# Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)

**Mohmmad Muhsin, Adi Fajaryanto**

Fakultas Teknik
Universitas Muhammadiyah Ponorogo
Email : mmuhsin69@gmail.com, adifajaryanto@gmail.com

**Abstrak**

Fakultas Teknik Universitas Muhammadiyah Ponorogo telah menerapkan Ujian Tengah Semester dan Ujian Akhir Semester menggunakan aplikasi "Si Ujo (Sistem Ujian Online) berbasis web. Sejak tahun 2012 sampai tahun 2014, Si Ujo telah beberapa kali mengalami pengembangan baik dari sisi fitur maupun data yang disimpan. Data tersebut menyimpan data nilai matakuliah setiap mahasiswa teknik Universitas Muhammadiyah Ponorogo. Mengingat pentingnya data yang tersimpan maka perlu diterapkan pengujian keamanan dari aplikasi Si Ujo. Pengujian keamanan tersebut dilakukan untuk mengetahui tingkat kerentanan agar terhindar dari serangan dari pihak yang tidak bertanggung jawab. Salah satu metode untuk menguji aplikasi berbasis web adalah metode OWASP (Open Web Application Security Project) versi 4 yang dikeluarkan oleh owasp.org sebuah organisasi non profit yang berdedikasi pada keamanan aplikasi berbasis web. Hasil pengujian menggunakan OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak stake holder Fakultas Teknik Universitas Muhammadiyah Ponorogo

***Kata kunci:*** *web server, pentest, owasp, framework.*

## PENDAHULUAN

Tahun 2012 Fakultas Teknik Universitas Muhammadiyah Ponorogo telah menerapkan Ujian Tengah Semester dan Ujian Akhir Semester menggunakan aplikasi "Si Ujo (Sistem Ujian Online) berbasis web. Sejak tahun 2012 sampai tahun 2014, Si Ujo telah beberapa kali mengalami pengembangan baik dari sisi fitur maupun data yang disimpan.

Data yang tersimpan pada database Si Ujo berdasarkan hasil wawancara dengan admin Si Ujo telah mencapai 100 megabyte. Database tersebut menyimpan data nilai matakuliah setiap mahasiswa teknik Universitas Muhammadiyah Ponorogo. Mengingat pentingnya data yang tersimpan maka perlu diterapkan pengujian keamanan dari aplikasi Si Ujo. Pengujian keamanan tersebut dilakukan untuk mengetahui tingkat kerentanan agar terhindar dari serangan dari pihak yang tidak bertanggung jawab.

Salah satu metode untuk menguji aplikasi berbasis web adalah metode OWASP (Open Web Application Security Project) versi 4 yang dikeluarkan oleh owasp.org sebuah organisasi non profit yang berdedikasi pada keamanan aplikasi berbasis web. Metode ini bebas digunakan oleh siapa saja yang ingin mengetahui kerentanan dari sebuah aplikasi web.

Dari penjelasan pada latar belakang diatas maka dilakukan penelitian untuk menerapkan pengujian keamanan aplikasi Ujian Online menggunakan metode OWASP versi 4 agar dapat diketahui tingkat kerentanan yang ada.

## PERUMUSAN MASALAH

Melihat latar belakang diatas maka akan rumusan masalah dari penelitian ini adalah sebagai berikut :

1. Bagaimana mengidentifikasi kerentanan aplikasi Ujian Online Fakultas Teknik Universitas Muhammadiyah Ponorogo?
2. Bagaimana hasil pengujian kerentanan aplikasi Ujian Online menggunakan metode OWASP versi 4?
3. Bagaimana analisa hasil dari penerapan metode OWASP versi 4 pada aplikasi Ujian Online?

