Assessment I (UTS)

Kelas RPL-Teknik Informatika
Mata Kuliah : Software Quality Assurance
Npm _Nama : 714222073_Ardini Yuanita Lubis

Studi Kasus 2 : Perusahaan B sedang mengembangkan platform e-commerce baru. (Ardini Yuanita Lubis)

1. **Bagaimana QA dapat memverifikasi keamanan platform e-commerce ini untuk melindungi data sensitif pelanggan, seperti informasi pembayaran dan data pribadi?**

Jawab :
Untuk memverifikasi kemanan data sebuah paltform e-commerce kita dapat membuat desain skenario pengujian keamanan yang mencakup pengujian kerentanan, pengujian penetrasi dan pengujian fungsionalitas yang berkaitan dengan keamanan data dimana semua aspek keamanan seperti enkripsi data, otentikasi, otorisasi dan manajemen sesi diuji secara menyeluruh.

2. **Bagaimana QA dapat menguji performa platform e-commerce ini dalam skenario beban tinggi, seperti saat ada peningkatan lalu lintas selama periode penjualan besar-besaran?**

Jawab :
Untuk menguji performa platform e-commerce, penguji dapat melakukan performance testing dimana indikator kinerja utama yang diuji meliputi :

a. Ketahanan : Pengujian ketahanan mengukur kemampuan perangkat lunak untuk menahan beban kerja untuk jangka waktu yang lama.
b. Beban : Pengujian beban mengukur kapasitas beban kerja perangkat lunak melalui simulasi interaksi pengguna.
c. Skalabilitas : Pengujian skalabilitas akan meningkatkan simulasi interaksi pengguna secara bertahap untuk menentukan kemampuan aplikasi terhadap jumlah pengguna yang lebih besar.
d. Spike : Pengujian lonjakan tiba-tiba atau spike meningkatkan simulasi interaksi pengguna untuk mengukur kinerja perangkat lunak dalam menangani lonjakan beban kerja.
e. Stress : Pengujian stres menerapkan beban kerja yang berat ke perangkat lunak untuk mengetahui seberapa banyak yang dapat ditanganinya sebelum berhenti bekerja.
f. Volume : Pengujian volume memberi perangkat lunak sejumlah besar data untuk diproses guna memeriksa kemampuan operasionalnya.

3. **Apa strategi yang tepat untuk menguji ketersediaan dan keandalan platform e-commerce ini, terutama saat menghadapi serangan DDoS atau serangan lainnya?**

Jawab :
Beberapa strategi yang dapat dilakukan untuk menguji ketersediaan dan keandalan platform e-commerce terhadap serangan DDoS atau serangan lainnya yaitu :

a. Melakukan uji beban dengan skenario pengujian yang mencakup serangan DDoS serta serangan lainnya. Lakukan pengujian berbagai jenis serangan DDoS dengan mengubah parameter seperti tingkat lalu lintas, frekuensi serangan, atau sumber serangan lalu mengamati perilaku sistem dan evaluasi kemampuan mitigasi serangan DDoS.

b. Melakukan pengujian Responsifitas yang bertujuan untuk melihat responsnya terhadap serangan atau situasi yang tidak terduga. Misalnya, uji respons terhadap serangan DDoS dan evaluasi kemampuan sistem dalam mengidentifikasi dan merespons serangan dengan cepat.
c. Melakukan pengujian pemulihan sistem setelah terjadinya serangan DDoS atau serangan lainnya. Verifikasi bahwa sistem dapat pulih dengan cepat setelah serangan, serta memulihkan data dan fungsi bisnis yang hilang atau terganggu. Kemudian memastikan adanya infrastruktur dan konfigurasi redundansi yang memungkinkan kelanjutan operasional e-commerce.
d. Melakukan pengujian keamanan jaringan. Selain serangan DDoS, pastikan juga menguji keandalan jaringan dan infrastruktur e-commerce terhadap serangan lainnya, seperti serangan penyusupan, serangan penyadapan, atau serangan penghancuran. Uji keefektifan sistem keamanan, firewall, deteksi intrusi, dan mekanisme proteksi lainnya dalam melindungi sistem dari serangan ini.
e. Melakukan simulasi skenario pemulihan bencana dan uji rencana pemulihan bencana e-commerce. Evaluasi kemampuan sistem untuk mengembalikan operasionalitas setelah terjadinya serangan besar atau bencana yang mengganggu operasi. Pastikan rencana pemulihan bencana diuji secara berkala dan diperbarui sesuai kebutuhan.
f. Melakukan evaluasi keamanan seperti firewall, enkripsi data, validasi input, dan pengelolaan akses yang tepat.

