**PROSEDUR PENGUJIAN KEAMANAN APLIKASI BERBASIS WEB**

**{{nama organisasi}}**

**{{logo organisasi}}**

|  |  |
| --- | --- |
| No Dokumen | : 0.2 (Draft) |
| Revisi | : 00 |
| Tanggal Terbit | : |

|  |  |  |
| --- | --- | --- |
| Disusun  oleh : | Diketetahui  oleh: | Disetujui / Disahkan  oleh : |
|  |  |  |
| **NN**  NN | **NN**  NN | **NN**  NN |

**Riwayat Dokumen**

|  |  |  |
| --- | --- | --- |
| **Versi** | **Tanggal** | **Perubahan** |
| 0.1 (Draft) | 28/02/2023 | Rilis draft awal dengan hanya menyalin sepenuhnya konten dari **PEDOMAN TATA KELOLA KEAMANAN APLIKASI BERBASIS WEB - BSSN** |
| 0.2 (Draft) | 03/03/2023 | Penambahan prosedur VAPT |
|  |  |  |

1. **TUJUAN:**
   1. Memberikan panduan pengujian keamanan Aplikasi Berbasis Web yang secara best practice dimaksudkan untuk dapat menemukan risiko keamanan dalam suatu sistem Aplikasi Berbasis Web.
   2. Memastikan bahwa setiap petugas/tim keamanan informasi dan Aplikasi Berbasis Web, tanggap dalam melakukan langkah untuk menghilangkan risiko keamanan yang terdapat dalam suatu sistem Aplikasi Berbasis Web.
   3. Memastikan Aplikasi Berbasis Web beserta datanya aman dari kemungkinan berbagai tindakan yang tidak sah (*unauthorized action*).
   4. Memastikan kegiatan pengujian keamanan Aplikasi Berbasis Web berjalan dengan baik dan efektif.
   5. Memastikan adanya *knowledge management* dan *repository* yang berkelanjutan dalam aktivitas pengujian keamanan Aplikasi Berbasis Web.
2. **RUANG LINGKUP:**
   1. Prosedur ini mencakup langkah-langkah pengujian keamanan Aplikasi Berbasis Web terhadap suatu risiko keamanan.
   2. Prosedur ini tidak secara rinci mencakup risiko keamanan terhadap Aplikasi Berbasis Web yang berkaitan dengan manajemen atau operasional yang mungkin terjadi, sehingga perlu dilakukan kajian lanjutan yang diantaranya meliputi: pengujian terhadap manusia (people), kebijakan (policy), dan proses (process) di dalam organisasi.
3. **REFERENSI:**
   1. OWASP Testing Guide version 4.0
   2. OWASP Top 10 - 2021: The Ten Most Critical Web Application Security Risks
4. **DEFINISI/ SINGKATAN:**
   1. TIK (Teknologi Informasi dan Komunikasi) adalah istilah dalam sistem komputer yang meliputi perangkat keras (*hardware*), perangkat lunak (*software*), jaringan data dan suara, aplikasi sistem informasi dan database, dan lain sebagainya.
   2. Pengguna (*User*) adalah akun yang digunakan untuk mengakses suatu aplikasi atau sistem TIK.
   3. Subbid KamTI adalah Sub Bidang Keamanan Teknologi Informasi yang merupakan salah satu Sub Bidang dalam Unit Keja Pusat Data dan Sistem Informasi (PDSI).
   4. Hak akses adalah hak akses suatu akun Pengguna terhadap suatu aplikasi atau sistem TIK (misal: read, *write, delete, upload, download*, dll).
   5. *Vulnerability* (Kerentanan) adalah suatu kelemahan berkaitan dengan keamanan sistem komputer (Aplikasi Berbasis Web), yang dapat dieksploitasi oleh suatu sumber ancaman (*threat source*), untuk melakukan suatu tindakan yang tidak sah (*unauthorized action*) dalam sistem komputer (Aplikasi Berbasis Web) tersebut.
   6. *Exploit* (Eksploitasi) adalah cara di mana suatu kerentanan dapat dimanfaatkan untuk melakukan aktivitas yang berbahaya (*malicious activity*) oleh peretas. Eksploitasi adalah langkah selanjutnya dari si penyerang setelah menemukan sebuah kerentanan dalam sistem komputer (Aplikasi Berbasis Web).
   7. *Vulnerability Scanning* adalah pemindaian terhadap suatu sistem komputer berbasis jaringan (misal: Aplikasi Berbasis Web) dengan menggunakan suatu program komputer yang dirancang untuk mencari berbagai kelemahan atau kerentanan yang terdapat dalam sistem komputer tersebut.
   8. *Penetration Testing* adalah simulasi serangan siber yang secara resmi dilakukan pada suatu sistem komputer (Aplikasi Berbasis Web) untuk mengevaluasi keamanan sistemnya. Pengujian ini dilakukan dengan mengeksploitasi kelemahan atau kerentanan sistem komputer yang teridentifikasi, khususnya terhadap potensi pihak yang tidak berwenang untuk bisa mendapatkan akses ke fitur dan data sistem komputer.
5. **PENANGGUNGJAWAB:**
   1. Penguji Keamanan Aplikasi Berbasis Web adalah staf Subbid KamTI atau pihak ketiga yang bertindak sebagai pelaksana atas kegiatan pengujian keamanan pada sistem Aplikasi Berbasis Web.
   2. Penanggungjawab Pengujian adalah tim yang dibentuk dan bertanggungjawab atas kegiatan pengujian keamanan pada sistem Aplikasi Berbasis Web, yang umumnya terdiri dari:
      1. Fungsi Pengaturan Pengguna dan Hak Akses TIK bertindak sebagai Penanggungjawab atas pengaturan pengguna dan pengendalian hak akses pada sistem aplikasi dan database.
      2. Fungsi Pengembang Aplikasi TIK bertindak sebagai Penanggungjawab atas pengembangan dan pemeliharaan sistem aplikasi dan database.
      3. Fungsi Pengembangan Infrastruktur dan Jaringan TIK bertindak sebagai Penanggungjawab atas pengembangan dan pemeliharaan perangkat keras, LAN, WAN, jaringan internet, administrasi database dan administrasi sistem operasi server.
      4. Fungsi Pengendali Keamanan TIK bertindak sebagai pelaksana pengendalian keamanan sistem infrastruktur dan sistem aplikasi.
      5. Fungsi Operasional TIK bertindak sebagai pelaksana operasional harian atas sistem infrastruktur dan sistem aplikasi.
6. **LANGKAH – LANGKAH:**
7. **Aktivitas Persiapan**