## TUJUAN

Tujuan dari penelitian ini adalah :

1. Mengetahui kerentanan aplikasi Ujian Online Fakultas Teknik Universitas Muhammadiyah Ponorogo
2. Mengetahui hasil pengujian kerentanan aplikasi Ujian Online Fakultas Teknik Universitas Muhammadiyah Ponorogo
3. Mengetahui hasil analisa dari penerapan pengujian metode OWASP versi 4

## BATASAN MASALAH

Batasan masalah dalam objek penelitian ini adalah:

1. Studi yang dilakukan hanya terbatas pada pengujian keamanan aplikasi web menggunakan framework OWASP versi 4 fokus pada Authentication Testing, Authorization Testing, Session Management Testing.
2. Metode pengujian keamanan diterapkan pada pemodelan aplikasi Ujian Online Fakultas Teknik Universitas Muhammadiyah Ponorogo

## TINJAUAN PUSTAKA

### Penetration Test

Pengujian keamanan dapat melakukan tiga jenis test (Whitaker & Newman, 2005), antara lain :

1. Black-box test, penetration tester tidak memiliki pengetahuan tentang jaringan perusahaan sebelumnya. Apabila test ini dilakukan maka tester mungkin akan diberikan alamat situs web atau alamat IP dan diberitahu untuk mencoba menyusup seolah-olah ia seorang hacker jahat luar.
2. White-box test, tester memiliki pengetahuan tentang jaringan internal yang lengkap. Tester mungkin diberikan peta jaringan atau daftar sistem operasi yang ada dan aplikasi yang terinstall sebelum melakukan tes. Meskipun bukan yang paling representatif dari serangan luar, tes jenis ini merupakan yang paling akurat karena menyajikan skenario terburuk di mana penyerang memiliki pengetahuan lengkap tentang jaringan yang ada.
3. Gray-box test, tester memposisikan diri sebagai karyawan dalam suatu perusahaan. Tester diberikan akun di jaringan internal dan akses standar ke jaringan. Tes ini dilakukan untuk menilai ancaman internal dari karyawan dalam perusahaan.

### OWAPS versi 4

OWASP merupakan organisasi non-profit amal di Amerika Serikat yang didirikan pada tanggal 21 April 2004 yang berdedikasi untuk membuat *framework* pengujian keamanan yang bebas digunakan oleh siapa saja.

Framework yang digunakan pada OWASP versi 4 adalah sebagai berikut :

- Authentication Testing

  Otentikasi merupakan tindakan membangun dan mengkonfirmasi sesuatu bahwa klaim yang dibuat adalah benar. Otentikasi sebuah objek dapat berarti mengkonfirmasikan sumbernya, sedangkan otentikasi seseorang sering terdiri dari verifikasi identitasnya. Otentikasi tergantung pada satu atau lebih faktor otentikasi.

  Dalam keamanan komputer, otentikasi adalah proses mencoba untuk memverifikasi identitas digital pengirim komunikasi. Sebuah contoh umum dari proses tersebut adalah log proses. Pengujian skema otentikasi berarti memahami bagaimana proses otentikasi bekerja dan menggunakan informasi tersebut untuk menghindari mekanisme otentikasi.

- Authorization Testing

  Otorisasi merupakan konsep yang memungkinkan akses ke sumber daya bagi mereka yang diizinkan untuk menggunakannya. Pengujian untuk otorisasi berarti memahami bagaimana proses otorisasi bekerja, dan menggunakan informasi tersebut untuk menghindari mekanisme otorisasi.

  Otorisasi adalah proses yang datang setelah otentikasi berhasil, sehingga tester akan memverifikasi titik ini setelah ia memegang identitas yang sah. Selama ini jenis penilaian, harus diverifikasi apakah mungkin untuk memotong skema otorisasi, menemukan kerentanan jalur traversal, atau menemukan cara untuk meningkatkan hak-hak istimewa yang ditugaskan untuk tester.

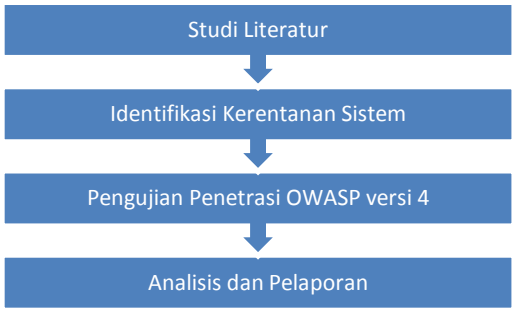
- Session Management Testing

  Session Management didefinisikan sebagai himpunan semua kontrol yang mengatur interaksi full state antara pengguna dan aplikasi berbasis web (Matteo Meucci and Friends : 2014). Ini secara luas mencakup apa pun dari bagaimana otentikasi pengguna dilakukan, bagaimana mereka logout.

