DESAIN DAN IMPLEMENTASI SISTEM KEAMANAN WEB PADA WEBSITE JURNAL TELISKA POLITEKNIK NEGERI SRIWIJAYA

Martinus Mujur Rose[1]
Ibnu Ziad[2]

Staf Pengajar Jurusan Teknik Elektro Politeknik Negeri Sriwijaya
Jl. Srijaya Negara Bukit Besar Palembang-30139
E-mail: mujurrose@yahoo.com
E-mail: ibnu_ziad@polsri.ac.id

ABSTRAK

Perancangan sistem keamanan web dalam tulisan ini bertujuan melengkapi Website Jurnal Teliska Politeknik Negeri Sriwijaya dengan suatu sistem keamanan yang akan membatasi hak akses terhadap *full-tex-paper* pada Jurnal tersebut. Pokok permasalahan dibatasi pada keamanan web sisi aplikasi yang meliputi bagaimana desain sistem keamanan yang diterapkan, bagaimana pengaturan hak akses terhadap setiap *fulltex-paper*, bagaimana menjamin agar ketika seorang user diberi password untuk mengakses sebuah *full-tex-paper*, password tersebut tidak dapat digunakan untuk mengakses *full-tex-paper* lainnya, serta seberapa handal sistem keamanan yang dibangun. Metode pembahasan yang digunakan adalah studi ilteratur dan observasi langsung dengan mendesain, mengimplementasikan sebuah sistem keamanan serta mengamati kehandalan sistem keamanan yang diterapkan pada jurnal online. Hasil desain keamanan setelah diuji coba menunjukkan bahwa sistemnya bekerja dengan baik, yang dapat diuji langsung pada laman http://jurnal_teliska.polsri.ac.id, sedangkan hasil uji kehandalan masih berlangsung terus, dimana sampai dengan tulisan ini dibuat tingkat kehandalannya masih 100% aman. Dengan demikian untuk sementara dapat disimpulkan bahwa hasil rancangan sistem keamanan pada website Jurnal Teliska Politeknik Negeri Sriwijaya yang telah diterapkan memberikan jaminan keamanan terhadap *full-tex-paper* para penulis dari kemungkinan pengunduhan yang tidak berizin.

Kata Kunci: keamanan web, kode-masuk, jurnal online, teks-lengkap.

ABSTRACT

Designing a web security system in this paper aims to complete the website of Journal Teliska Politeknik Negeri Sriwijaya with a security system that would restrict the right of access to a full-tex-paper on the Journal. The main problem is limited to the security of the web application which includes about how to design a security system that would be implemented, how to set permissions to each full-tex-paper, how to ensure that when a password given to a user to access a full-tex-paper, it can not be used to access the other full-tex-paper, and how to test and determind the reliability of the security system. The method used are ilteratur study and direct observation by designing and implementing a security system, and then observe the reliability of security systems implemented in the online journal. The results of the testing security design showed that the system worked well, which can be tested directly on the page http://jurnal_teliska.polsri.ac.id, while the results of reliability test of the security is still going on, which up to this writing, it showed 100 % reliability level safe. Thus, it can be concluded (for a while) that the results of security system design on the website of Jurnal Teliska Politeknik Negeri Sriwijaya have been sufficient to guarantee the security of anyone's full-tex-paper from the possibility of unlicensed downloading.

Keywords: web *security, password, online jurnal, full-text-paper.*

1. PENDAHULUAN

1.1 Latar Belakang

Jaminan keamanan hasil karya seseorang dari berbagai kemungkinan tindak plagiasi atau penggunaan tanpa seizin pemiliknya perlu dijaga dan memerlukan perhatian. Idealnya, sebuah hasil karya berupa tulisan orisinil dari seorang penulis tidak boleh disebarluaskan sebelum penulis yang bersangkutan dinyatakan secara sah sebagai penulis karya tersebut. Salah satu penyataan secara sah seorang penulis sebagai pemilik dari sebuah tulisan orisinil adalah dengan diterbitkannya pada suatu jurnal minimal jurnal lokal yang diakui. Perlu dipastikan bahwa yang

