Panduan Dan Manual

Panduan Log Masuk Pertama Kali

Panduan Log Masuk Pertama Kali

Untuk log masuk kedalam sistem E-booking buat pertama kalinya sila ikuti langkah di bawah

1. Sila gunakan No. Kad Pengenalan anda sebagai Id Pengguna.
2. Sila gunakan No. Gaji anda sebagai kata laluan.
3. Tukar dan kemaskini kata laluan kepada katalaluan yang lebih selamat.

Mencipta Halaman Baru Frontend Site

Mencipta Halaman (Page) Baru

Halaman (Page)

1. Pergi pada menu Backend -> Site
2. Pilih Halaman yang dikehendaki
3. Klik pada frontend site baru
4. Masukan Maklumat Site

BEST PRACTICE FOR CODING

Best Practice For CSP Coding Guide

Avoid "Unsafe Inline" (CSS)

Dont do this

> Avoid inline styling.

```
<div class="wrapper" style="overflow:hidden;background: #ffffff; ">
```

Do this ✔

> Either separate the css on other file then include it using **link**, or use **style tag** with **nonce**

```
## on php editor
echo <<<HTML
<style nonce="'.$nonce.'">
    .wrapper-1 {
        overflow:hidden;background: #ffffff;
    }
</style>
<div class="wrapper wrapper-1" >
HTML
;


## on html editor
<style nonce="{{nonce}}">
```

```
    .wrapper-1 {
        overflow:hidden;background: #ffffff;
    }
</style>
<div class="wrapper wrapper-1" >
```

Avoid "Unsafe Inline" (javascript)

Dont do this

> Avoid inline script.

```
<script>
       $(window).on("load", function() {}());
</script>
```

Do this ✔

> Either separate the script on other file then include the script, or use **script tag** with **nonce**

```
## on php editor
echo
<<<SCRIPT
<script nonce="'.$nonce.'">
       $(window).on("load", function() {}());
</script>
SCRIPT
;

## on html editor
<script nonce="{{nonce}}">
       $(window).on("load", function() {}());
</script>
```

Patching guide

App Patching

Step

1. login to the server
2. extract the content to root dir (C:\caddy\html) (use application like 7z for windows to extract).

DB Patching

Step

1. login to server
2. open terminal,
3. cd to mysql bin directory

```
cd "C:\Program Files\MySQL\MySQL Server 8.0\bin"
```

4. login to the mysql server using (the password in C:\ in text file mysql_pass.txt)

```
mysql.exe -u root -p
```

5. drop the existing database

```
DROP DATABASE ukas;
```

6. create the database

```
CREATE DATABASE ukas;
```

7. logout from mysql server

```
exit
```

8. import the new sql

```
mysql -u root -p ukas < path_to_sql_file.sql
```

Patching DRSA

Patching DRSA

Langkah-langkah yang dilaksanakan untuk patching

1. Backup terlebih dahulu database server sedia ada (10.29.217.31)

```
mysqldump -u root -p mampu > mampu-20250702.sql
```

2. Drop table berkaitan frontend

```
mysql -u root -p
```

```
DROP TABLE frontend_content
```

```
DROP TABLE frontend_content_assign
```

```
DROP TABLE frontend_page
```

3. Import semula SQL dari server dev (frontend.sql)

```
mysql -u root -p mampu < frontend.sql
```

4. Adjust setting NGINX untuk mengeluarkan nonce-requestid header server-app (10.29.217.162)
   4.1 Edit file conf

   ```
   vim /etc/nginx/drsa.conf
   ```

   4.2 Masukan code add header

   ```
   proxy_set_header X-Request-ID $request_id;


   add_header Content-Security-Policy "default-src 'self'; script-src 'self' 'nonce-
   $request_id'; style-src 'self' 'nonce-$request_id';";
   ```

```

```

Contoh:

```
server {
listen 80;
server_name example.com;

location / {

    # Add CSP header with nonce
    proxy_set_header X-Request-ID $request_id;

    add_header Content-Security-Policy "default-src 'self'; script-src 'self' 'nonce-
$request_id'; style-src 'self' 'nonce-$request_id';";
        # Other configurations...
        root /var/www/html;
        index index.html;
    }
}
```

4.5 Restart nginx

```
sudo service restart nginx
```

5. Panggil nonce dari php

```
<?php
$nonce = $_SERVER['HTTP_X_REQUEST_ID'];
?>
<script nonce="<?php echo $nonce; ?>">
    console.log('Script with nonce');
</script>
```

Xampp installation

XAMPP Apache SSL Certificate Installation Manual for Windows Server

Table of Contents

Prerequisites

Before starting, ensure you have:

- XAMPP installed on Windows Server
- Administrative privileges on the server
- SSL certificate files (`.crt`, `.key`, and optionally `.ca-bundle` or intermediate certificates)
- Domain name pointing to your server's IP address

Certificate Preparation

Step 1: Organize Certificate Files

Create a dedicated folder for your SSL certificates:

```
C:\xampp\apache\conf\ssl\
```

Place your certificate files in this directory:

- `your-domain.crt` (SSL certificate)
- `your-domain.key` (Private key)
- `intermediate.crt` (Intermediate/Chain certificate - if provided)

Step 2: Verify Certificate Files

Ensure your certificate files are in the correct format:

- **Certificate file**: Should start with `-----BEGIN CERTIFICATE-----`
- **Private key**: Should start with `-----BEGIN PRIVATE KEY-----` or `-----BEGIN RSA PRIVATE KEY-----`

XAMPP Configuration

Step 3: Enable SSL Module

1. Open XAMPP Control Panel as Administrator
2. Stop Apache if it's running
3. Navigate to `C:\xampp\apache\conf\httpd.conf`
4. Find and uncomment (remove `#`) the following line:

