PERANCANGAN KEAMANAN ELECTRONIC FLIGHT BAG BERBASIS WEB TERHADAP SERANGAN XSS DENGAN METODE WHITE-BOX TESTING

SECURITY DESIGN ELECTRONIC FLIGHT BAG BASED WEB TO XSS ATTACK USING WHITE-BOX TESTING METHOD

Rizka Ramadhayanti
Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom
rizkaramadhayantiii@gmail.com

Abstrak

Pesawat terbang merupakan alat transportasi udara yang mampu membawa penumpang baik jarak dekat maupun jarak jauh. *Less papper cockpit* digunakan untuk memudahkan dan meringankan pekerjaan pilot. Teknologi terbaru dari *less papper cockpit* yaitu EFB (*Electronic Flight Bag*). EFB(*Electronic Flight Web*) merupakan tablet PC yang dikhususkan untuk para pilot agar dapat mempermudah komunikasi antara pihak udara (*airborne flight*) dengan darat (*ground*), juga sebagai alat bantu dalam hal pemetaan landasan yang tersedia pada tiap-tiap bandara dan data-data lainnya terkait operasional penerbangan berbasis web.Banyak serangan yang terjadi pada web, salah satunya adalah serangan XSS. XSS (*Cross Site Script*) adalah jenis serangan injeksi code (*Code Injection Attack*) suatu jenis serangan web dimana penyerang berusaha untuk menyisipkan script yang berisikan kode terhadap suatu website untuk menjalankan suatu perintah. AntiXSS dibutuhkan untuk pengamanan pada EFB dari serangan XSS. Sebelum menggunakan AntiXSS, EFB dapat diserang dengan script XSS sebanyak 10 kali pengujian. Setelah menggunakan AntiXSS dengan 10 kali pengujian pada prototype EFB, prototype EFB telah berhasil diamankan dan tidak dapat diserang dengan XSS.

Kata Kunci: ***EFB, XSS,***

Abstract

Airplane is an air transportation which can carrying many passengers. it can flight with near location or far away. Less paper cockpit used for easier pilot work . the new techmology from less paper cockpit is EFB. EFB is a tablet pc especially for the pilot to communicate between aiebone flight and ground. beside that it use as helping tools for placing available land for landing in every airport and collect the data flight with web. Many attacks in the web, one of them is XSS. XSS (Cross Site Script) is a type of injection attack code (Code Injection Attack) is a type of web attacks where the attacker tries to insert a script that contains code to a website to execute some command. AntiXSS needed for secure the EFB from XSS attacks. Before using AntiXSS, EFB can be attacked by XSS script as much as ten times of testing. After using AntiXSS with ten times of testing the prototype EFB, EFB prototype has successfully secured and can not be attacked by XSS.Then needed security in EFB from XSS attack.

Keyword*: *EFB, XSS,

1. Pendahuluan

Latar Belakang

Seiring dengan berkembangnya arus globalisasi, yang didalamnya dituntut akan adanya pertukaran informasi yang semakin cepat. Tidak hanya kemajuan pada *smartphone* atau *gadget*, kemajuan teknologi transportasi juga ikut berkembang. Salah satunya adalah pesawat terbang. Pesawat terbang adalah alat transportasi udara yang mampu membawa penumpang baik jarak dekat maupun

antar Negara. *Less paper cockpit* digunakan untuk memudahkan dan meringankan pekerjaan pilot. Teknologi terbaru dari *less papper cockpit* yaitu EFB (*Electronic Flight Bag*). EFB adalah aplikasi berbasis web yang dikhususkan untuk para pilot agar dapat mempermudah komunikasi antara pihak udara (*airborne flight*) dengan darat (*ground*), juga sebagai alat bantu dalam hal pemetaan landasan yang tersedia pada tiap-tiap bandara dan data-data lainnya terkait operasional penerbangan.

Semakin majunya teknologi pada sistem penerbangan, tidak menutup kemungkinan adanya pihak yang tidak bertanggung jawab untuk meretas sistem yang ada pada pesawat terbang. Salah satunya yaitu serangan terhadap EFB yang menggunakan berbasis web. Contoh dari serangan web yaitu XSS. XSS atau *Cross Site Scipting* adalah salah satu jenis serangan injeksi code (*code injection attack*). XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan XSS pada EFB ini dapat menimbulkan masalah yang sangat besar, salah satunya kehilangan kordinat pada pesawat tersebut.

Berdasarkan masalah diatas maka dibutuhkan untuk pengamanan EFB pada pesawat terbang terhadap serangan XSS. AntiXSS merupakan pengamanan untuk halaman web membantu melindungi dari serangan XSS. Untuk mengetahui pengamanan pada web EFB maka dilalukan pengujian. Pengujian terhadap system ada dua salah satunya dengan metode *White-box testing*. *White-box testing* (juga dikenal dengan *clear box testing*, *glass box testing*, *transparent box testing*, dan *structural testing*). Dalam *White-box testing*, kita membuat *test cases* dengan melihat *source code* untuk mencari adanya kesalahan pada program. *White-box testing* dilakukan oleh *Software Engineer* karena membutuhkan pengetahuan tentang programming dan implementasinya. Hal-hal yang biasa diuji dalam *test cases* seperti Loops(*while or for loop*), *Decision Making* (*if statement or switch statement*) atau *data structure*. Oleh karena itu dalam proyek akhir ini akan dibuat perancangan keamanan EFB (*Electronic Fligth Bag*) berbasis web terhadap serangan XSS (*Cross Site Scripting*) dengan metode pengujian *white-box testing*.

