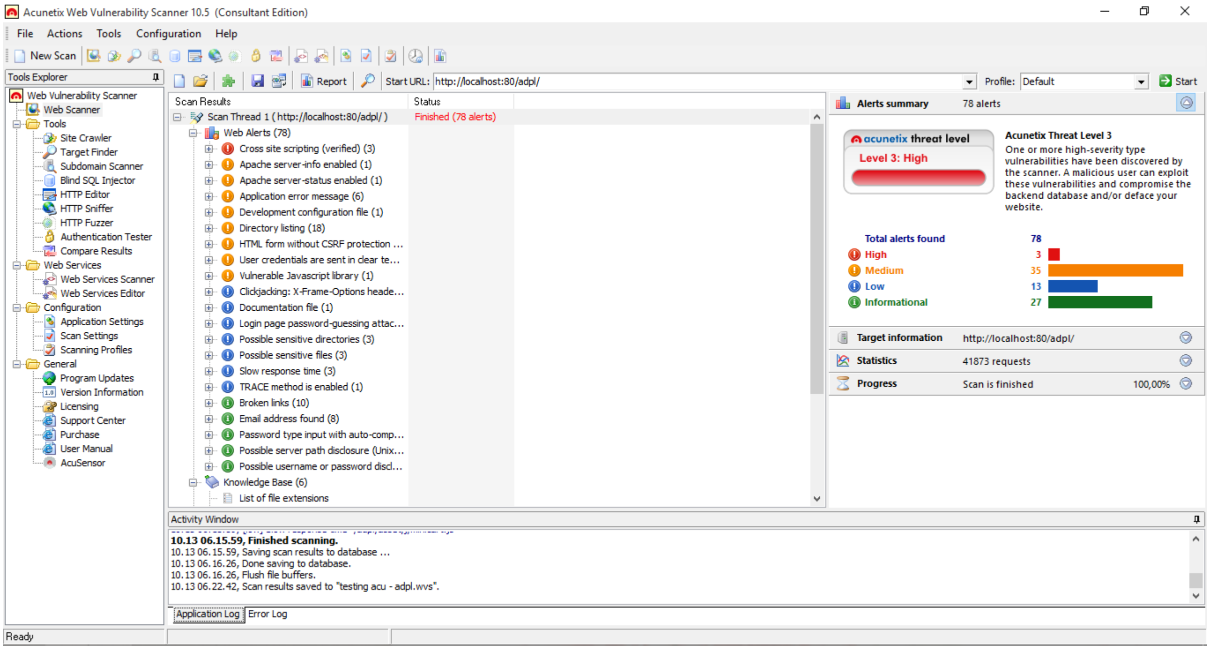
Testing KPPL (for Website E-KostOn)

Dibuat oleh :
Al Lilah Nur Hasanah 5215100007
Yayan Irfan 5215100062
KPPL - B

TEST acunetix :

Hasil dari testing dengan menggunakan acunetix untuk mentesting adanya vulnerability dalam website adalah sebagai berikut :



Start URL: http://localhost:80/adpl/
Profile: Default

Scan Results	Status
Scan Thread 1 (http://localhost:80/adpl/)	Finished (78 alerts)
Web Alerts (78)	
Cross site scripting (verified) (3)	
Apache server-info enabled (1)	
Apache server-status enabled (1)	
Application error message (6)	
Development configuration file (1)	
Directory listing (18)	
HTML form without CSRF protection ...	
User credentials are sent in clear te...	
Vulnerable Javascript library (1)	
Clickjacking: X-Frame-Options heade...	
Documentation file (1)	
Login page password-guessing attac...	
Possible sensitive directories (3)	
Possible sensitive files (3)	
Slow response time (3)	
TRACE method is enabled (1)	
Broken links (10)	
Email address found (8)	
Password type input with auto-comp...	
Possible server path disclosure (Unix...	
Possible username or password discl...	
Knowledge Base (6)	
List of file extensions	

Alerts summary 78 alerts

acunetix threat level
Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

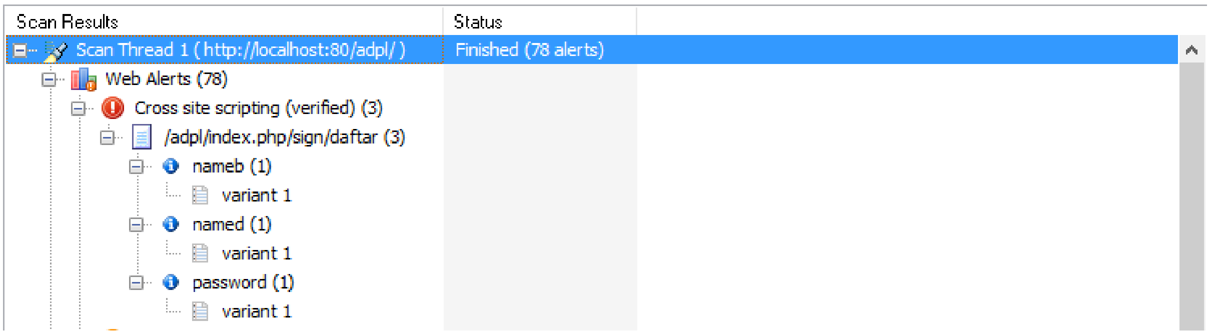
Total alerts found	78
High	3
Medium	35
Low	13
Informational	27

Target information	http://localhost:80/adpl/	
Statistics	41873 requests	
Progress	Scan is finished	100,00%

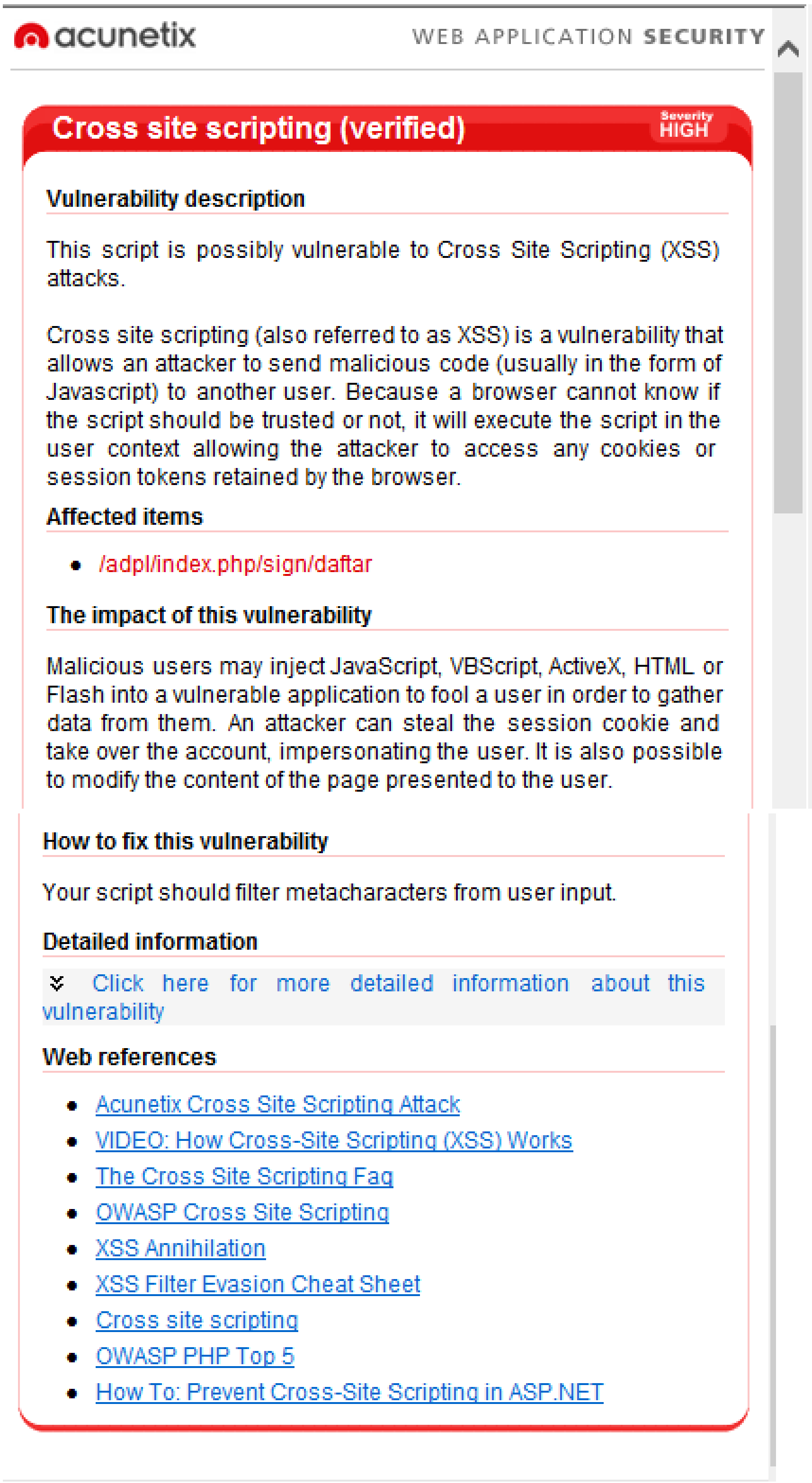
Activity Window

```
10.13 06.15.59, Finished scanning.
10.13 06.15.59, Saving scan results to database ...
10.13 06.16.26, Done saving to database.
10.13 06.16.26, Flush file buffers.
10.13 06.22.42, Scan results saved to "testing acu - adpl.wvs".
```