   ```
   Include conf/extra/httpd-ssl.conf
   ```

5. Also ensure the SSL module is loaded by uncommenting:

   ```
   LoadModule ssl_module modules/mod_ssl.so
   ```

Step 4: Configure SSL Settings

1. Open `C:\xampp\apache\conf\extra\httpd-ssl.conf`

2. Locate the default SSL virtual host section (usually starts around line 104)
3. Comment out or modify the default SSL virtual host to avoid conflicts

Virtual Host Setup

Step 5: Create Virtual Host Configuration

1. Open `C:\xampp\apache\conf\extra\httpd-vhosts.conf`
2. Add your HTTP virtual host (port 80):

```
<VirtualHost brspace.bankrakyat.com.my:80>
 ServerAdmin dev@dev.com
 DocumentRoot "C:/xampp/htdocs/brspace/www"
 ServerName brspace.bankrakyat.com.my
 ServerAlias brspace.bankrakyat.com.my
 ErrorLog "logs/brspace.local-error.log"
 CustomLog "logs/brspace.local-access.log" common
 DirectoryIndex index.php

 RewriteEngine On
 RewriteCond %{HTTPS} off
 RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI}



 <Directory "C:/xampp/htdocs/htdocs/brspace/www">
     AllowOverride all
     Options FollowSymLinks MultiViews
     Require all granted
 </Directory>
 </VirtualHost>
```

3. Add your HTTPS virtual host (port 443):

```
 <VirtualHost brspace.bankrakyat.com.my:443>
 ServerAdmin dev@dev.com
 DocumentRoot "C:/xampp/htdocs/brspace/www"
 ServerName brspace.bankrakyat.com.my
 ServerAlias brspace.bankrakyat.com.my
```

```
ErrorLog "logs/brspacessl.local-error.log"
CustomLog "logs/brspacessl.local-access.log" common
DirectoryIndex index.php

<Directory "C:/xampp/htdocs/htdocs/brspace/www">
    AllowOverride all
    Options FollowSymLinks MultiViews
    Require all granted
</Directory>

# SSL Engine Switch:
SSLEngine on
SSLCertificateFile C:\xampp\apache\conf\ssl\bundle.brspace.bankrakyat.com.my.crt
SSLCertificateKeyFile C:\xampp\apache\conf\ssl\new.brspace.bankrakyat.com.my.key

</VirtualHost>
```

Step 6: Enable Virtual Hosts

1. Open `C:\xampp\apache\conf\httpd.conf`
2. Find and uncomment:

```
Include conf/extra/httpd-vhosts.conf
```

Step 7: Enable Rewrite Module (for HTTP to HTTPS redirect)

In `C:\xampp\apache\conf\httpd.conf`, uncomment:

```
LoadModule rewrite_module modules/mod_rewrite.so
```

Testing and Verification

Step 8: Test Configuration

1. Open Command Prompt as Administrator
2. Navigate to `C:\xampp\apache\bin\`
3. Test Apache configuration:

   ```
   httpd.exe -t
   ```

   You should see "Syntax OK"

Step 9: Restart Apache

1. In XAMPP Control Panel, start Apache
2. Check for any error messages in the control panel

Step 10: Verify SSL Certificate

1. Open your browser and navigate to `https://brspace.bankrakyat.com.my`
2. Check that:
   - The site loads without SSL warnings
   - The padlock icon appears in the address bar
   - HTTP automatically redirects to HTTPS

Step 11: Online SSL Testing

Use online tools to verify your SSL installation:

- SSL Labs SSL Test: `https://www.ssllabs.com/ssltest/`
- SSL Checker: Various online SSL checker tools

Troubleshooting

Common Issues and Solutions

Issue 1: "Cannot load SSL certificate"

Solution:

- Verify file paths in virtual host configuration
- Ensure certificate files have proper permissions
- Check that certificate files are not corrupted

Issue 2: "SSL handshake failed"

Solution:

- Verify that port 443 is open in Windows Firewall
- Check that no other service is using port 443
- Ensure SSL module is properly loaded

Issue 3: "Certificate chain incomplete"

Solution:

- Add intermediate certificate using `SSLCertificateChainFile`
- Ensure intermediate certificate is in the correct order

Issue 4: Mixed content warnings

Solution:

- Update all internal links to use HTTPS
- Check for hardcoded HTTP resources in your website

Log File Locations

- Apache Error Log: `C:\xampp\apache\logs\error.log`
- Custom Error Logs: `C:\xampp\apache\logs\your-domain-ssl-error.log`
- Custom Access Logs: `C:\xampp\apache\logs\your-domain-ssl-access.log`

Useful Commands

```
# Test Apache configuration
C:\xampp\apache\bin\httpd.exe -t

# View loaded modules
C:\xampp\apache\bin\httpd.exe -M

# Check SSL certificate details
openssl x509 -in your-domain.crt -text -noout
```

Security Best Practices

1. **Keep certificates secure**: Store certificate files in a protected directory
2. **Regular updates**: Keep XAMPP and Apache updated
3. **Strong SSL configuration**: Use modern protocols and ciphers only
4. **HSTS headers**: Implement HTTP Strict Transport Security
5. **Regular certificate renewal**: Monitor certificate expiration dates
6. **Backup certificates**: Keep secure backups of your certificate files

This manual provides a complete guide for setting up SSL certificates with virtual hosts on XAMPP Apache in a Windows Server environment. Follow each step carefully and test thoroughly before deploying to production.

