PERLINDUNGAN *PROTOTYPE* EFB (*ELECTRONIC FLIGHT BAG)* TERHADAP SERANGAN XSS (*CROSS SITE SCRIPT)* DENGAN METODE PENGUJIAN *BLACKBOX TESTING*

Shabrina Yolanda Putri
Shabrinayolandaputri@gmail.com

Setia Juli Irzal Ismail,M.T
Jul@tass.telkomuniversity.ac.id

Mia Rosmiati S.Si, M.T.
mia@tass.telkomuniversity.ac.id

Program Studi Teknik Komputer Jurusan Network Engineering, FIT, Telkom University
Jl. Telekomunikasi no.1, Terusan Buah Batu, Bandung 40257

Abstrak

EFB *(Electronic Flight Bag)* adalah tablet PC yang dikhususkan untuk para pilot agar dapat mempermudah komunikasi antara pihak udara *(Airborne flight)* dengan darat *(Ground)*. EFB juga sebagai alat bantu dalam hal pemetaan landasan yang tersedia pada tiap-tiap bandara dan data-data lainnya terkait operasional penerbangan berbasis web. 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 jahat terhadap suatu website untuk menjalankan suatu perintah. Serangan XSS biasanya digunakan untuk mencuri cookie, penyebaran malware, session hijacking/pembajakan session, dan pembelokkan tujuan/malicious redirects. Pada proyek akhir ini dilakukan pengamanan terhadap serangan xss pada efb. Pengujian dilakukan dengan metode Blackbox-Testing dan telah berhasil melakukan pengamanan terhadap serangan XSS.

Kata kunci : EFB, XSS, Black-box testing

Abstract

Efb is a tablet pc especially for the pilot to communicate between airbone flight and ground. Efb is use as help tool for pacing the agvailable land in every airport and any data flight with web base. Xss is a kind of injection code attack, some kind of attack where the attacker try to enter the script to run some command. Sxx attack usually use to steal cookie from web, giving malware, session hijacking and malicious redirects. In this final project with black box testing method and done with giving security from xss attack.

Keyword : EFB,XSS,Black-box testing

1. Latar Belakang

Sistem transportasi udara khususnya di Indonesia semakin berperan dalam pengembangan perekonomian negara. Bandara merupakan prasarana pendukung transportasi udara yang sangat penting karena daerah-daerah yang sebelumnya sulit dijangkau melaluI jalur transportasi darat kini dapat diatasi melalui jalur transportasi udara. Dahulu alat bantu yang digunakan untuk memudahkan pekerjaan rutin pilot adalah berupa dokumen. Kini karena perkembangan teknologi, EFB *(ELECTRONIC FLIGHT BAG)* lebih meringankan pekerjaan pilot.

EFB (Electronic Flight Bag) adalah tablet PC yang dikhususkan untuk para pilot agar dapat mempermudah komunikasi antara pihak udara (Airborne flight) dengan darat (Ground). EFB juga sebagai alat bantu dalam hal pemetaan landasan yang tersedia pada tiap-tiap bandara dan data-data lainnya terkait operasional penerbangan berbasis web. Penggunaan EFB menimbulkan potensi keamanan peretasan / serangan terhadap sistem pesawat terbang. Salah satunya menggunakan teknik *XSS (Cross Site Script). XSS* adalah jenis serangan injeksi *code (Code Injection Attack*), suatu jenis serangan web dimana penyerang berusaha untuk menyisipkan script yang berisikan kode jahat terhadap suatu website. Serangan *XSS* biasanya digunakan untuk mencuri cookie, penyebaran malware, *session hijacking*/pembajakan *session*, dan pembelokkan tujuan/malicious redirects. Serangan ini tipikalnya adalah melakukan injeksi kode javascript terhadap sebuah website sehingga browser mengeksekusi kode/script yang diperintahkan oleh penyerang. Kelemahan ini mudah didapat tapi susah untuk diatasi. Inilah alasannya mengapa XSS banyak ditemukan di berbagai website. Berdasarkan permasalahan diatas maka dibuat solusi untuk mencegah peratasan dari serangan XSS pada EFB. Pengujian dilakukan pada prototype EFB. Pengujian dilakukan dengan metode Black-box.

2. Dasar Teori

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.

2.2 EFB (Elektronic Flight Bag)

Gambar 2-1 Electronic Flight Bag.[1]

EFB (Electronic Flight Bag) adalah tablet PC yang dikhususkan untuk para pilot agar dapat mempermudah komunikasi antara pihak udara (Airborne flight) dengan darat (Ground). EFB juga sebagai alat bantu dalam hal pemetaan landasan yang tersedia pada tiap-tiap bandara dan data-data lainnya terkait operasional penerbangan berbasis web.

