Edu Komputika 8 (1) (2021)

**Edu Komputika Journal**

http://journal.unnes.ac.id/sju/index.php/edukom

# Implementasi *Penetration Testing Execution Standard* Untuk Uji Penetrasi Pada Layanan *Single Sign-On*

**Septia Ulfa Sunaringtyas[1)]✉ dan Djodi Surya Prayoga[1)]**

[1]Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara, Bogor, Indonesia

## Info Artikel

*Sejarah Artikel:*
Diterima: Juni 2021
Direvisi: Juni 2021
Disetujui: Juni 2021

*Keywords:*
*PTES, Uji Penetrasi, Kerawanan, Risiko, Single Sign-On, Keamanan Informasi, Serangan Siber*

## Abstrak

Teknologi *single sign-on* kini banyak dimanfaatkan oleh penyedia layanan berbasis elektronik karena memudahkan pengguna layanan mengelola akun sehingga tidak perlu mengingat banyak *user name* dan *password.* Namun, teknologi *single sign-on* selain memberikan manfaat juga menimbulkan celah kerawanan. Uji penetrasi bertujuan untuk mengidentifikasi kerawanan dan menguji keamanan sistem dengan mengeskploitasi kerawanan tersebut. Penelitian ini mengimplementasikan *Penetration Testing Execution Standard* (PTES) untuk uji penetrasi layanan *single singn-on.* Dari tujuh tahap uji penetrasi yang dilakukan, berhasil teridentifikasi 12 kerawanan yang terdiri dari 3 kerawanan kategori sedang, 6 kerawanan kategori rendah dan 3 kerawanan kategori informasi. Enam serangan siber telah dilakukan untuk mengeksploitasi kerawanan dengan hasil 3 serangan berhasil dan 3 serangan gagal. Berdasarkan hasil analisis kerawanan dan eksploitasi diberikan rekomendasi berupa upaya *updating* dan *patching* secara berkala, konfigurasi CSP *header* dan *content-type-option header* pada *web server* dan server aplikasi, validasi konfigurasi *host header*, *x-content-type-options header* dan non aktifkan *x-forwarded- host* di setiap halaman *web,* konfigurasi '*secure' flag* pada *cookie,* tambahkan fitur filter metakarakter pada kode sumber, serta batasi percobaan *login.* Hasil implementasi PTES terbukti mempermudah penguji melakukan uji penetrasi dan efektif mencegah terjadinya perselisihan antara penguji dan *client* karena perbedaan lingkup pengujian.

## *Abstract*

*Increasing the use of single sign-on technology by electronic-based service providers in addition to providing benefits also creates vulnerability. Penetration testing needed to identify vulnerabilities and test system security by exploiting those vulnerabilities. This research implements the Penetration Testing Execution Standard (PTES) for penetration testing of single singn-on services. Seven stages of the penetration test had done and 12 vulnerabilities were identified, consisting of 3 medium vulnerabilities, 6 low vulnerabilities and 3 information vulnerabilities. Six cyberattacks have been carried out to exploit the vulnerability with the result of 3 successful attacks and 3 failed attacks. Based on the results of the vulnerability and exploitation analysis, recommendations are given consist of regular updating and patching efforts, configuration of the CSP header and content-type-option header on the web server and application server, validation of the host header configuration, x-content-type-options header and deactivation. x-forwarded- hosted on every web page, configure 'secure' flag on cookies, add metacharacter filter feature in source code, and limit login attempts. The results of the PTES's implementation are proven to make it easier for testers to carry out penetration tests and effectively prevent disputes between testers and clients due to differences in the scope of testing.*



✉ Alamat korespondensi:
Jurusan Keamanan Siber,
Politeknik Siber dan Sandi Negara, Bogor
E-mail: septia.ulfa@poltekssn.ac.id

ISSN 2252-6811
E-ISSN 2599-297X

## PENDAHULUAN

Jumlah penyedia layanan berbasis elektronik yang kian meningkat, selain memberikan kemudahan bagi pengguna dalam bertransaksi juga menyebabkan pengguna layanan harus membuat banyak akun dan mengingat masing-masing *user name* dan *password* (Putri, dkk., 2019). Teknologi *single sign-on* (SSO) merupakan solusi yang banyak diterapakan untuk menanggulangi hal tersebut. Dengan menerapkan SSO, pengguna layanan cukup melakukan satu kali *login* untuk mengakses beberapa layanan yang berbeda (Aminudin, 2014). Namun terdapat kerawanan pada pemanfaatan layanan SSO yang dapat dieksplotasi oleh peretas diantaranya *access token misuse* (Wang, dkk., 2013), *sign request misuse, app secret leak, user oauth credentials leak* (Zhou & Evans, 2014). Serangan siber yang umum dilakukan oleh peretas untuk mengeksploitasi layanan berbasis SSO antara lain *SQL injection, Denial Of Service* (DOS), *bruteforce attack, sniffing, dictionary attack* (Musliyana, dkk., 2016), *cross site scripting* (XSS) (Goutam & Tiwari, 2019), *clickjacking* (Sahren et al., 2019).

