Pengamanan Pengelolaan Hak Akses Web Berbasis Yii Framework

Qurotul Aini[1], Untung Rahardja[2], Harries Madiistriyatno[3], Yoke Dwi Martianda Setiaji[4]

[1,2,4]STMIK Raharja, Jl. Jend. Sudirman No.40, Modern Cikokol, Tangerang
[3]Universitas Persada Y.A.I. , Jl. Diponegoro No.74, Jakarta Pusat
e-mail: aini@raharja.info

Abstrak. Di era perkembangan teknologi seperti saat ini, sistem informasi berperan sangat penting. Banyak sekali yang mengandalkan sistem informasi untuk mendapatkan informasi yang akurat, menentukan keputusan, atau memecahkan permasalahan. Namun terkadang datang berbagai ancaman terhadap keamanan dari sistem tersebut terutama dalam akses data. Penelitian ini bertujuan untuk menginvestigasi salah satu solusi mencegah ancaman terhadap keamanan terutama pada sistem *web* berbasis Yii Framework. Dengan memanfaatkan fitur keamanan akses kontrol dari Yii Framework, maka dapat dikembangkan sebuah *web* yang dapat membedakan akses terhadap *user* dalam satu *web*. Pengamanan akses berfungsi mengamankan data dari *user* yang tidak memiliki hak untuk mengaksesnya. Penelitian ini dilakukan dengan menggunakan 3 metode penelitian, yaitu metode tinjauan pustaka untuk mempelajari Yii Framework dan pengelolaan hak akses pada *web*, metode analisis untuk menganalisa penggunaan hak akses *user* pada sistem serta metode perancangan untuk merancang dan membangun sistem. Fitur keamanan ini diimplementasikan pada sistem berbasis *web* VIKA (*Viewboard* Kepala Jurusan) dimana akan memberlakukan akses yang berbeda untuk kepala jurusan dan pimpinan. Penelitian ini berhasil membuat sistem dengan keamanan hak akses dan mampu menjaga keamanan data dari *user* yang tidak memiliki hak. Dengan pengelolaan hak akses ini, maka sistem memiliki integritas dan keamanan yang lebih baik.

Kata kunci: *Pengelolaan Hak Akses, VIKA, Yii Framework, Keamanan*

1 Pendahuluan

Pada era digital seperti ini sistem informasi berperan sangat penting dalam kehidupan sehari-hari. Sistem tersebut pastinya akan membuat sebuah perubahan dari era yang manualisasi ke era yang pastinya lebih komputerisasi dalam berbagai bidang pendidikan, perkuliahan, dan lain-lain [1]. Hampir semua aspek kehidupan manusia tidak terlepas dari sistem informasi. Mulai dari bidang bisnis, pelayanan, produksi, dan bahkan pada dunia pendidikan pun sangat membutuhkan sistem informasi.

Diterima 2 Maret 2018, Direvisi 5 Juni 2018, Diterima untuk publikasi 7 Juni 2018

Karena sistem informasi yang berkembang pesat dan banyaknya data-data penting yang terkandung di dalamnya, maka dibutuhkan suatu jaminan keamanan untuk sistem informasi tersebut. Agar keamanan data pada sistem informasi bisa terjaga. Sehingga tidak ada hal-hal yang tidak diinginkan seperti, pencurian data, perusakan data atau manipulasi data lainnya.

Menurut [2], faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

Keamanan sistem informasi tentunya berkaitan erat dengan keamanan basis datanya. Menurut [3], keamanan basis data adalah perlindungan basis data atas penggunaan yang tidak mempunyai hak. Tidak adanya langkah-langkah pengamanan yang tepat, integrasi membuat data menjadi rawan. Akses dari pengguna yang diizinkan dapat dibatasi oleh *operation type*.

Dari penelitian yang dilakukan oleh Ahmad Zakir, Yii Framework merupakan salah satu framework PHP yang cukup populer dikalangan PHP developer yang sifatnya *open source* [4]. Sebagai *framework* yang mengusung pola desain *Model-View-Controller* (MVC) yang memudahkan bagi pengembangan *web* dalam pengolahan logika aplikasi dengan tampilan antar muka. Sehingga pengembangan *web* menjadi lebih efektif dan efisien.