Lokasi EFB di tempatkan disamping kiri (capt) dan kanan (*first officer*) kedua komputer ini bekerja independent namun apabila seoarang captain ingin mengetahui atau membaca apa yang sedang di baca copilot dengan cara menekan tombol transfer.

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 taxy di airport yang besae dan complicated taxy waynya, terlebih dalam keadaan low visibility.

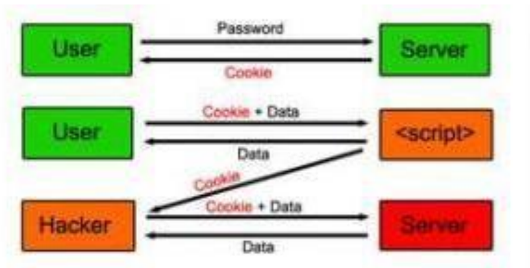
2. Performance : Membantu pilot dalam perhitungan weight and balance (a/c configuration, flap setting, thrust setting) sehingga bisa menghemat engine life/fuel consumption bahkan untuk landing apabila ada penalty sewaktu ada kerusakan seperti engine fail, hydraulic problem dsb.

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

5. Dokumen : Semua dokumen yang diperlukan dapat tersedia di dalam EFB seperti FCOM/AOM, MEL, pengumuman untuk kru/Air crew notice. [2]

2.3 XSS (Cross Site Script)

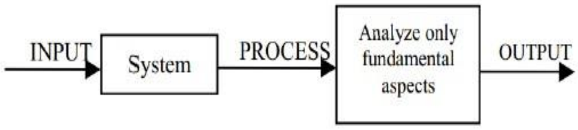


Gambar 2-2 XSS (Cross Site Script).[3]

XSS (*cross Site Script*) merupakan salah satu jenis serangan yang berbahaya dan paling banyak ditemukan di website manapun seperti google, facebook, Amazon, Paypal, dll. Jika anda cek laporan bug pada masing-masing website tersebut maka sebagian besar melaporkan serangan XSS.

Serangan *cross-site scripting* biasanya digunakan untuk mencuri cookie, penyebaran malware, session hijacking / pembajakan session, dan pembelokkan tujuan / *malicious redirects*. Serangan ini tipikalnya adalah melakukan injeksi kode javascript terhadap sebuah website sehingga browser mengeksekusi kode/script yang diperintahkan oleh penyerang. Kelemahan ini mudah didapat tapi susah untuk diatasi. Inilah alasannya mengapa XSS banyak ditemukan di berbagai website. Penjelasan mengenai XSS adalah suatu jenis serangan web dimana penyerang berusaha untuk menyisipkan script yang berisikan kode jahat terhadap suatu website untuk menjalankan suatu perintah. [3]

2.4 Metode Black-Box Testing



Gambar 2-3 Metode Black-Box Testing.[4]

a. Menurut Myers (1979) :

Proses menjalankan program dengan maksud menemukan kesalahan.

b. Menurut IEEE (1990) :

Pengujian yang mengabaikan mekanisme sistem atau komponen dan fokus semata-mata pada output yang dihasilkan yang merespon input yang dipilih dan kondisi eksekusi. Pengujian yang dilakukan untuk mengevaluasi pemenuhan sistem atau komponen dengan kebutuhan fungsional tertentu. [5]

Black-box Testing merupakan sebuah metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional aplikasi saat dioperasikan, apakah input diterima dengan benar dan output yang dihasilkan telah sesuai dengan yang diharapkan. Fokus dari pengujian mengunakan metode *Black-Box* adalah pada pengujian fungsionalitas dan output yang dihasilkan aplikasi. Pengujian *black-box* didesain untuk mengungkap kesalahan pada persyaratan *fungsional* dengan mengabaikan mekanisme internal atau komponen dari suatu program.
Menurut Williams (2006) pengujian perangkat lunak mempunyai beberapa level, untuk pengujian menggunakan metode Black Box, terdapat enam level yaitu *Integration, Functional, System, Acceptance, Beta,* dan *Regression.*
Salah satu dari pengujian Black-Box yang dapat dilakukan oleh seorang penguji independen adalah Functional testing. Basis uji dari functional testing ini adalah pada spesifikasi dari komponen perangkat lunak yang akan diuji. Functional testing memastikan bahwa semua kebutuhan-kebutuhan