Setiap penyedia layanan berbasis elektronik sudah seharusnya menerapkan upaya untuk mencegah terjadinya risiko serta menjamin keamanan informasi yang disimpan dan dikelola oleh sistem layanan berbasis elektronik khususnya yang memanfaatkan teknologi SSO. Dampak risiko yang ditimbulkan akibat kebocoran data pribadi pelanggan maupun data rahasia organisasi/ perusahaan tentunya akan memberikan kerugian bagi pemilik data baik organisasi penyedia layanan maupun pengguna layanan. Uji penetrasi merupakan salah satu upaya yang dapat dilakukan oleh penyedia layanan untuk mengidentifikasi kerawanan (Tarigan, dkk., 2017), menguji keamanan sistem dengan berperan layaknya peretas yang melakukan ekslpoitasi terhadap kerawanan, serta menentukan kontrol yang tepat guna menanggulangi terjadinya risiko (Patel, 2019). Untuk memudahkan penguji penetrasi melakukan perannya, telah tersedia beberapa standar uji penetrasi yang berisi teknik dan alat yang digunakan serta tahapan kerja sebagai panduan pelaksanaan uji penetrasi (Klíma, 2016). Standar uji penetrasi tersebut diantaranya ISAAF (*Information Systems Security Assessment Framework),* OSSTMM *(Open-Source Security Testing Methodology Manual),* NIST SP 800-115, OISSG *(Open Information Systems Security Group),* PETA *(Information Security Penetration Testing)* dan PTES *(Penetration Testing Execution Standard)* (Abu-Dabaseh & Alshammari, 2018).

Penelitian sebelumnya dilakukan oleh Klíma (2016) yang melakukan studi komparasi beberapa standar uji penetrasi. Dalam penelitian tersebut disebutkan bahwa PTES memiliki beberapa keunggulan dari standar uji penetrasi lainnya yaitu PTES merupakan metode uji penetrasi yang mudah digunakan karena selain memberikan penjelasan detail pada setiap tahap pengujian, metode ini memberikan panduan teknis yang disertai keterangan alat dan teknik penetrasi yang dapat digunakan. Walaupun metode ini tidak menjangkau level manajemen, namun PTES menyajikan laporan uji penetrasi yang bersifat strategis dan mudah dipahami oleh pimpinan tinggi organisasi/ *high level management.* Selain itu, PTES merupakan metode uji penetrasi yang selalu melakukan pembaharuan secara berkala menyesuaikan tren ancaman dan risiko siber (Klíma, 2016).

Berdasarkan penjelasan sebelumnya dapat dikatakan bahwa banyaknya pemanfaatan teknologi SSO pada layanan berbasis elektronik, adanya serangan siber yang mengeksploitasi kerawanan pada layanan SSO, serta kebutuhan penyedia layanan tersebut untuk melakukan uji penetrasi guna memastikan keamanan informasi yang dimiliki, menjadi latar belakang penelitian ini. Dengan mengimplementasikan metode PTES untuk melakukan uji penetrasi pada layanan SSO, penelitian ini diharapkan dapat memberikan gambaran nyata tentang tahapan melakukan uji penetrasi dengan metode PTES, menyajikan laporan hasil pengujian yang berisi tingkat risiko dan kerawanan pada layanan SSO, serta merekomendasikan upaya pengganggulangan terhadap kerawanan dan risiko yang teridentifikasi. Semoga dengan adanya penelitian ini dapat mempermudah penyedia layanan berbasis elektronik khususnya yang memanfaatkan teknologi SSO melakukan uji penetrasi sehingga dapat menyediakan layanan yang tahan terhadap serangan siber dan menjamin keamanan informasi yang ada di dalamnya.

## METODE PENELITIAN

Standar yang digunakan sebagai pedoman uji penetrasi pada penelitian ini adalah PTES *(Penetration Testing Execution Standard).* PTES berisi metode uji penetrasi yang terdiri dari tujuh tahap yaitu tahap pra interaksi (*pre-engagement interactions*), pengumpulan informasi (*intelligence gathering*), pemodelan ancaman (*threat modelling*), analisis kerawanan (*vulnerability analysis/VA*), ekspoitasi (*exploitation*), pasca eksploitasi (*post exploitation*) dan pelaporan (*reporting*) (PTES, 2017). Berikut adalah penjelasan setiap tahap uji penetrasi berdasarkan PTES.