4. Bagaimana QA dapat memastikan kesesuaian platform e-commerce ini dengan standar kepatuhan industri yang relevan, seperti PCI-DSS (Payment Card Industry Data Security Standard)?

Jawab :
Untuk memastikan kesesuaian sebuah sistem e-commerce dengan standar PCI-DSS terdapat 12 persyaratan yang harus dipenuhi yang tergabung dalam 6 sasaran yaitu :

a. Membangun dan memelihara sistem dan jaringan yang aman
b. Melindungi data pemegang kartu
c. Menjalankan program pengelolaan kerentanan (vulnerability program)
d. Menerapkan tindakan/ langkah-langkah akses kendali yang kuat
e. Memantau dan menguji jaringan secara teratur
f. Membuat dan menjalankan kebijakan keamanan informasi

PCI-DSS Requirements

Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Rertrict physcal access to cardholder data.
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for all personal.

5. Bagaimana QA dapat menguji integrasi platform e-commerce ini dengan sistem backend, seperti sistem manajemen inventaris atau sistem keuangan perusahaan?

Jawab :
Untuk menguji integrasi sebuha platform e-commerce dengan sistem backend dapat dilakukan dengan menggunakan tools pengujian integrasi seperti postman, JMeter, Apache Kafka, Selenium, Charles Proxy, Custom Scripts dan Frameworks dimana pilihan tools yang digunakan disesuaikan pada kebutuhan spesifik, teknologi yang digunakan dan tingkat kompleksitas integrasi sitem yang akan diuji.

6. Jelaskan langkah-langkah yang akan Anda ambil untuk menguji keandalan dan ketersediaan platform e-commerce selama periode lonjakan lalu lintas atau peningkatan beban kerja !

Jawab :
Langkah-langkah untuk menguji keandalan dan ketersediaan platform e-commerce selama periode lonjakan lalu lintas atau peningkatan beban kerja yaitu :

a. Melakukan analisis beban dan identifikasi situasi yang dapat menyebabkan lonjakan lalu lintas ketika ada event seperti perayaan hari besar, penjualan khusus, atau acara promosi lalu membuat perencanaan pengujian untuk menguji keandalan dan ketersediaan platform e-commerce selama periode lonjakan tersebut.
b. Membuat skenario pengujian yang mencakup berbagai kasus penggunaan yang realistis selama periode lonjakan lalu lintas.
c. Melakukan uji beban dengan menggunakan alat pengujian beban seperti Apache JMeter untuk mensimulasikan beban lalu lintas yang tinggi pada platform e-commerce.
d. Melakukan evaluasi kinerja sistem e-commerce selama periode lonjakan lalu lintas. Ukur kecepatan respon, waktu muat halaman, dan latensi sistem saat beroperasi pada beban tinggi.
e. Melakukan uji skalabilitas sistem e-commerce untuk mengatasi peningkatan beban kerja.
f. Simulasikan skenario pemulihan setelah lonjakan lalu lintas.
g. Melakukan pengujian pada tingkat beban yang melebihi kapasitas normal sistem e-commerce.
h. Selama pengujian, gunakan alat pemantauan dan analisis kinerja untuk mengamati perilaku sistem dan menganalisis data.
i. Berdasarkan hasil pengujian, identifikasi dan perbaiki masalah yang ditemukan.
j. Setelah pengujian, pastikan untuk terus memantau dan memonitor kinerja sistem e-commerce secara berkala, termasuk selama periode lonjakan lalu lintas.

7. Buatlah serangkaian skenario pengujian untuk memverifikasi integrasi platform e-commerce dengan sistem backend yang relevan, seperti sistem manajemen inventaris atau sistem keuangan !