Tujuan

Tujuan proyek akhir ini berdasarkan rumusan masalah yang ada adalah sebagai berikut :

1. Melindungi EFB dari serangan XSS dengan menggunakan AntiXSS.
2. Melakukan pengujian EFB dengan metode *white-box testing*.

Identifikasi masalah

Batasan masalah pada proyek akhir ini adalah sebagai berikut :

1. Operating sistem dengan menggunakan Ubuntu 12.04.
2. Penyerang diasumsikan berada di darat.
3. Tidak melakukan pengujian pada pesawat terbang langsung.
4. Web EFB merupakan *prototype*

Metode Penelitian

Metode yang digunakan adalah studi literature, analisis, perancangan, implementasi dan pengujian.

- Studi Literatur

  Memperpelajari hal yang berkaitan dengan proyek akhir, seperti XSS Attack, Kemanan pada web, dan AntiXSS.

- Analisis Kebutuhan Sistem

  Langkah ini diperlukan untuk mengetahui kebutuhan *hardware* dan *software* yang akan digunakan, Mempersiapkan perangkat komputer serta peralatan yang lain yang mendukung proyek akhir.

- Perancangan Model

  Setelah melakukan analisis, perancangan diperlukan untuk membuat model, seperti *design* model pengujian dengan menggunakan metode *white-box testing*.

- Implementasi

  Langkah selanjutnya adalah implementasi. Implementasi termasuk juga kegiatan instalasi dan konfigurasi semua layanan yang dibutuhkan.

- Pengujian

  Pengujian dilakukan setelah instalasi dan konfigurasi berjalan dengan baik, berupa pengujian dengan metode *white-box testing* terhadap EFB.

- Penyusunan Laporan

  Pada langkah ini semua metode yang telah dilakukan akan di buat dokumentasinya.

2. Tinjauan Pustaka

2.1 Web Server

Web Server yaitu sebuah sarana dari layanan sebuah website atau biasa disebut dengan WWW (*World Wide Web*). Sebuah web server akan menunggu permintaan dari seorang client untuk menggunakan sebuah browser, seperti browser Internet Explorer, Google chrome, Mozilla Firefox, Opera dan browser lainnya. Jika ada sebuah permintaan dari browser, maka sebuah web server akan langsung memproses sebuah permintaan tersebut dan kemudian akan memberikan hasil prosesnya yaitu berupa data yang diinginkan dan akan menampilkan pada sebuah browser.

Sehingga jika sebuah proses yang dimulai dari permintaan web client atau dari (browser), maka akan langsung diterima oleh web server, kemudian diproses, dan kemudian dikembalikan hasil prosesnya oleh web server ke web client lagi dilakukan secara transparansi. Jadi bisa dikatakan, setiap orang akan dapat dengan mudah mengetahui apa yang akan terjadi pada tiap-tiap proses. Namun secara garis besarnya yaitu sebuah web server hanya akan memproses semua masukan yang diperolehnya dari sebuah permintaan dari web clientnya. (Anonymos, 2015)

2.2 Electronic Flight Bag

EFB (*Elektronik Flight Bag*) adalah tambahan suatu alat bantu berupa penambahan seperangkat komputer untuk memudahkan dan meringankan pekerjaan rutin pilot dan tidak menggunakan kertas lagi (*less paper cockpit*). Lokasi EFB sendiri di tempatkan disamping kiri (*capt*) dan kanan (*first officer*) kedua komputer ini bekerja independent namun demikan apabila seorang *captain* ingin mengetahui atau membaca apa yang sedang dibaca *copilot* dengan cara menekan tombol transfer

Gambar 1

Fitur dari EFB bergantung pada option atau pilihan dari masing-masing airline. Biasanya airline sudah mempunyai patokan atau standar option apa saja yang di perlukan untuk penerbangannya dalam EFB yang terpasang di pesawatnya. Yang dapat ditampilkan oleh penerbang dalam sebuah EFB antara lain :

1. Airport Map : Berguna untuk raxy di airport yang besar dan complicated taxy waynya, terlebih dalam keadaan *low visibility*.
2. Performance : Membantu pilot dalam perhitungan *weight and balane* (*a/c configuration, flap setting, thruat setting*) sehingga bisa menghemat engine life/fuel consumption bahkan untuk landing apabila ada penalty sewaktu ada kerusakan seperti engine fail, hydralic problem dsb.
3. Terminal Chart : Penerbangan tidak perlu lagi membuka chart dalam bentuk kertas sehingga akan mempersingkat waktu briefing
4. Video : Untuk *security pilot* sehingga pilot akan mengetahui siapa yang akan masuk ke cockpit atau ada di depan pintu cockpit.
5.