  Lingkungan aplikasi web yang populer, seperti ASP dan PHP, memberikan pengembang dengan built-in rutinitas penanganan sesi. Beberapa jenis identifikasi token biasanya akan dikeluarkan, yang akan disebut sebagai "ID Sesi" atau Cookie.

## METODE PENELITIAN

Metode penelitian ini diselesaikan dengan tahap-tahap kegiatan dalam Gambar 3.1.




Gambar 3.1 Tahapan Penelitian

### Studi Literatur

Tahap ini bertujuan untuk menjelaskan kajian pustaka dari teori-teori penunjang yang mendukung konstruksi penelitian. Kegiatan ini dilakukan dengan membaca buku, jurnal, artikel laporan penelitian, dan situs-situs di internet.

**Identifikasi Kerentanan Sistem**

Identifikasi kerentanan pada model web server IKIP PGRI Madiun menggunakan aplikasi Acunetix.

**Implementasi Pengujian OWAPS versi 4**

OWASP merupakan organisasi non-profit amal di Amerika Serikat yang didirikan pada tanggal 21 April 2004 yang berdedikasi untuk membuat *framework* pengujian keamanan yang bebas digunakan oleh siapa saja.

Framework yang digunakan pada OWASP versi 4 adalah sebagai berikut :

- Authentication Testing

  Otentikasi merupakan tindakan membangun dan mengkonfirmasi sesuatu bahwa klaim yang dibuat adalah benar. Otentikasi sebuah objek dapat berarti mengkonfirmasikan sumbernya, sedangkan otentikasi seseorang sering terdiri dari verifikasi identitasnya. Otentikasi tergantung pada satu atau lebih faktor otentikasi.

  Dalam keamanan komputer, otentikasi adalah proses mencoba untuk memverifikasi identitas digital pengirim komunikasi. Sebuah contoh umum dari proses tersebut adalah log proses. Pengujian skema otentikasi berarti memahami bagaimana proses otentikasi bekerja dan menggunakan informasi tersebut untuk menghindari mekanisme otentikasi.
- Authorization Testing

  Otorisasi merupakan konsep yang memungkinkan akses ke sumber daya bagi mereka yang diizinkan untuk menggunakannya. Pengujian untuk otorisasi berarti memahami bagaimana proses otorisasi bekerja, dan menggunakan informasi tersebut untuk menghindari mekanisme otorisasi.

  Otorisasi adalah proses yang datang setelah otentikasi berhasil, sehingga tester akan memverifikasi titik ini setelah ia memegang identitas yang sah. Selama ini jenis penilaian, harus diverifikasi apakah mungkin untuk memotong skema otorisasi, menemukan kerentanan jalur traversal, atau menemukan cara untuk meningkatkan hak-hak istimewa yang ditugaskan untuk tester.
- Session Management Testing

  Session Management didefinisikan sebagai himpunan semua kontrol yang mengatur interaksi full state antara pengguna dan aplikasi berbasis web (Matteo Meucci and Friends : 2014). Ini secara luas mencakup apa pun dari bagaimana otentikasi pengguna dilakukan, bagaimana mereka logout.

  Lingkungan aplikasi web yang populer, seperti ASP dan PHP, memberikan pengembang dengan built-in rutinitas penanganan sesi. Beberapa jenis identifikasi token biasanya akan dikeluarkan, yang akan disebut sebagai "ID Sesi" atau Cookie.