# Tabel 4.6 Langkah Persiapan Prosedur Pengujian Keamanan Aplikasi Berbasis Web

|  |  |  |  |
| --- | --- | --- | --- |
| **LANGKAH** | | **AKTIVITAS** | **AKTOR** |
| 1 | | Membentuk Tim Penanggungjawab Pengujian yang akan terlibat dalam proses pengujian keamanan Aplikasi Berbasis Web, berikut para personilnya yang umumnya berasal dari fungsi antara lain:   * Fungsi Pengaturan Pengguna dan Hak Akses TIK * Fungsi Pengembang Aplikasi TIK * Fungsi Pengembangan Infrastruktur dan Jaringan TIK * Fungsi Pengendali Keamanan TIK * Fungsi Operasional TIK | Penanggungjawab Pengujian |
|  | 1.1 | Menentukan metode koordinasi dan komunikasi antar personil dalam Tim Penanggungjawab Pengujian, dan komunikasi dengan pihak lain yang terlibat dalam pengujian | Penanggungjawab Pengujian |
| 1.2 | Menyiapkan berbagai sumber daya yang mungkin akan dipergunakan oleh Tim Penanggungjawab Pengujian dalam proses pengujian Aplikasi Berbasis Web | Penanggungjawab Pengujian |
| 2 | | Menentukan ruang lingkup pekerjaan pengujian keamanan Aplikasi Berbasis Web | Penanggungjawab Pengujian |
| 3 | | Merumuskan persyaratan keamanan Aplikasi Berbasis Web (*security requirements*) yang ingin dicapai dan menentukan hasil keluaran (*deliverables*) pengujian keamanan Aplikasi Berbasis Web | Penanggungjawab Pengujian |
| 4 | | Menyusun dokumentasi terkait persiapan pengujian Aplikasi Berbasis Web sebagai acuan pelaksanaan kegiatan bagi Tim Penanggungjawab Pengujian dan pelaksana Penguji Keamanan Aplikasi Berbasis Web | Penanggungjawab Pengujian |