Dalam penelitian ini penulis akan menyisipkan fitur keamanan hak akses (*Access Control*) pada *web Viewboard* Kepala Jurusan (VIKA) yang berbasis framework Yii. Sebagai pengamanan *web* untuk mencegah *user* yang tidak diizinkan melihat isi dari halaman *web* atau melakukan sesuatu pada halaman *web* tersebut. Selain itu, penggunaan fitur keamanan ini dapat mengelola *web* sehingga lebih terjaga dan terhindar dari ancaman keamanan.

VIKA adalah sebuah sistem *web* pada Perguruan Tinggi Raharja yang digunakan untuk mengecek mahasiswa layak KKP dan melakukan tambah pembimbing bagi mahasiswa tersebut oleh kepala jurusan. VIKA berguna bagi kepala jurusan, sehingga tidak perlu melakukan cek manual terhadap siswa yang layak KKP. Mempermudah proses *add* pembimbing bagi mahasiswa yang telah layak KKP [5].

Digunakanannya sistem VIKA sebagai objek pada penelitian kali ini dikarenakan, VIKA memiliki *user* yang berbeda-beda dengan hak akses yang berbeda pula. Sehingga dalam hal ini dirasa tepat untuk mendapatkan data yang diperlukan didalam penelitian kali ini.

2 Metode Penelitian

Dalam penelitian kali ini, peneliti menggunakan beberapa metode penelitian yang menjadi kerangka penulis untuk menjalankan tahapan dalam penelitian ini. Ada 2 (dua) metode penelitian, antara lain Metode Tinjauan Pustaka dan Metode Analisa.

2.1 Metode Tinjauan Pustaka

Adapun 9 (sembilan) literatur ilmiah yang digunakan sebagai sumber tinjauan pustaka sebagai berikut:

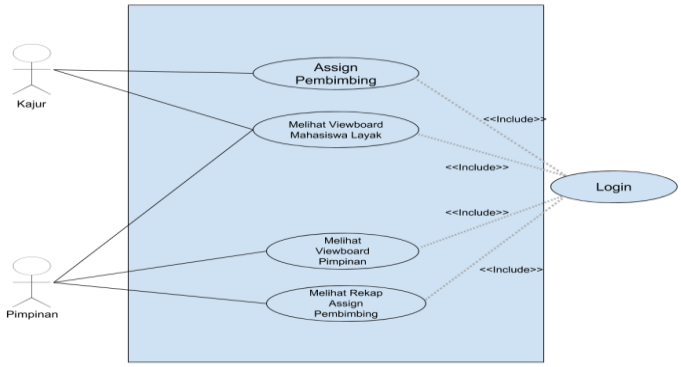
a. Penelitian yang dilakukan oleh Untung Rahardja, Hidayati dan Reny Ardyanti pada tahun 2010 dengan judul "Keamanan Batasan Data Menggunakan Metode Write Validation Dalam Distribute Database System" yang menjelaskan tentang perkembangan *distributed database*. Dimana dijelaskan semakin bertambahnya data maka membuat sistem semakin lama dalam *display* data. Sehingga munculah DMQ (*Data Mart Query*) namun kendalanya data menjadi tidak *realtime*. Dengan sistem tersebut *display* data butuh validasi dengan metode baru yaitu *write validation* sehingga data yang ditampilkan ke pengguna menjadi lebih aman saat dieksekusi [6].
b. Penelitian yang dilakukan oleh Martinus Mujur Rose dan Ibnu Zaid pada tahun 2014 dengan judul "Desain dan Implementasi Sistem Keamanan Web pada Website Jurnal TELISKA Politeknik Negeri Sriwijaya" yang menjelaskan tentang keamanan data jurnal pada *web* jurnal Teliska yang hanya dapat diakses oleh *user* yang sudah *login* [7].
c. Penelitian yang dilakukan oleh Sodikin pada tahun 2011 dengan judul "Perancangan Sistem Penggajian Dengan Hak Akses Karyawan Berbasis Web" yang menjelaskan tentang *web* sistem penggajian berbasis *web* PHP dengan hak akses karyawan [8].
d. Penelitian yang dilakukan oleh Erliyah Nurul Jannah, Mukhammad Masrur, dan Siti Asiyah pada tahun 2015 dengan judul "Penerapan Framework Yii dalam Pembangunan Sistem Informasi Asrama Santri Pondok Pesantren Sebagai Media Pencarian Asrama Berbasis WEB" yang menghasilkan sebuah *web* dengan fasilitas *login* bagi pengurus pondok pesantren, sehingga membatasi bagi pihak yang tidak punya wewenang mengakses *web* [9].
e. Penelitian yang dilakukan oleh Johni S. Pasaribu pada tahun 2017 dengan judul "Penerapan Framework Yii Pada Pembangunan Sistem PPDB SMP BPPI Baleendah Kabupaten Bandung" yang menghasilkan sistem yang memiliki fasilitas *login* dan akses yang berbeda-beda bagi *admin* dan calon siswa pada SMP BPPI Baleendah [10].