**PEMBAHASAN**

**Identifikasi Kerentanan**

Identifikasi kerentanan dalam penelitian ini menggunakan aplikasi Acunetix untuk mengetahui tingkat kerentanan yang ada. Berikut adalah hasil *scan* Acunetix :

## Scan of 192.168.0.200

### Scan details

| Scan information | |
|---|---|
| Starttime | 07/07/2015 8:57:45 |
| Finish time | 07/07/2015 9:02:52 |
| Scan time | 5 minutes, 7 seconds |
| Profile | Default |

| Server information | |
|---|---|
| Responsive | True |
| Server banner | Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 |
| Server OS | Windows |
| Server technologies | PHP,mod_ssl,mod_perl,OpenSSL,Perl |

### Threat level


**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

### Alerts distribution

| | |
|---|---|
| **Total alerts found** | **316** |
| High | 3 |
| Medium | 144 |
| Low | 12 |
| Informational | 157 |

### Executive summary

| Alert group | Severity |
|---|---|
| Cross Site Scripting | High |
| Apache httpd Remote Denial of Service | Medium |
| Application error message | Medium |
| Backup files | Medium |
| Directory Listing | Medium |
| Error message on page | Medium |
| PHP hangs on parsing particular strings as floating point number | Medium |
| Login page password-guessing attack | Low |

| | |
|---|---|
| Session Cookie without HttpOnly flag set | Low |
| Session Cookie without Secure flag set | Low |
| TRACE method is enabled | Low |
| TRACK method is enabled | Low |
| User credentials are sent in clear text | Low |
| Broken links | Informational |
| Email address found | Informational |
| GHDB | Informational |
| Password type input with autocomplete enabled | Informational |
| Possible internal IP address disclosure | Informational |
| Possible username or password disclosure | Informational |

Berdasarkan infomasi diatas dapat diidentifikasi kerentanan dari Aplikasi Ujian Online mempunyaoi tingkat kerentanan tinggi. Dengan tingginya tingkat kerentanan yang ada maka dilakukan pengujian lanjut dengan menggunakan OWASP versi 4.

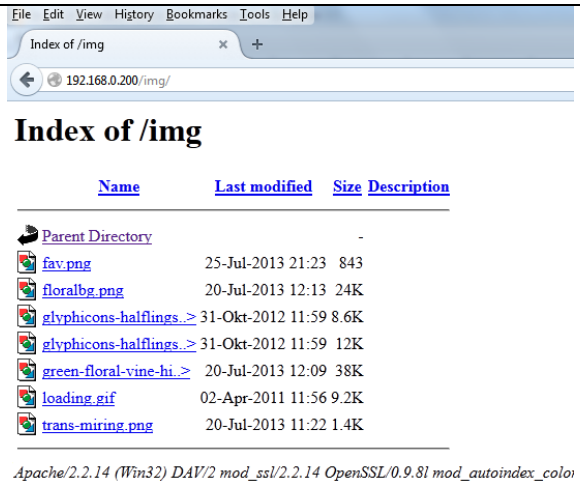
**Penetrasi OWASP versi 4**

Dalam pengujian ini dilakukan pengujian pada alamat 192.168.0.200/dosen saja, hal ini dilakukan sebab penelitian ini difokuskan pada penggunaan dosen seperti terlihat pada tabel 4.1

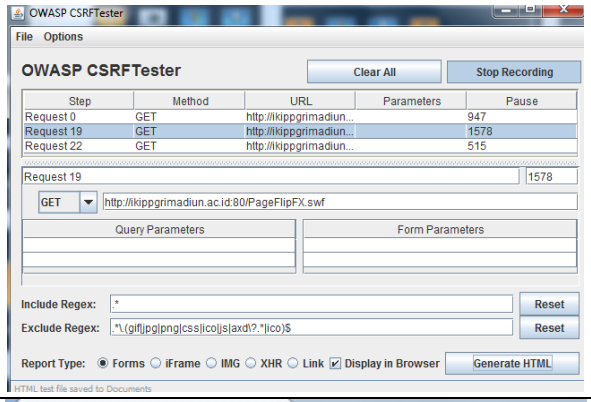
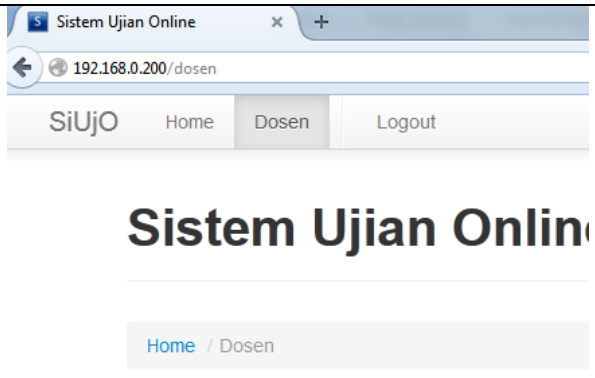
**Tabel 4.1 Hasil Pengujian OWASP versi 4**