1. **Diagram Alir Aktivitas Persiapan**

**Gambar 4.7 Diagram Alir Penanganan Insiden Phising**

|  |  |  |  |
| --- | --- | --- | --- |
| **Penguji Keamanan Aplikasi Berbasis**  **Web** | **Penanggung Jawab Pengujian** | | |
| Tim Penanggung Jawab Pengujian  Dokumen Persiapan Pengujian Keamanan Website | Membentuk Tim Penanggung Jawab Pengujian  Menentukan Ruang Lingkup Pengujian  Merumuskan *Website Security Requirements & Deliverables*  Menyusun Dokumentasi | | |
|  | Dokumen Persiapan Pengujian Keamanan Website |  |

1. **Aktivitas Pra-Pengujian**

# Tabel 4.7 Langkah Pra-Pengujuan Keamanan Aplikasi Berbasis Web

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **AKTOR** |
| 1 | Membuat rencana dan program pengujian, menentukan strategi pelaksanaan berdasarkan ruang lingkup dan persyaratan keamanan. Rincian item-item yang diuji mengacu pada dokumen *“Standar Pengujian Kerentanan Aplikasi Web”*, diantaranya berkaitan dengan komponen penting Aplikasi Berbasis Web berikut: server, aplikasi web, kode statis, middleware, dan database | Penguji Keamanan Aplikasi Berbasis Web |
| 2 | Membuat rincian jadwal pengujian dan alokasi sumber daya yang diperlukan dalam kegiatan pengujian keamanan Aplikasi Berbasis Web | Penguji Keamanan Aplikasi Berbasis Web |
| 3 | Jika pengujian menggunakan metode whitebox/ greybox, maka:   * Mengumpulkan dan menganalisis informasi terkait Aplikasi Berbasis Web yang akan diuji keamanannya, serta bila dimungkinkan juga data-data teknis pendukung, seperti infrastruktur jaringan dan perangkat keamanan terkait lainnya | Penguji Keamanan Aplikasi Berbasis Web |
| 4 | Menentukan jenis tool pengujian yang akan dipergunakan sesuai dengan rencana dan program pengujian, serta strategi pelaksanaan pengujian | Penguji Keamanan Aplikasi Berbasis Web |
| 5 | Jika sistem Aplikasi Berbasis Web yang akan diuji dianggap kritikal dan berisiko untuk dilakukan pengujian secara langsung agar pengujian keamanan Aplikasi Berbasis Webbisa dilakukan tanpa mengganggu kinerja sistem yang live: | Penanggung jawab Pengujian |

|  |  |  |
| --- | --- | --- |
|  | * Membuat web server backup di lingkungan “iso-production” yang benar-benar identik dengan sistem di lingkungan “production”. |  |
| 6 | Menyusun dokumentasi dan pelaporan terkait rencana dan program pengujian sebagai acuan pelaksanaan kegiatan pengujian keamanan Aplikasi Berbasis Web. Menyerahkan dokumen laporan pra-pengujian keamanan Aplikasi Berbasis Web kepada Penanggungjawab Pengujian | Penguji Keamanan Aplikasi Berbasis Web |

1. **Diagram Alir Aktivitas Pra-Pengujian**

**Gambar 4.8 Diagram Alir Pra-Pengujian**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Penguji Keamanan Aplikasi Berbasis Web** | | | | **Penanggung jawab Pengujian** |
| Mengumpulkan & |  | Membuat Rencana & Program  Pengujian  Menyusun Jadwal  Rinci Pengujian  Blackbox Testing?  Ya Memilih Tool  Untuk Pengujian  Lingkungan Iso-Production  ?  Tidak  Menyusun Dokumentasi & Pelaporan |  |  |
| Menganalisa Data Teknis |  |  |  |
| Terkait Website | Tidak |  |  |
|  |  | Ya | Membuat Lingkungan |
|  |  |  | Iso-Production |
|  |  |  | Laporan Pra-Pengujian  Keamanan Website |
|  |  |  |  |

