

**5212100092 – Arbintoro Mas**

**5215100056 – Evia Nanda Irawati**

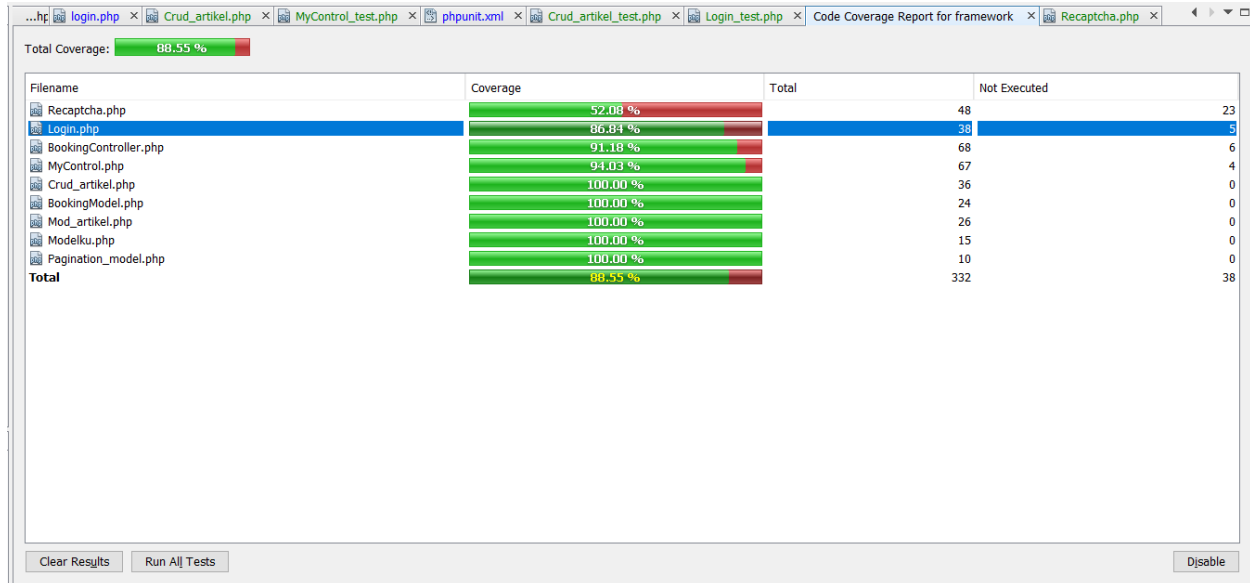
**5215100138 – Ardo Fachrizal Ilmy**

**Hasil Black Box testing :**

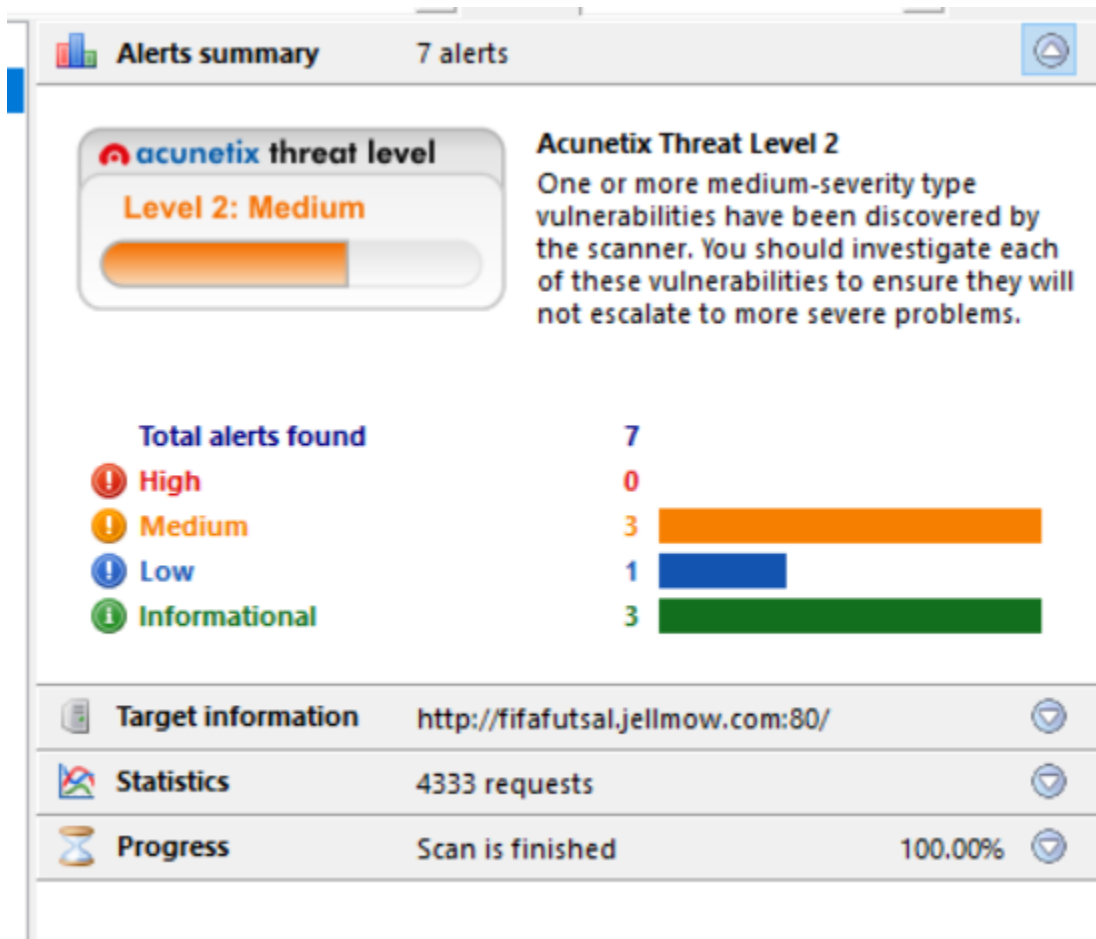
<b>Functional Requirement</b>	<b>Berhasil</b>
Staff(admin) lapangan futsal dapat login	<b>V</b>
❑ Sistem dapat menampilkan jadwal yang telah ditandai dengan status lapangan. Jadi nanti ada 3 status lapangan dalam sistem: a. Status Badge Hijau : Jadwal masih kosong belum ada yang pesan b. Status Badge Kuning : Jadwal sudah dipesan, tetapi belum dibayar. c. Status Badge Merah : Jadwal sudah dipesan dan dibayar.	<b>X</b>
❑ Customer dapat memesan lapangan futsal secara online dengan memilih jadwal lapangan dan mensubmit form ke website	<b>V</b>
Customer dapat memesan lapangan futsal secara offline dengan memilih jadwal dan form pemesanan online yang diisikan oleh staff.	<b>V</b>
❑ Sistem dapat menampilkan foto lapangan kepada seluruh user.	<b>V</b>
Staff dapat menambahkan daftar kompetisi futsal yang dilaksanakan di FIFA Futsal .	<b>V</b>
❑ Sistem dapat menampilkan seluruh jadwal kapan lapangan digunakan atau yang sedang kosong.	<b>X</b>