Deployment Plan and rollback

SSL Certificate Deployment and Rollback Plan for XAMPP Apache

Document Information

- **Version**: 1.0
- **Date**: August 26, 2025
- **Environment**: Windows Server with XAMPP Apache
- **Prepared by**: System Administrator

DEPLOYMENT PLAN

1. Pre-Deployment Checklist

1.1 Environment Verification

- ☐ Verify XAMPP version and Apache status
- ☐ Confirm administrative access to Windows Server

- [ ] Ensure domain DNS is properly configured
- [ ] Verify current website functionality
- [ ] Check available disk space (minimum 100MB free)
- [ ] Confirm network connectivity and firewall settings

1.2 Certificate Validation

- [ ] Verify SSL certificate files are present and valid
- [ ] Check certificate expiration date (should be > 30 days)
- [ ] Validate private key matches the certificate
- [ ] Confirm intermediate/chain certificates are available
- [ ] Test certificate files with OpenSSL (if available)

1.3 Backup Preparation

- [ ] Create backup directory: `C:\xampp\backups\ssl-deployment-YYYYMMDD`
- [ ] Backup current Apache configuration files
- [ ] Backup current website files
- [ ] Document current Apache service status
- [ ] Take system snapshot (if virtualized)

2. Deployment Schedule

2.1 Recommended Deployment Window

- **Primary Window**: Sunday 02:00 AM - 06:00 AM (Local Server Time)
- **Alternative Window**: During scheduled maintenance window
- **Duration Estimate**: 2-3 hours (including testing)
- **Team Required**: 1-2 System Administrators

2.2 Pre-Deployment Communication

- [ ] Notify stakeholders 48 hours before deployment

- [ ] Send maintenance window notification to users
- [ ] Prepare status page updates
- [ ] Coordinate with DNS provider if needed

3. Deployment Steps

Phase 1: Preparation (30 minutes)

```
Start Time: T+0
Duration: 30 minutes
```

Step 1.1: Create Backup

```
# Create backup directory
mkdir C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%

# Backup configuration files
copy "C:\xampp\apache\conf\httpd.conf" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\"
copy "C:\xampp\apache\conf\extra\httpd-vhosts.conf" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\"
copy "C:\xampp\apache\conf\extra\httpd-ssl.conf" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\"

# Backup htdocs if needed
robocopy "C:\xampp\htdocs" "C:\xampp\backups\ssl-deployment-%date:~-4,4%%date:~-10,2%%date:~-7,2%\htdocs" /MIR
```

Step 1.2: Document Current State

- [ ] Record current Apache version: `httpd.exe -v`
- [ ] Document loaded modules: `httpd.exe -M`
- [ ] Test current website functionality
- [ ] Record current port bindings: `netstat -an | findstr :80`

Phase 2: SSL Configuration (45 minutes)

```
Start Time: T+30
Duration: 45 minutes
```

Step 2.1: Certificate Installation

- [ ] Create SSL directory: `mkdir C:\xampp\apache\conf\ssl`
- [ ] Copy certificate files to SSL directory
- [ ] Set appropriate file permissions
- [ ] Verify certificate file integrity

Step 2.2: Apache Configuration

- [ ] Enable SSL module in `httpd.conf`
- [ ] Configure SSL settings in `httpd-ssl.conf`
- [ ] Update virtual hosts in `httpd-vhosts.conf`
- [ ] Enable rewrite module for redirects

Step 2.3: Configuration Validation

```
# Test Apache configuration
C:\xampp\apache\bin\httpd.exe -t
```

Expected Result: `Syntax OK`

Phase 3: Service Restart and Testing (45 minutes)

```
Start Time: T+75
Duration: 45 minutes
```

Step 3.1: Service Management

- [ ] Stop Apache service gracefully
- [ ] Wait 30 seconds for complete shutdown
- [ ] Start Apache service

- [ ] Verify service is running without errors
- [ ] Check Apache error logs for any issues

Step 3.2: Basic Functionality Testing

- [ ] Test HTTP access (should redirect to HTTPS)
- [ ] Test HTTPS access with SSL certificate
- [ ] Verify certificate chain is complete
- [ ] Test website functionality over HTTPS
- [ ] Check browser security indicators

Phase 4: Comprehensive Testing (30 minutes)

```
Start Time: T+120
Duration: 30 minutes
```

Step 4.1: SSL Certificate Verification

- [ ] Browser certificate validation
- [ ] SSL Labs test (if internet accessible)
- [ ] Certificate expiration date verification
- [ ] Mixed content checking

Step 4.2: Performance and Security Testing

- [ ] Page load time comparison
- [ ] Security headers verification
- [ ] HSTS functionality test
- [ ] Cross-browser compatibility check

4. Post-Deployment Tasks

4.1 Monitoring Setup

- [ ] Configure SSL certificate expiration monitoring
- [ ] Set up log monitoring for SSL errors
- [ ] Update monitoring dashboards
- [ ] Schedule regular SSL health checks

4.2 Documentation Update

- [ ] Update system documentation
- [ ] Record SSL certificate details and expiration
- [ ] Update network diagrams
- [ ] Create maintenance schedules

4.3 Communication

- [ ] Send deployment success notification
- [ ] Update status pages
- [ ] Notify stakeholders of completion
- [ ] Schedule post-deployment review

ROLLBACK PLAN

1. Rollback Triggers

1.1 Critical Issues Requiring Immediate Rollback

- SSL certificate validation failures
- Website completely inaccessible via HTTPS
- Apache service failing to start
- Significant performance degradation (>50% slower)
- Critical functionality broken

1.2 Non-Critical Issues (Monitor and Fix)

- Minor SSL warnings in some browsers
- Non-critical mixed content warnings
- Minor performance impact (<20% slower)
- Cosmetic SSL indicator issues

2. Rollback Decision Matrix

Issue Severity	Impact Level	Action Required	Time Frame
Critical	High	Immediate Rollback	15 minutes
Major	Medium	Rollback within 1 hour	60 minutes
Minor	Low	Monitor and schedule fix	Next maintenance

