BAB V
PENUTUP

5.1 Simpulan

Penelitian ini telah berhasil dilakukan karena dapat mengidentifikasi dan menganalisis kerentanan yang ada pada web aplikasi *Inventory Management* terkhusus pada bagian fitur *upload* melalui *penetration testing* yang dilakukan sesuai standar keamanan *OWASP ASVS*. Implementasi pengujian ini dilakukan dengan bantuan *tools* seperti *Burp Suite.*

Selama proses pengujian, *tools* seperti *Burp Suite* membantu untuk menangkap *request,* memanipulasi parameter, dan eksploitasi terhadap fitur yang tidak divalidasi dengan baik. Temuan ini menunjukkan bahwa fitur *upload* dalam aplikasi belum menerapkan mekanisme keamanan yang memadai.

Dengan adanya penelitian ini, diharapkan pengembang dapat lebih memahami pentingnya pengamanan terhadap sebuah web aplikasi sehingga pihak-pihak terkait tidak ada yang dirugikan.

5.2 Saran

Pertama penulis ingin berterima kasih kepada pengembang web aplikasi ini, karena hal itu penulis dapat mempelajari dan mengeksplorasi teknik pengujian keamanan pada media yang diberikan untuk penelitian penulis mengenai keamanan suatu aplikasi dalam dunia digital dan modern ini. Namun, ada beberapa saran dari penulis untuk pengembang adalah untuk lebih memperhatikan keamanan web yang dibuat agar lebih dipertimbangkan untuk implementasinya di masa mendatang:

1. Tingkat Kesadaran Keamanan Developer

Pengembang disarankan untuk lebih memperhatikan aspek keamanan, terutama dalam hal validasi input pada fitur upload file. Fitur ini sering menjadi titik masuk bagi serangan seperti backdoor jika tidak ditangani dengan benar.

Implementasi filter tipe file, pembatasan ukuran file, dan pemisahan direktori penyimpanan merupakan langkah awal yang penting.

2. Simulasi Pengujian di Lingkungan Aman

Penetration testing sebaiknya dilakukan di lingkungan lokal (localhost) atau sandbox guna menghindari dampak yang tidak diinginkan pada sistem produksi. Hal ini juga mendukung praktik keamanan yang lebih terkontrol dan bertanggung jawab sehingga tidak merusak ekosistem aplikasi lainnya.

3. Fokus pada Teknik dan Skema *Bypass*

Praktisi pengujian keamanan diharapkan untuk mendalami teknik manipulasi seperti file extension spoofing, content-type spoofing, serta kelemahan pada filter sisi server. Pemahaman mendalam terhadap teknik-teknik ini akan meningkatkan efektivitas dalam mendeteksi dan mencegah celah keamanan.

4. Pentingnya Dokumentasi dan Etika Uji

Setiap tahapan pengujian keamanan wajib didokumentasikan dengan baik dan dilakukan secara etis. Penelitian atau pengujian sebaiknya dilakukan setelah mendapatkan izin eksplisit dari pemilik sistem. Hal ini penting untuk memastikan bahwa proses pengujian dilakukan dalam koridor hukum, etika, serta tanggung jawab akademik.