A. Pra Interaksi

Tahap ini disebut juga tahap persiapan yang bertujuan untuk menyepakati objek/target, lingkup, teknik yang digunakan untuk uji penetrasi dan *timeline* pelaksanaan pengujian. Tahap ini juga bertujuan untuk mencegah terjadinya masalah pelanggaran hukum dan kebijakan akibat penetrasi yang dilakukan penguji. Tahap ini melibatkan *pentester*/ penguji penetrasi dan *client*/ pemilik layanan. Adapun kegiatan yang dilakukan pada tahap ini antara lain:

1. Identifikasi lingkup;
2. Menentukan tujuan uji penetrasi;
3. Analisis kesiapan organisasi;
4. Menyusun *ROE (Roles Of Engagement);*
5. Rapat pendalaman lingkup;
6. Menyepakati biaya tambahan di luar kontrak;
7. Mengisi kuisioner;
8. Menyusun jalur komunikasi.

B. Pengumpulan Interaksi

Tahap kedua yaitu pengumpulan informasi yang berkaitan dengan target pengujian. Informasi ini akan digunakan untuk menyusun strategi serangan untuk mengeksploitasi kerawanan target. Semakin banyak informasi yang terkumpul, maka semakin banyak *attack vector* yang dapat digunakan. Tabel 1 menjelaskan tentang metode pengumpulan informasi, perangkat dan teknik yang digunakan.

Tabel 1. Metode Pengumpulan Informasi

| Metode | Perangkat/teknik |
|---|---|
| 1. *Internal Information Gathering* | |
| Pasif | Studi literatur<br>Telaah dokumen |
| Semi-Pasif | Observasi |
| Aktif | Wawancara<br>FGD *(Forum Group Discussion)* |
| *Humint/ Human Intelligence* | *Social engineering*<br>*Phising* |
| 2. OSINT/ *Open Source Intelligence*: *Footprinting* | |
| 2.1. *Internal Footprinting* | |
| Pasif | *Packet sniffing (Wireshark)* |
| Aktif | nmap |
| 2.2. *External Footprinting* | |
| Pasif | - *Whois Lookups*<br>- *Geo Data Tool*<br>- *Netcraft*<br>- *Maltego* |
| Aktif | - *Port scanning (nmap)*<br>- *Dirsearch*<br>- *Nikto* |

C. Pemodelan Ancaman

Tahap pemodelan ancaman bertujuan untuk mengidentifikasi aset yang berkaitan dengan layanan SSO, ancaman, pelaku ancaman, motivasi pelaku dan peluang terjadinya ancaman. Pemodelan ancaman menggunakan model STRIDE dengan mengelompokkan jenis ancaman menjadi S/ *spoofing,* T/*tampering,* R/ *repudiation,* I/ *information disclosure,* D/ *denial of service,* E/ *elevation of privilege* (Shostack, 2013).

Standar penilaian peluang dilakukan secara kualitatif dengan skala rendah (risiko tidak pernah atau sangat jarang terjadi), sedang (risiko pernah terjadi atau mungkin terjadi), tinggi (risiko sering terjadi). Model ancaman ini merupakan hasil dari *brain storming*/diskusi antara *client* dan *pentester* yang merupakan bagian dari skenario serangan yang akan dilakukan pada tahap eksploitasi.

D. Analisis Kerawanan

Tahap analisis kerawanan bertujuan untuk mengidentifikasi celah kerawanan pada layanan SSO yang nantinya akan dieksploitasi. Hasil analisis kerawanan selanjutnya divalidasi dengan metode triangulasi dengan basis data kerawanan yaitu CWE *(Common Weakness Enumeration)*. Tabel 2 menjelaskan jenis/metode analisis kerawanan, serta tehnik/perangkat yang digunakan.

Tabel 2. Hasil Analisis Kerawanan

| Metode | Tehnik/perangkat |
|---|---|
| Aktif-Manual | - *BurpSuite Community Edition* |
| Aktif-Otomatis | - OWASP ZAP versi 2.10.0 (Nagpure & Kurkure, 2018) |
| Pasif | *Packet sniffing (Wireshark)* |

E. Eksploitasi

Tahap eksloitasi dilakukan dengan menyusun skenario serangan siber yang menargetkan kerawanan pada layanan SSO yang telah teridentifikasi sebelumnya. Skenario serangan menjelaskan metode serangan serta jenis ancaman berdasarkan dampak yang ditimbulkan, sesuai model ancaman. Tujuan dari tahap eksploitasi adalah memperoleh akses terhadap aset namun dengan meminimalisir gangguan terhadap kinerja layanan SSO. Tabel 3 merupakan *confussion matrix* yang digunakan sebagai kriteria penilaian hasil eksploitasi.

Tabel 3. *Confussion Matrix*

| | ***True*** | ***False*** |
|---|---|---|
| ***Possitive*** | *True-Possitve* | *False-Possitive* |
| ***Negative*** | *True-Negative* | *False-Negative* |

*Confussion matrix* membagi kriteria penilaian hasil eksploitasi menjadi:

1. *True-Possitve* jika terdapat notifikasi kerawanan dan penguji berhasil mengeksploitasi kerawanan;
2. *False-Possitive* jika terdapat notifikasi kerawanan namun penguji gagal mengeksploitasi kerawanan;
3. *True-Negative* jika tidak ada notifikasi kerawanan dan penguji gagal melakukan penetrasi;
4. *False-Negative* jika tidak ada notifikasi kerawanan namun penguji berhasil melakukan penetrasi.