3. Rollback Procedures

Quick Rollback (Emergency - 15 minutes)

Step 1: Stop Apache Service

```
# Stop Apache immediately
net stop apache2.4
# or via XAMPP Control Panel
```

Step 2: Restore Configuration Files

```
# Restore backup configurations
copy "C:\xampp\backups\ssl-deployment-YYYYMMDD\httpd.conf" "C:\xampp\apache\conf\"
copy "C:\xampp\backups\ssl-deployment-YYYYMMDD\httpd-vhosts.conf"
"C:\xampp\apache\conf\extra\"
copy "C:\xampp\backups\ssl-deployment-YYYYMMDD\httpd-ssl.conf" "C:\xampp\apache\conf\extra\"
```

Step 3: Start Apache Service

```
# Test configuration
C:\xampp\apache\bin\httpd.exe -t

# Start Apache service
net start apache2.4
```

Full Rollback (Comprehensive - 45 minutes)

Step 1: Complete Service Shutdown

- ☐ Stop Apache service
- ☐ Terminate any remaining Apache processes
- ☐ Clear any temporary files

Step 2: Full Configuration Restore

- ☐ Restore all Apache configuration files
- ☐ Remove SSL certificate files
- ☐ Restore original virtual host configurations
- ☐ Restore original htdocs if modified

Step 3: Verification and Testing

- ☐ Test Apache configuration syntax
- ☐ Start Apache service
- ☐ Verify HTTP website functionality
- ☐ Test all critical website features
- ☐ Monitor error logs for 15 minutes

4. Rollback Verification Checklist

4.1 Service Level Checks

- [ ] Apache service is running
- [ ] Website accessible via HTTP
- [ ] All website functionality working
- [ ] No errors in Apache error logs
- [ ] Performance metrics restored to baseline

4.2 Business Continuity Checks

- [ ] Critical business functions operational
- [ ] User access restored
- [ ] Database connectivity confirmed
- [ ] External integrations working

5. Post-Rollback Activities

5.1 Immediate Actions (0-2 hours)

- [ ] Document rollback reason and timeline
- [ ] Notify stakeholders of rollback completion
- [ ] Update status pages
- [ ] Begin root cause analysis

5.2 Follow-up Actions (2-24 hours)

- [ ] Complete incident report
- [ ] Schedule post-mortem meeting
- [ ] Plan remediation strategy
- [ ] Update deployment procedures if needed

5.3 Recovery Planning (24-72 hours)

- [ ] Analyze failed deployment

- [ ] Correct identified issues
- [ ] Plan new deployment approach
- [ ] Schedule retry deployment

RISK ASSESSMENT

1. Risk Matrix

Risk	Probability	Impact	Mitigation Strategy
Certificate validation failure	Medium	High	Thorough pre-deployment testing
Apache configuration error	Low	High	Configuration backup and testing
DNS propagation issues	Low	Medium	Verify DNS before deployment
Performance degradation	Medium	Medium	Load testing and monitoring
User access interruption	Medium	High	Deployment during low-usage hours

2. Contingency Plans

2.1 Certificate Issues

- Keep old certificate as backup
- Have certificate authority contact information ready
- Prepare temporary self-signed certificate if needed

2.2 Configuration Issues

- Maintain multiple backup copies
- Have Apache expert on standby

- Prepare minimal working configuration

2.3 Service Interruption

- Implement health checks during deployment
- Have alternative access methods ready
- Prepare user communication templates

SKM Code Changes

EONLINE

mpCustomer.master

```
218
219     <%-- Added at 10-12-2025 by allif --%>
220     <dx:MenuItem Name="skmv2portal" runat="server"
221                  Text="Portalv2 SKM"
222                  NavigateUrl=""
223                  Enabled="True">
224         <Image Height="32px" Url="~/App_Themes/shakehand.png" W
225     </dx:MenuItem>
```

1. 1ine 219 - 225

mpCustomer.master.vb

```
3   '' Add by allif on 5 Dec 2025
4   Imports System.Security.Cryptography
```

1. line 3 - 4

```
11      '' Add by allif on 5 Dec 2025
12
13      Dim item = ASPxMenu1.Items.FindByName("skmv2portal")
14      If item IsNot Nothing Then
15
16
17          If Session("UserID") Is Nothing OrElse String.IsNullOrEmpty(Session("UserID").ToString()) Then
18              item.Enabled = False
19              item.NavigateUrl = "javascript:void(0);"
20          Else
21              Dim secret As String = ConfigurationManager.AppSettings("HmacSecret")
22              If String.IsNullOrEmpty(secret) Then
23                  Throw New InvalidOperationException("HmacSecret not configured in web.config")
24              End If
25
26              Dim token As String = CreateSecureToken(Session("UserID").ToString(), Session("UserType").ToStri
27              Dim baseUrl As String = ConfigurationManager.AppSettings("PortalBaseUrl")
28              If String.IsNullOrEmpty(baseUrl) Then
29                  Throw New InvalidOperationException("PortalBaseUrl not configured in web.config")
30              End If
31
32              Dim url As String = baseUrl & "/site/auth-token?token=" & HttpUtility.UrlEncode(token)
33              item.Enabled = True
34              item.NavigateUrl = url
35
36          End If
37
38      End If
39
40      '' end add
```

2. line 11 - 40

```
71      '' Add by allif on 5 Dec 2025
72      Private Function CreateSecureToken(username As String, usertype As String, secretKey As String) As Strin
73
74          Dim timestamp As String = DateTime.UtcNow.ToString("s") ' ISO8601
75          Dim payload As String = String.Format("{0}|{1}|{2}", username, usertype, timestamp)
76          Dim payloadBytes As Byte() = Encoding.UTF8.GetBytes(payload)
77
78          Using hmac As New HMACSHA256(Encoding.UTF8.GetBytes(secretKey))
79              Dim sig As Byte() = hmac.ComputeHash(payloadBytes)
80              Return Convert.ToBase64String(payloadBytes) & "." & Convert.ToBase64String(sig)
81          End Using
82      End Function
```