Tabel 2-Error! No text of specified style in document.**-1 Spesifikasi EFB**

SIZE	9.6x6.3X1.1 inches
Operating sistem	Linux/Windows
Battery Life	+4hours
Interface	USB, PCMCIA, Wireless, Touchscreen, integrated GPS.

2.4 Cross Site Script(XSS)

XSS merupakan salah satu jenis serangan injeksi code (*code injection attack*). XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. Akibat serangan ini antara lain penyerang

dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya. Karena EFB merupakan aplikasi berbasis web. Maka kemungkinan EFB dapat diserang dengan XSS pada suatu inputan biasanya dihalaman login.

2.5 AntiXSS

AntiXSS membantu untuk melindungi web dari serangan XSS. AntiXSS mempunyai fungsi :

1. Peningkatan kinerja web.
2. Melindungi web dari serangan XSS yang dikodekan banyak bahasa pemograman.

2.6 White box testing

White-box testing (juga dikenal dengan *clear box testing, glass box testing, transparent box testing,* dan *structural testing*) Dalam *White-box testing*, kita membuat *test cases* dengan melihat *source code* untuk mencari adanya kesalahan pada program. *White-box testing* dilakukan oleh Software Engineer karena membutuhkan pengetahuan tentang programming dan implementasinya. Hal-hal yang biasa diuji dalam *test cases* seperti Loops (*while or for loop*), *Decision Making* (*if statement or switch statement*) atau *data structure.*

Keuntungan *White-box testing*:

1. Sebagai *Software engineer* yang memiliki akses ke source code, hal ini menjadi sangat mudah untuk melakukan skenario pengujian secara efektif.
2. Membantu *Software engineer* untuk mengoptimalkan *source code*.
3. Baris kode yang tidak efisien dapat dihilangkan agar mencegah *bugs* pada program.

Kerugian *White-box testing*:

1. Karena dibutuhkan *Software engineer* yang berpengalaman dalam *White-box testing* sehingga mengeluarkan biaya tambahan.
2. Terkadang sangat sulit melihat setiap baris kode untuk mencari *bugs* pada program yang akan diuji.

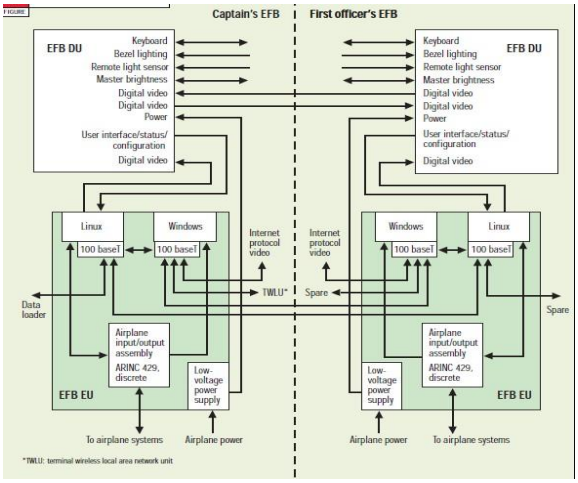
3. Ananlisis dan perancangan sistem

3.1 Gambaran Sistem Saat Ini (atau Produk)

Sistem yang digunakan pada proyek akhir ini dengan judul "Perancangan keamanan EFB berbasis web terhadap serangan XSS menggunakan metode White box Testing" adalah sistem yang dibangun untuk melindungi EFB dari serangan XSS. Sebelumnya EFB tidak menggunakan keamanan sehingga sangat mudah attacker meretas EFB tersebut.

Dengan tidak adanya keamanan pada EFB, maka disarankan untuk melakukan perlindungan pada EFB, untuk melakukan keamanan EFB dari serangan XSS menggukan AntiXSS.

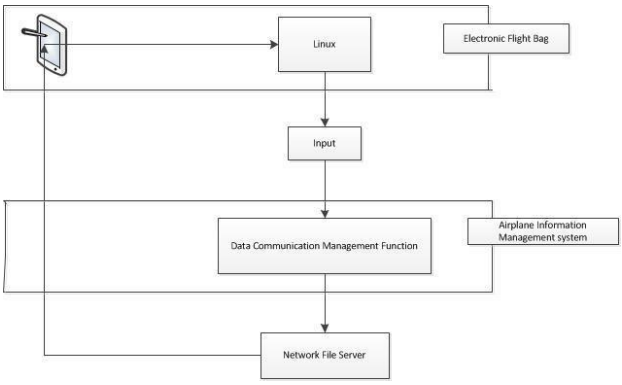
3.1.1 Sistem Electronic Flight Bag



Gambar 3-1 Sistem EFB Asli

Sistem EFB mempunyai dua Display Unit(DU) dan dua Electronic Unit(EU) yang dipasang pada peralatan utama. EU mempersiapkan tampilan untuk DU, dimana dapat menampilkan aplikasi yang dipilih untuk ditampilkan pada DU dan kontrol unit kecerahan. Saat ini EFB tidak memiliki sistem kemanan, kemungkinan resiko yang terjadi pada sistem yaitu berupa ancaman pada pengembangan sistem tersebut. kemungkinan ancaman-ancaman yang terjadi memberikan dampak yang merugikan pada sistem EFB terkait operasional penerbangan. kemungkinan-kemungkinan hal yang dapat terjadi pada sistem EFB. kerentanan pada sistem sehingga sangat mudah untuk diretas dan komunikasi EFB dapat terganggu, sehingga bisa terjadi *miss-communication* antara pihak udara dan darat. Maka langkah-langkah yang harus dilakukan yaitu melakukan identifikasi ancaman, identifikasi kerentanan, dan mengamankan sistem EFB agar tidak terjadi hal-hal yang tidak diinginkan.