F. Pasca Eksploitasi

Terdapat dua kegiatan yang perlu dilakukan pada tahap pasca eksploitasi yaitu menyusun rencana aksi dan melakukan *clean-up*. Tentunya tahap pasca eksploitasi hanya dapat dilakukan dengan berpedoman pada ROE yang telah disusun pada tahap pra-interaksi.

1. Rencana Aksi

Rencana aksi bertujuan untuk menyusun langkah selanjutnya setelah eksploitasi yang dilakukan penguji menghasilkan nilai *true positive.*

2. *Clean-Up*

Proses terakhir yang dilakukan setelah pengujian selesai adalah penghapusan *script,* kode, akun sementara yang digunakan untuk uji penetrasi. Tujuan tahap ini adalah mengembalikan konfigurasi sistem seperti sedia kala yaitu kondisi sebelum pengujian dilakukan.

G. Pelaporan

Standar PTES menyajikan laporan hasil uji penetrasi dalam dua bentuk yaitu *executive summary* dan laporan teknis. *Executive summary* merupakan laporan yang ditujukan kepada manajemen tingkat tinggi sebagai dasar pengambilan keputusan. Bentuk laporan ini berisi hasil analisis uji penetrasi yang bersifat strategis yang terdiri dari level risiko yang teridentifikasi dan rekomendasi penangunangan risiko. Sedangkan laporan teknis menjelaskan lebih detail tentang ruang lingkup, skenario serangan, dampak risiko dan rekomendasi penanggulangan risiko.

## HASIL DAN PEMBAHASAN

A. Hasil Pra Interaksi

Pada tahap pra interaksi terdapat beberapa kegiatan yang tidak dilakukan berdasarkan hasil kesepakatan antara penguji dan pemilik sistem. Tabel 4 menjelaskan tentang kegiatan yang dilakukan pada tahap pra-interaksi dan hasilnya.

Tabel 4. Hasil Pra Interaksi

| Kegiatan | Status | Hasil |
|---|---|---|
| Identifikasi lingkup | Dikerjakan | - Target uji penetrasi: layanan SSO |
| Menentukan tujuan uji penetrasi | Dikerjakan | - Tujuan primer: Identifikasi kerawanan dan risiko pada layanan SSO, serta menyusun strategi perbaikan guna mencegah terjadinya kebocoran informasi<br>- Tujuan Sekunder: melaksanakan Amanah UU ITE, PP PSTE, Perpres SPBE |
| Analisis Kesiapan Organisasi | Dikerjakan | - Kesiapan organisasi rendah sehingga perlu analisis kerawanan |
| Menyusun *ROE (Roles Of Engagement)* | Dikerjakan | - *Timeline:* durasi pengujian 5 bulan<br>- Lokasi: Indonesia<br>- Surat izin uji penetrasi<br>- Perlindungan hukum |
| Rapat pendalaman lingkup | Dikerjakan | - NDA *(Non-Disclosure Agreement)* |
| Menyepakati Biaya Tambahan di luar kontrak | Tidak Dikerjakan | |
| Mengisi Kuisioner | Dikerjakan | - Daftar target *web application* |
| Menyusun jalur komunikasi | Dikerjakan | - Membuat grup *instant messaging* |

B. Hasil Pengumpulan Informasi

Informasi yang diperoleh dari tahap pengumpulan informasi dengan metode *internal information gathering* dan *opensource intelligence/ footpringtin*g disajikan pada Tabel 5.