3. line 71- 82

web.config

```
28      <add key="HmacSecret" value="cms-skm-vpH8K0bbnE5lsEk3kT4SSZyMkbjn1BCq" />
29      <add key="PortalBaseUrl" value="http://10.2.100.194" />
```

1. line 28-29 // for base url, change to production url/domain

INFOKOP

defaultDark

```
274                 <asp:LinkButton runat="server" ID="skmv2portal" BackColor="#FF9900" Width="400px" Height="18"
275                     Style="display: block; padding: 0; border-style: outset;"
276                     ForeColor="White" Text="Cms Skm Portal V2">
277                 </asp:LinkButton>
```

l. 1ine 274 - 277

defaultDark.vb

```
4   Imports System.Security.Cryptography ''Added for encrypt
```

1. line 4

```
828     '' Add by allif on 5 Dec 2025
829     Private Function CreateSecureToken(username As String, secretKey As String) As String
830         Dim nonce As String = DateTime.UtcNow.Ticks.ToString()
831         Dim payload As String = username & "|" & nonce
832         Dim payloadBytes As Byte() = Encoding.UTF8.GetBytes(payload)
833         Using hmac As New HMACSHA256(Encoding.UTF8.GetBytes(secretKey))
834             Dim sig As Byte() = hmac.ComputeHash(payloadBytes)
835             Return Convert.ToBase64String(payloadBytes) & "." & Convert.ToBase64String(sig)
836         End Using
837     End Function
838
839     '' Add by allif on 5 Dec 2025
840     Private Sub skmv2portal_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles skmv2portal.Click
841         RekodLog(skmv2portal.Text)
842
843         ' Option A: Open external system with token (secure)
844         Dim secret As String = ConfigurationManager.AppSettings("HmacSecret")
845         Dim token As String = CreateSecureToken(Session("Pengguna").ToString(), secret)
846         Dim url As String = "https://10.2.100.194/admin/site/auth-token?token=" & HttpUtility.UrlEncode(token)
847
848         ClientScript.RegisterStartupScript(Me.GetType(), "ClientScript", _
849             "<script type='text/javascript'>window.open('" & JsEncode(url) & "', '_blank');</script>")
850
851     End Sub
```

2. line 828 - 851
3. line 846 - // change the url to live/prod [https://10.2.100.194] to production url

```
Private Function JsEncode(ByVal s As String) As String
    If String.IsNullOrEmpty(s) Then Return ""
    Return s.Replace("\", "\\").Replace("'", "\'").Replace("""", "\""").Replace(vbCrLf, "\n").Replace(vbCr, "\r").Replace(vbTab, "\t")
End Function
```

4. line 853 - 856

web.config

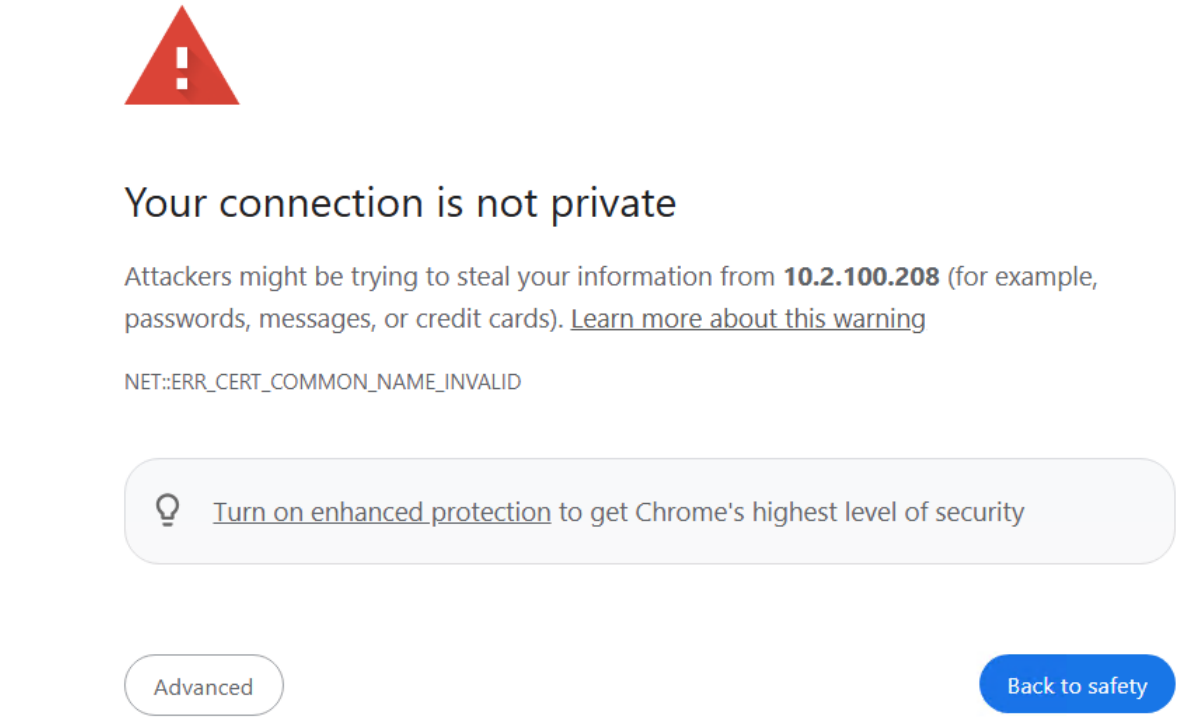
```
170        <add key="HmacSecret" value="cms-skm-vpH8K0bbnE5lsEk3kT4SSZyMkbjn1BCq" />
```