telah dipenuhi dalam sistem aplikasi. Dengan demikian fungsinya adalah tugas-tugas yang didesain untuk dilaksanakan sistem. *Functional testing* berkonsentrasi pada hasil dari proses, bukan bagaimana prosesnya terjadi
Black Box dapat menemukan kesalahan dalam kategori berikut :

a. Fungsi-fungsi yang tidak benar atau hilang

b. Kesalahan interface

c. Kesalahan dalam struktur data atau akses basisdata eksternal

d. Inisialisasi dan kesalahan terminasi

e. Validitas Fungsional

f. Kesensitifan Sistem Terhadap Nilai Input Tertentu

g. Batasan Dari Suatu Data. [6]

3. Analisis dan Perancangan

3.1 Gambaran Sistem Saat Ini (atau Produk)

Sistem yang digunakan pada proyek akhir ini dengan judul "Perlindungan Prototype EFB (Electronic Flight Bag) terhadap serangan XSS (Cross Site Script) dengan metode pengujian BlackBox-Testing" sebuah sistem yang dibangun untuk melindungi prototype EFB dari serangan XSS, sebelumnya prototype EFB tidak menggunakan keamanan sehingga sangat mudah bagi attacker menyerang prototype EFB tersebut.
EFB merupakan teknologi berbasis web, sehingga tidak menutup kemungkinan banyak ancaman-ancaman serangan dari orang-orang yang tidak bertanggung jawab. Maka dari itu pengamanan web EFB untuk saat ini sangat diperlukan untuk melindungi web EFB dari serangan pada web.

3.2 Analisis Kebutuhan Sistem

Analisis kebutuhan merupakan proses identifikasi atau analisa kebutuhan dalam pembuatan prototype EFB (Electronic Flight Bag). Dalam membangun prototype EFB dibutuhkan beberapa analisis dalam perancangan,diantaranya :

1. Mempersiapkan semua aplikasi yang dibutuhkan.
2. Mempelajari semua hal yang berkaitan dengan teori dan aplikasi yang digunakan.
3. Menginstal software dan Sistem Operasi yang dibutuhkan, seperti :
   a. Tamper data
   b. VirtualBox/Vmware
   c. Ubuntu 12.04
   d. Menginstal DNS Server
   e. Menginstal Web server

4. Melakukan pengencekan semua aplikasi yang sudah terinstal.

5. Membuat dan mencari script yang akan dipakai untuk melakukan penyerangan terhadap prototype EFB (Electronic Flight Bag).

6. Membuat prototype EFB (*Electronic Flight Bag*) dengan membangun web sederhana.

7. Melakukan skenario pengujian.

8. Menganalisis hasil pengujian.

9. Membuat laporan proyek akhir.

3.2.1 Kebutuhan Perangkat Keras Dan Perangkat Lunak

Pada subbab ini akan dijelaskan kebutuhan perangkat keras dan perangkat lunak

3.2.2 Perangkat Keras

Dalam membangun prototype EFB, perangkat keras yang digunakan adalah sebagai berikut.

Tabel 3-1 Spesifikasi perangkat

Jenis	Spesifikasi	Keterangan
Laptop	Processor : Intel ® Core™ i3-2370M CPU @2.40 GHz Memory : 2048 MB RAM HDD : 500 GB	Minimal spesifikasi laptop yang dapat digunakan : Processor : intel ® Core™ Memory : 1024 MB RAM HDD : 500 GB

3.2.3 Perangkat Lunak

Dalam membangun prototype EFB (Electronic Flight Bag), perangkat yang dibutuhkan adalah sebagai berikut.

a. Sistem Operasi

   Sistem operasi yang digunakan untuk server menggunakan 12.04

b. Apache2

   Aplikasi yang digunakan untuk membuat web server

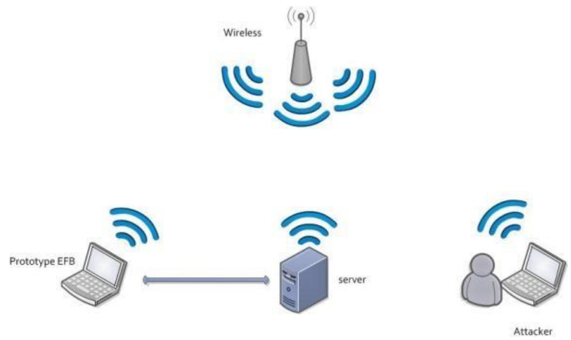
c. Bind9

   Bind9 berfungsi sebagai DNS Server untuk prngalamatan web EFB

d. Tamper Data

   Tamper data sebuah aplikasi yang digunakan untuk mengetahui informasi tentang suatu web memberikan informasi seperti jenis browser yang digunakan, username dan password, dan mendapatkan cookie pada suatu web.