Tabel 5. Hasil Pengumpulan Informasi

| Indikator | Hasil |
|---|---|
| 1. *Internal Information Gathering* | |
| Visi, misi, tugas dan fungsi organisasi | Menyediakan layanan untuk mengelola kearsipan organisasi, mengalola data pribadi dan kepegawaian serta mengelola gaji tunjangan pegawai. |
| Latar belakang pengembangan layanan SSO | Memudahkan pengguna mengelola akun |
| Daftar mekanisme proteksi | Tidak tersedia |
| Infrastruktur jaringan dan sistem layanan SSO | Tidak tersedia |
| Riwayat pengembangan sistem layanan SSO | Tidak tersedia |
| Alamat email pengguna layanan | Tidak tersedia |
| URL layanan SSO | Tidak tersedia |
| 2. OSINT/ *Open Source Intelligence*: *Footprinting* | |
| Alamat *website* | jaxxxxx.go.id |
| Alamat IP | 103.xxx.xxx.xxx |
| Lokasi | Indonesia |
| Nomor telepon | +628xxxxxxxxxx |
| Pemilik layanan | Instansi pemerintah xxx |
| *Autonomous System Number* | ASxxxxxx |
| Tipe server | Apache/2.4.29 (Ubuntu) |
| Waktu terregistrasi | 2018 |
| Algoritma kunci publik | RSA |
| Protokol jaringan | TLS v1.3 |
| Alamat email | xxx@xxx.go.id |
| Subdomain dan alamat IP-nya | xxx.xxx.go.id<br>yyy.yyy.go.id |
| Penyedia ISP | PT. xxx |
| Rentang alamat IP | 103.xxx.xxx.xxx – 103.yyy.yyy.yyy |
| Daftar *port* terbuka | 110/tcp : pop3-proxy – Astaro Firewall pop3 proxy<br>443/tcp : openvpn – Open VPN<br>1723/tcp : pptp – linux (firmware)<br>2000/tcp : cisco-sccp –<br>4444/tcp : http – Apache httpd<br>5060/tcp : sip |
| Direktori pada layanan SSO | https://xxx/auth<br>https://xxx/index.html<br>https://xxx/robots.txt |
| Informasi SSL (subjek, algoritma kriptografi, penerbit setifikat) | Subject : xxx<br>Ciphers : ECDHE-RSA-AES256-GCM-SHA384<br>Issuer : /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA<br>Allowed HTTP Methods: GET, HEAD, POST |

C. Hasil Pemodelan Ancaman

Hasil pemodelan ancaman terdiri dari aset informasi yang dijadikan target serangan, skenario serangan (pelaku/sumber ancaman dan motivasinya), jenis ancaman berdasarkan STRIDE serta peluang terjadinya ancaman. Hasil pemodelan ancaman disajikan pada Tabel 6.

Tabel 6. Hasil Pemodelan Ancaman

| **Aset** | Data pribadi, finansial dan kepegawaian pengguna layanan SSO | | |
|---|---|---|---|
| **Pelaku** | **Motivasi** | **Ancaman** | **Peluang** |
| Internal:<br>- Rekan kerja | - Balas dendam<br>- Keuntung-an pribadi | S<br>T<br>R<br>I<br>D<br>E | Rendah<br>Sedang<br>Sedang<br>Sedang<br>Rendah<br>Rendah |
| **Pelaku** | **Motivasi** | **Ancaman** | **Peluang** |
| Eksternal:<br>- *Hactivist*<br>- Pelaku kriminal | - Pengaku-an<br>- Kesenang-an<br>- Keuntung an pribadi | S<br>T<br>R<br>I<br>D<br>E | Tinggi<br>Sedang<br>Sedang<br>Tinggi<br>Tinggi<br>Tinggi |

D. Hasil Analisis Kerawanan

Analisis kerawanan yang dilakukan pada penelitian ini menggunakan metode aktif-manual dan aktif-otomatis. Daftar kerawanan yang dihasilkan kemudian divalidasi dengan mengacu pada CWE *(Common Weakness Enumeration)*. Tabel 7 merupakan hasil analisis kerawanan yang telah tervalidasi.

Tabel 7. Hasil Analisis Kerawanan Tervalidasi

| Ke-rawanan | Penjelasan | CWE | Ter-validasi |
|---|---|---|---|
| Kategori Sedang | | | |
| CSP: *Wildcard directive* | *Directive* mengizinkan *wildcard source* yang tidak ditentukan / terlalu luas sehingga rentan serangan XSS | CWE-16 | Ya |
| *Vulnerable JS library* | Aplikasi menggunakan *library* JQuery 3.4.1 yang rentan serangan XSS | CWE-829 | Ya |
| *X-frame options header not set* | Aplikasi tidak menerapkan *header x-frame options* dalam proses http sehingga rentan | CWE-16 | Ya |

| Kerawanan | Penjelasan | CWE | Tervalidasi |
|---|---|---|---|
| | terhadap *clickjacking* | | |
| Kategori Rendah | | | |
| *Absence of anti CSRF tokens* | Tidak terdapat token anti CSRF | CWE-352 | Ya |
| *Incomplete or no cache control and pragma http header set* | *Chace control* tidak dikonfigurasi dengan benar sehingga *browser* dapat menyimpan konten dan *cache* | CWE-525 | Ya |
| *X-content type options header missing* | *Anti MIME sniffing x-content* tidak 'nonsniff' sehingga *browser* versi lama dapat melakukan MIME-*sniffing* pada *response body* | CWE-16 | Ya |
| *Cookie without same site attribute* | *Cookie* dikonfigurasi tanpa atribut *samesite* menyebabkan *cookie* dapat dikirim sebgaai hasil *request 'cross-site'* | CWE-16 | Ya |
| *Cookie without secure flag* | *Cookie* dikonfigurasi tanpa *secure flag* menyebabkan *cookie* dapat diakases melalui koneksi tanpa enkripsi | CWE-614 | Ya |
| *Login page password-guessing attack* | Tidak ada batas percobaan login | CWE-307 | Ya |
| Kategori Informasi | | | |
| *Information disclosure - suspicious comments* | *Response* mengandung komen mencurigakan yang dapat dieksplotasi | CWE-200 | Ya |
| *Information disclosure - sensitive information in URL* | *Request* berisi informasi sensitive yang terdapat pada URL | CWE-200 | Ya |
| *Timestamp disclosure-Unix* | Aplikasi */web server* – UNIX membuka *timestamp* | CWE-200 | Ya |