❑ Sistem dapat menampilkan order history kepada Staff.	<b>V</b>
Staff lapangan futsal dapat mengupdate status lapangan.	<b>X</b>
Sistem dapat mengupdate otomatis status lapangan dari status badge merah ke status badge putih apabila waktu pada sistem telah melewati jadwal pemesanan yang terekam.	<b>X</b>
Sistem dapat mengupdate otomatis status lapangan dari status badge kuning ke status badge putih apabila dalam 3 jam staff tidak mengupdate status lapangan ke status badge kuning	<b>X</b>

## Hasil Whitebox Testing :

Kelompok kami menggunakan PHPUnit untuk mengetes aplikasi kami, berikut kami lampirkan hasilnya :



## Hasil Scan Acunetix:



Scan Results: Scan Thread 1 (http://fifafutsal.jellmow.com:80/) Status: Finished (7 alerts)

Web Alerts (7)

- HTML form without CSRF protection ...
- Broken links (1)
- Email address found (1)
- Possible server path disclosure (Unix...)

Knowledge Base (6)

- List of file extensions
- Top 10 response times
- List of client scripts
- List of files with inputs
- List of external hosts
- List of email addresses

Site Structure

- /
- assets
- img
- Login
- MyControl
- BookingController
- Cookies
- d\_session