3.3 Perancangan Sistem

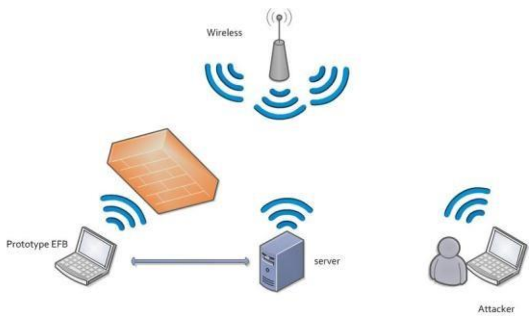


Gambar 3-4 Gambaran sistem sebelum menggunakan keamanan

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 .

3.3.1 Gambaran sistem setelah menggunakan keamanan



Gambar 3-5 Gambaran sistem setelah 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 keamanan pada prototype EFB, script yang dipakai untuk mengamankan prototype EFB sebagai berikut :

```
<?php
        if(isset($_POST['username'])){
                $data= htmlentities($_POST
['username']);          ?>
        <p style="display: none;"><?php echo $data; ?></p>
<?php   }
?>
```

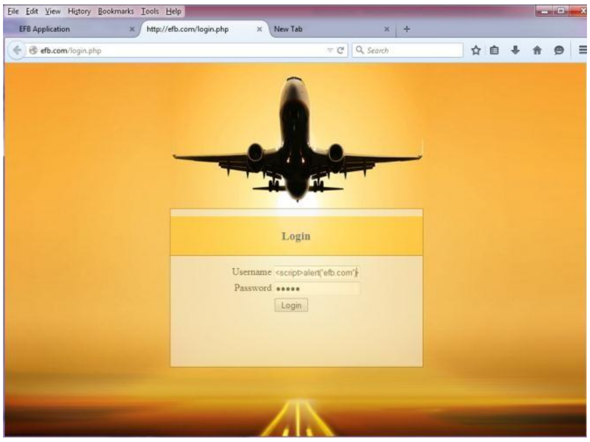
Gambar 3-6 Script untuk mengamankan prototype EFB

4. PENGUJIAN

4.1 Pengujian serangan XSS terhadap web EFB tanpa perlindungan

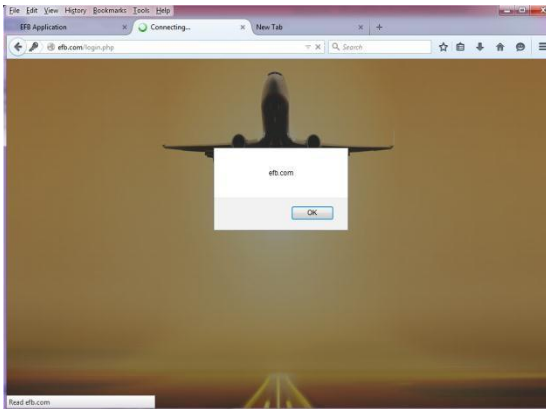
1. Pengujian kesatu untuk serangan xss dilakukan dengan memasukan script script seperti di bawah ini

#<script>alert('efb.com');</script>



Gambar 4-7 Tampilan login

Kemudian masukkan script **#<script>alert('efb.com');</script>** dibagian kolom username dan masukkan password secara asal, maka akan muncul tampilan seperti pada Gambar 4-19 pengujian hasil 1.