pertama kali mempublikasikan tulisan orisinil seseorang dalam suatu jurnal adalah benar pemiliknya, sehingga ketika di kemudian hari ada seseorang yang menulis ulang dan mempublikasikannya, maka akan ketahuan siapa pemilik asli dan siapa yang melakukan plagiasi. Ketika jurnal sudah diterbitkan maka itu menjadi bukti fisik yang sah akan kepemilikan seseorang terhadap suatu tulisan. Namun tidak semua penulis atau pemilik jurnal (pimpinan redaksi jurnal) mau mempublikasikan online secara gratis keseluruhan teks tulisan (full-text-paper). Mungkin saja ada tulisan yang seluruh teksnya (*full-text*) boleh di-*share* online secara gratis, dan mungkin juga ada yang hanya abstraknya. Kemungkinan lainnya adalah butuh selang waktu tertentu setelah diterbitkan baru kemudian *full-text* tulisan tersebut boleh di-*share* online secara gratis. Untuk mengakomodasi semua kemungkinan ini maka penulis menerapkan sebuah sistem keamanan pada sebuah jurnal online yaitu dengan judul Desain dan Implementasi Sistem Keamanan Web pada Website Jurnal Teliska Politeknik Negeri Sriwijaya.

1.2 Tujuan dan Manfaat

Tujuan dari penelitian ini adalah melengkapi Sistem Online Jurnal Teliska Politeknik Negeri Sriwijaya dengan suatu sistem keamanan yang akan membatasi boleh-tidaknya seorang user mengakses secara online *full-text paper* pada Jurnal ini, serta untuk mengetahui sejauh mana tingkat kehandalan sebuah sistem keamanan web yang digunakan. Sedangkan manfaat yang diharapkan adalah menjaga hak para penulis yang tidak ingin *full-text paper*-nya dishare gratis secara online, dan memberikan peluang bagi user yang ingin mengakses secara online *full-text paper* Jurnal Teliska dengan terlebih dahulu melakukan request dan atas persetujuan pemegang hak (penulis dan/ atau pimpinan redaksi jurnal).

1.3 Permasalahan

Pokok permasalahan dalam penelitian ini dibatasi pada keamanan web sisi aplikasi yang meliputi bagaimana desain sistem keamanan yang diterapkan, bagaimana pengaturan hak akses terhadap setiap *full-text paper*, bagaimana menjamin agar ketika seorang user diberi password untuk mengakses sebuah *full-text paper*, password tersebut tidak dapat digunakan untuk mengakses *full-text paper* lainnya, serta seberapa handal sistem keamanan yang dibangun.

1.4 Metode Pembahasan

Metode pembahasan dalam penelitian ini adalah sebagai berikut:

- Studi literatur tentang sistem keamanan jaringan dan keamanan halaman website.
- Observasi yang dilakukan dengan mendesain, mengimplementasikan sebuah sistem keamanan serta mengamati kehandalan sistem keamanan yang diterapkan pada jurnal online.

2. TINJAUAN PUSTAKA

2.1 Jenis-jenis security pada web

Keamanan pada web dapat dibedakan atas keamanan dari sisi aplikasi, keamanan dari sisi server, dan keamanan dari sisi infrastruktur [2]. Keamanan dari sisi aplikasi dapat berupa Enkripsi Password. Ada beberapa jenis enkripsi yang bisa di pakai yaitu MD2, MD4, MD5, SHA, RC4, Base64. Segi keamanan dari sisi aplikasi adalah seorang user tidak dapat mengakses suatu laman atau mendownload suatu file jika tidak mengetahui password yang terpasang.

2.2 Keamanan dari sisi Server (Server www)

Menurut sumber [4]: http://br.paume.itb.ac.id/courses/ec5010/06-www-security.pdf. *Keamanan Sistem www.* diakses tanggal 8 Februari 2014) dan [5]: http://ahazka.files.wordpress.com/2012/01/www1.ppt. *Computer Security*. diakses tanggal 8 Februari 2014), Keamanan server WWW merupakan tanggung jawab administrator jaringan. Dengan dijadikannya server WWW, maka ada akses yang dibuka untuk orang luar. Server WWW menyediakan fasilitas agar client dapat mengambil informasi. Informasi yang diambil dalam bentuk file. Menggunakan perintah GET. Informasi yang diambil dieksekusi di server (PHP, ASP, CGI, dll). Kedua servis di atas (mengambil dan mengeksekusi file) memiliki potensi lubang keamanan. Lubang keamanan sistem WWW dapat menghasilkan serangan berupa: Informasi yang ditampilkan diubah (deface); Informasi yang seharusnya untuk kalangan terbatas ternyata berhasil ditampilkan oleh orang yang tidak berhak; Informasi dapat disadap (seperti Pengiriman nomer CC dan monitoring kemana saja seseorang melakukan surfing); DoS Attack; Server WWW yang terletak dibelakang firewall, lubang keamanan server WWW dapat melemahkan dan bahkan menghilangkan fungsi firewall. Upaya mengamankan server www antara lain adalah membatasi akses melalui Kontrol Akses yang dapat dilakukan dengan membatasi domain atau Nomor IP yang dapat mengakses, menggunakan user dan password, serta mengenkripsi data