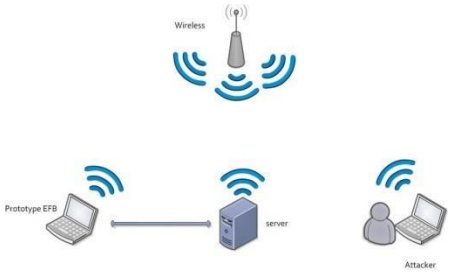
3.1.1.1 Cara kerja EFB



Gambar 3-2 Cara Kerja EFB

Cara kerja EFB pada pesawat, EFB menggunakan OS Linux pada pesawat. masukan/inputan akan dikelola oleh Aiplane Management Function System pada data communication Management function yang berfungsi untuk menghubungkan Network File server dan EFB. Network file server menyediakan data-data terkait operasional penerbangan. kemudian data yang pinta akan ditampilkan pada EFB.

3.1.2 Perancangan sistem sebelum menggunakan keamanan pada sistem pada prototype EFB

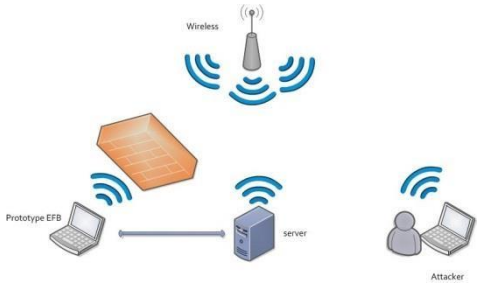


Gambar 3-3 Sistem sebelum menggunakan keamanan.

Berdasarkan *Gambar 3-1 Gambaran sistem sebelum menggunakan keamanan* menjelaskan sistem sebelum menggunakan keamanan pada prototype EFB. Berikut adalah cara penyerangan melakukan penyerangan terhadap prototype EFB.

1. Attacker masuk kedalam jaringan wireless yang sama dengan prototype EFB.
2. Kemudian Attacker melakukan sniffing untuk mendapatkan IP dari prototype EFB.
3. Setelah mendapatkan IP dari prototype EFB attacker dapat melakukan penyerangan untuk mencuri cookie dari prototype EFB .

3.1.3 Gambaran sistem sesudah menggunakan keamanan pada sistem



Gambar 3-4 Sistem sudah menggunakan keamanan

Berdasarkan *Gambar 3-2 Gambaran sistem setelah menggunakan keamanan* menjelaskan sistem setelah menggunakan keamanan pada prototype EFB, Sehingga Attacker tidak dapat melakukan penyerangan terhadap prototype EFB. Prototype EFB diamankan dengan cara menyelipkan script AntiXSS keamanan pada prototype EFB

3.1.4 Script antiXSS

Berikut script AntiXSS yang digunakan untuk melindungi prototype EFB, seperti gambar dibawah ini :

```php
<?php
        function antixss($data){
                $xss= htmlspecialchars(trim($data));
                return $xss;
        }
        $username= antixss($_POST['username']);
        if($username){ ?>
        <p style="display: none;"><?php echo $username;?> </p>
<?php   }
?>
```

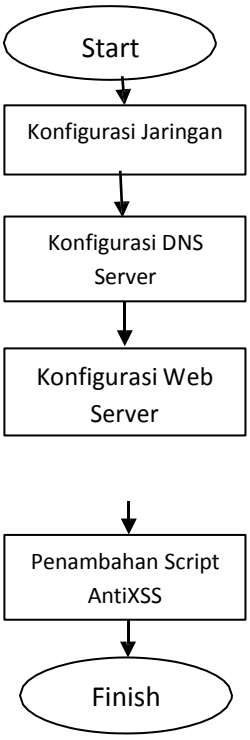
Gambar 3-5 Script AntiXss

Penjelasan tentang script diatas yaitu :

Htmlspecialchars : berfungsi untuk mengabaikan tag html, misal spasi dirubah menjadi %20, sehingga ketika ada attacker menyisipkan kode html, maka tidak akan terbaca sebagai Tag HTML, tetapi teks biasa.

Trim : trim disini berfungsi untuk menghapus karakter spasi di depan teks.

3.2 Tahapan pembangunan sistem



3.3 Scenario Pengujian

Berikut scenario pengujian pada proyek akhir ini :

1. Akan dilakukan pengujian serangan XSS sebanyak 10 kali pada prototype EFB.
2. Akan dilakukan pencurian cookies pada EFB.
3. Akan dicek kemampuan keamanan EFB dengan serangan XSS dengan menggunakan Script AntiXSS.