1. line 170

SIT TESTING LOGIN PAGE

Infokop

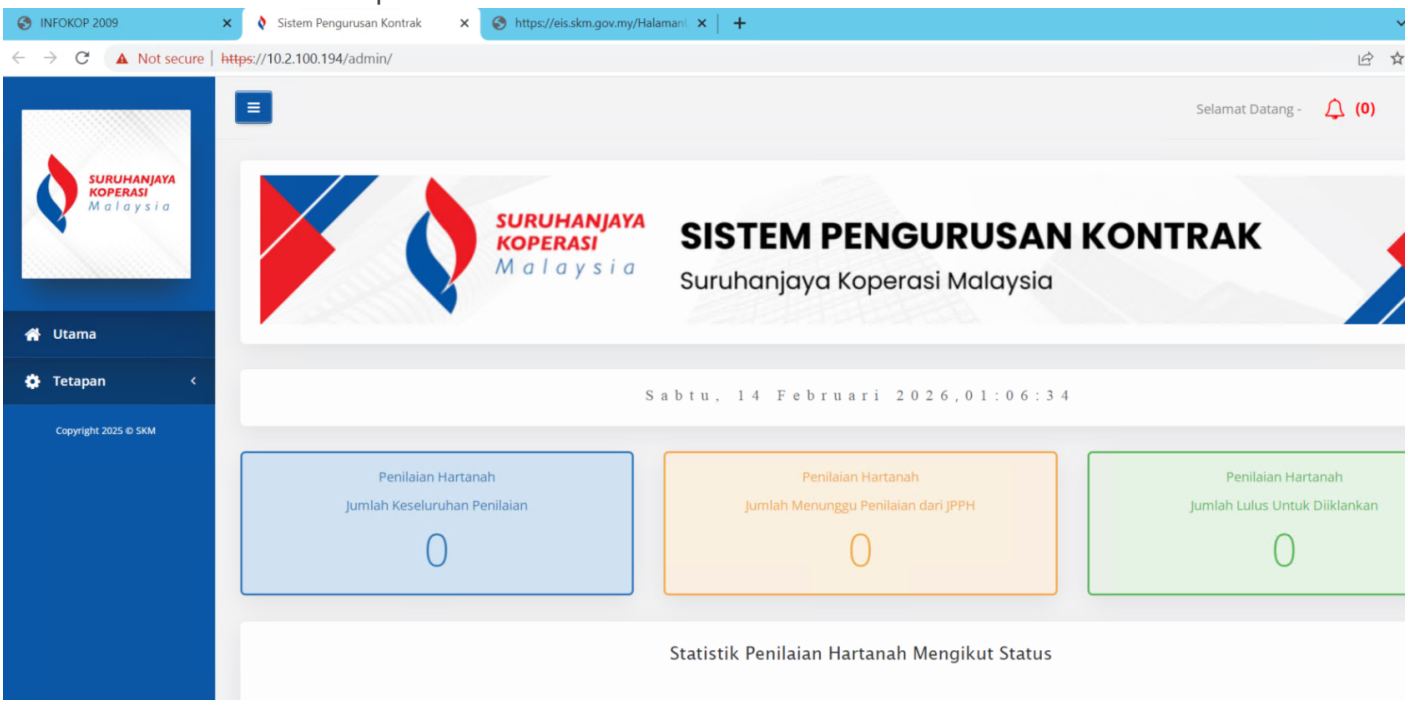
1. Open browser goto url 10.2.100.211'



2. if greet with unsecured, just click advance / procceed

3. fill the cred user:demo password: Demo$kM123

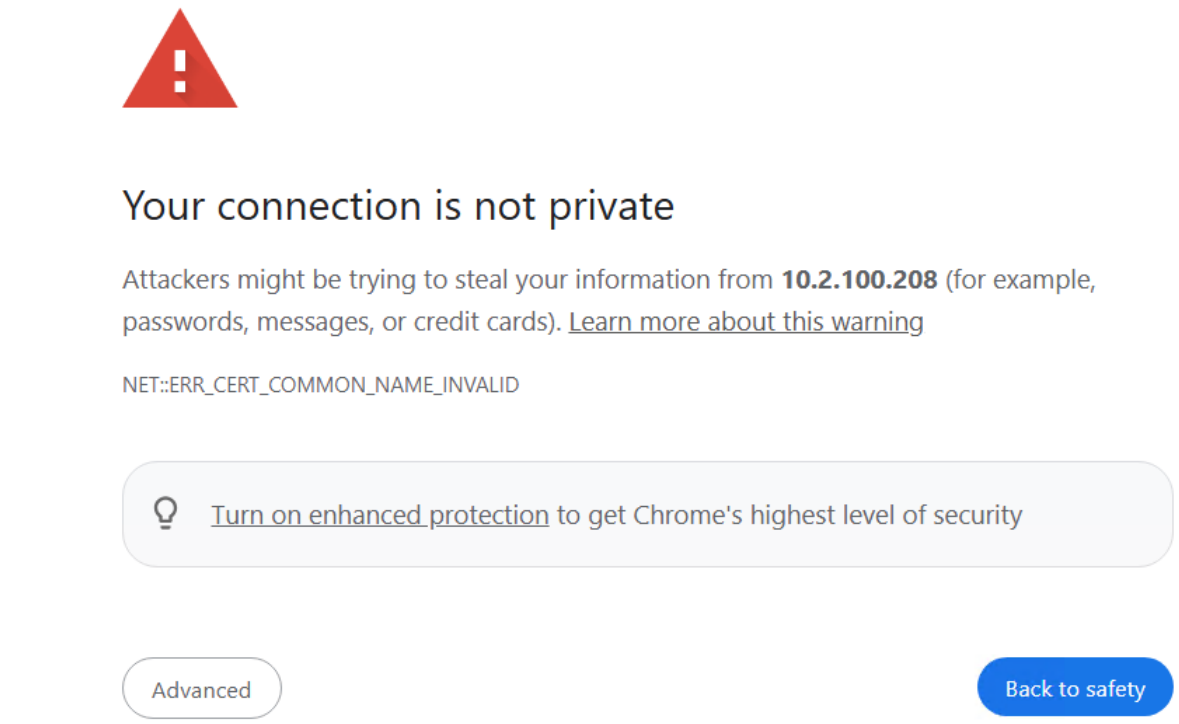
4. klik on menu "cms skm portalv2"