Jawab :
a. Skenario Pengujian Sinkronisasi Data Produk :
   - ✓ Mengubah atau memperbarui informasi produk di sistem keuangan perusahaan.
   - ✓ Memverifikasi bahwa perubahan data produk tersebut terlihat secara akurat di platform e-commerce.
   - ✓ Memastikan bahwa informasi harga, deskripsi, dan atribut produk yang ditampilkan di platform e-commerce sesuai dengan data yang disimpan di sistem keuangan.

b. Skenario Pengujian Proses Pembayaran :
   - ✓ Melakukan transaksi pembayaran melalui platform e-commerce.
   - ✓ Memverifikasi bahwa data pembayaran yang dikirim dari platform e-commerce ke sistem keuangan perusahaan sesuai dengan persyaratan yang ditetapkan.
   - ✓ Memastikan bahwa sistem keuangan dapat memproses pembayaran dengan benar dan menghasilkan konfirmasi pembayaran yang akurat.

c. Skenario Pengujian Integrasi Faktur:
   - ✓ Mengirimkan faktur ke pelanggan melalui platform e-commerce.

- ✓ Memverifikasi bahwa data faktur yang dibuat di platform e-commerce tersinkronisasi dengan sistem keuangan perusahaan.
- ✓ Memastikan bahwa sistem keuangan dapat menghasilkan dan mengelola faktur secara akurat, termasuk pengiriman, penagihan, dan pencatatan pembayaran.

d. Skenario Pengujian Rekonsiliasi Pembayaran :
   - ✓ Memverifikasi bahwa informasi pembayaran yang dicatat di platform e-commerce sesuai dengan data pembayaran yang diterima dan diproses di sistem keuangan perusahaan.
   - ✓ Melakukan pembandingan antara laporan pembayaran di platform e-commerce dengan laporan keuangan di sistem keuangan untuk memastikan keselarasan data.

e. Skenario Pengujian Pelaporan Keuangan :
   - ✓ Memverifikasi bahwa data transaksi dari platform e-commerce terintegrasi dengan benar ke dalam sistem keuangan untuk menyusun laporan keuangan perusahaan.
   - ✓ Memastikan bahwa informasi seperti pendapatan, biaya, laba, dan saldo akun terdokumentasi dengan benar dan sesuai dalam laporan keuangan.

f. Skenario Pengujian Pembaruan Data Pelanggan:
   - ✓ Mengubah atau memperbarui informasi pelanggan di sistem keuangan perusahaan.
   - ✓ Memverifikasi bahwa perubahan data pelanggan tersebut tercermin secara akurat di platform e-commerce.
   - ✓ Memastikan bahwa data seperti alamat, informasi kontak, atau preferensi pelanggan yang ditampilkan di platform e-commerce selaras dengan data yang disimpan di sistem keuangan.

g. Skenario Pengujian Integritas Data:
   - ✓ Memverifikasi bahwa data yang ditransfer antara platform e-commerce dan sistem keuangan perusahaan tidak mengalami kehilangan atau distorsi selama proses integrasi.
   - ✓ Memastikan bahwa integritas data dipertahankan, termasuk data transaksi, data pelanggan, dan data keuangan lainnya.

h. Skenario Pengujian Keamanan dan Otorisasi:
   - ✓ Memastikan bahwa data keuangan yang ditukar antara platform e-commerce dan sistem keuangan perusahaan dilindungi dengan baik melalui mekanisme keamanan seperti enkripsi data, otorisasi, dan autentikasi.
   - ✓ Memverifikasi bahwa sistem keuangan hanya menerima dan memproses data dari platform e-commerce yang sah dan diotorisasi.

i. Skenario Pengujian Ketergantungan Sistem :
   Menguji integrasi antara platform e-commerce dan sistem keuangan dalam situasi ketergantungan data atau proses bisnis. Misalnya, memastikan bahwa perubahan status pesanan di platform e-commerce mempengaruhi pembayaran dan penagihan yang sesuai di sistem keuangan.

j. Skenario Pengujian Pemulihan :
   - ✓ Simulasikan skenario pemulihan setelah terjadinya kegagalan sistem atau pemadaman.
   - ✓ Memverifikasi kemampuan sistem e-commerce dan sistem keuangan untuk pulih dan memastikan data terintegrasi dapat dipulihkan tanpa kehilangan atau kerugian.

8. Jelaskan bagaimana Anda akan menguji kemampuan platform e-commerce untuk melindungi informasi sensitif pelanggan, seperti data pembayaran !

