

Title : Information Disclose

Status : Medium

Reporter : Feri Harjulianto

Vuln Summary :

Ditemukan repository bernama prod-new milik user dengan nama dait23. Setelah ditelusuri lebih jauh ternyata repo tersebut merupakan data lama milik ruang guru. Pada folder databases saya menemukan sebuah file yang bernama ruanggur_updated-20150204-data.sql yang sepertinya merupakan file database backup ruangguru pada tahun 2015.

```
-- phpMyAdmin SQL Dump
-- version 4.0.10.7
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: Feb 03, 2015 at 11:25 PM
-- Server version: 5.5.40-cll
-- PHP Version: 5.4.22

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;

--
-- Database: 'ruanggur_updated'
--
-- Dumping data for table 'admin'
--

INSERT INTO `admin` (`admin_id`, `admin_username`, `admin_password`) VALUES
(1, 'admin', '77838f73a78dd604a77a1358f4be34cb'),
(2, 'arieditya.prdrh@live.com', '83d655aecbadb4907f1a44056e11b909');

--
-- Dumping data for table 'bank'
--

INSERT INTO `bank` (`bank_id`, `bank_title`) VALUES
(1, 'BANK CENTRAL ASIA Tbk'),
(2, 'BANK HANDEKA Tbk'),
(3, 'BANK NEGARA INDONESIA Tbk'),
(4, 'BANK RAKYAT INDONESIA Tbk'),
(5, 'BANK PAMULAT INDONESIA'),
(6, 'BANK MEGA Tbk'),
(7, 'BANK CIBB NEGARA Tbk'),
(8, 'BANK NISP Tbk'),
(9, 'BANK BNI SYARIAH'),
(10, 'BANK SYARIAH HANDEKA'),
(11, 'BANK MEGA SYARIAH'),
(12, 'BANK BCA SYARIAH'),
(13, 'BANK TABUNGSIH NEGARA'),
(14, 'BANK EKOPIN'),
(15, 'BANK GABAWIN INDONESIA Tbk'),
(16, 'BANK INTERNASIONAL INDONESIA Tbk'),
(17, 'BANK PAVAPADA INTERNATIONAL Tbk'),
(18, 'BANK PERKATA Tbk'),
(19, 'BANK BRI'),
(20, 'BANK BRI SYARIAH'),
(21, 'BANK BJB');

--
-- Dumping data for table 'cs_email'
--
```

Adapun informasi penting yang saya temukan dari database tersebut antara lain :

Admin

(1, 'admin', '77838f73a78dd604a77a1358f4be34cb'), #Ruangguru123
(2, 'arieditya.prdrh@live.com', '83d655aecbadb4907f1a44056e11b909'); agnusdei151979

Duta_guru

(1098, '0000-00-00 00:00:00', 'reandynamdiansyah20@gmail.com',
'f477c0bb9610eb864ae279995b200882', 'Reandy Ramdiansyah', 'Dusun Krajan 1A
RT02/01 Kecamatan Kutawaluya Kabupaten Karawang Jawa Barat', 'Jl.H.Hasan
RT003/009 Kelurahan Baru Kecamatan Pasar Rebo Jakarta Timur', 3, '085714800953', "",
1, 'Karawang', '1991-03-17', '7', 1, 10, '7069521252', 'Reandy Ramdiansyah'), R9mYaqyJ

(12, 'rifqahiamalia@gmail.com', '036abe038db598bae6d39f45f3faf015', 'Rifqah Indri Amalia', '3175086305920003', '', NULL, 1, 2, 0, '', 0, 'Jakarta', '1992-05-23', '081932995913', NULL, NULL, NULL, 'Jalan Radar Selatan, RT 07 RW 05 No.75 Jaticempaka, Pondok Gede, Bekasi, 17411', NULL, 'https://www.facebook.com/rifqah.i.amalia', 'https://twitter.com/Rifkamalia', 'lqfLP0yiJfA', 0, 0, NULL, 6, 10, '0', '0', '1', '3', '0', '0', '0', '0', '0', '1', '0', '1', '0', '0', '0', '0', '', NULL, 'Kemampuan berbahasa asing khususnya bahasa inggris dan mengoperasikan komputer menjadi kebutuhan yang harus dipenuhi oleh anak-anak yang terlahir di era digital seperti sekarang ini. Saya percaya, anak-anak yang terpapar lebih dini terhadap dua keahlian tersebut akan menjadi lebih ahli dibandingkan teman sebayanya yang tidak terpapar oleh keterampilan bahasa Inggris dan mengenal komputer sejak kecil. Saya memiliki pengalaman dalam berinteraksi dengan anak-anak dan belajar bersama anak-anak menjadi kesenangan tersendiri bagi saya. Belajar dari pengalaman saya sewaktu kecil, apabila anak-anak mau meluangkan waktu yang cukup dan konsisten berlatih komputer

atau bahasa Inggris maka tidak membutuhkan waktu yang lama untuk menguasai kedua materi tersebut.\n\nDisamping itu terkait latar belakang saya sebagai lulusan dari Ilmu Gizi, saya memiliki pemahaman yang baik dalam pelajaran Biologi, khususnya Ilmu Biologi Manusia. Sejak SD saya juga sudah menyukai pelajaran Biologi dan nilai-nilai Biologi saya selama sekolah tergolong bagus. \n\nSaya memang tidak berasal dari jurusan ilmu pendidikan, namun saya memiliki berbagai pengalaman dalam melakukan penyuluhan tentang ilmu gizi dan kesehatan kepada berbagai kalangan. Saya pernah memberikan penyuluhan kepada anak usia PAUD hingga Lansia. Pengalaman tersebut menambahkan kemampuan saya dalam mengedukasi orang lain sehingga saya percaya diri untuk menjadi pengajar.\nSaya berkomitmen untuk memberikan pengajaran kepada setiap murid saya hingga mereka memiliki pemahaman yang baik.\n", " 'S1 Ilmu Gizi, Universitas Indonesia', ", " 1, 0, NULL, NULL, NULL, '2014-04-08 00:00:00', '0000-00-00 00:00:00'), [amalia23](#)