sehingga hanya dapat dibuka oleh orang yang memiliki kunci.

2.3 Pembuatan password yang aman (*strong password*).

Menurut sumber [3]: (http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password, diakses tanggal 20 Januari 2014), sebuah *strong password* memiliki kriteria antara lain adalah minimal 8 karakter, tidak mengandung nama user, nama diri (*real name*) atau nama perusahaan, tidak mengandung kata utuh (*complete word*), berbeda signifikan dengan password sebelumnya, merupakan kombinasi dari 4 kelompok karakter. Adapun keempat kelompok karakter yang dimaksud adalah *Uppercase letters* (A, B, C, ...), *Lowercase letters* (a, b, c, ...) *Numbers* (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), serta Symbols (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /).

2.4 User name dan Password untuk Web Security

Menurut sumber [1], Ketika hendak menggunakan autentikasi user maka perlu dibuat *password file* (file kata kunci). Hal ini dapat dilakukan dengan program *htpasswd*, menggunakan option "-c" untuk membuat filenya. Contohnya seperti berikut:

```
# ./htpasswd -c /usr/local/etc/httpd/pw/auth sascha
Adding password for sascha.
New password:deus333
Re-type new password:deus333
#
```

User lainnya beserta passwordnya dapat ditambahkan dengan program *htpasswd*. Untuk menambahkannya tidak boleh menggunakan option "-c" kecuali kalau mau menghapus semua user yang sudah ada di dalam file.

```
# ./htpasswd /usr/local/etc/httpd/pw/auth wendy
Adding password for wendy.
New password:excom22
Re-type new password:excom22
#
```

File kata kunci ini serupa tapi tidak identik dengan file standard */etc/passwd*:

```
# cat /usr/local/etc/httpd/pw/auth
sascha:ZdZ2f8MOeVcNY
wendy:ukJTIFYWHKwtA
#
```

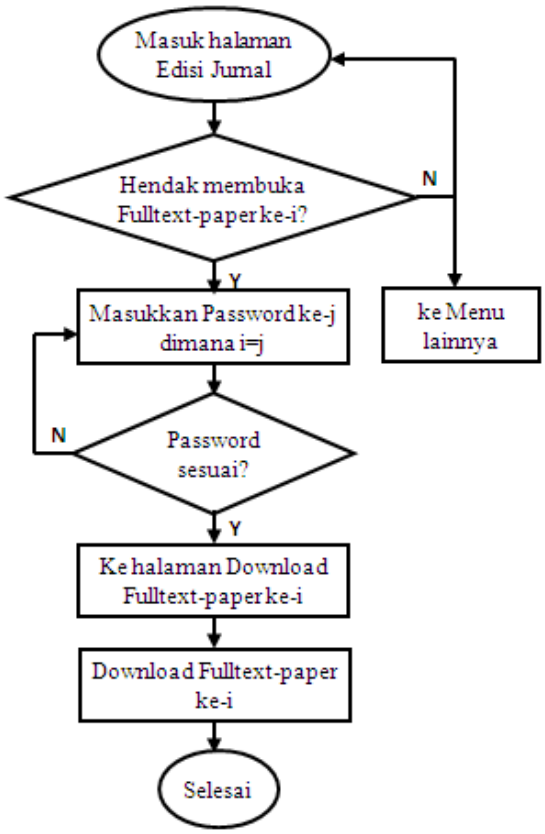
Oleh karena web server menggunakan password-password *crypt*-style, maka semestinya file password tersebut tidak dapat diakses oleh user biasa di server (dan user-user di web) untuk mencegah suatu serangan yang ambisius igin menebak password menggunakan suatu program seperti *Crack*.