f. Penelitian yang dilakukan oleh Untung Rahardja, Muhamad Yusup, dan Qurotul Aini pada tahun 2014 dengan judul "Aplikasi Campus Learning System *iOU (Integrated Online Ujian)* dalam mendukung kegiatan *iLearning Education* (iDU) Pada Perguruan Tinggi" yang menghasilkan sistem ujian *online* yang memiliki akses yang berbeda bagi dosen dan mahasiswa yang berguna untuk menunjang kegiatan ujian yang lebih efektif dan efisien [11].
g. Penelitian yang dilakukkan oleh Ezedine Barka, Sujith Samuel Mathew, dan Yacine Atif pada tahun 2015 dengan judul "Securing the web of things with role-based access control" yang menjelaskan tentang sebuah arsitektur menggunakan fitur *Role-Based Access Control* (RBAC) untuk menentukan kebijakan kontrol akses ke *Web of Things* (WoT) serta menggunakan kriptografi untuk menerapkan kebijakan semacam itu [12].
h. Penelitian yang dilakukan oleh Qasim Mahmud Rajpoot, Christian Damsgard Jensen, dan Ram Krishnan pada tahun 2015 dengan judul "Integrating attributes into role-based access control" yang menghasilkan usulan mengusulkan sebuah model kontrol akses yang menggabungkan dua model dengan cara baru untuk menyatukan manfaat *Role-Based Access Control* dan *Attribute Based Access Control* dimana dalam pendekatannya menyediakan mekanisme *fine-grained access control* yang memperhitungkan informasi kontekstual saat ini sementara membuat keputusan kontrol akses [13].
i. Penelitian yang dilakukan oleh Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu, dan Jin Li pada tahun 2016 dengan judul "Fine-grained two-factor access control for web-based cloud computing services" yang menghasilkan sistem akses kontrol dengan 2 faktor atau 2FA (*Fine-Grained Two-Factor Authentication)* untuk layanan *web* berbasis komputasi awan. Dimana *user* diharuskan memiliki kedua syarat autentikasi untuk bisa mengakses sistem [14].

Dari 9 literatur ilmiah di atas dapat diambil kesimpulan bahwa banyak metode dalam melakukan akses kontrol dan menunjukan betapa pentingnya akses kontrol untuk mengontrol perilaku *user* di dalam sistem. Sehingga dapat menjaga keamanan sistem dari ancaman. Maka dari itu dibutuhkan sebuah sistem dengan akses kontrol yang baik guna menunjang keamanan sistem tersebut.

2.2 Metode Analisis

Metode analisa dilakukan untuk menganalisa kebutuhan dari sistem yang akan dibangun. Dengan metode ini dicoba untuk menganalisa sistem VIKA agar lebih memahami sistem yang sedang berjalan saat ini.



Gambar 1 *Use case* diagram VIKA

Pada *use case* diagram diatas dapat dilihat aktor yang ada didalam sistem adalah Kajur dan Pimpinan. Masing-masing aktor memiliki interaksi tersendiri terhadap sistem. Semua interaksi yang ada pada sistem harus melewati *login* dahulu menggunakan Rinfo agar interaksi dapat dilakukan. Menurut Untung Rahardja [15], Rinfo ini adalah media komunikai sekaligus alat pendukung dalam proses pembelajaran di Perguruan Tinggi Raharja. Saat melihat *Viewboard* Layak KKP, sehingga harus ada akses yang berbeda terhadap aktor pada sistem tersebut.