E. Hasil Eksploitasi

Daftar kerawanan yang telah diperoleh dari tahap analisis kerawanan kemudian dieksploitasi menggunakan serangan yang sesuai. Tabel 8 berisi tentang skenario serangan yang digunakan untuk mengeksploitasi kerawanan tersebut dan hasil eksploitasi berupa nilai berdasarkan kriteria *confussion matrix.*

Tabel 8. Skenario Serangan dan Hasil Eksploitasi

| Skenario Serangan | Kerawanan dieksploitasi | Output |
|---|---|---|
| - Metode: *Cross-site Scripting* (XSS)<br>- Ancaman: S - T- I | - *CSP: Wildcard directive*<br>- *Vulnerable JS library* | *False Positive* |
| - Metode: *Host header attack*<br>- Ancaman: S - I - E | *X-frame options header not set* | *True Positive* |
| - Metode: *Clickjacking*<br>- Ancaman: S - T- I | *X-content type options header missing* | *True Positive* |
| - Metode: *Sniffing*<br>- Ancaman: I | - *Cookie without secure flag*<br>- *Cookie without same site attribute* | *True Positive* |
| - Metode: *SQL Injection*<br>- Ancaman: S - T- I - E | Kode sumber tidak menggunakan filter terhadap metakarakter | *True Negative* |
| Metode:<br>- *Password guessing attack*<br>- *Brute force attack*<br>Ancaman: S - I - E | *Login page password-guessing attack* | *False Positive* |

F. Pasca Eksploitasi

Setelah penyerang berhasil melakukan eksploitasi kerawanan, selanjutnya adalah melakukan rencana aksi misalnya *port forwarding,* membangun *proxy* untuk mengakses intranet, membangun VPN untuk mengakses intranet, esekusi *remote exploit*, dan menyalagunakan kredensial yang telah bocor. Namun pada penelitian ini, pemilik sistem tidak memberikan izin kepada penyerang untuk melakukan rencana aksi demi menghindari dampak serangan. Sehingga pada tahap eksploitasi hanya dilakukan *clean-up* untuk mengembalikan kondisi sistem seperti sedia kala yaitu kondisi sebelum dilakukan uji penetrasi.

G. Pelaporan

Hasil uji penetrasi berdasarkan PTES disajikan dalam dua bentuk laporan yaitu *executive summary* dan laporan teknis.

1. *Executive Summary*

2.1. Latar Belakang dan Tujuan

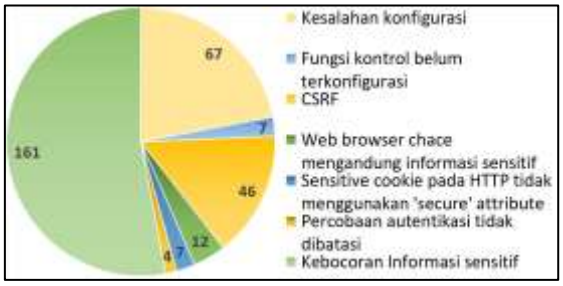
Kewajiban penyedia layanan berbasis elektronik untuk menjamin keamanan informasi yang ada di dalamnya sesuai peraturan dan kebijakan yang berlaku. Tujuan uji penetrasi adalah mengidentifikasi kerawanan dan risiko pada layanan berbasis elektronik yang memanfaatkan teknologi SSO serta menyusun rencana penanggulangan untuk mencegah terjadinya risiko.

2.2. Postur Target Pengujian

Target pengujian adalah halaman *login* layanan SSO. Organisasi belum pernah melakukan uji penetrasi pada layanan tersebut. Layanan SSO mengintegrasikan 3 layanan yang masing-masing tujuan layanan tersebut adalah mengelola kearsipan organisasi, mengalola data pribadi dan kepegawaian serta mengelola gaji tunjangan pegawai.

2.3. Temuan Umum

Temuan umum yang dimaksud merupakan hasil analisis kerawanan berupa jenis kerawanan dan jumlah notifikasi kerawanan yang disajikan pada Gambar 1. Berdasarkan Gambar 1. diketahui bahwa kerawanan dengan jumlah terbanyak sehingga perlu diwaspadai adalah kerawanan terhadap kebocoran informasi sensitif.




Gambar 1. Jumlah kerawanan yang teridentifikasi

2.4. Profil Risiko

Profil risiko disajikan pada Tabel 9, berisi nilai risiko yang dihitung berdasarkan keberhasilan eksploitasi sebagai penentu nilai *likelihood* dan dampak yang ditimbulkan. Perhitungan nilai risiko menggunakan nilai kualitatif berdasarkan kriteria yang telah ditetapkan pada NIST SP 800-30.