Ditemukan 3 threat dengan kategori High :



Scan Results	Status
Scan Thread 1 (http://localhost:80/adpl/)	Finished (78 alerts)
Web Alerts (78)	
Cross site scripting (verified) (3)	
/adpl/index.php/sign/daftar (3)	
nameb (1)	
variant 1	
named (1)	
variant 1	
password (1)	
variant 1	



acunetix WEB APPLICATION SECURITY

Cross site scripting (verified)

Severity HIGH

Vulnerability description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Affected items

- /adpl/index.php/sign/daftar

The impact of this vulnerability

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

How to fix this vulnerability

Your script should filter metacharacters from user input.

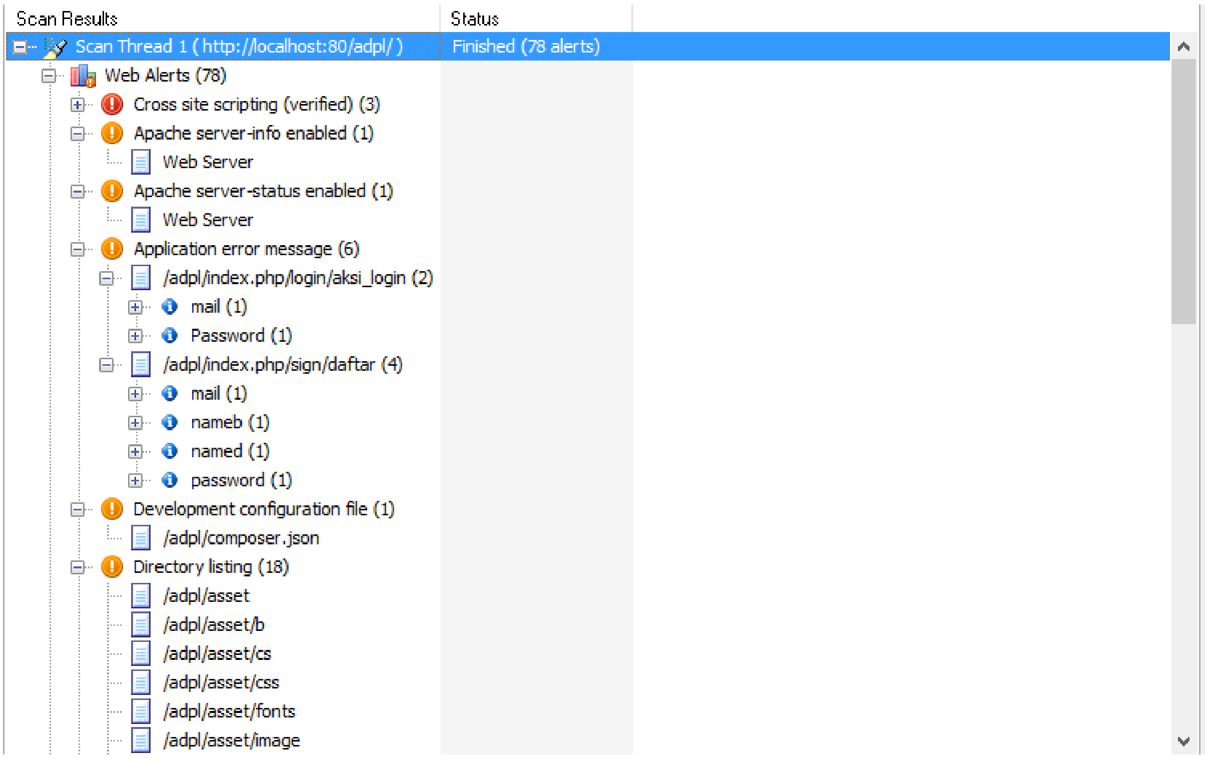
Detailed information

Click here for more detailed information about this vulnerability

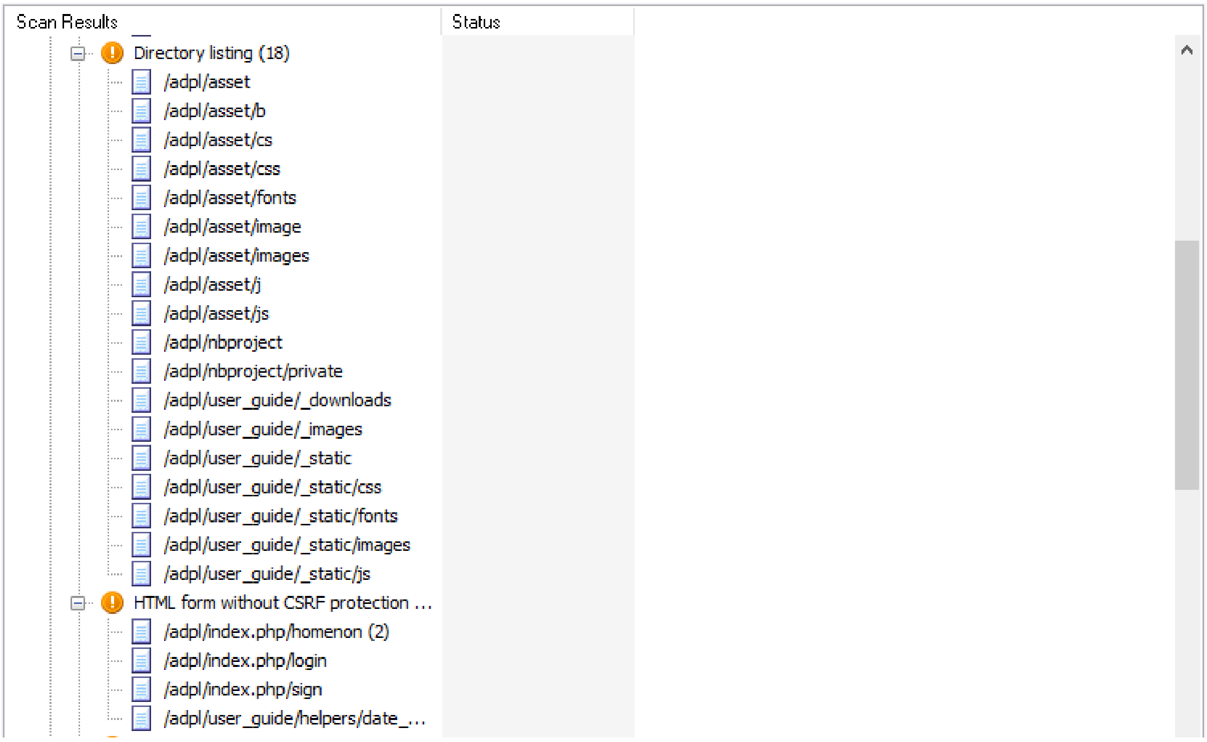
Web references

- Acunetix Cross Site Scripting Attack
- VIDEO: How Cross-Site Scripting (XSS) Works
- The Cross Site Scripting Faq
- OWASP Cross Site Scripting
- XSS Annihilation
- XSS Filter Evasion Cheat Sheet
- Cross site scripting
- OWASP PHP Top 5
- How To: Prevent Cross-Site Scripting in ASP.NET