2.3 Metode Perancangan

Metode perancangan digunakan untuk membuat rancang bangun sistem. Pada tahap ini, mulai perancangan sistem *Viewboard* Kepala Jurusan (VIKA) yang didalamnya telah terdapat pengelolaan hak akses.

3 Hasil Dan Pembahasan

Sistem yang baik adalah harus memiliki keamanan yang baik. Keamanan data pada sistem harus terjaga dari hal-hal yang bisa menganggu sistem. Salah satu caranya adalah dengan pengendalian hak akses atau *access control*. Seperti pada penelitian yang dilakukan oleh Suryo Guritno, Untung Rahardja, dan Valent Setiatmi dengan judul, "*Access Restriction* Sebagai Bentuk Pengamanan Dengan Metode IP Token". Pada penelitian tersebut dibahas tentang pembatasan akses bagi *user* yang memiliki *IP Address* tertentu saja. Pembatasan tersebut digunakan pada sistem AO (Absensi *Online*) yang akan membatasi akses untuk dosen yang telah klik hadir pada komputer di kelas tertentu. Sehingga proses absensi mahasiswa hanya dapat dilakukan pada komputer tempat dosen melakukan absen hadir. Dengan metode ini memberikan keamanan dan integritas terhadap data absensi *online* [16].

Sementara pada penelitian yang dilakukan oleh Herru Arranuri dan Erwin Gunadhi dengan jurnal yang berjudul, "Pengamanan Basis Data Pengelolaan Hak Akses Dengan Metode Role-Based Access Control" yang membahas tentang pengendalian hak akses pada koperasi Padamukti Garut yang memanfaatkan metode Role Based Access Control (RBAC). Dengan mendefinisikan *role user* pada tabel yang ada pada *database* sehingga *web* dapat membedakan akses bagi *user* dan memberikan hak yang berbeda antara *user*. Sehingga *user* yang tidak memiliki akses, akan dibatasi hak untuk melakukan *action* tertentu di dalam *web*. Misalnya *user* anggota hanya bisa melihat tabel-tabel yang ada tetapi tidak dapat melakukan aksi apapun. Tidak seperti *user* bendahara yang dapat melihat tabel data simpanan dan juga dapat memasukan *record* baru pada tabel tersebut. Tetapi *user* bendahara tidak memiliki akses yang luas seperti *user* ketua yang memiliki akses keseluruh tabel dan dapat menghapus *record* yang ada pada tabel tersebut [17].

Pada penelitian yang dilakukkan oleh Diah Aryani, Qurotul Aini dan Tasya Novelia sebagai sebuah jurnal yang diterbitkan pada SENSI Journal dengan judul, "Perancangan PEN+ Menggunakan Yii Framework Pada Perguruan Tinggi Raharja" yang membahas tentang sistem penilaian *online* yang memudahkan dosen dalam memberikan penilaian terhadap mahasiswa. Di dalam sistem ini memiliki banyak sekali *user* yang memiliki akses yang berbeda. Dengan menggunakan Yii Framework dan tentunya metode RBAC karena setiap *user* pasti memiliki akses yang berbeda di dalam sistem. Contohnya hanya Dosen saja yang memiliki akses untuk memasukan nilai, sementara Kajur hanya memiliki akses untuk melihat *Viewboard* untuk memantau performa dosen binaannya. Dan RPU memiliki akses untuk menerima hasil masukan nilai dari dosen dan merekap data nilai mahasiswa [18].

Dengan menggunakan metode dan konsep yang ada pada penelitian yang telah dijelaskan sebelumnya, penelitian ini menggunakan Yii Framework dan konsep RBAC pada web VIKA (*Viewboard* Kepala Jurusan) yang akan membedakan akses pada *user*.