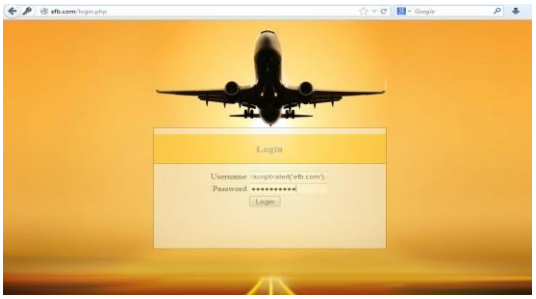
4.1 Pengujian

Pengujian pada keamanan EFB ada 2 pengujian , sebelum menggunakan keamanan dan sesudah menggunakan sistem keamanan pada EFB.

4.1.1 Pengujian sebelum menggunakan kemanan

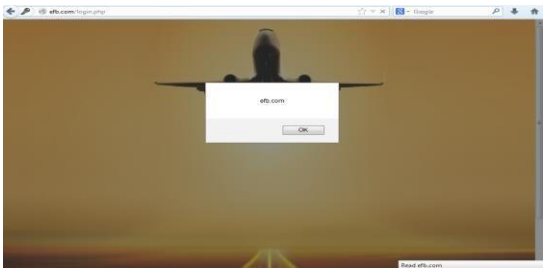
1. Sebelum menggunakan keamanan pada EFB akan execute script yang di inputkan , berikut script-script yang diinputkan untuk pengujian sebelum menggunkan keamanan pada sistem. Pengujian dilakukan sebanyak 10 kali.

   a. Input script pada halaman login pada kolom username , masukan password secara asal. Isi script dengan : ***#<script>alert('efb.com');</script>***



Gambar 4-6 pengujian 1

Maka akan muncul gambar seperti dibawah ini :



Gambar 4-7 hasil pengujian 1

b. Pengujian dengan script yang lain , masukan script dikolom username dan isi password dengan asal. Masukan script : ***<script type="text/javascript">window.location='http://google.com/';</script>.*** maka output yang keluar yaitu halaman awal Google.com

Gambar 4-8 hasil pengujian 2

c. Pengujian yang ketiga dengan memasukan script lain, seperti pengujian yang lainnya masukan script pada kolom username dan isi password dengan asal. Masukan script : ***<h1>Hello I'm Attacker</h1>.*** Maka output yang keluar seperti gambar dibawah ini :

Gambar 4-9 hasil pengujian 3

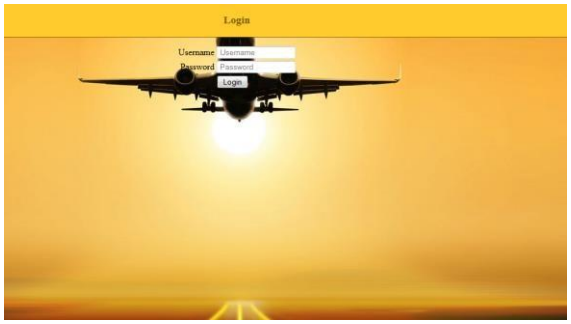
d. Pengujian selanjutnnya dengan memasukan script lain dengan memasukan script pada kolom username. Masukan script : ***<marquee>hacked by security</marquee>.*** Maka output yang keluar berupa huruf yang berjalan.

Gambar 4-10 hasil pengujian 4

e. Pengujian kelima dengan menggunakan script lainnya, masukan script ***<table background="javascript:alert(([code])"></table>*** pada kolom username dan isi password secara asal seperti gambar dibawah ini:

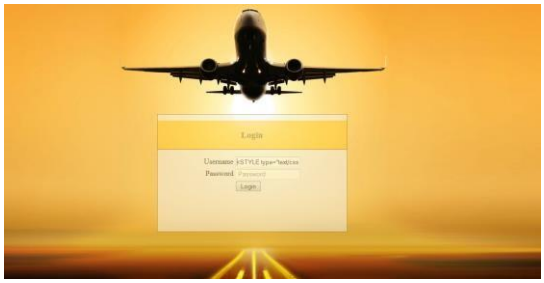
Gambar 4-11 Gambar pengujian 5

Kemudian klik login , maka hasil dari script tersebut seperti dibawah ini:



Gambar 4-12 Gambar hasil pengujian 5

f. Pengujian ke-enam dengan menggunakan script ***<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>*** yang dimasukan pada kolom username dan password diisi secara asal. Seperti gambar dibawah ini:

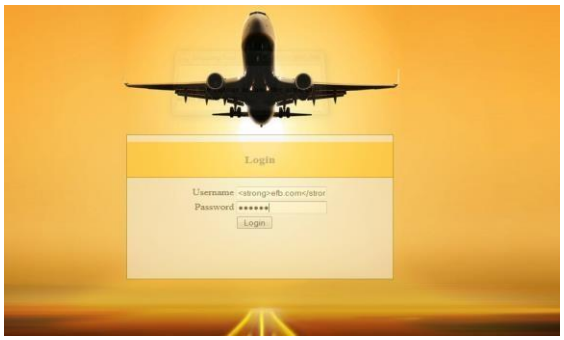


Gambar 4-13 Gambar pengujian 6

Maka hasil yang dari script tersebut seperti gambar dibawah ini:

Gambar 4-14 Gambar hasil pengujian 6

g. Pengujian berikutnya yang ke tujuh script ***efb.com*** masukan pada kolom username seperti gambar dibawah ini :

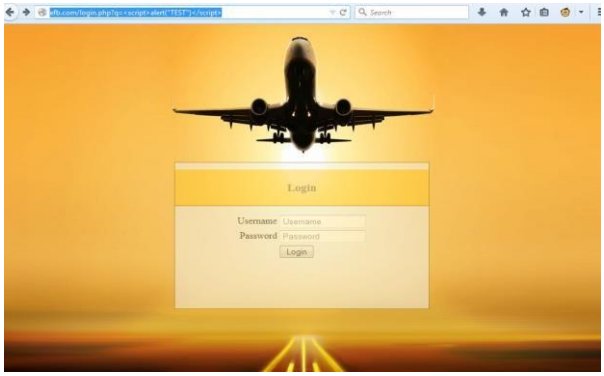


Gambar 4-15 Gambar pengujian 7

Maka hasil yang dari script tersebut berupa tulisan tebal di bagian atas kiri seperti gambar dibawah ini :

Gambar 4-16 Gambar hasil pengujian 7

h. Untuk pengujian yang ke delapan akan dicoba dengan memasukan script pada kolom url dengan alamat http://efb.com/login.php/c=<STYLE type="text/css">BODY{background:url("javascript.alert('XSS')");</STYLE<A CLASS=XSS></A> seperti gambar berikut ini:

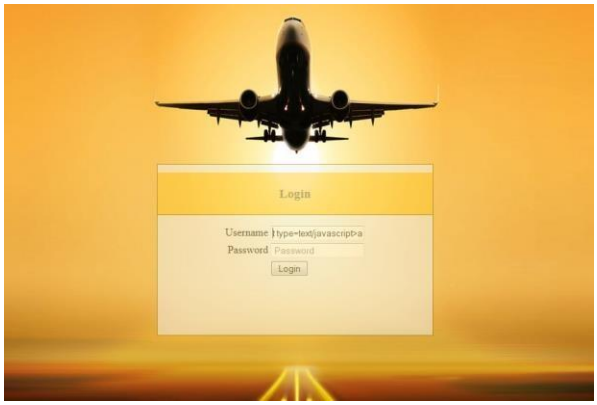


Gambar 4-17 Gambar pengujian 8

Maka hasil yang dari script tersebut seperti gambar dibawah ini :

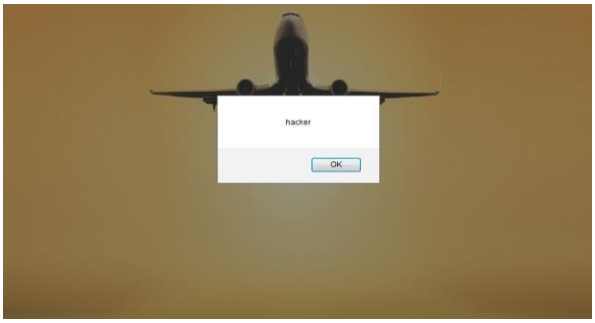
Gambar 4-18 Gambar hasil pengujian 8

i. Pengujian kesembilan dengan menggunakan script ***<script type=text/javascript>alert("Hacker")</script>*** dengan memasukan pada kolom username dan isi password secara asal, seperti gambar dibawah ini:



Gambar 4-19 Gambar pengujian 9

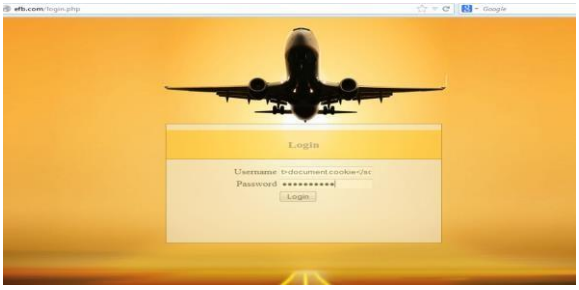
Maka hasil dari script diatas sebagai berikut :