Jawab :
Untuk menguji kemampuan sebuah platform e-commerce untuk melindungi informasi sensitif pembayaran maka akan dilakukan hal berikut :

a. Verifikasi Keamanan Komunikasi : Memastikan bahwa komunikasi antara platform e-commerce dan pengguna dilindungi dengan protokol enkripsi yang kuat, seperti HTTPS. Periksa sertifikat SSL dan pastikan bahwa pengguna melihat ikon gembok atau indikator keamanan lainnya yang menunjukkan koneksi aman.
b. Uji Enkripsi Data : Mengirimkan data pembayaran palsu melalui formulir pembayaran pada platform e-commerce dan memeriksa apakah data tersebut dienkripsi dengan benar sebelum dikirim. Periksa apakah data pembayaran dienkripsi saat disimpan dalam sistem dan apakah hanya pengguna yang berwenang yang dapat mengaksesnya.
c. Validasi Input : Memverifikasi bahwa platform e-commerce menerapkan validasi yang memadai terhadap data pembayaran yang dimasukkan oleh pengguna. Coba masukkan data yang tidak valid atau mencurigakan (misalnya, karakter khusus, skrip berbahaya, dll.) dan periksa apakah sistem mampu mencegah atau menolak input yang tidak sah.
d. Uji Proteksi Terhadap Serangan Injeksi : Mengirimkan data pembayaran yang berpotensi menyebabkan serangan injeksi, seperti serangan SQL atau XSS, dan memastikan bahwa platform e-commerce dapat mencegah atau mengatasi serangan tersebut. Pastikan bahwa input yang diterima diolah dengan benar dan tindakan mitigasi yang sesuai diterapkan.
e. Pengujian Keaslian Pengguna : Memeriksa keamanan autentikasi dan otorisasi pada platform e-commerce. Coba untuk melakukan akses yang tidak sah atau mencoba login dengan kredensial palsu. Pastikan bahwa sistem dapat mendeteksi dan mencegah akses yang tidak sah, dan hanya pengguna yang memiliki hak akses yang tepat yang dapat mengakses informasi data pembayaran.
f. Uji Proteksi Terhadap Serangan Pemalsuan : Melakukan serangan pemalsuan identitas pada data pembayaran yang dikirimkan dari platform e-commerce. Periksa apakah sistem dapat mendeteksi atau mencegah pengiriman data palsu dan memastikan bahwa hanya data yang valid yang dapat diterima dan diproses.
g. Pengujian Metode Pembayaran : Menguji berbagai metode pembayaran yang didukung oleh platform e-commerce, seperti kartu kredit, transfer bank, dompet digital, dan lainnya. Pastikan bahwa data pembayaran yang dikirim melalui setiap metode diperlakukan dengan benar, disimpan secara aman, dan tidak terjadi kebocoran atau manipulasi data.
h. Pengujian Proteksi Data : Memeriksa apakah platform e-commerce melindungi data pembayaran dengan metode seperti tokenisasi atau enkripsi end-to-end. Coba untuk memperoleh atau mengakses data pembayaran yang tersimpan dalam sistem dan pastikan bahwa data tersebut tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang.
i. Pengujian Kebocoran Informasi: Memeriksa apakah terdapat potensi kebocoran informasi dalam platform e-commerce yang dapat mengakibatkan akses tidak sah ke data pembayaran. Gunakan alat penguji kebocoran informasi untuk memindai platform dan memastikan bahwa tidak ada data sensitif yang dapat ditemukan secara tidak sengaja.
j. Pemantauan Keamanan : Mengimplementasikan sistem pemantauan keamanan yang dapat mendeteksi atau memberi peringatan terhadap aktivitas mencurigakan atau anormal yang terkait dengan data pembayaran. Pastikan bahwa platform e-commerce dilengkapi dengan mekanisme pemantauan yang dapat mengidentifikasi potensi serangan atau pelanggaran keamanan.

9. Identifikasi beberapa metode pengujian yang dapat digunakan untuk memverifikasi keamanan platform e-commerce terhadap serangan potensial, seperti serangan injeksi SQL atau cross-site scripting (XSS) !

Jawab :
Metode Pengujian yang digunakan untuk memverifikasi keamanan e-commerce terhadap serangan potensial seperti serangan Injeksi SQL yaitu :

a. Pengujian Serangan Injeksi :
   - ✓ Menguji aplikasi e-commerce untuk mengidentifikasi celah serangan injeksi seperti SQL injection, XML injection, atau command injection.
   - ✓ Memasukkan input yang jahat atau berbahaya ke dalam formulir atau parameter aplikasi untuk melihat apakah aplikasi dapat memfilter dan memvalidasi input dengan benar

b. Pengujian Cross-Site Scripting (XSS) :
   - ✓ Menguji aplikasi e-commerce untuk menemukan kerentanan XSS yang dapat memungkinkan serangan injeksi kode berbahaya ke dalam halaman web.
   - ✓ Memasukkan skrip atau tag HTML yang tidak aman ke dalam input pengguna untuk melihat apakah aplikasi dapat menyaring dan menghindari eksekusi skrip yang tidak diinginkan.