Seperti pada *framework* umumnya Yii menggunakan konsep MVC yang lazim digunakan oleh *framework* pada umumnya. Menurut [19], MVC adalah sebuah metode pengembangan aplikasi dengan memisahkan data (*Model*), tampilan (*View*) dan pengolahannnya (*Controller*). Sehingga membuat pengembangan menjadi lebih efektif dan efisien karena *developer* dapat membagi pekerjaan antara tampilan aplikasi dan logika di dalam programnya.

Fitur keamanan pada Yii sangat lengkap dan sudah terbukti tangguh, mencakup autentikasi dan otorisasi, *hash password*, RBAC dan *tools* mencegah *SQL*

injection. *Developer* Yii sangat baik dalam memberikan fitur keamanan, karena juga bekerja sama dengan berbagai ahli dalam keamanan *web*. Sehingga keamanan pada aplikasi Yii sangat terjamin [20].

Pada penelitian ini dengan memanfaatkan fitur autentikasi dan pengelolaan hak akses pada Yii yang dimaksudkan untuk memisahkan hak akses pada *web Viewboard* Kepala Jurusan (VIKA). Dimana terdapat 2 aktor, yaitu kepala jurusan dan pimpinan. Pada *web* VIKA kepala jurusan dapat melakukan tambah pembimbing bagi mahasiswa layak KKP. Sementara pimpinan hanya dapat melihat *Viewboard* tetapi tidak bisa melakukan tambah pembimbing.

Menurut [21], Role based access control (RBAC) atau pengelolaan hak akses memiliki keuntungan untuk mendukung berbagai tugas hak akses dan pengguna dimungkinkan mengaktifkan hak akses yang dibutuhkan untuk melakukan tugas pada setiap sesi. Ini artinya di dalam satu sistem dapat memiliki banyak pemakai yang mempunyai hak akses yang berbeda dan mempunyai tugas yang berbeda-beda.

	Viewboard	Add Pembimbing
Kepala Jurusan	✓	✓
Pimpinan	✓	✗

Gambar 2 Tabel hak akses *web* VIKA

Gambar 2 merupakan tabel hak akses yang menjelaskan tentang pemisahan hak akses pada *web* VIKA. Kepala Jurusan mempunyai akses untuk *add* pembimbing dan melihat *Viewboard* mahasiswa layak KKP. Sementara pimpinan hanya memiliki akses pada tampilan *Viewboard* saja.

Berdasarkan tabel di atas sebagai acuan pembuatan tabel *user* pada MYSQL dengan memberikan *role* yang spesifik. Kemudian pada *app\models\User* Yii definisikan *role* tersebut dengan membuat sebuah *constant* pada model agar Yii dapat membacanya. Lalu buat lah *file AccessRule* pada *app\components* yang meng-*extend library Access Rule* yang telah disediakan oleh Yii. Ekstensi ini lah yang akan mengecek *role* dari *user*, apakah *role user* tersebut cocok. Lalu pada *controller action* yang menangani *add* pembimbing, batasi hanya *role* kepala jurusan saja yang dapat mengaksesnya. Dengan membuat *rule* pada *function behavior* yang ada pada *controller* tersebut.

Column	Type	Comment
IdUserVika	int(11)	
NamaLengkap	varchar(55)	
AlamatEmail	varchar(50) [**untung@raharja.info**]	
Password	varchar(20) [**1234**]	
Type	tinyint(2) [**1**]	1=>'Admin',2=>'Pimpinan',3=>'Kajur

Gambar 3 Tampilan struktur basis data

Gambar 3 memperlihatkan tampilan struktur basis data tabel *user*. Dapat terlihat pada kolom *type* merupakan pembeda bagi setiap *user* yang ada pada sistem. Setiap grup *user* dibedakan dengan angka dari satu sampai tiga yang mewakili identitas *user* tersebut. Pada akhirnya akan membedakan hak akses dari masing masing *user* yang ada.

```php
public function Level($idType) {
  $username = Yii::$app->Goplus->getUsernameID();
  $user = VikaUser::find()->where(['AlamatEmail' =>$username,'Type'=>$idType])->one();
  if ($user != NULL) {
    return 1;
  } else {
    return 0 ;
  }
}
```