Gambar 4-20 Gambar hasil pengujian 9

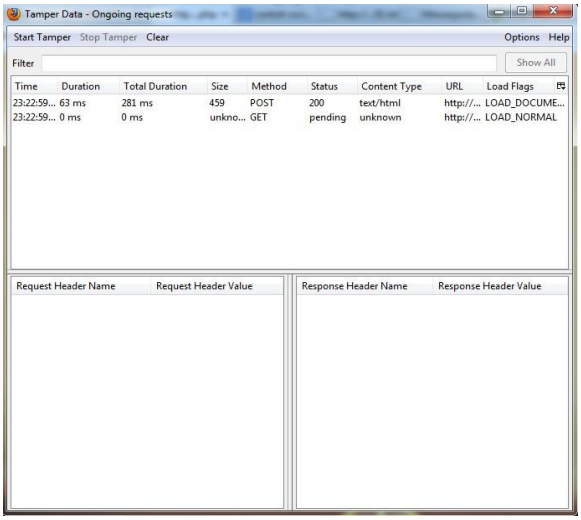
2. Selain untuk mengexecute perintah yang di inputkan , script tersebut juga bisa untuk menggambil cookies pada EFB. Berikut pengujian yang ke-10 untuk mencuri cookie :

   a. Langkah pertama masukan script pada kolom username dengan script ***<script>document.cookie</script>***



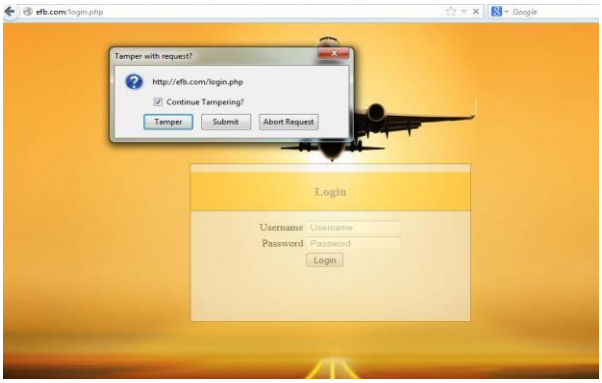
Gambar 4-21 pengujian 10

   b. Kemudian klik login, lalu klik tamper data pada menubar. Maka akan muncul gambar seperti dibawah ini:



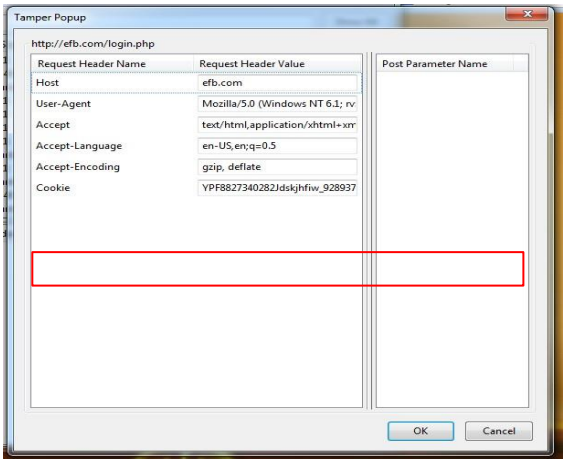
Gambar 4-22 Start Tamper

Setelah itu klik start tamper , dan silahkan reload halaman web. Maka akan muncul gambar seperti dibawah ini :



Gambar 4-23 Tamper

Klik tamper untuk mendapatkan cookie , maka akan muncul gambar seperti dibawah ini:



Gambar 4-24 Cookie

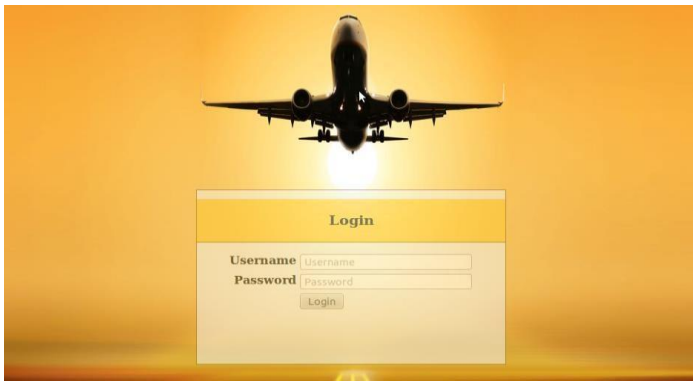
4.1.2 Pengujian setelah menggunakan AntiXSS

1. Pengujian dilakukan dengan memasukan script berikut :

Tabel 4-2 Script penyerangan

Script
<script>alert(‘hallo’);</script>
<marquee>test for xss</marquee>
<script type="text/javascript">window.location='http://google.com/';</script>
<h1>hacked<h1>
<script>document.cookie</script>
<table background="javascript:alert(([code])"></table>
<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
efb.com
Pada URL : http://efb.com/login.php/c=<STYLE type="text/css">BODY{background:url("javascript.alert('XSS')");</STYLE<A CLASS=XSS></A>
<script type=text/javascript>alert("Hacker")</script>

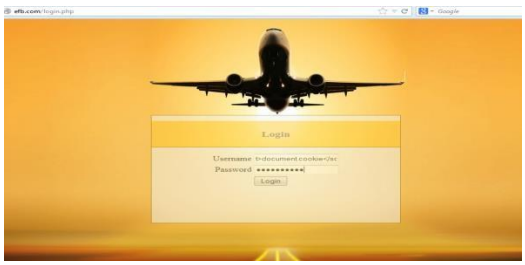
Setelah dilakukan penyerangan dengan menggunakan script diatas web EFB tidak merespon apapun. Seperti gambar dibawah ini :