| Tahapan | Tool | Hasil | Status |
|---|---|---|---|
| Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001) | WebScarab | POST /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 29<br><br>kode=999999&password=dload123 | X |
| Testing for default credentials (OTG-AUTHN-002) | Brutus | Proses brute force selama 7 jam tidak berhasil | OK |
| Testing for Weak lock out mechanism (OTG-AUTHN-003) | Browser Mozilla Firefox | Tidak ada mekanisme penguncian | X |
| Testing for bypassing | WebScarab | ---- Scanning URL: http://192.168.0.200/ ----<br>FOUND: http://192.168.0.200/ [STATE: 403 - 296] | X |

| Tahapan | Tool | Hasil | Status |
|---|---|---|---|
| authentication schema (OTG-AUTHN-004) | | (*) DIRECTORY: http://192.168.0.200/css<br>(*) DIRECTORY: http://192.168.0.200/foto<br>(*) DIRECTORY: http://192.168.0.200/images<br>(*) DIRECTORY: http://192.168.0.200/img<br>(*) DIRECTORY: http://192.168.0.200/js | |
| Test remember password functionality (OTG-AUTHN-005) | WebScarab | POST /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 29<br><br>kode=999999&password=dload123 | X |
| Testing for Browser cache weakness (OTG-AUTHN-006) | Browser Mozilla Firefox | POST /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 29<br><br>kode=999999&password=dload123 | X |
| Testing for Weak password policy (OTG-AUTHN-007) | Brutus | Proses brute force selama 5 jam tidak berhasil | OK |
| Testing for Weak security question/answer (OTG-AUTHN-008) | - | Fitur lupa password tidak ada, apabila user lupa password langsung menghubungi admin | OK |
| Testing for weak password change or reset functionalities (OTG- | - | Tidak ada fitur reset password | OK |

| Tahapan | Tool | Hasil | Status |
|---|---|---|---|
| AUTHN-009) | | | |
| Testing for Weaker authentication in alternative channel (OTG-AUTHN-010) | - | Tidak ada akses lain selain website utama | OK |
| Testing Directory traversal/file include (OTG-AUTHZ-001) | WFuzz | Tidak berhasil menemukan dokumen root maupun root *directory* | OK |
| Testing for bypassing authorization schema (OTG-AUTHZ-002) | Dirb | ---- Scanning URL: http://192.168.0.200/ ----<br>FOUND: http://192.168.0.200/ [STATE: 403 - 296]<br>(*) DIRECTORY: http://192.168.0.200/css<br>(*) DIRECTORY: http://192.168.0.200/foto<br>(*) DIRECTORY: http://192.168.0.200/images<br>(*) DIRECTORY: http://192.168.0.200/img<br>(*) DIRECTORY: http://192.168.0.200/js | X |
| Testing for Privilege Escalation (OTG-AUTHZ-003) | WebScarab | Tidak ada | OK |
| Testing for Insecure Direct Object References (OTG-AUTHZ-004) | Browser Mozilla Firefox |  | X |
| Testing for Bypassing Session Management Schema (OTG-SESS-001) | Dirb | ---- Scanning URL: http://192.168.0.200/ ----<br>FOUND: http://192.168.0.200/ [STATE: 403 - 296]<br>(*) DIRECTORY: http://192.168.0.200/css<br>(*) DIRECTORY: http://192.168.0.200/foto<br>(*) DIRECTORY: http://192.168.0.200/images<br>(*) DIRECTORY: http://192.168.0.200/img<br>(*) DIRECTORY: http://192.168.0.200/js | X |
| Testing for Cookies | Zed Attack | POST /dosen HTTP/1.1<br>Host: 192.168.0.200 | OK |