Gambar 4 Listing program pada *file models*

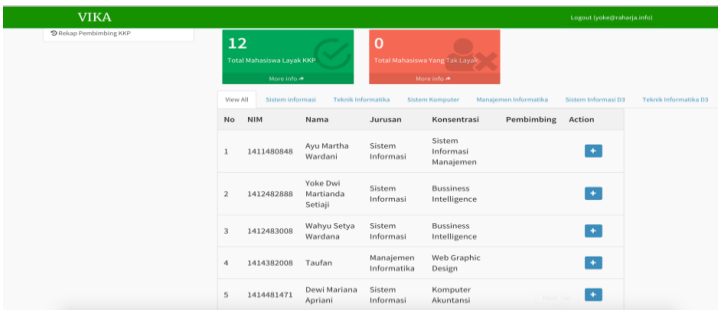
Gambar 4 terdapat pada *file models* yang menangani tabel *user* yang sebelumnya dibuat. Pada model *user* ini tambahkan *function level* dengan parameter $idType yang didapatkan dari *field type* yang ada di tabel *user*. Ini akan menerjemahkan *level* atau tipe *user* seperti apa yang sedang *login* didalam sistem.

```php
    <th>No</th>
    <th>NIM</th>
    <th>Nama</th>
    <th>Jurusan</th>
    <th>Konsentrasi</th>
    <th>Pembimbing</th>
    <th>Action</th>
  </tr>
<?php
  $no = 1 ;
?>
  <?php foreach ($models as $data): ?>
          <tr>
              <td><?php echo $no ;  ?></td>
              <td><?= $data['NIM'] ?></td>
              <td><?= $data['NamaLengkap'] ?></td>
              <td><?= $data['Jurusan'] ?></td>
              <td><?= $data['Konsentrasi'] ?></td>
              <td><?= $data['NamaDosen'] ?></td>
              <td style="width:15%;text-align:center;">

                <?php if ($Kajur ['Type']) { ?>
                <?php if (isset($data['NamaDosen'])) { ?>
              <button type="button" class="btn btn-primary btn-sm disabled" href="#"><i class="glyphicon glyphicon-plus"></i></button>
                <a class="btn btn-warning btn-sm" href="<?php echo Yii::$app->urlManager->createUrl(['viewboard/update']).'/?id='.$data['PlotID']; ?>">
                 <i class="fa fa-refresh"></i></a>
                <a class="btn btn-danger btn-sm" href="<?php echo Yii::$app->urlManager->createUrl(['viewboard/delete']).'/?id='.$data['PlotID']; ?>">
                 <i class="fa fa-trash"></i></a>
                <?php } else { ?>
                <button type="button" class="btn btn-primary btn-sm disabled" href="#"><i class="glyphicon glyphicon-plus"></i></button>
                <?php } ?>
```

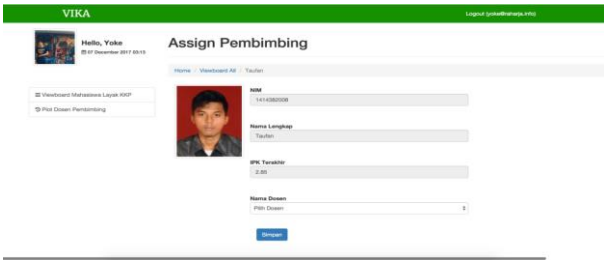
Gambar 5 Listing program pada tampilan *viewboard* layak KKP

Kemudian pada tampilan *Viewboard* layak berikan pengecualian jika *type user* Kajur saja yang dapat mengakses *button assign* pembimbing. Sehingga selain Kajur hanya akan menemukan *button* yang *disabled* yang artinya tidak dapat mengakses *assign* pembimbing.



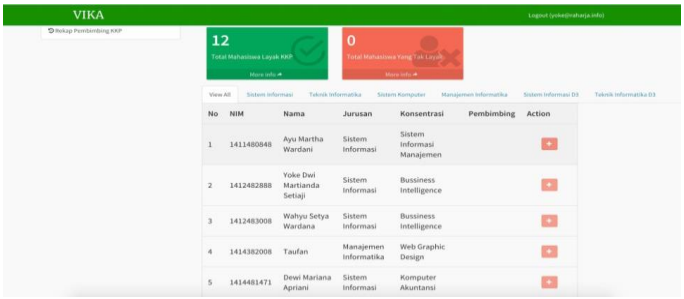
Gambar 6 Tampilan *viewboard* layak KKP (Kajur)

Gambar 6 menampilkan *Viewboard* mahasiswa layak KKP pada saat tampilan *login* kepala jurusan. Dapat dilihat pada *action add* pembimbing berwarna biru dan dapat di klik.