Gambar 4-25 Tampilan login setelah diamankan

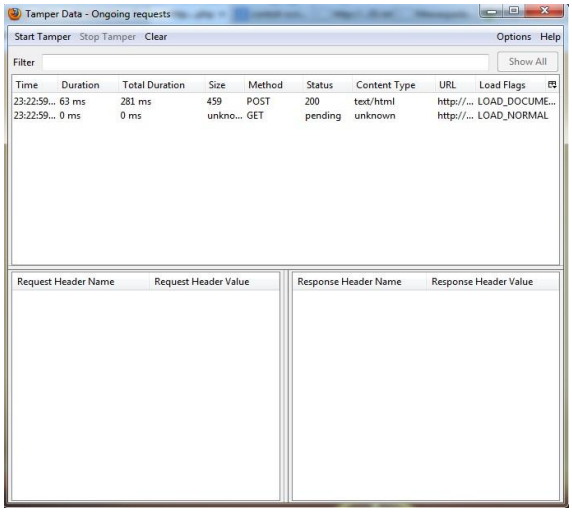
2. Pengujian pengambilan cookie setelah menggunakan AntiXSS.

   a. Pengujian dilakukan dengan memasukan script :<script>document.cookie</script> kemudian klik login.



Gambar 4-26 script cookie

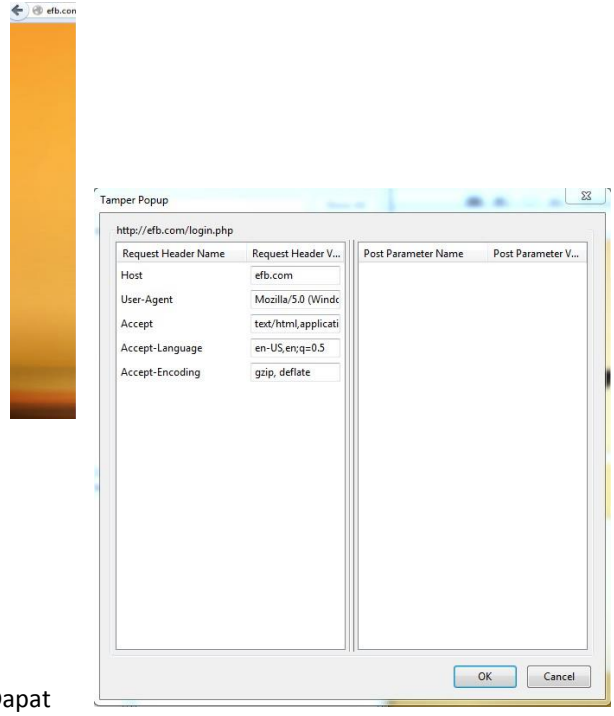
b. Kemudian buka tamper data , lalu start tamper data.



Gambar 4-27 Tamper data

c. Setelah itu re-load kembali halaman login EFB.

d. Kemudian akan muncul gambar dibawah ini :



Gambar 4-28 tamper start

e. Klik tamper maka akan muncul gambar seperti dibawah ini:

Gambar 4-29 No cookie

Cookie tidak didapatkan setelah sistem menggunakan keamanan dengan menggunakan AntiXSS.

5.1 Kesimpulan

Dapat disimpulkan hasil dari proyek akhir ini:

Telah dilakukan pengujian serangan XSS dengan metode White-box testing dimana penyerangan

dilakukan dengan cara menaruh script-script pada halaman login dari web EFB. Serangan XSS dapat dihindari dengan menggunakan script AntiXSS dan dilakukan pengujian serangan sebanyak 10 kali.

5.2 Saran

1. Pengujian berikutnya dilakukan dengan menggunakan tools untuk mendeteksi adanya serangan XSS.
2. Penambahan variasi serangan XSS.

Daftar Pustaka

[1] B. Setiawan, 9 Februari 2015. [Online]. Available: http://www.ilmuterbang.com/artikel-mainmenu-29/teori-penerbangan-mainmenu-68/45-electronic-flight-bag#top.

[2] Iwan, 9 Februari 2015. [Online]. Available: http://www.slideshare.net/iwankurniarasa/metodepengujianblackbox.

[3] Dimas, 9 Februari 2015. [Online]. Available: http://www.ethic.ninja/2014/10/bagaimana-mengatasi-serangan-xss.html.

[4] Anonymos, 10 Februari 2015. [Online]. Available: http://www.elektroindonesia.com/elektro/li1299a.html.

[5] D. Allen, "EFB (Electronic Flight Bag)," *EFB,* pp. 18-21, 14 July 2003.

[6] M. F. Fitzsimmons, "The Electronic Flight Bag : A Multi-Function Tool For Modern Cookpit," *EFB,* pp. 2-3, 22 Agustus 2002.

[7] D. Allen, "Electronic Flight Bag : Real-Time Information Across an Airline's Enterprise," *Electronic FLight Bag,* p. 26, 17 Februari 2008.

[8] Anonymos. [Online]. Available: http://www.it-newbie.com/2013/02/penjelasan-dasar-tentang-web-server.html. [Accessed 10 Februari 2015]