//// snip here 16676 row

Murid

(37, 'zaharannissa@gmail.com', '54021106dbb545238342a16d2460a287', 'annissa', '3201134606910009', 'Jl. Petogogan I no. 29 RT 003/ RW 012', 'Jl. Kunir VI', 5, '085691015414', ", '02140915415', ", ", 2, 'Jakarta', '1995-08-17', 0, '4', 1, 0, 0, 0, '0000-00-00 00:00:00'), [9xNSd2xn](#)

(2, 'indahfajarwati835@ymail.com', '893ceb073db1a1efe98d65bbd62accc3', 'indah fajarwati', NULL, 'jl. masjid alfajri rt.18 rw.001 no.39D pejaten barat pasar minggu', NULL, 2, '085691460900', NULL, NULL, NULL, ", 2, 'jakarta', '1994-10-05', 0, NULL, 1, 0, 0, 0, '0000-00-00 00:00:00'), [indahfajarwati](#)

(4, 'nurazifah.sef@gmail.com', '7c84aa183420a2ed9b330c8e73e5ef11', 'Nur Azifah', '3201134606910009', 'Kp. Citayam Ds. Ragajaya No. 145 RT. 01/02 Kec. Bojonggede Kab. Bogor, Jawa Barat - 16320', ", 6, '085691628278', '08159606119', '02193038696', '02192003040', ", 2, 'Bogor', '1991-06-06', 1001, NULL, 1, 0, 0, 0, '0000-00-00 00:00:00'), [1ndones1a](#)

(5, 'nikita.halim@yahoo.com', '8e3c82bbe74ba6ca39e4e9add7d8ba2a', 'nikita halim', NULL, 'Jalan.bambu runcing no 134', NULL, 15, '085758715437', NULL, NULL, NULL, ", 2, 'jakarta', '1997-03-03', 0, NULL, 1, 0, 0, 0, '0000-00-00 00:00:00'), [147896325](#)

Catatan :

Walaupun database yang ditemukan merupakan data lama (2015) namun sebagian besar account tersebut masih menggunakan password yang sama. Selain itu jumlah data yang besar meliputi email, password dan nomer handphone merupakan data yang sangat sensitif.

Contoh akun guru :

The screenshot shows the 'Lengkapi Profil Anda' (Complete Your Profile) page for a teacher named Derry Fahrizal Ulum. The page is divided into two main sections. On the left, there is a sidebar with a profile picture and a list of tabs: 'Profile', 'Identitas', 'Bahan Ajar', 'Jadwal', 'Pengalaman', and 'Ubah Kata Sandi'. The 'Profile' tab is currently selected. On the right, there is a form titled 'Lengkapi Profil Anda' with a sub-header 'Kelengkapan profil Anda adalah hal yang utama. Informasi ini akan digunakan oleh pengguna Ruangguru dalam memilih guru untuk mengajar. Untuk itu, pastikan bahwa informasi Anda lengkap, menarik, dan berbahasa sopan.' The form includes fields for 'Nama Lengkap' (Derry Fahrizal Ulum), 'Nomor Handphone' (62857787837), 'Jenis Kelamin' (laki-laki), 'Provinsi (KTP)' (JAWA TENGAH), 'Kota (KTP)' (Pilih...), 'Kecamatan (KTP)' (Pilih...), and 'Alamat Tempat Tinggal (KTP)*' (Dusun Sindanghaji RT 06 RW 05 Desa Bantarpanjang). There is also a 'Ganti Avatar' button and an 'Unggah Foto' button. A chat widget on the right says 'Bingung dengan fitur Ruangguru? Yuk tanya!'.

Contoh Akun Siswa :

The screenshot shows the student dashboard of the Ruang Guru website. The top navigation bar includes links for 'Tentang Kami', 'Produk Kami', 'ruangbaca', 'Bimbel Online', and 'Bantuan'. The main content area has a header with 'HOME', 'RUANG LES', 'RUANG KELAS', and 'RUANG UJI'. Below the header, there is a 'Kode Referral' section with a gift icon and the code 'nurccwva'. The text explains that the code can be shared with friends to get a discount on purchases. Below this, there is a section for downloading the 'GRATIS Aplikasi Ruangguru' with links to the Google Play and App Store. The footer contains four columns: 'TENTANG RUANGGURU' (Tentang Kami, Karir, Bantuan, Kontak Kami), 'PAKET DIGITAL BOOTCAMP TERPOPULER' (UN SMA + SBMPIN, UN SMP, SBMPIN (3 bulan), UN SD, Kelas X), 'LAINNYA' (Blog Ruangguru, Press kit, Kebijakan Privasi, Syarat dan Ketentuan, Menjadi Guru), and 'IKUTI KAMI DI' (Facebook, Twitter, Instagram, YouTube, WhatsApp). A chat widget on the right says 'Bingung dengan fitur Ruangguru? Yuk tanya!'.

How To Fix :

Public repo not your friend, just delete it and that will fix your problem