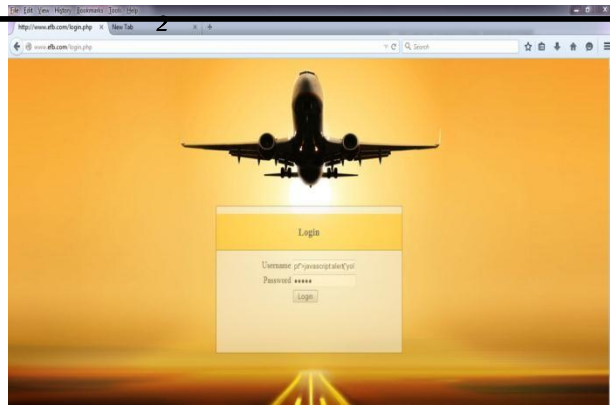


Gambar 4-8 Pengujian

2. Pengujian kedua untuk melakukan serangan xss dilakukan dengan memasukan script script seperti di bawah ini

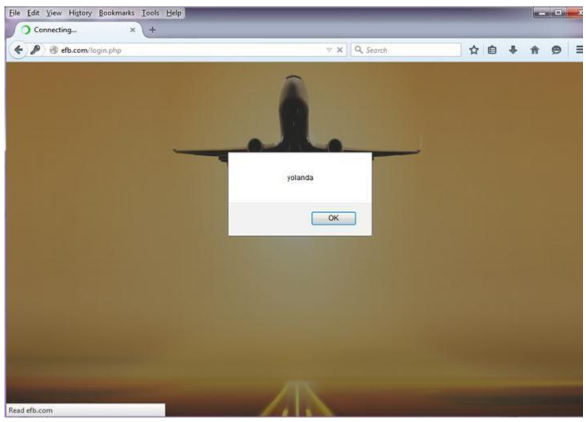
<scripttype="text/javascript">javascript:alert('yolanda');</script>

2



Gambar 4-20 Pengujian 2

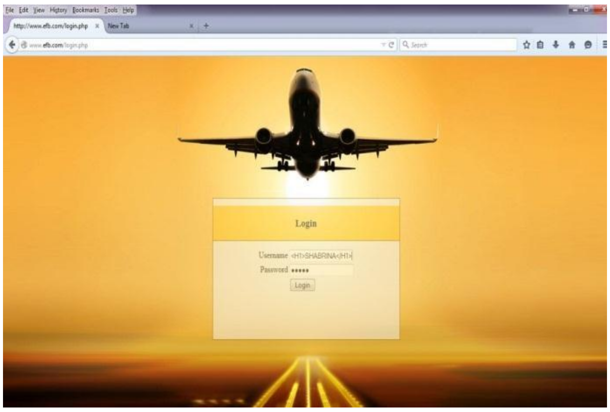
Lalu setelah memasukkan script di atas dibagian username dan password, maka hasil pengujian seperti pada gambar **Gambar 4-21 hasil pengujian 2**.



Gambar 4-9 hasil pengujian 2

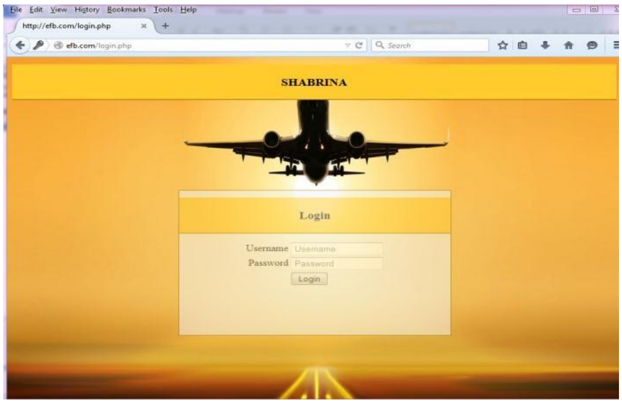
3. Pengujian ketiga untuk melakukan serangan xss dilakukan dengan

<H1>SHABRINA</H1>



Gambar 4-10 pengujian 3

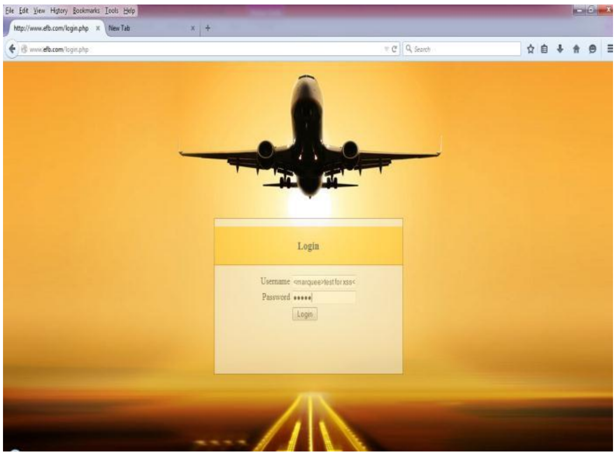
Lalu masukkan script **#<H1>SHABRINA</H1>** dibagian kolom username dan masukkan password secara asal, maka hasil pengujian seperti pada **Gambar** ***4-23 hasil pengujian 3.***