Gambar 7 Tampilan *add* pembimbing

Pada Gambar 7 merupakan tampilan saat kepala jurusan meng-klik tombol *add* pembimbing, maka akan muncul tampilan untuk kepala jurusan untuk melakukan *add* pembimbing bagi mahasiswa layak KKP.



Gambar 8 Tampilan *viewboard* layak KKP (Pimpinan)

Gambar 8 memperlihatkan tampilan saat *login* dengan *role* sebagai pimpinan. Terlihat masih dapat mengakses *Viewboard* mahasiswa layak KKP namun pada *action add* pembimbing berubah menjadi merah dan *disabled* (tidak bisa di klik). Sehingga pimpinan tidak dapat mengakses halaman *add* pembimbing

Dengan hasil uji coba di atas dapat disimpulkan bahwa pengelolaan hak akses berdasarkan *role user* sangat efektif dalam memisahkan peran antara kepala jurusan yang berwenang terhadap *add* pembimbing dan pimpinan yang berwenang untuk mengawasi tugas juga memantau kinerja dari kepala jurusan. Serta dapat mengantisipasi keamanan halaman *web* berdasarkan *role* yang spesifik dari *user* pada web VIKA.

4 Kesimpulan

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa pengelolaan hak akses pada sistem VIKA (*Viewboard* Kepala Jurusan) bisa mengidentifikasi *user* yang sedang *login* dan membatasi *user* untuk mengakses halaman tertentu. Sehingga *user* yang tidak memiliki hak akses terhadap halaman tersebut tidak mungkin dapat mengakses halaman. Hal ini memberikan keamanan terhadap suatu halaman *web* dari *user* yang tidak memiliki kewenangan dalam mengaksesnya. Pimpinan yang bukan kewenangannya melakukan *add* pembimbing tidak dapat mengakses halaman *input* karena itu merupakan wewenang kepala jurusan.

5 Saran

Keamanan dengan menggunakan *role-user* sebagai pedoman dalam mengakses pada *web* VIKA ini sudah cukup baik. Namun, penulis sadar bahwa sistem ini masih belum sempurna, masih ada kemungkinan lain untuk menembus keamanan pada sistem ini. Oleh karena itu ada baiknya juga ditambahkan oleh kemanan lainnya untuk *web* yang telah banyak disediakan oleh Yii, seperti enksripsi dan deksripsi *password*, *tools* pencegah SQL *Injection*, *Access Filter*,

dan lainnya. Dengan menambahkan fitur kemanan pada *web*, setidaknya semakin memperkecil kemungkinan *web* terserang isu keamanan. Sangat disarankan untuk mengkombinasikan fitur keamanan lain yang sudah tersedia pada Yii, sehingga *web* dapat bertahan dari serangan kemanan pada segi apapun.

6 Referensi

[1] Aini, Q., Graha, Y. I., & Zuliana, S. R. (2017). Penerapan Absensi QRCode Mahasiswa Bimbingan Belajar pada Website berbasis YII Framework. *SISFOTENIKA*, *7*(2), 207-218.

[2] Lenawati, M., & Winarno, W. W. (2017). Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001: 2013 Dan Cobit 5. *Speed-Sentra Penelitian Engineering dan Edukasi*, *9*(1).

[3] Darudiato, S., Sam, A., & Hadi, G. P. (2006). Analisis dan Perancangan Basis Data Eksplorasi Berbasis Objek Studi Kasus Kondur Petroleum SA. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*.

[4] Zakir, A. (2017). IMPLEMENTASI TEKNOLOGI FRAMEWORK YII PADA APLIKASI BERBASIS WEB. *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, *2*(1), 45-48.