c. Pengujian Cross-Site Request Forgery (CSRF) :
   - ✓ Menguji aplikasi e-commerce untuk menemukan kerentanan CSRF yang dapat memungkinkan serangan yang memanipulasi tindakan yang dilakukan oleh pengguna yang terautentikasi.
   - ✓ Mencoba mengirimkan permintaan palsu (forged request) yang merusak atau mengubah data pengguna yang sah untuk melihat apakah aplikasi dapat mendeteksi dan mencegah serangan CSRF.

d. Pengujian Manipulasi Parameter URL
   - ✓ Menguji aplikasi e-commerce untuk menemukan kerentanan URL manipulation yang dapat memungkinkan serangan seperti pengubahan parameter URL atau akses ke halaman terlarang.
   - ✓ Memodifikasi parameter URL untuk melihat apakah aplikasi dapat memvalidasi dan memverifikasi parameter dengan benar sebelum mengambil tindakan yang diinginkan.

e. Pengujian Brute Force dan Kehandalan Kata Sandi
   - ✓ Menguji aplikasi e-commerce untuk melihat apakah ada kerentanan terhadap serangan brute force yang mencoba menebak kata sandi dengan mencoba berbagai kombinasi.
   - ✓ Menguji keandalan kata sandi yang digunakan oleh pengguna, seperti panjang minimal, kompleksitas, dan kebijakan pergantian kata sandi.

f. Pengujian Keamanan Sesi dan Otentikasi
   - ✓ Menguji aplikasi e-commerce untuk menemukan kerentanan keamanan sesi atau celah autentikasi yang dapat memungkinkan serangan seperti sesi hijacking atau penggunaan otentikasi palsu.
   - ✓ Memeriksa apakah aplikasi menggunakan mekanisme sesi yang aman, menerapkan otentikasi yang kuat, dan melindungi informasi otentikasi pengguna dengan baik.

g. Pengujian Enkripsi dan Proteksi Data
   - ✓ Menguji penggunaan protokol enkripsi seperti HTTPS untuk melindungi komunikasi antara pengguna dan aplikasi e-commerce.
   - ✓ Memeriksa apakah data sensitif seperti informasi pembayaran atau data pengguna dienkripsi dengan benar saat disimpan atau ditransmisikan.

h. Pengujian Manajemen Kesalahan
   - ✓ Menguji aplikasi e-commerce untuk menemukan kerentanan manajemen kesalahan yang dapat memberikan informasi sensitif atau memaparkan kelemahan sistem.
   - ✓ Mencoba memasukkan input yang tidak valid atau mencoba memanipulasi aplikasi untuk melihat apakah aplikasi memberikan tanggapan yang tepat dan tidak memberikan informasi sensitif yang tidak seharusnya.

10. Bagaimana Anda akan melakukan pengujian fungsional untuk memverifikasi bahwa platform e-commerce beroperasi dengan benar dan memenuhi persyaratan bisnis yang ditetapkan?

Jawab :
Untuk melakukan pengujian fungsional serta memverifikasi bahwa sebuah sistem e-commerce sudah sesuai dengan requirement bisnis maka akan dilakukan hal berikut ini :

a. Pengujian Fungsional Modul :
   - ✓ Menguji setiap modul fungsional di platform e-commerce, seperti pendaftaran pengguna, pencarian produk, penambahan produk ke keranjang belanja, proses pembayaran, pengiriman, dll.
   - ✓ Memastikan bahwa setiap modul beroperasi sesuai dengan kebutuhan dan persyaratan bisnis yang ditetapkan.
   - ✓ Menguji fungsionalitas kunci, seperti validasi input, perhitungan harga, integrasi dengan sistem keuangan, pembaruan stok, dll.

b. Pengujian Fungsional Aliran Bisnis :
   - ✓ Menguji aliran bisnis utama di platform e-commerce, mulai dari proses pemesanan hingga pengiriman dan penagihan.
   - ✓ Memverifikasi bahwa aliran bisnis berjalan dengan benar sesuai dengan langkah-langkah yang diharapkan.
   - ✓ Menguji skenario khusus, seperti pembatalan pesanan, pengembalian barang, atau perubahan informasi pengiriman.