Gambar 4-11 hasil pengujian 3

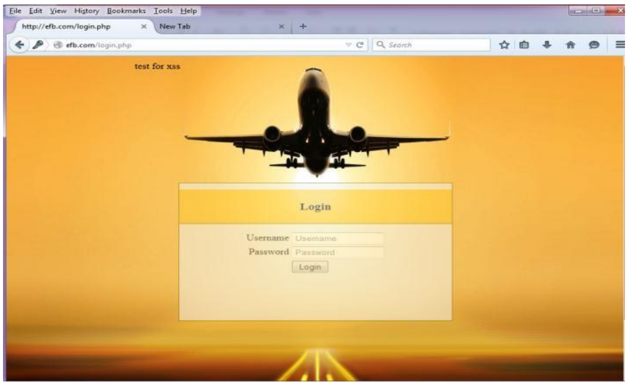
4. Pengujian keempat untuk melakukan serangan xss dilakukan dengan memasukan script script seperti di bawah ini

#<marquee>test for xss</marquee>



Gambar 4-13 pengujian 4

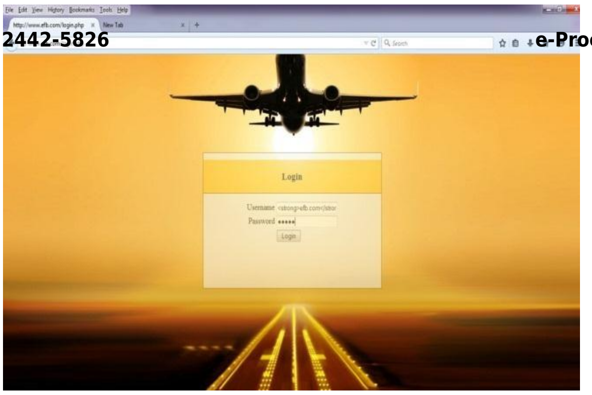
Masukkan script **#<marquee>test for xss</marquee>** dibagian kolom username dan masukkan password secara asal, maka hasil dari prngujian berupa text yang berjalan seperti pada **Gambar** ***4-25 pengujian hasil 4.***



Gambar 4-14 pengujian hasil 4

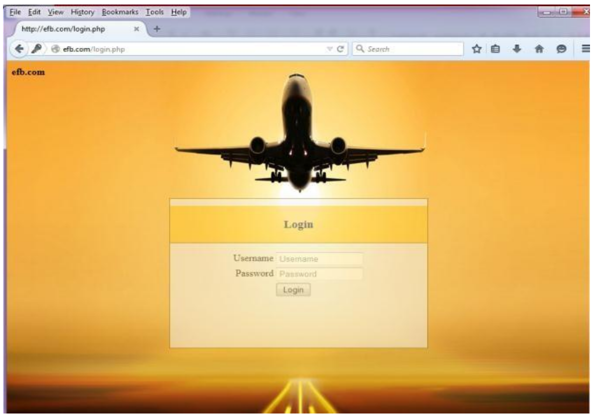
5. Pengujian kelima untuk melakukan serangan xss dilakukan dengan memasukan script script seperti di bawah ini

efb.com



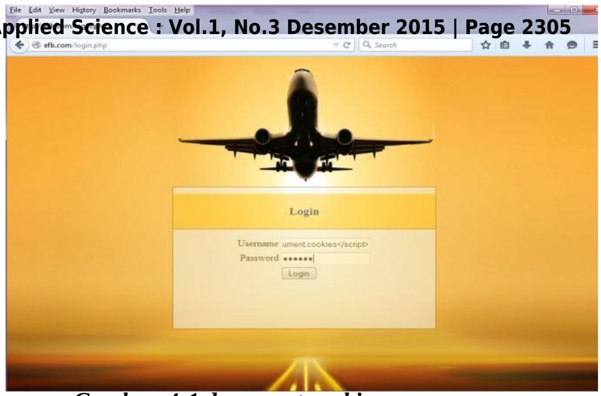
Gambar 4-16 pengujian 5

Pada kolom username masukkan script **#efb.com** dan dibagian kolom password masukkan password secara asal, maka hasil dari pengujian adalah sebuah text yang yang berada pada sisi kiri atas, seperti pada **Gambar 4-27 hasil pengujian 5.**



