = ".number_format($tjumlah,0,',','');
$sude=$sude."array('TANGGAL'=>$fiel2,'NPM'=>
'fiel1','KODE PEMBAYARAN'=>$fiel3, 'JENIS
PEMBAYARAN'=>$fiel4,'SKS'=>$fiel5,'JUMLAH'
=>$c_fiel6,'NO. KWITANSI'=>$fiel7),\n";
}
```

```
$sude=$sude."array('TANGGAL'=>','NPM'=>','KODE
PEMBAYARAN'=>','JENIS
PEMBAYARAN'=><b>Total:</b>','SKS'=>','JUMLAH'
=><b>$c_tjumlah</b>','NO. KWITANSI'=>)\n";
```

```
//error T_ARRAY muncul disebabkan karena DATA
tidak ada yang masuk ke array.
$sude="<?php
```

```
\$brs=807;
$pdf-
>addJpegFromFile('images/stiemp.jpg',55,780,50);
\$brs=811;
$pdf->addText(120,\$brs,15,<b>STIE MULIA
PRATAMA</b>);
\$brs=\$brs-12;
$pdf->addText(120,\$brs,8,'Program Sarjana Strata 1
(S1)');
\$brs=\$brs-11;
$pdf->addText(120,\$brs,8,'Program Studi o
Manajemen o Akuntansi');
\$brs=\$brs-36;
$pdf->addText(180,\$brs,14,<b>DAFTAR
PEMBAYARAN $bt</b>);
$all = $pdf->openObject();
$pdf->saveState();
$pdf->restoreState();
$pdf->closeObject();
$pdf->addObject($all,'all');
\$brs=\$brs-12;
$pdf->ezSetDy(-80);
$data = array($sude);
$cols =
array('TANGGAL'=>'TANGGAL','NPM'=>'NPM','KODE
PEMBAYARAN'=>'KODE PEMBAYARAN','JENIS
PEMBAYARAN'=>'JENIS PEMBAYARAN',
'SKS'=>'SKS','JUMLAH'=>'JUMLAH','NO.
KWITANSI'=>'NO. KWITANSI');
$pdf->ezTable($data,$cols,"
array('xPos'=>55,'xOrientation'=>'right','cols'=>array(
'TANGGAL'=>array('width'=>70,'justification'=>'left'),
'NPM'=>array('width'=>50,'justification'=>'left'),
'KODE
PEMBAYARAN'=>array('width'=>80,'justification'=>'left'
),
'JENIS
PEMBAYARAN'=>array('width'=>130,'justification'=>'lef
t'),
'SKS'=>array('width'=>38,'justification'=>'right'),
'JUMLAH'=>array('width'=>68,'justification'=>'right'),
'NO.
KWITANSI'=>array('width'=>75,'justification'=>'left'
)));
```

```
?>
";
$namafile="daftar_bayaran.php";
if (file_exists($namafile)) {
    unlink($namafile);
}
$handle= fopen($namafile,'a');
fputs($handle, $sude);
echo
"<script>location.href='gene_daftar_bayaran.php'</scri
pt>";
exit;
?>
```

Script gene_daftar_bayaran.php:

```
<?php
//gene_daftar_bayaran.php
include getcwd().'class.ezpdf.php';
$pdf =& new Cezpdf("a4");
$pdf->selectFont(getcwd().'fonts/Helvetica.afm');
$pdf->openHere("Fit");
$pdf -> ezSetMargins(30,40,20,20);
include "daftar_bayaran.php";
$pdf->ezStream();
?>
```

Conclusion

There are four focus to develop a web application :

1. Application must be secure.
 - a. User must be using strong Password
 - b. Secure while login (push off SQL Injection) and
 - c. Check IP and User Agent.
 - d. Secure while Update Data.

Only the user who was login can update data. Every doing update, need to log some information such as username, date and time, username, and what data has changed.

To optimal your application security, you can protect each your page with this script:

```
<?php
Include "cekses.php";
If (!$userOK) {
    Echo "You are not Authorize!";
    Exit;
}
?>
```

For Additional , the application need also having backup system, because data is critical assets (Sartain, 2007).

2. Application must be user friendly and easy to use.

Need Help File showing at every page (Give instruction step by step for user)
3. Application must be fast.
 - a. Fast searching data (minimize table and use index).
 - b. Fast query and showing data (use index).
4. Application must be can generated Good Report

Use ClassPDF

References

- A. Good, Nathan. 2008. Seven habits for writing secure PHP applications. <http://www.ibm.com/developerworks/opensource/library/os-php-secure-apps/index.html> (Access 15 October, 2009).
- Hakim, Lukmanul. 2008. Membongkar Trik Raksasa para Master PHP. Jakarta : Lokomedia.
- Peranginangin, Kasiman. 2006. Aplikasi Web dengan PHP dan MySQL. Yogyakarta : Andi Publisher.
- Rahmat, Putra. 2009. Panduan Lengkap Hacking PC. Jakarta : Kawan Pustaka.
- Ricky, Anselmus. 2009. On The Spot Hacking. Jakarta : PT. Elex Media Komputindo.
- Sartain, Julie, 2007, Tips For Better Security & Compliance. http://www.processor.com/articles/PDFMagazine/Good/P_2913.PDF?GUID= (Access 15 October, 2009).
- S'to. 2009. CEH Certified Ethical Hacker 100% Illegal. Jakarta: Jasakom.
- Thalib, Abdul. 2003. Keamanan pada Aplikasi Web dengan PHP. <http://www.cert.or.id/~budi/courses/ec7010/dikmenur/thalib-report.pdf> (Access 15 October, 2009).
- W. Purbo, Onno & Akhmad Daniel S. 2005. Membangun Web e-commerce. Jakarta : PT. Elex Media Komputindo.