3. METODOLOGI

Pokok pembahasan dalam tulisan ini adalah dibatasi pada (keamanan aplikasi yaitu) bagaimana mengamankan atau melindungi file-file tertentu yaitu *full-text paper* dari setiap tulisan pada Jurnal. Dalam kenyataanya bisa terjadi bahwa beberapa tulisan diperbolehkan untuk dishare gratis secara online *full-text-paper*-nya, dan beberapa tulisan tidak diperbolehkan oleh yang berhak yaitu penulisnya atau pimpinan redaksi jurnalnya. Dalam sistem keamanan web ini, setting awalnya adalah semua *full-text-paper* dari semua tulisan dilindungi namun tetap tersedia online, dan diperlukan suatu gerbang keamanan untuk mengaksesnya.

3.1 Flow Chart proses pada sisi User

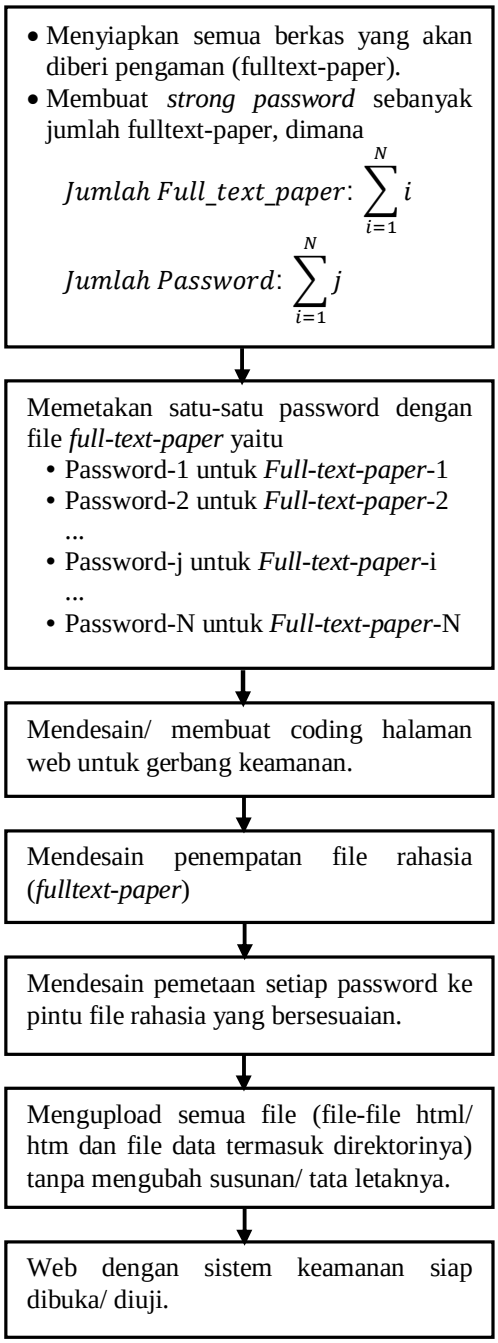
Sebelum masuk ke tahap merancang sistem keamanan, perlu dirumuskan gambaran tentang proses yang akan dialami oleh user ketika hendak mengakses laman web yang akan diberi pengaman. Gambaran tersebut dituangkan dalam flow chart seperti pada Gambar 1.



Gambar 1. Flow Chart proses pada sisi user

3.2 Langkah-langkah Desain

Berdasarkan perkiraan proses yang akan dirancang untuk dilalui user, maka dalam merancang sistem keamanan, penulis melakukan langkah-langkah desain seperti diagram blok pada Gambar 2.



Gambar 2. Diagram Langkah-langkah Desain.

3.3 Penyiapan dan Penataan Directory File

Penyiapan dan penataan seluruh berkas baik berkas yang tidak ber-*password* maupun yang akan dilindungi dengan password ditempatkan sedemikian rupa dalam serangkaian direktori dimana susunan direktori ini biasanya sesuai dengan *style* pengarsipan masing-masing orang. Pada desain ini, dengan mengacu ke sumber [7], penataan halaman web untuk gerbang keamanan dan halaman-halaman lainnya yang akan dilindungi diatur sedemikian rupa dengan membuat Target url-nya berada pada frame yang tersembunyi sehingga detail urlnya tidak tampak. Adapun penataan berkas dan direktori pada Jurnal Teliska Politeknik Negeri Sriwijaya ini telah dilakukan sejak pertama kali penulis mendesain dan meng-*online*-kan website Jurnal ini, dan ditambahkan setiap kali ada terbitan baru, serta sewaktu-waktu penataan tersebut dapat diubah.