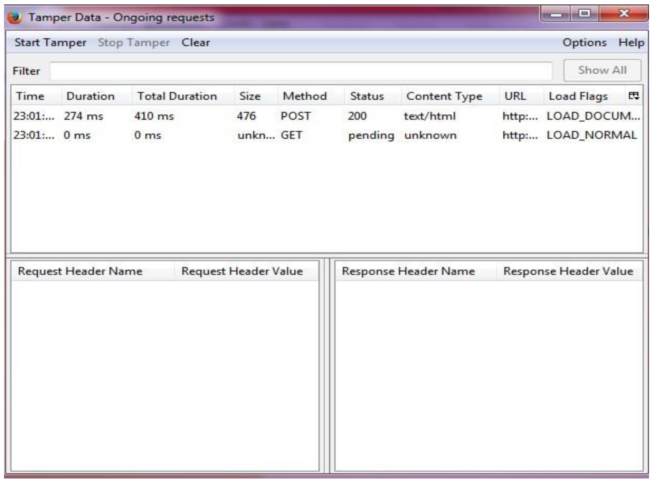
Gambar 4-17 hasil pengujian 5

5. Pengujian serangan xss dengan menggunakan Tamper data untuk mendapatkan cookies. Pada kolom username silahkan ketikkan **#<script>document.cookies</script>** untuk mendapatkan cookies.



Gambar 4-1 document.cookie

Setelah memasukkan script **#<script>document.cookies</script>**, langkah selanjutnya adalah klik tools pada menu bar kemudian klik tamper data. Setelah itu silahkan klik login. Lalu start tamper data untuk mendapatkan cookies.



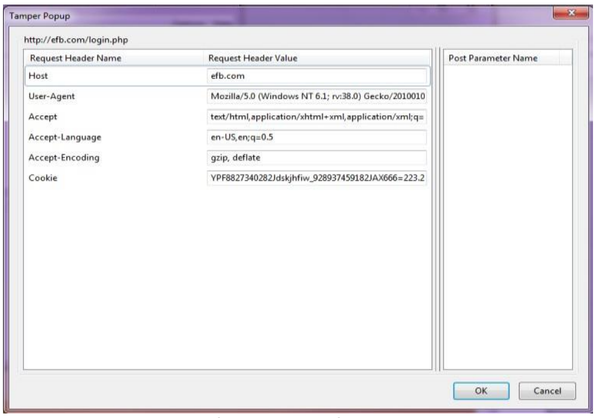
Gambar 4-2 Tamper Data

Langkah berikutnya setelah klik start tamper akan muncul tampilan dibawah ini dan kemudian klik tamper untuk mendapatkan cookies.

Gambar 4-3 Start Tamper

Setelah itu akan muncul tampilan seperti dibawah ini, tampilan ini menunjukan bahwa sudah mendapatkan cookie.

.



Gambar 4-4 Cookie

4.1.2 Pengujian serangan XSS terhadap web EFB setelah menggunakan keamanan pada sistem

1. Pengujian dilakukan dengan memasukkan beberapa script seperti di bawah di bagian login, berikut beberapa script untuk penyerangan :

#<script>alert('efb.com');</script>

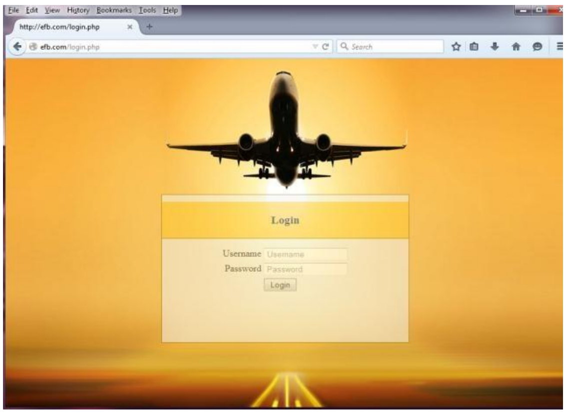
#<scripttype="text/javascript">javascript:alert('yolanda');</script

#<H1>SHABRINA</H1>

#<marquee>test for xss</marquee>

#efb.com

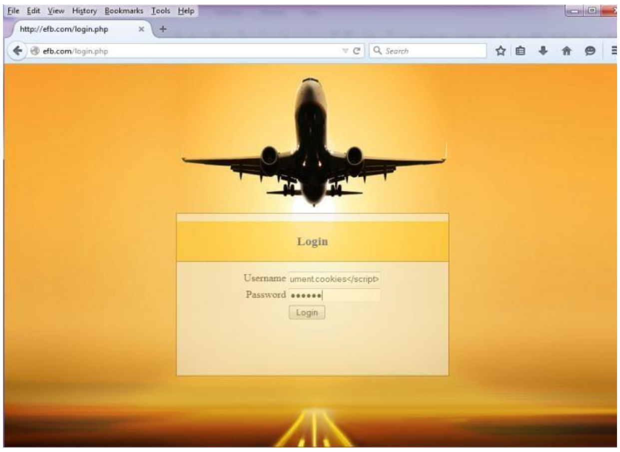
Setelah memasukkan beberapa script diatas pada bagian username pada web EFB tidak merespon apapun, seperti gambar dibawah ini :