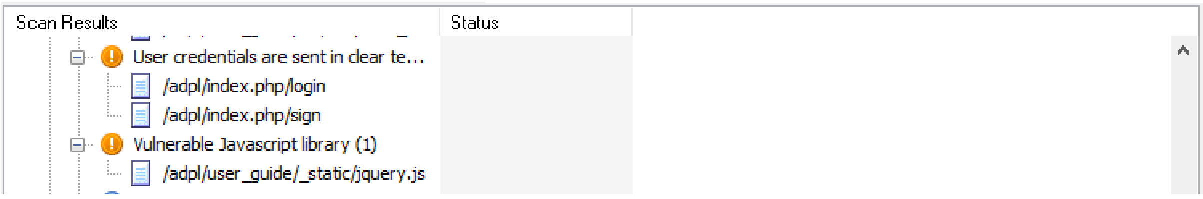
Ditemukan 35 Threat dengan kategori Medium :



```
Scan Results                                                   Status
⊟ Scan Thread 1 ( http://localhost:80/adpl/ )                  Finished (78 alerts)
   ⊟ Web Alerts (78)
      ⊞ Cross site scripting (verified) (3)
      ⊟ Apache server-info enabled (1)
           Web Server
      ⊟ Apache server-status enabled (1)
           Web Server
      ⊟ Application error message (6)
         ⊟ /adpl/index.php/login/aksi_login (2)
            ⊞ mail (1)
            ⊞ Password (1)
         ⊟ /adpl/index.php/sign/daftar (4)
            ⊞ mail (1)
            ⊞ nameb (1)
            ⊞ named (1)
            ⊞ password (1)
      ⊟ Development configuration file (1)
           /adpl/composer.json
      ⊟ Directory listing (18)
           /adpl/asset
           /adpl/asset/b
           /adpl/asset/cs
           /adpl/asset/css
           /adpl/asset/fonts
           /adpl/asset/image
```

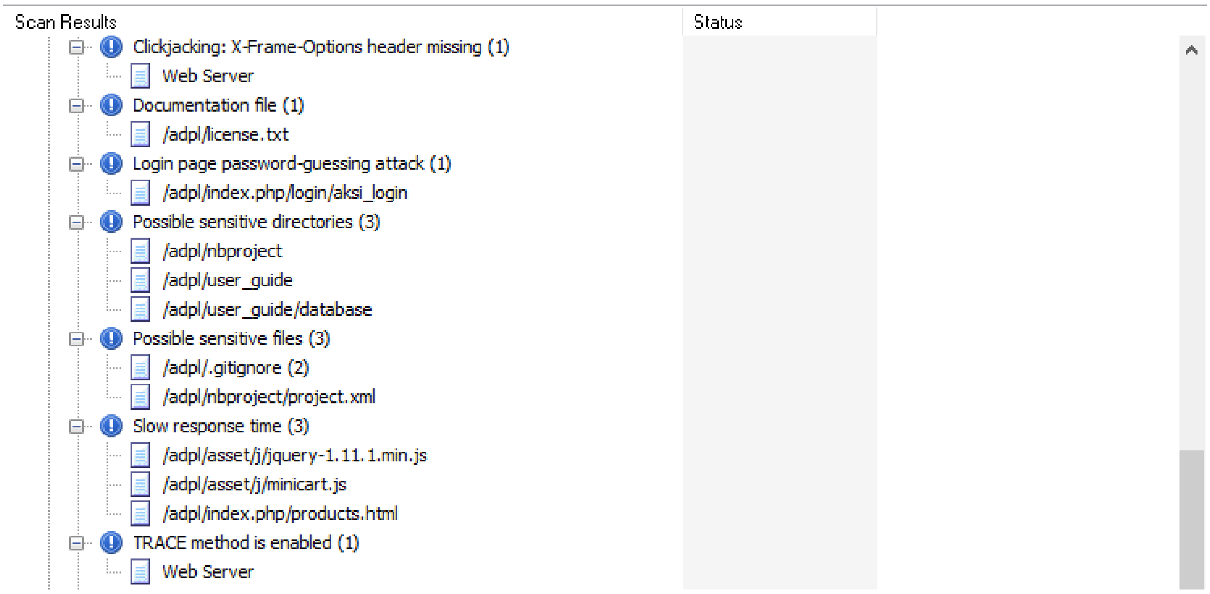


```
Scan Results                                                   Status
      ⊟ Directory listing (18)
           /adpl/asset
           /adpl/asset/b
           /adpl/asset/cs
           /adpl/asset/css
           /adpl/asset/fonts
           /adpl/asset/image
           /adpl/asset/images
           /adpl/asset/j
           /adpl/asset/js
           /adpl/nbproject
           /adpl/nbproject/private
           /adpl/user_guide/_downloads
           /adpl/user_guide/_images
           /adpl/user_guide/_static
           /adpl/user_guide/_static/css
           /adpl/user_guide/_static/fonts
           /adpl/user_guide/_static/images
           /adpl/user_guide/_static/js
      ⊟ HTML form without CSRF protection ...
           /adpl/index.php/homenon (2)
           /adpl/index.php/login
           /adpl/index.php/sign
           /adpl/user_guide/helpers/date_...
```



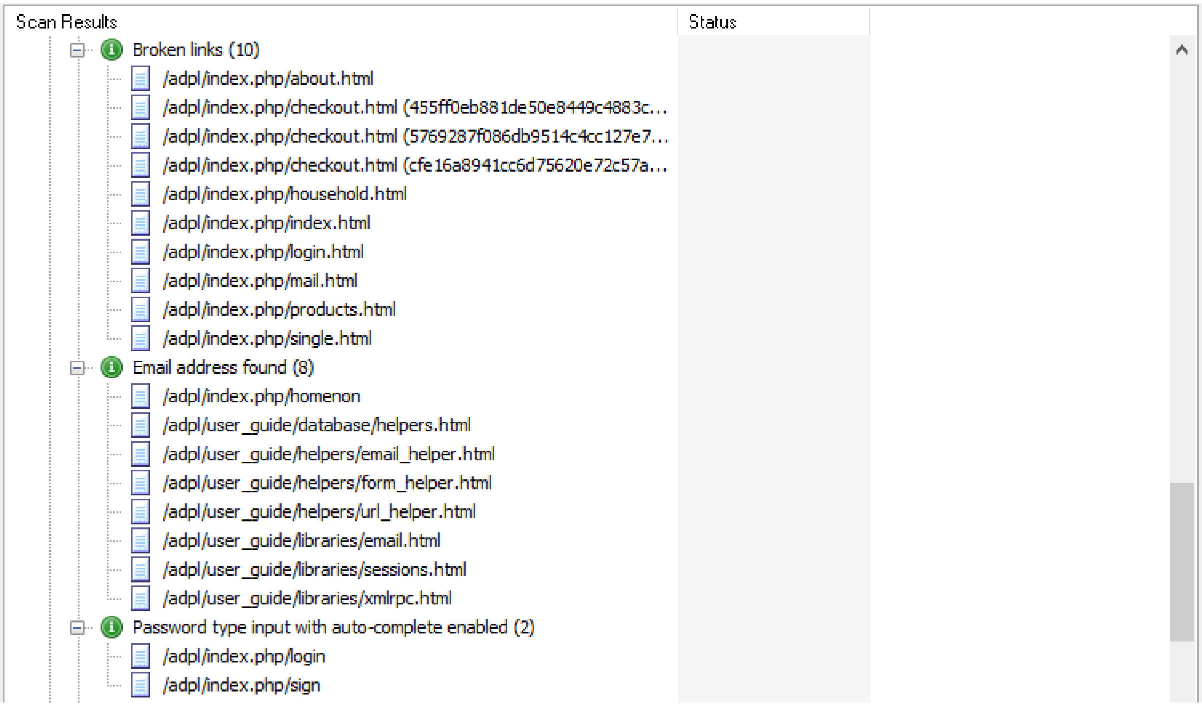
```
Scan Results                                                   Status
      ⊟ User credentials are sent in clear te...
           /adpl/index.php/login
           /adpl/index.php/sign
      ⊟ Vulnerable Javascript library (1)
           /adpl/user_guide/_static/jquery.js
```

Ditemukan 13 threat dengan kategori Low :