3.4 Pemberian password

Pada sistem keamanan web ini, setting password selain memperhatikan rekomendasi tips untuk *strong password* seperti pada tinjauan pustaka [3], penulis juga mempertimbangkan faktor kemudahan administrator dalam pengelolaannya. Oleh karena itu dapat diatur bahwa beberapa bagian dari password dibuat dengan sebuah pola tertentu tetapi sulit ditebak oleh user. Sebagai contoh, karakter pertama password adalah nomor urut edisi ditambah 3, misalnya untuk edisi pertama diawali dengan angka 1+3=4, untuk edisi kedua diawali dengan 5, dan seterusnya. Begitu pun dengan karakter berikutnya, ada pola tertentu yang tentu saja tidak akan dibocorkan dalam tulisan ini. Selain itu akan dilakukan update atau perubahan password dalam jangka waktu tertentu secara berkala atau pun secara insidentil.

3.5 Desain Gerbang Keamanan

Gerbang keamanan yang dirancang di sini tidak hanya satu pintu untuk semua *full-text-paper* setiap terbitan, melainkan satu pintu keamanan untuk satu *full-text-paper* tulisan. Hal ini dimaksudkan untuk menjaga fleksibilitas hak akses terhadap setiap judul tulisan. Dengan demikian, jika ada satu judul yang *full-text paper*-nya diperbolehkan oleh pemegang hak (penulis dan/ atau pimpinan redaksi) untuk diakses oleh seorang user yang meminta, maka keamanan *full-text-paper* untuk tulisan-tulisan lainnya tetap terjaga. Untuk menjamin keamanan tiap tulisan (tiap judul) maka dibuat sebuah halaman terlindungi bagi setiap tulisan (judul) yang diberi passwod masing-masing.

Adapun desain file html yang dibuat untuk gerbang keamanan yang akan berfungsi sebagai halaman Login diperlihatkan pada Gambar 3 berikut ini.

```
<HTML><HEAD>
<TITLE> Priv Doc</TITLE>
<SCRIPT language="JavaScript">
<!-- hanya untuk Browser versi 3.0 ke
atas
 function passwd()
 {
 form = document.Password.form.value;
 form = form+".htm";
 location.href=form;
 }
 // -->
</SCRIPT>
</HEAD>

<BODY>
```

```
<BR><FONT size="14">Dokumen ini pakai
password</FONT>
<BR><B>(Masukkan password lalu klik
tombol login, bukan enter)</B><BR>

<FORM name="Password">
 Password:
 <INPUT type="password" name="form"
value="">
 <INPUT type="button" name="Tombol"

 value="login" onclick="passwd()">

</FORM>
</BODY>
</HTML>
```

File untuk halaman Login ini disimpan misalnya dengan nama *index.htm* dan diletakkan dalam suatu direktori bersama dengan file halaman web yang dituju setelah Login yang dalam tulisan ini disebu halaman download. Sedangkan file-file yang dituju atau yang hendak didownload dari halaman download dapat disimpan lebih tersembunyi lagi dalam direktori tertentu [7].

3.6 Pengujian

Uji coba hasil desain keamanan web ini dilakukan untuk mengetahui apakah sistemnya bekerja dengan baik atau tidak. Misalnya apakah tampilannya sesuai dengan yang diinginkan dalam perancangan, apakah dengan memasukkan password yang benar memang kita dapat mendownload file yang bersesuaian dengan password tersebut, apakah dengan memasukkan password yang salah memang kita tidak dapat mengakses file yang dituju, dan sebagainya. Uji coba hasil desain ini telah dilakukan oleh penulis sendiri, bahkan dalam tahap pembuatannya penulis sambil menguji sistem dalam tahap-tahap tertentu sebelum melanjutkan ke tahap berikutnya.