Tabel 9. Profil Risiko

| Serangan | *Nilai Likeli-hood* | Nilai Dampak | Nilai Risiko |
|---|---|---|---|
| XSS | Rendah | Sedang | Rendah |
| *Host header attack* | Tinggi | Sedang | Sedang |
| *Clickjacking* | Tinggi | Sedang | Sedang |
| *Sniffing* | Tinggi | Sedang | Sedang |
| *SQL Injection* | Rendah | Tinggi | Sedang |
| *Password guessing attack* | Sedang | Sedang | Sedang |
| *Brute force attack* | Sedang | Sedang | Sedang |

2.5. Rekomendasi

Rekomendasi disusun berdasarkan hasil analisis kerawanan dan eksploitasi. Rekomendasi berisi saran perbaikan sistem untuk mencegah terjadinya risiko di kemudian hari yang disajikan pada Tabel 10.

Tabel 10. Rekomendasi Penanggulangan Risiko dan Kerawanan

| Risiko Serangan | Kerawanan dieksploitasi | Rekomendasi |
|---|---|---|
| *Cross-site Scripting* (XSS) | - *CSP: Wildcard directive*<br>- *Vulnerable JS library* | - Perbarui *JS library* menjadi versi terbaru<br>- Perlu konfigurasi CSP *Header* pada *web server, server* aplikasi, dan *load balancer* |
| *Host header attack* | *X-frame options header not set* | - Memvalidasi *host header* setiap halaman *web*<br>- Non aktifkan *x-forwarded- host* |
| *Clickjacking* | *X-content type options header missing* | - Aktifkan *content-type-option header* pada *web server* dan *server* aplikasi<br>- Konfigurasi *x-content-type-options header* dengan menambahkan 'nosniff' pada setiap halaman *web* |
| *Sniffing* | - *Cookie without secure flag*<br>- *Cookie without same site attribute* | - Konfigurasi *secure flag* pada *cookie* |
| *SQL Injection* | Kode sumber tidak menggunakan filter terhadap metakarakter | - Menambahkan filter metakarakter pada kode sumber<br>- *Updating* dan *patching* secara berkala |

| Risiko Serangan | Kerawanan dieksploitasi | Rekomendasi |
|---|---|---|
| - *Password guessing attack*<br>- *Brute force attack* | *Login page password-guessing attack* | - Batasi percobaan *login* jika mengalami kegagalan *login* melebihi batas percobaan, blokir akun. |

2. Laporan Teknis

2.1. Lingkup Uji Penetrasi

Lingkup uji penetrasi dijelaskan pada Tabel 11, yang berisi informasi hasil tahap pra interaksi.

Tabel 11. Lingkup Uji Penetrasi

| ***Client*** | Penyedia layanan SSO |
|---|---|
| **Tim Penguji Penetrasi** | 1. Djodi Surya Prayoga<br>2. Septia Ulfa S |
| **Target Pengujian** | Layanan SSO |
| **Lingkup Pengujian** | Halaman *login* SSO |
| **Tujuan Pengujian** | 1. Identifikasi kerawanan dan risiko<br>2. Menyusun rekomendasi penanggulangan risiko |

2.2. Tehnik Pengumpulan Informasi

Pengumpulan informasi yang berkaitan dengan target pengujian menggunakan beberapa tehnik antara lain studi literatur, telaah dokumen, observasi, wawancara, FGD *(Forum Group Discussion), social engineering, phising, Whois lookups, Geo Data Tool, Netcraft, Maltego, Port scanning (nmap), Dirsearch,* dan *Nikto.*

2.3. Tehnik Analisis Kerawanan

Analisis kerawanan pada layanan SSO menggunakan tehnik analisis manual dengan memanfaatkan *BurpSuite Community Edition* dan tehnik analisis otomatis dengan OWASP ZAP versi 2.10.0.

2.4. Tehnik Ekslpoitasi

Eksploitasi kerawanan yang telah teridentifikasi *dilakukan* berdasarkan beberapa skenario serangan siber yang terdiri dari *Cross-site Scripting* (XSS), *host header attack, clickjacking, sniffing, SQL injection, password guessing attack,* dan *brute force attack.*