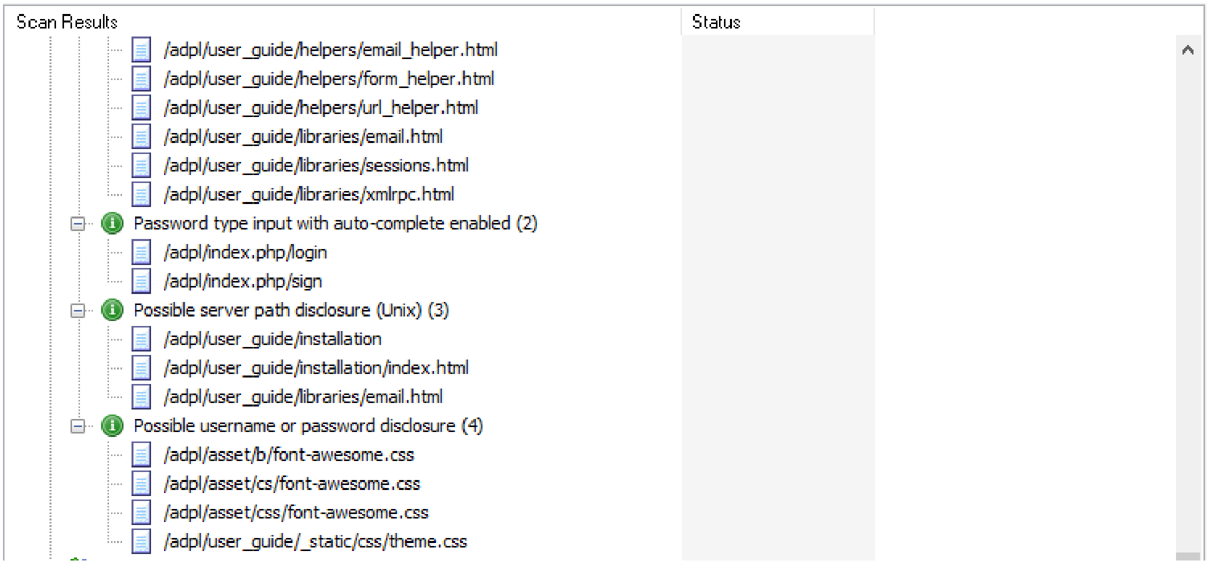


```
Scan Results                                                    Status
  Clickjacking: X-Frame-Options header missing (1)
    Web Server
  Documentation file (1)
    /adpl/license.txt
  Login page password-guessing attack (1)
    /adpl/index.php/login/aksi_login
  Possible sensitive directories (3)
    /adpl/nbproject
    /adpl/user_guide
    /adpl/user_guide/database
  Possible sensitive files (3)
    /adpl/.gitignore (2)
    /adpl/nbproject/project.xml
  Slow response time (3)
    /adpl/asset/j/jquery-1.11.1.min.js
    /adpl/asset/j/minicart.js
    /adpl/index.php/products.html
  TRACE method is enabled (1)
    Web Server
```

Ditemukan 27 Threat dengan kategori Informational :



```
Scan Results                                                    Status
  Broken links (10)
    /adpl/index.php/about.html
    /adpl/index.php/checkout.html (455ff0eb881de50e8449c4883c...
    /adpl/index.php/checkout.html (5769287f086db9514c4cc127e7...
    /adpl/index.php/checkout.html (cfe16a8941cc6d75620e72c57a...
    /adpl/index.php/household.html
    /adpl/index.php/index.html
    /adpl/index.php/login.html
    /adpl/index.php/mail.html
    /adpl/index.php/products.html
    /adpl/index.php/single.html
  Email address found (8)
    /adpl/index.php/homenon
    /adpl/user_guide/database/helpers.html
    /adpl/user_guide/helpers/email_helper.html
    /adpl/user_guide/helpers/form_helper.html
    /adpl/user_guide/helpers/url_helper.html
    /adpl/user_guide/libraries/email.html
    /adpl/user_guide/libraries/sessions.html
    /adpl/user_guide/libraries/xmlrpc.html
  Password type input with auto-complete enabled (2)
    /adpl/index.php/login
    /adpl/index.php/sign
```



```
Scan Results                                                      Status
        /adpl/user_guide/helpers/email_helper.html
        /adpl/user_guide/helpers/form_helper.html
        /adpl/user_guide/helpers/url_helper.html
        /adpl/user_guide/libraries/email.html
        /adpl/user_guide/libraries/sessions.html
        /adpl/user_guide/libraries/xmlrpc.html
    Password type input with auto-complete enabled (2)
        /adpl/index.php/login
        /adpl/index.php/sign
    Possible server path disclosure (Unix) (3)
        /adpl/user_guide/installation
        /adpl/user_guide/installation/index.html
        /adpl/user_guide/libraries/email.html
    Possible username or password disclosure (4)
        /adpl/asset/b/font-awesome.css
        /adpl/asset/cs/font-awesome.css
        /adpl/asset/css/font-awesome.css
        /adpl/user_guide/_static/css/theme.css
```

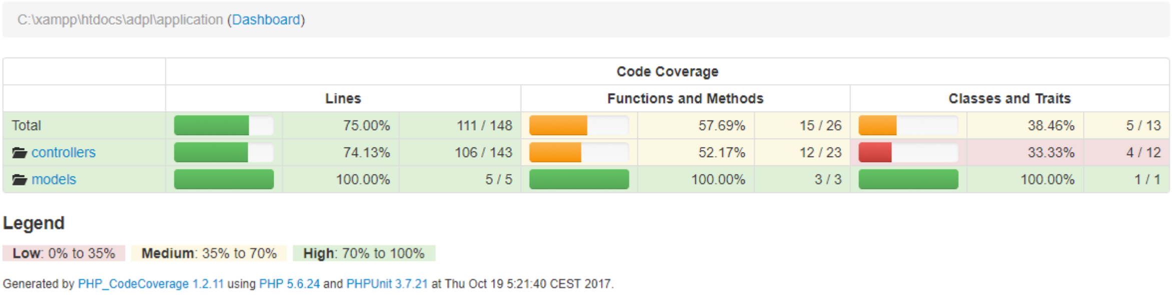
TEST Usability:

Pengujian	Sukses	Gagal
Mengklik tombol login redirect ke halaman login	v	
Mengklik tombol search redirect ke halaman search kos/kontrakan	v	
Login dengan username dan passowrd benar	v	
Login dengan username benar dan password random		v
login dengan username random dan password benar		v
login dengan username kosong dan password benar		v
login dengan username benar dan password kosong		v
login dengan username dan password kosong		v
Login dengan hak akses “user” bisa masuk ke halaman admin		v
Login dengan hak akses “user” tidak bisa masuk ke halaman admin	v	
Login dengan hak akses “user” bisa masuk ke dashboard user	v	
login dengan hak akses “admin” bisa masuk ke dashboard user		v
login dengan hak akses “admin” bisa masuk ke dashboard admin	v	
Klik list user bisa menampilkan list user di	v	

admin		
Klik list kontrakan bisa menampilkan list kontrakan di admin	v	
Klik signup di halaman login user bisa redirect ke halaman register	v	
klik logout bisa keluar dari halaman admin	v	
Klik masukkan persewaan di bagian user bisa redirect ke halaman input data kos	v	
Mengisi data kos dengan isi kosong bisa sukses input		v
klik logout user bisa keluar dari dashboard user	v	
Klik back (kembali) setelah logout user, bisa kembali ke halaman dashboard user	v	

TEST Code Coverage :

Hasil Code coverage :



C:\xampp\htdocs\adpl\application (Dashboard)

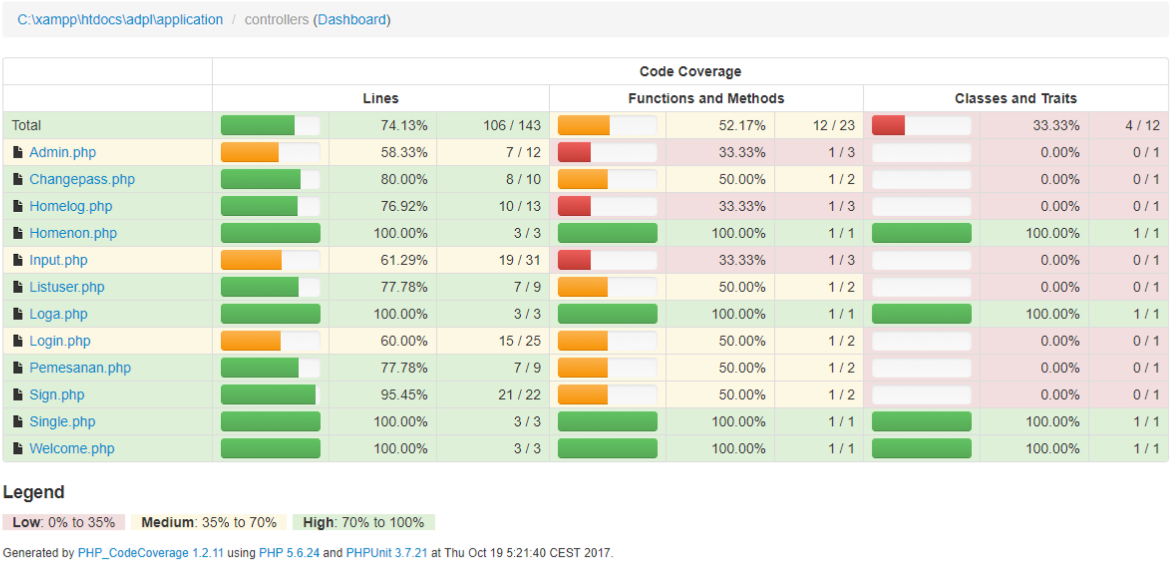
	Code Coverage								
	Lines			Functions and Methods			Classes and Traits		
Total	🟩	75.00%	111 / 148	🟧	57.69%	15 / 26	🟧	38.46%	5 / 13
controllers	🟩	74.13%	106 / 143	🟧	52.17%	12 / 23	🟥	33.33%	4 / 12
models	🟩	100.00%	5 / 5	🟩	100.00%	3 / 3	🟩	100.00%	1 / 1

Legend

Low: 0% to 35% **Medium**: 35% to 70% **High**: 70% to 100%

Generated by PHP_CodeCoverage 1.2.11 using PHP 5.6.24 and PHPUnit 3.7.21 at Thu Oct 19 5:21:40 CEST 2017.