Selain uji coba tentang apakah sistem bekerja dengan baik atau tidak, pengujian lain yang dilakukan adalah apakah sistem keamanan yang dirancang ini cukup handal atau tidak. Salah satu caranya adalah dengan memasang counter pada halaman web terlindungi (untuk mengetahui ada tidaknya serta jumlah user yang berhasil membobol sistem keamanan web ini). Pengujian ini akan berlangsung terus-menerus, sehingga tingkat kehandalannya bernilai relatif. Artinya sekarang bisa dikatakan sangat handal tetapi mungkin 3 tahun kemudian sistem keamanan ini sudah tidak handal lagi.

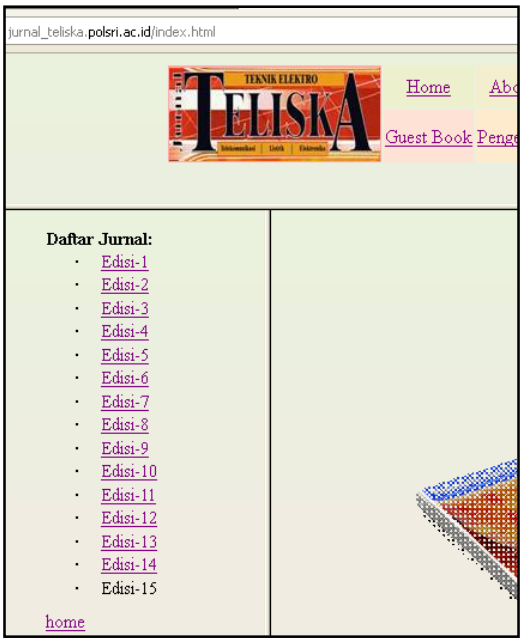
4. HASIL DAN PEMBAHASAN

4.1 Hasil Desain Sistem Keamanan

Berikut ini diperlihatkan tampilan hasil desain yang meliputi: Tampilan halaman depan, halaman Edisi Jurnal, halaman mengakses Abstrak dan Full-text jurnal, halaman Login, halaman sesudah Login berhasil (halaman mendownload *Full-text-paper*), Tampilan counter, dan halaman setelah full-text-paper berhasil diakses.

Gambar 3. Halaman depan website Jurnal Teliska Politeknik Negeri Sriwijaya dengan alamat http://jurnal_teliska.polsri.ac.id

File-file yang diamankan ada pada menu **Edisi Jurnal**, yang ketika diklik akan menampilkan halaman seperti pada Gambar 4.



Gambar 4. Tampilan halaman Edisi Jurnal

Misalkan user hendak mengakses jurnal Edisi 12, maka setelah meng-klik menu **Edisi-12**, jurnal tersebut tampil seperti pada Gambar 5.

Gambar 5. Halaman mengakses abstrak dan full-text jurnal

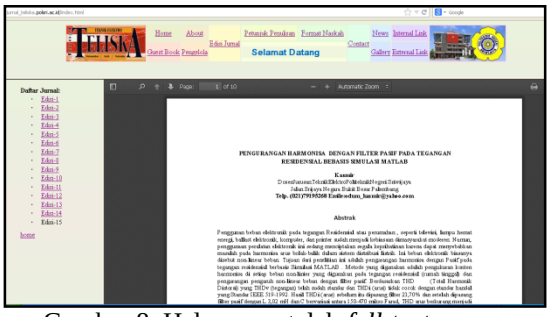
Untuk mengakses abstrak langsung tanpa password, sedangkan untuk mengakses *full-text-paper*, user akan digiring ke halaman Login seperti pada Gambar 6.

Gambar 6. Tampilan halaman Login

Jika user memiliki hak akses maka setelah memasukkan password, akan tampil halaman Download Full-Text seperti pada Gambar 7.

Gambar 7. Halaman Download Full-text-paper

Dari halaman Download Full-Text, maka full-text-paper dari sebuah tulisan jurnal dapat didownload dan ditampilkan seperti pada Gambar 8.



Gambar 8. Halaman setelah *full-text-paper* berhasil diakses

Dari halaman web seperti pada Gambar 8, file PDF full-text-paper tersebut dapat disimpan/ didownload sebagai file PDF.

4.2 Hasil Pengujian Kehandalan Keamanan

Hasil monitoring pengakses berupa counter yang dipasang pada laman terlindungi sejak sistem keamanan ini diterapkan sampai pada saat tulisan ini dibuat, menunjukkan bahwa belum ada satu pun user lain selain penulis sendiri yang memasuki laman terlindungi tersebut.