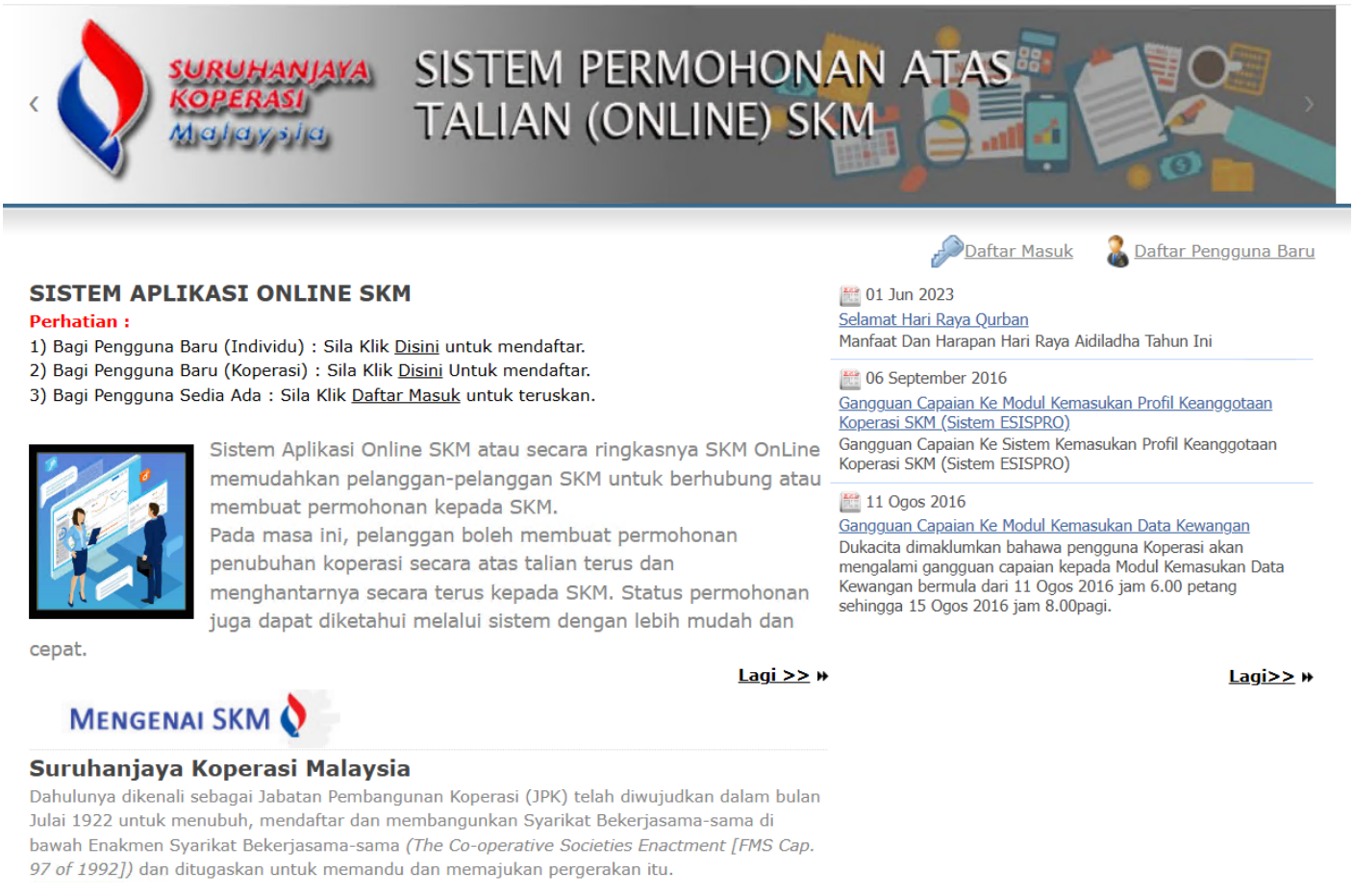
5. you will be redirected to page dashboard cms skm