Controller :



C:\xampp\htdocs\adpl\application / controllers (Dashboard)

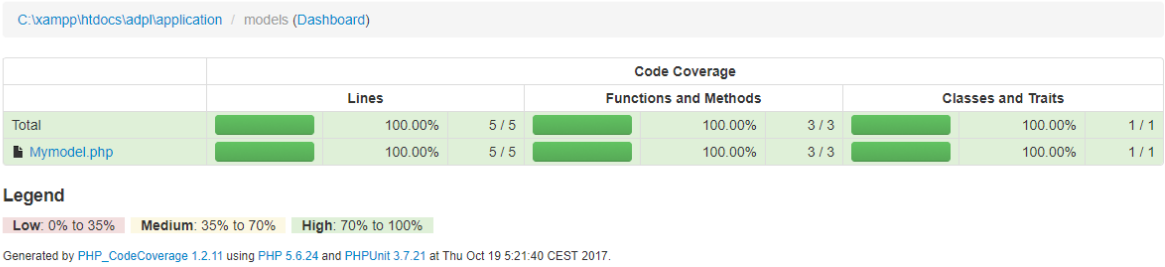
	Code Coverage								
	Lines			Functions and Methods			Classes and Traits		
Total	🟩	74.13%	106 / 143	🟧	52.17%	12 / 23	🟥	33.33%	4 / 12
Admin.php	🟧	58.33%	7 / 12	🟥	33.33%	1 / 3		0.00%	0 / 1
Changepass.php	🟩	80.00%	8 / 10	🟧	50.00%	1 / 2		0.00%	0 / 1
Homelog.php	🟩	76.92%	10 / 13	🟥	33.33%	1 / 3		0.00%	0 / 1
Homenon.php	🟩	100.00%	3 / 3	🟩	100.00%	1 / 1	🟩	100.00%	1 / 1
Input.php	🟧	61.29%	19 / 31	🟥	33.33%	1 / 3		0.00%	0 / 1
Listuser.php	🟩	77.78%	7 / 9	🟧	50.00%	1 / 2		0.00%	0 / 1
Loga.php	🟩	100.00%	3 / 3	🟩	100.00%	1 / 1	🟩	100.00%	1 / 1
Login.php	🟧	60.00%	15 / 25	🟧	50.00%	1 / 2		0.00%	0 / 1
Pemesanan.php	🟩	77.78%	7 / 9	🟧	50.00%	1 / 2		0.00%	0 / 1
Sign.php	🟩	95.45%	21 / 22	🟧	50.00%	1 / 2		0.00%	0 / 1
Single.php	🟩	100.00%	3 / 3	🟩	100.00%	1 / 1	🟩	100.00%	1 / 1
Welcome.php	🟩	100.00%	3 / 3	🟩	100.00%	1 / 1	🟩	100.00%	1 / 1

Legend

Low: 0% to 35% **Medium**: 35% to 70% **High**: 70% to 100%

Generated by PHP_CodeCoverage 1.2.11 using PHP 5.6.24 and PHPUnit 3.7.21 at Thu Oct 19 5:21:40 CEST 2017.

Model :



C:\xampp\htdocs\adpl\application / models (Dashboard)

	Code Coverage								
	Lines			Functions and Methods			Classes and Traits		
Total	🟩	100.00%	5 / 5	🟩	100.00%	3 / 3	🟩	100.00%	1 / 1
Mymodel.php	🟩	100.00%	5 / 5	🟩	100.00%	3 / 3	🟩	100.00%	1 / 1

Legend

Low: 0% to 35% **Medium**: 35% to 70% **High**: 70% to 100%

Generated by PHP_CodeCoverage 1.2.11 using PHP 5.6.24 and PHPUnit 3.7.21 at Thu Oct 19 5:21:40 CEST 2017.

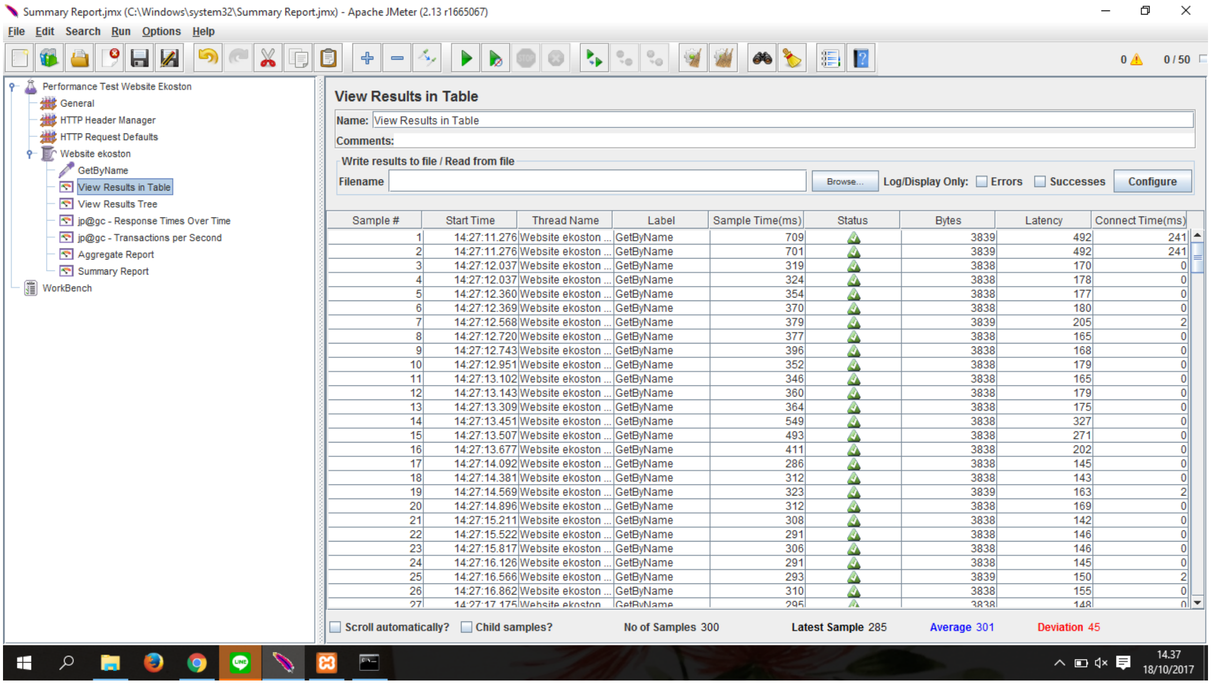
Test Case :

Test case terdapat pada netbeands

TEST Performance :

Test dengan menggunakan Jmeter :

View result in table :


Summary Report.jmx (C:\Windows\system32\Summary Report.jmx) - Apache JMeter (2.13 r1665067)
File Edit Search Run Options Help
0
0 / 50
Performance Test Website Ekoston
General
HTTP Header Manager
HTTP Request Defaults
Website ekoston
GetByName
View Results in Table
View Results Tree
jp@gc - Response Times Over Time
jp@gc - Transactions per Second
Aggregate Report
Summary Report
WorkBench
Browse...
Configure
14.37
18/10/2017

View Results in Table

Name: View Results in Table

Comments:

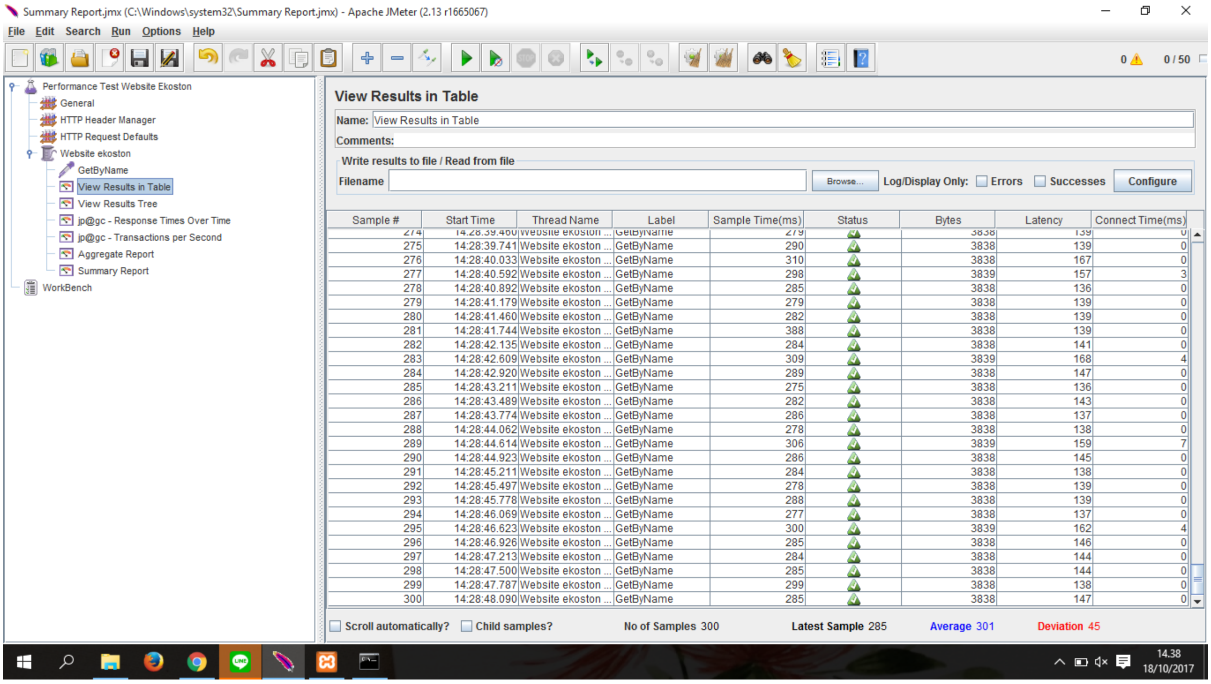
Write results to file / Read from file

Filename

Log/Display Only: □ Errors □ Successes

Sample #	Start Time	Thread Name	Label	Sample Time(ms)	Status	Bytes	Latency	Connect Time(ms)
1	14:27:11.276	Website ekoston ...	GetByName	709	✓	3839	492	241
2	14:27:11.276	Website ekoston ...	GetByName	701	✓	3839	492	241
3	14:27:12.037	Website ekoston ...	GetByName	319	✓	3838	170	0
4	14:27:12.037	Website ekoston ...	GetByName	324	✓	3838	178	0
5	14:27:12.360	Website ekoston ...	GetByName	354	✓	3838	177	0
6	14:27:12.369	Website ekoston ...	GetByName	370	✓	3838	180	0
7	14:27:12.568	Website ekoston ...	GetByName	379	✓	3839	205	2
8	14:27:12.720	Website ekoston ...	GetByName	377	✓	3838	165	0
9	14:27:12.743	Website ekoston ...	GetByName	396	✓	3838	168	0
10	14:27:12.951	Website ekoston ...	GetByName	352	✓	3838	179	0
11	14:27:13.102	Website ekoston ...	GetByName	346	✓	3838	165	0
12	14:27:13.143	Website ekoston ...	GetByName	360	✓	3838	179	0
13	14:27:13.309	Website ekoston ...	GetByName	364	✓	3838	175	0
14	14:27:13.451	Website ekoston ...	GetByName	549	✓	3838	327	0
15	14:27:13.507	Website ekoston ...	GetByName	493	✓	3838	271	0
16	14:27:13.677	Website ekoston ...	GetByName	411	✓	3838	202	0
17	14:27:14.092	Website ekoston ...	GetByName	286	✓	3838	145	0
18	14:27:14.381	Website ekoston ...	GetByName	312	✓	3838	143	0
19	14:27:14.569	Website ekoston ...	GetByName	323	✓	3839	163	2
20	14:27:14.896	Website ekoston ...	GetByName	312	✓	3838	169	0
21	14:27:15.211	Website ekoston ...	GetByName	308	✓	3838	142	0
22	14:27:15.522	Website ekoston ...	GetByName	291	✓	3838	146	0
23	14:27:15.817	Website ekoston ...	GetByName	306	✓	3838	146	0
24	14:27:16.126	Website ekoston ...	GetByName	291	✓	3838	145	0
25	14:27:16.566	Website ekoston ...	GetByName	293	✓	3839	150	2
26	14:27:16.862	Website ekoston ...	GetByName	310	✓	3838	155	0
27	14:27:17.175	Website ekoston	GetByName	295	✓	3838	148	0

□ Scroll automatically? □ Child samples? No of Samples 300 Latest Sample 285 Average 301 Deviation 45


Summary Report.jmx (C:\Windows\system32\Summary Report.jmx) - Apache JMeter (2.13 r1665067)
File Edit Search Run Options Help
0
0 / 50
Performance Test Website Ekoston
General
HTTP Header Manager
HTTP Request Defaults
Website ekoston
GetByName
View Results in Table
View Results Tree
jp@gc - Response Times Over Time
jp@gc - Transactions per Second
Aggregate Report
Summary Report
WorkBench
Browse...
Configure
14.38
18/10/2017

View Results in Table

Name: View Results in Table

Comments:

Write results to file / Read from file

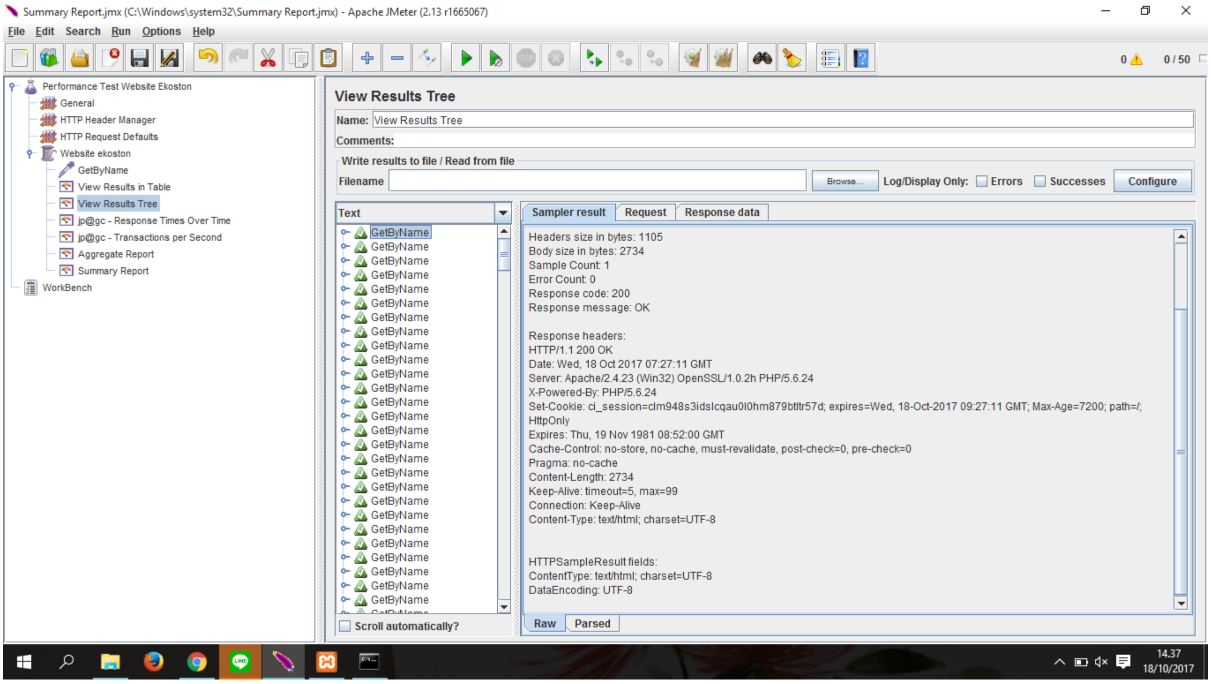
Filename

Log/Display Only: □ Errors □ Successes

Sample #	Start Time	Thread Name	Label	Sample Time(ms)	Status	Bytes	Latency	Connect Time(ms)
274	14:28:39.460	Website ekoston ...	GetByName	279	✓	3838	139	0
275	14:28:39.741	Website ekoston ...	GetByName	290	✓	3838	139	0
276	14:28:40.033	Website ekoston ...	GetByName	310	✓	3838	167	0
277	14:28:40.592	Website ekoston ...	GetByName	298	✓	3839	157	3
278	14:28:40.892	Website ekoston ...	GetByName	285	✓	3838	136	0
279	14:28:41.179	Website ekoston ...	GetByName	279	✓	3838	139	0
280	14:28:41.460	Website ekoston ...	GetByName	282	✓	3838	139	0
281	14:28:41.744	Website ekoston ...	GetByName	388	✓	3838	139	0
282	14:28:42.135	Website ekoston ...	GetByName	284	✓	3838	141	0
283	14:28:42.609	Website ekoston ...	GetByName	309	✓	3839	168	4
284	14:28:42.920	Website ekoston ...	GetByName	289	✓	3838	147	0
285	14:28:43.211	Website ekoston ...	GetByName	275	✓	3838	136	0
286	14:28:43.489	Website ekoston ...	GetByName	282	✓	3838	143	0
287	14:28:43.774	Website ekoston ...	GetByName	286	✓	3838	137	0
288	14:28:44.062	Website ekoston ...	GetByName	278	✓	3838	138	0
289	14:28:44.614	Website ekoston ...	GetByName	306	✓	3839	159	7
290	14:28:44.923	Website ekoston ...	GetByName	286	✓	3838	145	0
291	14:28:45.211	Website ekoston ...	GetByName	284	✓	3838	138	0
292	14:28:45.497	Website ekoston ...	GetByName	278	✓	3838	139	0
293	14:28:45.778	Website ekoston ...	GetByName	288	✓	3838	139	0
294	14:28:46.069	Website ekoston ...	GetByName	277	✓	3838	137	0
295	14:28:46.623	Website ekoston ...	GetByName	300	✓	3839	162	4
296	14:28:46.926	Website ekoston ...	GetByName	285	✓	3838	146	0
297	14:28:47.213	Website ekoston ...	GetByName	284	✓	3838	144	0
298	14:28:47.500	Website ekoston ...	GetByName	285	✓	3838	144	0
299	14:28:47.787	Website ekoston ...	GetByName	299	✓	3838	138	0
300	14:28:48.090	Website ekoston ...	GetByName	285	✓	3838	147	0

□ Scroll automatically? □ Child samples? No of Samples 300 Latest Sample 285 Average 301 Deviation 45

View result in tree :



Summary Report.jmx (C:\Windows\system32\Summary Report.jmx) - Apache JMeter (2.13 r1665067)

Name: View Results Tree

Comments:

Filename

Log/Display Only: □ Errors □ Successes Configure

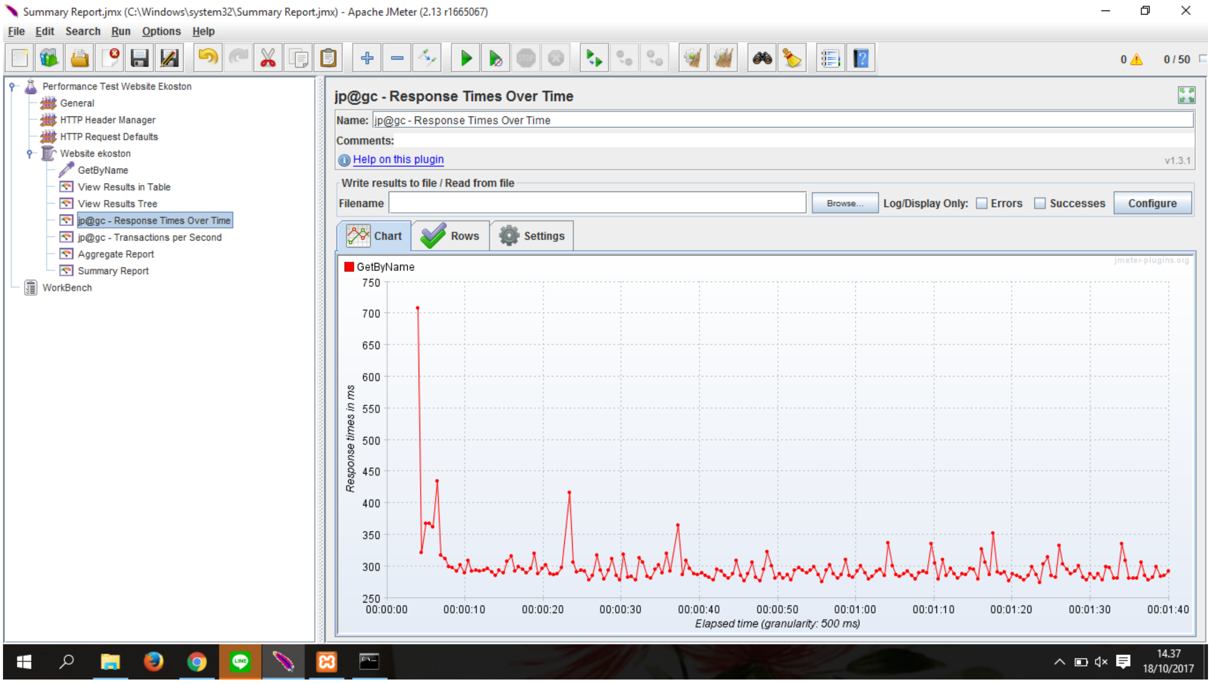
□ Scroll automatically?

```
Headers size in bytes: 1105
Body size in bytes: 2734
Sample Count: 1
Error Count: 0
Response code: 200
Response message: OK

Response headers:
HTTP/1.1 200 OK
Date: Wed, 18 Oct 2017 07:27:11 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.24
X-Powered-By: PHP/5.6.24
Set-Cookie: ci_session=clm948s3idslcqau0l0hm879btltr57d; expires=Wed, 18-Oct-2017 09:27:11 GMT; Max-Age=7200; path=/;
HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 2734
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


HTTPSampleResult fields:
ContentType: text/html; charset=UTF-8
DataEncoding: UTF-8
```

Response Times Over Time :



Summary Report.jmx (C:\Windows\system32\Summary Report.jmx) - Apache JMeter (2.13 r1665067)

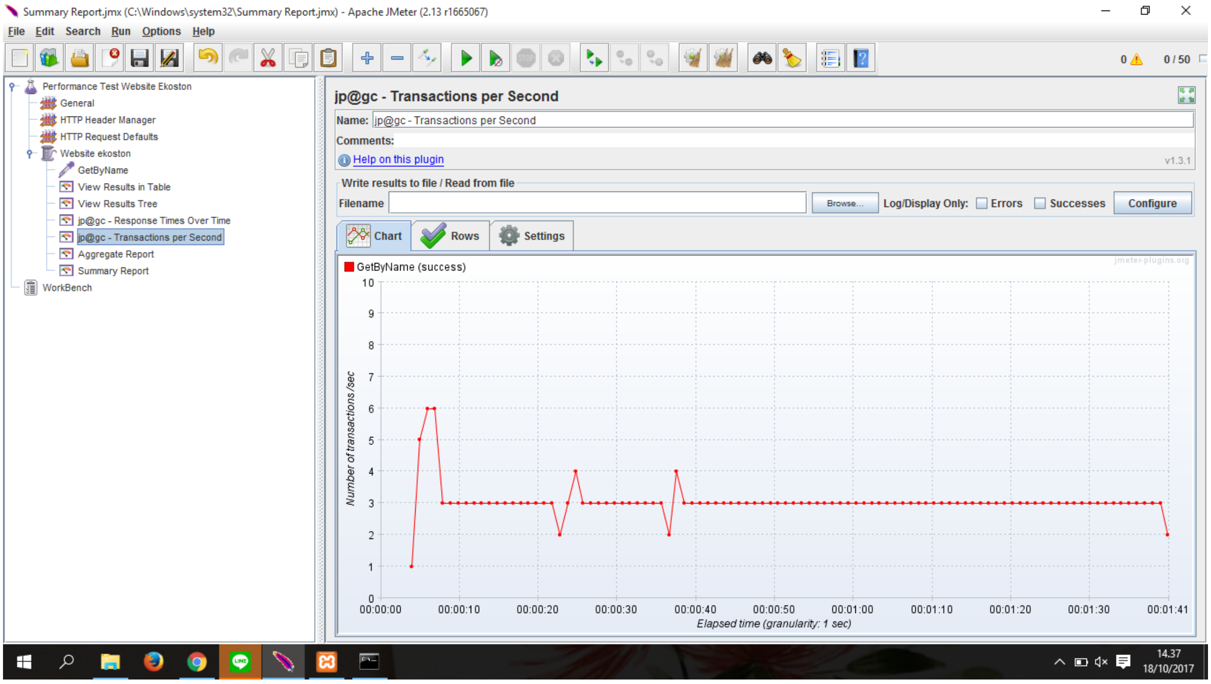
Name: jp@gc - Response Times Over Time

Comments:

Filename

Log/Display Only: □ Errors □ Successes Configure

Transactions per seconds:



Summary Report.jmx (C:\Windows\system32\Summary Report.jmx) - Apache JMeter (2.13 r1665067)

- Performance Test Website Ekoston
  - General
  - HTTP Header Manager
  - HTTP Request Defaults
  - Website ekoston
    - GetByName
    - View Results in Table
    - View Results Tree
    - jp@gc - Response Times Over Time
    - jp@gc - Transactions per Second
    - Aggregate Report
    - Summary Report
- WorkBench

jp@gc - Transactions per Second

Name: jp@gc - Transactions per Second

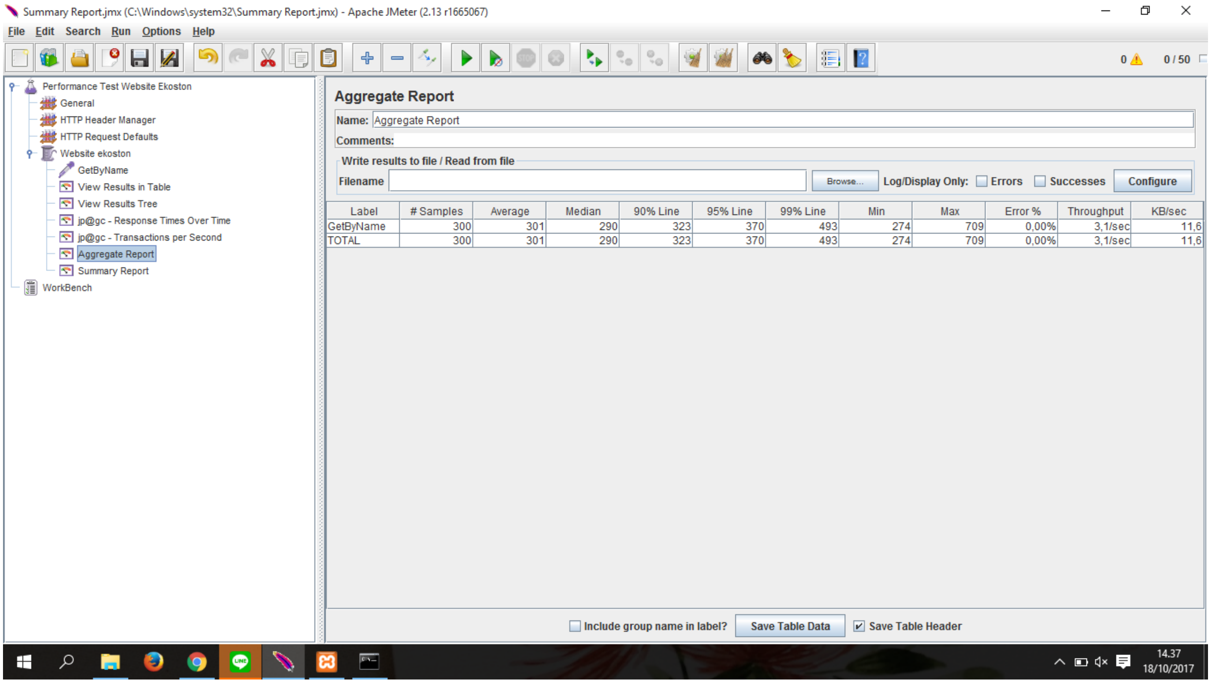
Comments:

Help on this plugin v1.3.1

Write results to file / Read from file

Filename Browse... Log/Display Only: □ Errors □ Successes Configure

Agregate report :



Summary Report.jmx (C:\Windows\system32\Summary Report.jmx) - Apache JMeter (2.13 r1665067)

- Performance Test Website Ekoston
  - General
  - HTTP Header Manager
  - HTTP Request Defaults
  - Website ekoston
    - GetByName
    - View Results in Table
    - View Results Tree
    - jp@gc - Response Times Over Time
    - jp@gc - Transactions per Second
    - Aggregate Report
    - Summary Report
- WorkBench

Aggregate Report

Name: Aggregate Report

Comments:

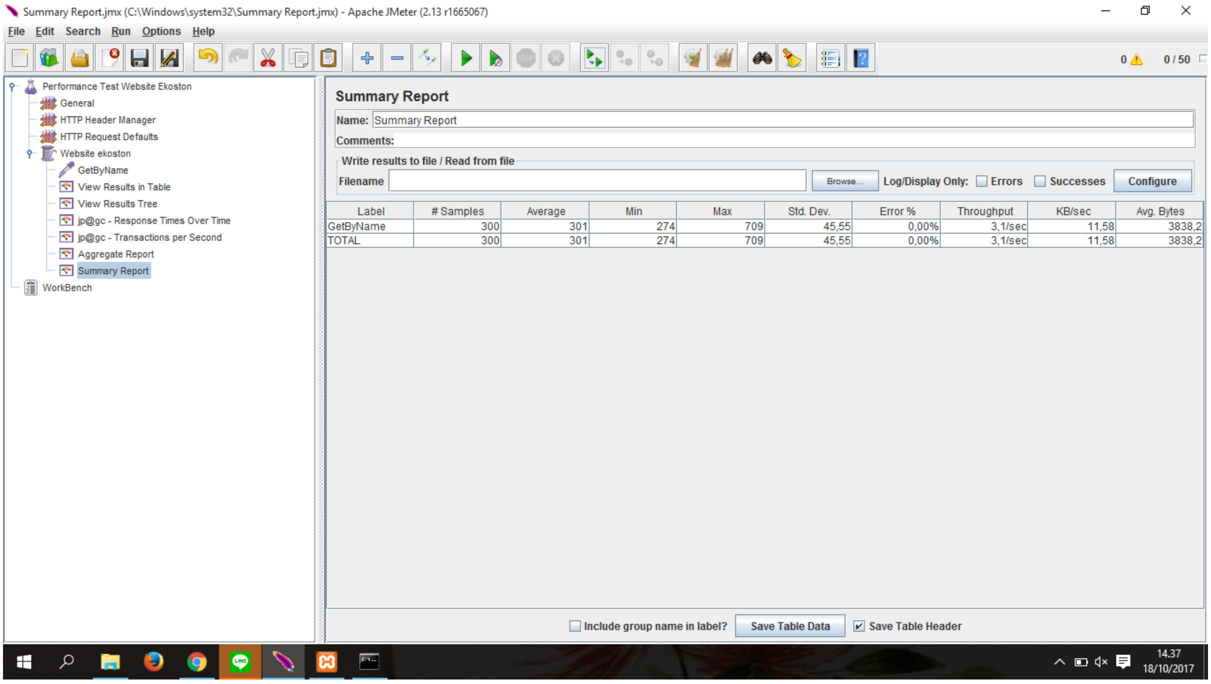
Write results to file / Read from file

Filename Browse... Log/Display Only: □ Errors □ Successes Configure

Label	# Samples	Average	Median	90% Line	95% Line	99% Line	Min	Max	Error %	Throughput	KB/sec
GetByName	300	301	290	323	370	493	274	709	0,00%	3,1/sec	11,6
TOTAL	300	301	290	323	370	493	274	709	0,00%	3,1/sec	11,6

□ Include group name in label? Save Table Data ☑ Save Table Header

Summary Report :



Summary Report.jmx (C:\Windows\system32\Summary Report.jmx) - Apache JMeter (2.13 r1665067)

- Performance Test Website Ekoston
  - General
  - HTTP Header Manager
  - HTTP Request Defaults
  - Website ekoston
    - GetByName
    - View Results in Table
    - View Results Tree
    - jp@gc - Response Times Over Time
    - jp@gc - Transactions per Second
    - Aggregate Report
    - Summary Report
- WorkBench

Summary Report

Name: Summary Report

Comments:

Write results to file / Read from file

Filename ____ Browse... Log/Display Only: □ Errors □ Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	KB/sec	Avg. Bytes
GetByName	300	301	274	709	45,55	0,00%	3,1/sec	11,58	3838,2
TOTAL	300	301	274	709	45,55	0,00%	3,1/sec	11,58	3838,2

□ Include group name in label? Save Table Data ☑ Save Table Header