1. **Aktivitas Pengujian**

# Tabel 4.8 Langkah Pengujian Keamanan Aplikasi Berbasis Web

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **AKTOR** |
| 1 | Melakukan vulnerability scanning terhadap sistem Aplikasi Berbasis Web sesuai dengan rencana dan program pengujian | Penguji Keamanan Aplikasi Berbasis Web |
| 2 | Melakukan klasifikasi terhadap hasil vulnerability scanning, terutama yang berkaitan dengan exploitable vulnerabity | Penguji Keamanan Aplikasi Berbasis Web |
| 3 | Menyusun prioritas pengujian lanjutan berdasarkan potensi risiko keamanan aplikasi web, misalnya berdasarkan OWASP Top 10 | Penguji Keamanan Aplikasi Berbasis Web |
| 4 | Melakukan pengujian lanjutan, penetration testing berdasarkan klasifikasi dan prioritas yang ditetapkan | Penguji Keamanan Aplikasi Berbasis Web |
| 5 | Jika penetration testing untuk suatu vulnerability memungkinkan untuk menghasilkan pelanggaran keamanan, maka:   * Menyusun tingkat vulnerability berdasarkan risiko keamanan dan kemungkinan untuk menghasilkan pelanggaran keamanan | Penguji Keamanan Aplikasi Berbasis Web |
| 6 | Membuat dokumentasi dan laporan hasil pengujian keamanan Aplikasi Berbasis Web, diantaranya:   * Meliputi vulnerability yang ditemukan dan bagaimana vulnerability tersebut dapat dieksploitasi oleh penyerang, serta rekomendasi untuk memperbaiki. * Dokumentasi tersebut perlu ditulis secara rinci dan sistematis sebagai bahan untuk ditindaklanjuti oleh PENANGGUNGJAWAB Pengujian | Penguji Keamanan Aplikasi Berbasis Web |

1. **Diagram Alir Aktivitas Pengujian**

**Gambar 4.9 Diagram Alir Aktivitas Pengujian**

|  |  |  |  |
| --- | --- | --- | --- |
| **Penguji Keamanan Aplikasi Berbasis Web** | | | **Penanggung Jawab Pengujian** |
| False Positive | Tidak | Vulnerability Scanning  Klasifikasi  Exploitable Vulnerability  Penetration Testing  Menghasilkan Pelanggaran Keamanan?  Ya  Menyusun Dokumentasi & Pelaporan  Pengujian Keamanan | Laporan Klasifikasi |
| Exploitable Vulnerability |
| Laporan Hasil |
| Pengujian Keamanan |

1. **Aktivitas Tindak Lanjut Hasil Pengujian**

# Tabel 4.9 Tindak Lanjut Hasil Pengujian Keamanan Aplikasi Berbasis Web

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **AKTOR** |
| 1 | Menganalisis hasil pengujian untuk menilai tingkat urgensi  terhadap risiko keamanan Aplikasi Berbasis Web dan menentukan prioritas penanganan serta tindak lanjutnya | Penanggungjawab Pengujian |
| 2 | Menyusun rencana tindak lanjut dan prioritasnya terkait resolusi perbaikan dari kerentanan-kerentanan Aplikasi Berbasis Web yang didapatkan dari hasil pelaksanaan  pengujian | Penanggungjawab Pengujian |
| 3 | Jika sebelumnya pengujian keamanan Aplikasi Berbasis Web dilakukan langsung pada sistem yang live, maka:   * Membuat web server backup di lingkungan “iso-production” yang benar-benar identik dengan sistem yang live * Sedapat mungkin resolusi perbaikan dilakukan di   lingkungan “iso-production” sebelum menerapkannya di sistem yang live | Penanggungjawab Pengujian |
| 4 | Menjalankan resolusi perbaikan di lingkungan “iso-  production” sesuai dengan rencana tindak lanjut yang telah dibuat | Penanggungjawab Pengujian |
| 5 | Melakukan verifikasi dan pengujian ulang setelah dilakukan resolusi perbaikan terhadap kerentanan Aplikasi Berbasis Web, untuk mengetahui apakah perbaikan yang dilakukan telah berhasil menghilangkan kerentanan yang  ada. | Penguji Keamanan Aplikasi Berbasis Web(didampingi oleh Penanggungjawab Pengujian) |
| 6 | Jika hasil pengujian ulang berhasil menghilangkan kerentanan yang ada, maka:   * Memastikan bahwa tidak muncul kerentanan baru yang disebabkan oleh perbaikan yang dilakukan sebelumnya * Menerapkan resolusi perbaikan tersebut pada   lingkungan “production” (live) | Penanggungjawab Pengujian |
| 6 | Membuat dokumentasi dan laporan hasil resolusi  perbaikan yang telah selesai dilakukan, agar dapat dipakai sebagai catatan histori dan referensi | Penanggungjawab Pengujian |