Activity Window

acunetix WEB APPLICATION SECURITY

**HTML form without CSRF protection** MEDIUM

**Vulnerability description**

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

**Affected items**

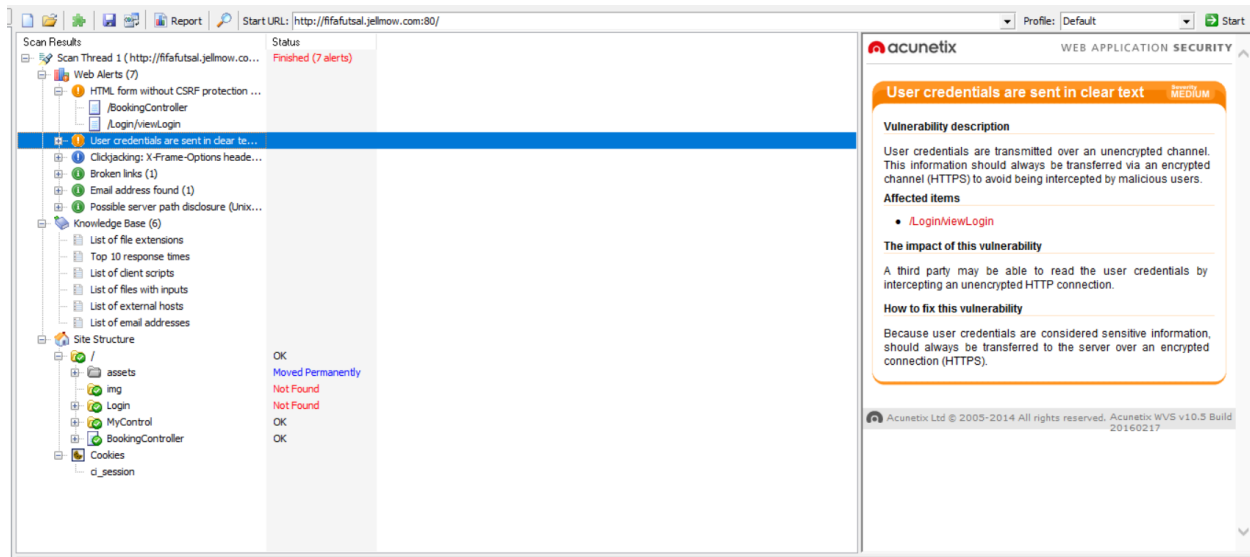
- /BookingController
- /LoginView/Login

**The impact of this vulnerability**

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

**How to fix this vulnerability**

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.



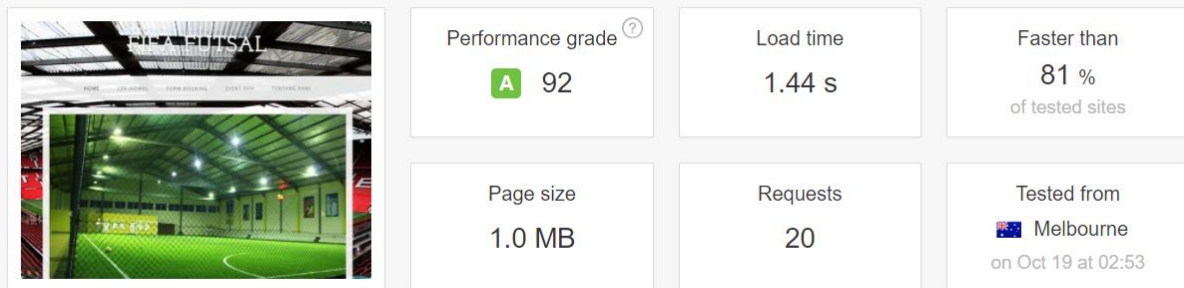
### Kesimpulan dari Security Testing using acunetix:

Ditemukan celah dimana website masih bisa dihack karena server dari hostngan yang belum HTTPS.

### Hasil Performance Testing:

Ada 3 server Amerika, Inggris dan Australia . Saya menggunakan server yang ada di Australia karena yang letaknya paling dekat dengan Indonesia.




### Summary








### Performance insights

GRADE	SUGGESTION	
C 70	Avoid bad requests	▼
B 81	Serve static content from a cookieless domain	▼
B 85	Leverage browser caching	▼
A 100	Minimize redirects	▼
A 100	Minimize request size	▼
A 100	Remove query strings from static resources	▼
A 100	Specify a cache validator	▼
A 100	Specify a Vary: Accept-Encoding header	▼






## Response codes

RESPONSE CODE	RESPONSES
 200 OK	16
 404 Not Found	1
 ERROR Connection error	1

## Content size by content type

CONTENT TYPE	PERCENT	SIZE
 Image	80.6 %	811.25 KB
 Other	10.2 %	102.57 KB
 Script	5.8 %	58.62 KB
 CSS	3.1 %	31.53 KB
 HTML	0.3 %	2.69 KB
Total	100.00 %	1006.65 KB

## Requests by content type

CONTENT TYPE	PERCENT	REQUESTS
 CSS	31.3 %	5
 Image	25.0 %	4
 Script	18.8 %	3
 Other	18.8 %	3
 HTML	6.3 %	1
Total	100.00 %	16

## Hasil Readability Testing :

### Readability Results

The following table contains the readability results for <http://fifafutsal.jellmow.com/>.

#### Reading Level Results

Summary	Value
Total sentences	26
Total words	53
Average words per Sentence	2.04
Words with 1 Syllable	10
Words with 2 Syllables	34
Words with 3 Syllables	9
Words with 4 or more Syllables	0
Percentage of word with three or more syllables	16.98%
Average Syllables per Word	1.98
Gunning Fog Index	7.61
Flesch Reading Ease	37.16
Flesch-Kincaid Grade	8.58

