



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA
Kampus 2 Universitas Siliwangi Gedung Informatika Fakultas Teknik
Kel. Mugarsari, Kec. Tamansari, Kota Tasikmalaya
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: if.unsil.ac.id Posel: informatika@unsil.ac.id

**NASKAH SOAL UJIAN TENGAH SEMESTER
SEMESTER GENAP TAHUN AJARAN 2024/2025**

Kode/Nama Mata Kuliah : Keamanan Informasi (A, B, C, D, E, F)
SKS : 3 SKS
Hari/ Tanggal : Selasa / 13 Maret 2025
Waktu : 100 Menit
Dosen Pengampu : Ir. Alam Rahmatulloh, S.T., M.T., MCE., IPM.
Program Studi : Informatika

Petunjuk Umum:

1. Ujian ini bersifat kelompok (setiap kelompok terdiri dari maksimal 5 orang).
2. Setiap kelompok harus menganalisis satu studi kasus yang berbeda mengenai bug/vulnerability pada aplikasi/sistem berbasis web. Boleh app/sistem sendiri atau dari Repository orang lain/public.
3. Hasil analisis harus mencakup langkah-langkah identifikasi, pemasangan Web Application Firewall (WAF), serta evaluasi ulang setelah pemasangan keamanan.
4. Berikan rekomendasi perbaikan berdasarkan hasil analisis setelah pemasangan WAF.
5. Laporan dikumpulkan dalam bentuk dokumen tertulis dan dipresentasikan di kelas.
6. Aplikasi/sistem yang dianalisis dapat dijalankan pada virtualisasi (VM) atau Virtual Private Server (VPS). Jenis virtualisasi yang digunakan bebas sesuai preferensi kelompok.
7. Pengujian keamanan (penetration testing) dapat mengacu pada standar OWASP Top 10 vurl, dengan fokus pada eksploitasi dan mitigasi dari ancaman yang relevan dengan sistem yang dianalisis.

Soal:

1. Identifikasi Bug/Vulnerability
 - a. Pilih salah satu aplikasi/sistem berbasis web sebagai studi kasus (setiap kelompok harus memilih sistem yang berbeda).
 - b. Lakukan analisis terhadap bug atau celah keamanan yang ada dalam aplikasi/sistem tersebut.
 - c. Jelaskan metode yang digunakan untuk mengidentifikasi vulnerability (misalnya: scanning tools, manual testing, penetration testing yang mengacu pada OWASP Top 10).
2. Implementasi Keamanan dengan WAF
 - a. Pasang Web Application Firewall (WAF) pada server yang digunakan oleh sistem tersebut.
 - b. Konfigurasi WAF sesuai dengan kebutuhan sistem untuk menanggulangi vulnerability yang telah ditemukan.
 - c. Dokumentasikan proses pemasangan dan konfigurasi WAF secara sistematis.
3. Evaluasi Setelah Pemasangan Keamanan
 - a. Lakukan pengujian ulang terhadap aplikasi/sistem setelah pemasangan WAF.
 - b. Bandingkan hasil sebelum dan sesudah pemasangan keamanan.
 - c. Analisis efektivitas WAF dalam menangani bug/vulnerability yang ditemukan sebelumnya.
4. Rekomendasi Perbaikan
 - a. Berdasarkan hasil analisis, berikan rekomendasi perbaikan untuk meningkatkan keamanan aplikasi/sistem secara keseluruhan.



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS SILIWANGI
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA
Kampus 2 Universitas Siliwangi Gedung Informatika Fakultas Teknik
Kel. Mugarsari, Kec. Tamansari, Kota Tasikmalaya
Telepon (0265) 330634, 333092 Faksimil (0265) 325812
Laman: if.unsil.ac.id Posel: informatika@unsil.ac.id

- b. Sertakan solusi jangka pendek dan jangka panjang untuk mengatasi potensi serangan serupa di masa depan.

Soal	Bobot	Kaitan CPMK/ Sub-CPMK
Identifikasi bug/vulnerability (25%)	25	Sub-CPMK-1
Implementasi keamanan dengan WAF (25%)	25	Sub-CPMK-2
Evaluasi setelah pemasangan WAF (25%)	25	Sub-CPMK-3
Rekomendasi perbaikan (15%)	15	Sub-CPMK-1
Presentasi dan laporan akhir (10%)	10	Sub-CPMK-3

Ketua Program Studi

Unit Penjaminan Mutu

.....

.....