1. **Diagram Alir Aktivitas Tindak Lanjut Hasil Pengujian**

**Gambar 4.10 Diagram Alir Aktivitas Tindak Lanjut Hasil Pengujian**



|  |  |
| --- | --- |
| **Penguji Keamanan Aplikasi Berbasis Web** | **Penanggungjawab Pengujian** |
| Melakukan Analisa Hasil Pengujian  Membuat Rencana Tindak Lanjut  Membuat Lingkungan Lingkungan Iso-Production Iso-Production  Siap?  Ya  Menjalankan Resolusi Perbaikan di  Lingkungan Iso-Producion  Verifikasi & Pengujian Ulang  Mengaplikasikan Resolusi Perbaikan di Lingkungan Production  Perbaikan  Tidak Berhasil?  Menyusun  Ya Dokumentasi  Hasil Perbaikan  Dokumen Hasil Dokumen Hasil  Perbaikan Keamanan Perbaikan Keamanan  Website Website | |

**Usulan/Eksisting - Prosedur Pengujian Keamanan dalam bentuk Vulnerability Assessment & Penetration Testing (VAPT) pada Aplikasi Web**

* 1. Analis Keamanan TI bersama-sama Pengembang Aplikasi melakukan Threat Modeling umum terhadap apalikasi menggunakan aplikasi draw.io dengan bantuan *library* threat modeling, lalu eksport hasilnya dalam bentuk file XML
  2. Analis Keamanan TI Bersama Pengembang Aplikasi melakukan *contextual* Threat Modeling menggunakan aplikasi OWASP Threat Dragon pada fungsional spesifik aplikasi yang memiliki kemungkinan adanya *threat* terbanyak, seperti fungsionalitas Login, Register, Forgot Password, Account Detail, Payment Process, Logout, dsb, lalu eksport hasilnya dalam bentuk file JSON
  3. File hasil threat modeling (XML dan JSON) disimpan ke dalam satu folder dengan *source code* dari aplkikasi agar dapat dilakukan versioning
  4. Analis Keamanan TI memasukkan seluruh daftar *threat* dijadikan sebagai Backlog pada project aplikasi yang ada di project management tool (Taiga/Jira/dll)
  5. Analis Keamanan TI melakukan aktivitas SAST dan Secure Code Review jika mendapatkan akses ke *source code* aplikasi. Hasil temuan kerentanan dilaporkan pada fitur Issue/Bug Report pada project aplikasi yang ada di project management tool (Taiga/Jira/dll)
  6. Analis Keamanan TI melakukan aktivitas Vulnerability Assessment atau Penetration Testing sesuai Standar dan Prosedur Pengujian Keamanan Aplikasi Berbasis Web. Hasil temuan kerentanan dilaporkan pada fitur Issue/Bug Report pada project aplikasi yang ada di project management tool (Taiga/Jira/dll)
  7. VAPT yang dimaksud adalah mulai dari melakukan Information Gathering pada target untuk mencari sebanyak-banyak informasi pada target aplikasi
  8. Kemudian Analis Keamanan TI melakukan Infrastruktur Penetration Testing menggunakan tools seperti nmap, nikto, dan Nuclei
  9. Terakhir, Analis Keamanan TI melakukan Web Application Penetration Testing menggunakan tool Burp Suite Professional dan/atau OWASP Zap dengan detail sebagai berikut:

Diagram

Description automatically generated

* 1. Seluruh hasil temuan didokumentasikan menjadi laporan akhir VAPT, lalu seluruh daftar kerentanan di eksport ke aplikasi OWASP Defectdojo untuk dilakukan Vulnerability Tracking & Management.
  2. Pengembang aplikasi WAJIB melakukan Vulnerability Triaginguntuk setiap temuan daftar *threat* dan kerentanan *(vulnerability)* yang telah dilaporkan oleh Analis Keamanan TI pada project management tool (Taiga/Jira/dll) di project aplikasi terkait dan juga pada laporan akhir dari aktivitas VAPT.
  3. Analis Keamanan TI meng-*update* setiap status perubahan masing-masing *threat* maupun *vulnerability* hasil Vulnerability Triaging yang dilakukan oleh Pengembang Aplikasi pada aplikasi OWASP Defectdojo yang merupak Centralized Vulnerability Tracking & Management seluruh kerentanan yang ditemukan
  4. Pekerjaan VAPT selesai dilakukan.