## SIMPULAN

Implementasi *Penetration Testing Execution Standar* (PTES) untuk uji penetrasi pada layanan SSO mempermudah proses pengujian karena tersedia panduan detail terkait metode dan tehnik yang digunakan disetiap tahap pengujian. Hal ini sesuai dengan penelitian sebelumnya yang menyatakan bahwa PTES lebih mudah digunakan sebagai panduan uji penetrasi dibandingkan dengan standar sejenis lainnya yaitu ISAAF, OSSTMM, NIST SP 800-115, OISSG, dan PETA. Tahapan pengujian diawali dengan tahap pra interaksi yang efektif mencagah perselisihan karena ketidakjelasan lingkup pengujian, dilanjutkan tahap pengumpulan informasi, pemodelan ancaman, analisis kerawanan, dan eksploitasi. Terdapat 12 kerawanan layanan SSO yang teridentifikasi pada tahap analisis kerawanan yaitu 3 kerawanan kategori sedang (CSP: *wildcard directive, vulnerable JS library, X-frame options header not set)*, 6 kerawanan kategori rendah (*anti CSRF tokens, incomplete or no cache control and pragma http header set, X-content type options header missing, cookie without same site attribute, cookie without secure flag, login page password-guessing attack),* dan 3 kerawanan kategori informasi (*information disclosure-suspicious comments, information disclosure-sensitive information in URL, timestamp disclosure- Unix).* Pada tahap eksploitasi, dari 6 skenario serangan yang dilakukan hanya 3 serangan yang berhasil yaitu *host header attack, clickjacking* dan *sniffing.* Sedangkan 3 skenario serangan yang gagal yaitu XSS, *SQL injection,* dan *password guessing attack/bruteforce attack.* Aktivitas yang dilakukan pada tahap pasca eksploitasi hanya *clean up.* Rencana aksi tidak dilakukan karena tidak diizinkan *client* sesuai yang tercantum pada ROE. Pada tahap pelaporan diberikan rekomendasi penanggulangan kerawanan dan risiko diantaranya melakukan *updating* dan *patching* secara berkala, konfigurasi CSP *header* dan *content-type-option header* pada *web server* dan server aplikasi, validasi konfigurasi *host header*, *x-content-type-options header* dengan menambahkan 'nosniff' dan non aktifkan *x-forwarded- host* di setiap halaman *web,* konfigurasi '*secure' flag* pada *cookie,* tambahkan fitur filter metakarakter pada kode sumber, serta batasi percobaan *login.* Penelitian ini diharapkan dapat memberikan gambaran cara implementasi PTES untuk uji penetrasi layanan berbasis elektronik khususnya yang memanfaatkan teknologi SSO sehingga penyedia layanan dapat menyediakan layanan yang tahan terhadap serangan siber dan menjamin keamanan informasi yang ada di dalamnya.

## DAFTAR PUSTAKA

Abu-Dabaseh, F., & Alshammari, E. (2018). Automated Penetration Testing : An Overview. *CS & IT-CSCP*, *October*, 121–129.https://doi.org/10.5121/csit.2018.80610

Aminudin, A. (2014). Implementasi Single Sign On (SSO) Untuk Mendukung

Interaktivitas Aplikasi E-Commerce Menggunakan Protocol Oauth. *Jurnal Gamma*, *10*(1), 109–115.

Goutam, A., & Tiwari, V. (2019). Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application. *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, 601–605. https://doi.org/10.1109/ISCON47742.2019.9036175

Klíma, T. (2016). PETA: Methodology of Information Systems Security Penetration Testing. *Acta Informatica Pragensia*, *5*(2), 98–117. https://doi.org/10.18267/j.aip.88

Musliyana, Z., Arif, T. Y., & Munadi, R. (2016). Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. *Jurnal Rekayasa Elektrika*, *12*(1), 21. https://doi.org/10.17529/jre.v12i1.2896

Nagpure, S., & Kurkure, S. (2018). Vulnerability Assessment and Penetration Testing of Web Application. *2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017*, 1–6. https://doi.org/10.1109/ICCUBEA.2017.8463920

Patel, K. (2019). A survey on vulnerability assessment penetration testing for secure communication. *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, *Icoei*, 320–325. https://doi.org/10.1109/ICOEI.2019.8862767

PTES, T. (2017). *The Penetration Testing Execution Standard Documentation*. 9.

Putri, T. D., Sugeng, W., & Katri, R. (2019). Sistem Otentikasi Login Dengan Single Sign-On Untuk Mengakses Banyak Sistem. *MIND Journal*, *4*(2), 96–110. https://doi.org/10.26760/mindjournal.v4i2.17-31

Sahren, Ashari Dalimuthe, R., & Amin, M. (2019). *Prosiding Seminar Nasional Riset Information Science (SENARIS) Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus*. *September*, 994–1001.

Shostack, A. (2013). Threat modeling : designig for security. In *Journal of Chemical Information and Modeling* (Vol. 53, Issue 9).

Tarigan, B. V., Kusyanti, A., & Yahya, W. (2017). Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(3), 206–214.

Wang, R., Zhou, Y., Chen, S., Qadeer, S., Evans, D., & Gurevich, Y. (2013). Explicating SDKs: Uncovering assumptions underlying secure authentication and authorization. *Proceedings of the 22nd USENIX Security Symposium*, *August*, 399–414.

Zhou, Y., & Evans, D. (2014). SSOScan: Automated testing of web applications for single sign-on vulnerabilities. *Proceedings of the 23rd USENIX Security Symposium*, 495–510.