Gambar 4-5 tampilan setelah diamankan dari serangan XSS

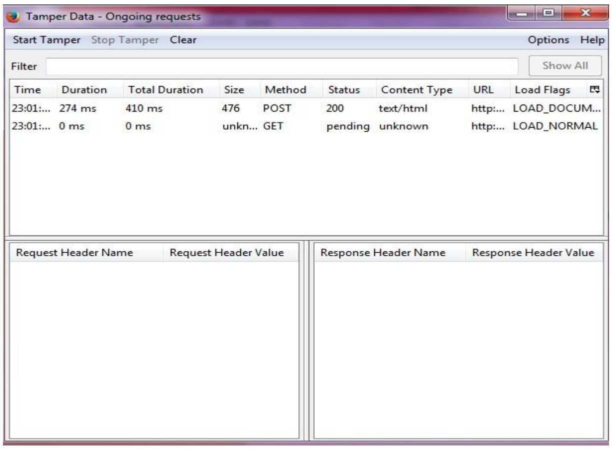
2. Pengujian pengambilan cookie setelah menggunakan keamanan Pengujian dilakukan dengan memasukkan script, kemudian klik login.

<script>document.cookies</script>



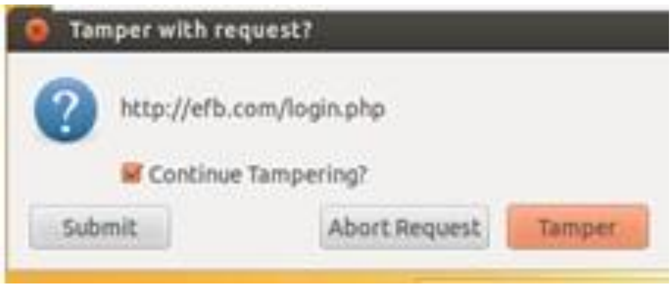
Gambar 4-6 login dengan memasukan cookie

Kemudian setelah memasukkan script pada kolom username buka Tamper data, lalu start tamper data.



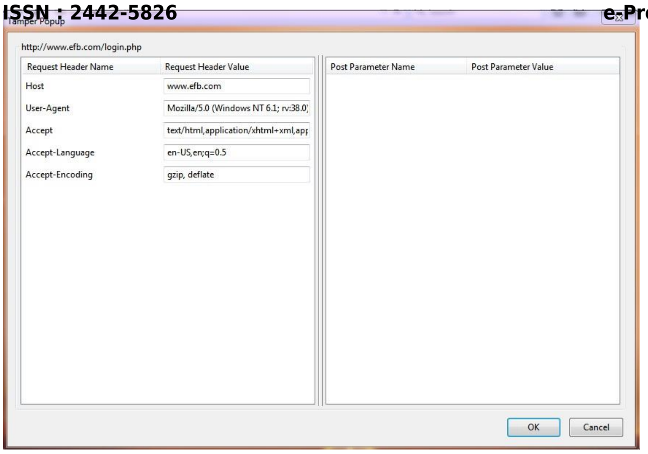
Gambar 4-7 Tamper data

Kemudian setelah klik start Tamper data re-load kembali halaman login EFB, kemudian akan muncul tampilan seperti pada ***gambar 4-35 Tamper with request***



Gambar 4-8 Tamper with request

Setelah tekan enter pada tamper data maka akan muncul tampilan seperti di bawah ini :



Gambar 4-9 Tamper data

Pada gambar 4-36 Tamper data menunjukkan bahwa pengujian menggunakan Tamper data untuk mendapatkan cookie tidak berhasil karena EFB sudah dilindungi oleh keamanan filtering.

5.1 Kesimpulan

Kesimpulan dari Proyek akhir ini, adalah :

1. Prototype EFB(Electronic Flight Bag) dapat dilindungi dari serangan XSS.

2. Pengujian serangan XSS pada prototype EFB dengan metode Blackbox-testing berhasil dilakukan.

5.2 Saran

Saran dari proyek akhir ini, adalah :

1. Untuk pengujian pengamanan pada prototype EFB terhadap serangan XSS dapat menggunakan *AntiSamy*.

2. Untuk pengambilan cookie pada pengujian selanjutnya dapat menggunakan aplikasi *GreaseMonkey*.