c. Pengujian Fungsional Integrasi :
   - ✓ Memverifikasi integrasi antara platform e-commerce dan sistem backend yang relevan, seperti sistem inventaris, sistem keuangan, atau sistem pengiriman.
   - ✓ Menguji transfer data dan informasi yang tepat antara platform e-commerce dan sistem backend.
   - ✓ Memastikan bahwa sistem backend memberikan respons yang akurat dan sesuai dengan permintaan dari platform e-commerce.

d. Pengujian Fungsional Responsif :
   - ✓ Menguji responsivitas platform e-commerce terhadap tindakan pengguna, seperti mengklik tombol, mengisi formulir, atau melakukan transaksi.
   - ✓ Memverifikasi bahwa platform e-commerce memberikan umpan balik yang tepat waktu dan menunjukkan indikasi yang jelas tentang proses yang sedang berlangsung.
   - ✓ Menguji kinerja platform e-commerce dalam menanggapi permintaan pengguna dengan waktu respons yang cepat.

e. Pengujian Fungsional Kompatibilitas Perangkat dan Browser :
   - ✓ Menguji platform e-commerce di berbagai perangkat dan browser yang umum digunakan oleh pengguna, termasuk desktop, ponsel, dan tablet.
   - ✓ Memastikan bahwa platform e-commerce terlihat dan berfungsi dengan baik di semua perangkat dan browser yang didukung.
   - ✓ Menguji responsivitas tata letak, tampilan, dan interaksi pada berbagai ukuran layar dan resolusi.

f. Pengujian Fungsional Manajemen Konten :
   - ✓ Menguji fungsionalitas manajemen konten, seperti penambahan produk, pengeditan deskripsi, pengaturan harga, atau perubahan halaman utama.
   - ✓ Memastikan bahwa manajemen konten dilakukan dengan benar dan perubahan yang diterapkan terlihat di platform e-commerce.
   - ✓ Menguji validasi dan validitas data yang dimasukkan dalam manajemen konten, serta kemampuan sistem untuk menyimpan dan menampilkan data dengan benar.

g. Pengujian Fungsional Fitur Khusus :
   - ✓ Menguji fitur khusus yang unik atau inovatif yang ada di platform e-commerce, seperti rekomendasi produk, sistem ulasan pengguna, filter pencarian yang kompleks, atau fitur sosial.
   - ✓ Memverifikasi bahwa fitur-fitur ini beroperasi sesuai dengan kebutuhan dan persyaratan bisnis yang ditetapkan.
   - ✓ Menguji skenario penggunaan yang berbeda untuk fitur-fitur khusus tersebut dan memastikan bahwa hasilnya sesuai dengan yang diharapkan.

h. Pengujian Fungsional Responsif pada Beban Tinggi :
   - ✓ Menguji platform e-commerce dengan meningkatkan beban kerja atau lalu lintas pengguna secara signifikan.
   - ✓ Memastikan bahwa platform e-commerce tetap beroperasi dengan baik dan memberikan respons yang cepat bahkan dalam situasi beban tinggi.
   - ✓ Menguji kapasitas skala platform e-commerce untuk menangani jumlah pengguna dan transaksi yang lebih tinggi dari biasanya.

i. Pengujian Fungsional Keamanan :
   - ✓ Menguji fitur keamanan platform e-commerce, seperti autentikasi pengguna, perlindungan data sensitif, perlindungan terhadap serangan injeksi atau XSS, dan pengaturan izin akses.
   - ✓ Memverifikasi bahwa fitur keamanan berfungsi dengan baik dan melindungi informasi data pengguna, data pembayaran, dan data sensitif lainnya.
   - ✓ Menguji keamanan transaksi dan pengiriman data melalui enkripsi dan protokol keamanan yang sesuai.

j. Pengujian Fungsional Ketersediaan dan Kinerja :
   - ✓ Menguji ketersediaan dan kinerja platform e-commerce dalam situasi penggunaan nyata dengan menggunakan alat pengujian beban dan pemantauan kinerja.
   - ✓ Memastikan bahwa platform e-commerce tetap dapat diakses dan memberikan respons yang cepat bahkan dalam situasi beban tinggi atau kondisi jaringan yang buruk.
   - ✓ Menguji toleransi kesalahan dan pemulihan dari kegagalan sistem untuk memastikan bahwa platform e-commerce dapat pulih dengan cepat dan tanpa kehilangan data atau fungsionalitas.