| Tahapan | Tool | Hasil | Status |
|---|---|---|---|
| attributes (OTG-SESS-002) | Proxy | User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 29<br><br>kode=999999&password=dload123<br><br>GET /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive | |
| Testing for Session Fixation (OTG-SESS-003) | Zed Attack Proxy | POST /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 29<br><br>kode=999999&password=dload123<br><br>GET /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive | OK |
| Testing for Exposed | Zed Attack | POST /dosen HTTP/1.1<br>Host: 192.168.0.200 | OK |

| Tahapan | Tool | Hasil | Status |
|---|---|---|---|
| Session Variables (OTG-SESS-004) | Proxy | User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 29<br><br>kode=999999&password=dload123<br><br>GET /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive | |
| Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005) | OWASP CSRF Tester |  | X |
| Testing for logout functionality (OTG-SESS-006) | Browser Mozilla Firefox |  | OK |
| Test Session Timeout (OTG-SESS-007) | Browser Mozilla Firefox | Tidak ada session timeout | X |

| Tahapan | Tool | Hasil | Status |
|---|---|---|---|
| Testing for Session puzzling (OTG-SESS-008) | Zed Attack Proxy | POST /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 29<br><br>kode=999999&password=dload123<br><br>GET /dosen HTTP/1.1<br>Host: 192.168.0.200<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8<br>Accept-Language: en-US,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Referer: http://192.168.0.200/dosen<br>Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7<br>Connection: keep-alive | X |

Dari tabel 4.1 terlihat bahwa pada proses otentifikasi terdapat kerentanan yaitu pada pengujian OTG-AUTHN-001, OTG-AUTHN-003, OTG-AUTHN-004, OTG-AUTHN-005, OTG-AUTHN-006 sehingga proses ini perlu mendapat perbaikan. Pada proses pengujian otorisasi terdapat kerentanan pada OTG-AUTHZ-002, OTG-AUTHZ-004, namun setelah dilakukan pengecekan diatas hasilnya adalah *false alarm* sehingga proses otorisasi sudah berjalan dengan baik, sedangkan pada manajemen sesi terdapat kerentanan pada OTG-SESS-001, OTG-SESS-005, OTG-SESS-007, OTG-SESS-008. Tidak adanya *session timeout* memungkinkan pemakai yang meninggalkan komputer dimanfaatkan oleh pemakai lain yang tidak berhak. Pada OTG-SESS-008, aplikasi ini menggunakan variabel session yang sama selama lebih dari satu tujuan sehingga penyerang dapat mengakses halaman secara acak.

## KESIMPULAN DAN SARAN

### Kesimpulan

Hasil pengujian menggunakan OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak stake holder Fakultas Teknik Universitas Muhammadiyah Ponorogo

### Saran

Berdasarkan kesimpulan diatas maka perlu dilakukan penelitian dengan metode ISSAF (Information System Security

Assessment Framework) agar dapat diketahui kerentanan dari sisi web server.

## DAFTAR PUSTAKA


Alfred Basta, W. H. (2008). *Computer Security and Penetration Testing.*

Allsopp, W. (2009). *Unauthorised Access: Physical Penetration Testing for it Security Teams.*

*Assosiasi Penyelenggara Jasa Internet Indoneisa*. (2012). Retrieved May 17, 2014, from http://www.apjii.or.id/v2/read/page/halaman-data/9/statistik.html

Chow, E. (2011). *Ethical Hacking & Penetration Testing.*

Friends, N. N. (2009). *Penetration Testing A Roadmap to Network.*

J Thomson, F. (2013, Desember). *Akamai*. Retrieved Mei 19, 2014, from http://www.akamai.com/dl/akamai/akamai-soti-q413.pdf?WT.mc_id=soti_Q413