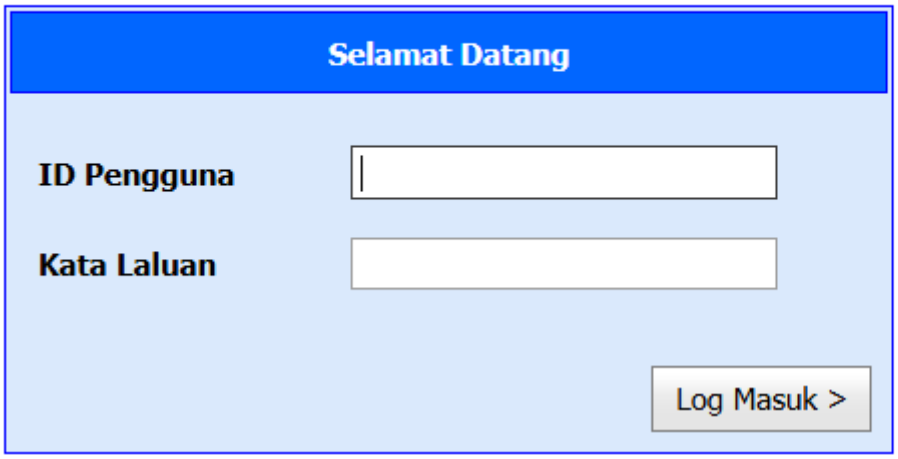
Eonline

1. Open browser goto url 10.2.100.208



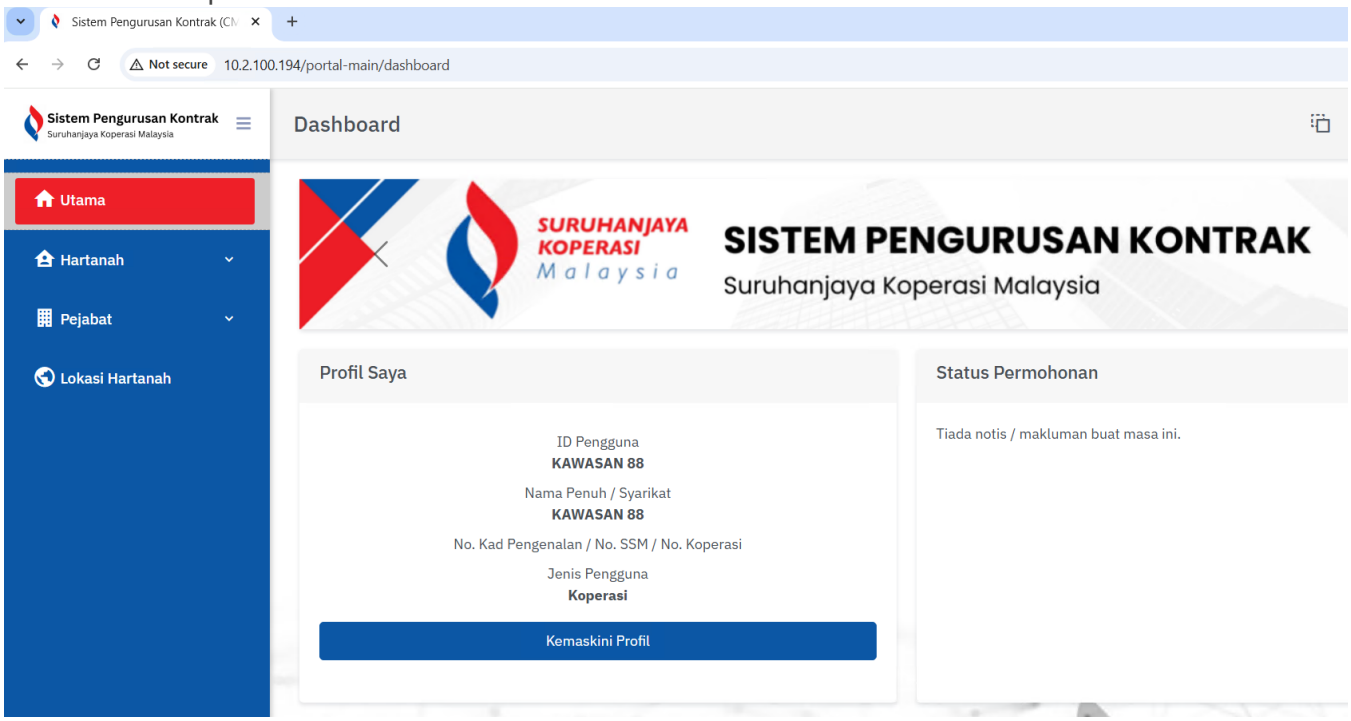
2. if greet with unsecured, just click advance / procceed





3. click on daftar masuk -> fill the cred user:kawasan 88, note: user kawasan with space, password: Demo$kM123

4. klik on menu "portalv2 skm"



5. you will be redirected to page dashboard cms skm

User Migration Prod Go Live

1. Login psql

```
sudo -u postgres psql
```

2. Renambe to back if exist

```
ALTER DATABASE rtvm RENAME TO rtvm_backup_1;
```

Remove SET transaction_timeout line

```
sed -i '/SET transaction_timeout/d' kkr-rtvmdb-202601300827.sql
```

Remove LOCALE_PROVIDER clause from CREATE DATABASE

```
sed -i 's/LOCALE_PROVIDER = [^ ]* //' kkr-rtvmdb-202601300827.sql
```

Kerberos Setting Request

I'm requesting assistance to enable seamless Windows Authentication (password-less login) for an internal IIS-hosted PHP application. To support both Kerberos and NTLM fallback, we need the following:

Requested Actions:

1. **Create a dedicated domain service account**
   - Suggested name: `svc_iis_[appname]`
   - Standard user privileges
   - "Log on as a service" right
2. **Assign this account** as the Identity for IIS Application Pool: `[DefaultAppPool]` on server `[BRUATEMOHONAPP (10.1.101.89)]`
3. **Register SPNs** to the new account:
   - `HTTP/eformuat.bankrakyat.com.my`
   - `HTTP/eformuat`
4. **Deploy a GPO** to all domain-joined workstations for automatic credential delegation:
   - Policy: `AuthServerWhitelist`
   - Value: `*.bankrakyat.com.my,eformuat.bankrakyat.com.my,eformuat`

This configuration ensures reliable Single Sign-On using Kerberos when available, with NTLM as a secure fallback. No manual registry changes or per-PC configuration will be required for end users.

Once implemented, I will validate end-to-end authentication and confirm successful user resolution in the application. Please let me know if you prefer a specific naming convention or need additional details.

Thank you for your support.