[5] Yoke Dwi Martianda Setiaji. Analisa Sistem Pengecekan Mahasiswa Layak KKP. Retrieved from http://widuri.raharja.info/index.php/KP1412482888. (Diakses pada tanggal 23 Februari 2018)

[6] RRahardja, Untung, Hidayati dan Ardyanti, Reny. (2010). Keamanan Batasan Data Menggunakan Metode Write Validation Dalam Distribute Database System. CCIT Journal, 2(1), 12-42.

[7] Rose, M. M., & Ziad, I. (2014). DESAIN DAN IMPLEMENTASI SISTEM KEAMANAN WEB PADA WEBSITE JURNAL TELISKA POLITEKNIK NEGERI SRIWIJAYA. *TELISKA*, *15*(3).

[8] Sodikin, 2011, Perancangan Sistem Penggajian Dengan Hak Akses Karyawan Berbasis Web, *Skripsi*, Program Studi Teknik Informatika, UIN Syarif Hidayatullah, Jakarta.

[9] Jannah, E. N., Masrur, M.,& Asiyah, S. (2015). Penerapan Framework Yii dalam Pembangunan Sistem Informasi Asrama Santri Pondok Pesantren sebagai Media Pencarian Asrama Berbasis Web. *Journal of Information Systems Engineering and Business Intelligence*, *1*(2), 49-58.

[10] Pasaribu, J. S. (2017). PENERAPAN FRAMEWORK YII PADA PEMBANGUNAN SISTEM PPDB SMP BPPI BALEENDAH KABUPATEN BANDUNG. *Jurnal Ilmiah Teknologi Informasi Terapan*, *3*(2).

[11] Rahardja, U., Yusup, M., & Aini, Q. (2014). Aplikasi Campus Learning System iOU (integrated Online Ujian) Dalam Mendukung Kegiatan

iLearning Education (iDu) Pada Perguruan Tinggi. *CCIT Journal*, *7*(3), 368-383.

[12] Barka, E., Mathew, S. S., & Atif, Y. (2015, May). Securing the web of things with role-based access control. In *International Conference on Codes, Cryptology, and Information Security* (pp. 14-26). Springer, Cham.

[13] Rajpoot, Q. M., Jensen, C. D., & Krishnan, R. (2015, July). Integrating attributes into role-based access control. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 242-249). Springer, Cham.

[14] Liu, J. K., Au, M. H., Huang, X., Lu, R., & Li, J. (2016). Fine-grained two-factor access control for web-based cloud computing services. *IEEE Transactions on Information Forensics and Security*, *11*(3), 484-497.

[15] Rahardja, U., Tiara, K., & Wijaya, R. I. T. (2014). Penerapan Rinfo Sebagai Media Pendukung Untuk Proses Pembelajaran Pada Perguruan Tinggi Raharja. *Jurnal CCIT*, *8*(1).

[16] Untung, R., Suryo, G., & Valent, S. (1978). Access Restriction Sebagai Bentuk Pengamanan Dengan Metode IP Token. *CCIT Journal ISSN*, *8282*.

[17] Gunadhi, E., & Aranuri, H. (2015). PENGAMANAN BASIS DATA PENGELOLAAN HAK AKSES DENGAN METODE ROLE-BASED ACCESS CONTROL. *Jurnal Algoritma*, *12*(1).

[18] Aryani, Diah, Aini, Qurotul dan Novelia, Tasya, 2017, Perancangan PEN+ Menggunakan Metode Yii Framework Pada Perguruan Tinggi Raharja, SENSI Journal No.1, Vol.3, 48-63.

[19] Pertiwi, D. H. (2011). Desain dan Implementasi Sistem Informasi Perpustakaan Berbasis WEB dengan MVC (Model View Controler). *Jurnal Teknologi Informatika (TEKNOMATIKA)*, *1*.

[20] Sukerti, N. K., & Pratami, N. W. C. A. (2016). Rancang Bangun Ujian Online Di SMP Negeri 2 Nusa Penida. *Data Manajemen dan Teknologi Informasi*, *17*(4), 1-6.

[21] Ardiansyah, S. S., Raharjo, S., & Triyono, J. (2017). ANALISIS KEAMANAN SERANGAN SQL INJECTION BERDASARKAN METODE KONEKSI DATABASE. *Jurnal Script*, *4*(1).