4.3 Pembahasan

Desain file untuk halaman web gerbang keamanan di sini dilakukan secara manual, tanpa menginstall suatu software seperti Apache dan sebagainya. File gerbang keamanan ini dibuat dengan menyisipkan suatu *JavaScript* ke dalam file html.

Pada desain ini, penataan halaman web untuk gerbang keamanan dan halaman-halaman lainnya yang akan dilindungi diatur sedemikian rupa dengan membuat Target url-nya berada pada frame yang tersembunyi sehingga detail urlnya tidak tampak.

Pada Desain ini, untuk mengakses suatu file terlindungi cukup dengan memasukkan password tanpa harus memasukkan user name. Alasan penulis hanya menyeting password tanpa user name adalah semata-mata untuk kesederhanaan dan agar sistem tidak terlalu dibebani dengan database, sedangkan yang lebih diutamakan adalah tingkat kehandalan dari sistem kemanan ini yaitu bahwa passwordnya sulit untuk dimasuki.

Pada Desain ini penempatan file-file terlindungi tidak dikumpulkan dalam satu direktori terlindungi saja melainkan dipisah-pisah ke direktori terlindungi lainnya. Hal ini dimaksudkan agar ketika misalkan satu direktori berhasil dijebol oleh seorang user, file lain pada direktori lain masih aman.

Hasil pegujian yang dilakukan terhadap sistem keamanan web ini dibedakan atas 2 macam, yaitu yang pertama adalah Uji coba hasil desain keamanan web apakah sistemnya bekerja dengan baik atau tidak, dan yang kedua adalah

apakah sistem keamanan yang dirancang cukup handal atau tidak. Pengujian jenis pertama telah menunjukkan hasil yang bagus, artinya sistem yang didesain dapat bekerja sebagaimana mestinya. Pengujian jenis kedua sampai saat tulisan ini dibuat menunjukkan bahwa sistem keamanan yang dirancang handal 100%, namun pengujian ini akan berlangsung terus-menerus, sehingga tingkat kehandalan dari sistem keamanan ini bernilai reltif seiring dengan waktu. Sekarang dapat dikatakan handal 100% tetapi mungkin saja beberapa tahun kemudian sudah tidak handal lagi.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Sistem keamanan pada website Jurnal Teliska Politeknik Negeri Sriwijaya yang telah diterapkan memberikan jaminan keamanan terhadap *full-text paper* para penulis dari kemungkinan pengunduhan yang tidak berizin.
2. Hasil pengujian kehandalan sistem keamanan ini sampai saat tulisan ini ditulis, masih menunjukkan bahwa belum ada satu pun user yang membobol sistem keamanan ini.

5.2 Saran

1. Sistem keamanan website yang telah diterapkan pada website Jurnal Teliska Politeknik Negeri Sriwijaya masih perlu pengembangan/ penyempurnaan misalnya tentang cara lain menyembunyikan detail url dari setiap isi web yang diakses, seperti halnya pada website forlap.dikti.go.id.
2. Secara khusus jika ada user yang berhasil menjebol sistem keamanan ini maka saran perbaikannya sangat diharapkan untuk meningkatkan keamanan website jurnal ini demi menjaga hak-hak penulis.

DAFTAR PUSTAKA

[1] Garfinkel, S. Gene Spafford. 2002. *Web Security, Privacy and Commerce.* 2nd Edition. O'Reilly Media, Inc. Sebastopol - California - USA.

[2] http://03fas.wordpress.com/2013/08/25/jenis-jenis-security-web/, diakses tanggal 21 Januari 2014.

[3] http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password, diakses tanggal 20 Januari 2014.

[4] http://br.paume.itb.ac.id/courses/ec5010/06-www-security.pdf. *Keamanan Sistem www.* diakses tanggal 8 Februari 2014.

[5] http://ahazka.files.wordpress.com/2012/01/www1.ppt. *Computer Security.* diakses tanggal 8 Februari 2014.

[6] http://www.totallyfreecounter.com/?gclid=CPnl_73lxLwCFYYipQod9UoAPw, diakses tanggal 3 Februari 2014.

[7] Rose, M. M. *Desain Web dan Uji Coba Transfer File dari FTP Client ke FTP Server dengan Memanfaatkan Free Hosting.* Teknika-Polsri. 2010. Vol.XXIX No.1 Hal 45-53.