BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian *penetration testing* pada *website* XYZ yang telah dilakukan menggunakan metode OWASP *Web Security Testing Guide* (WSTG) menggunakan tujuh teknik yaitu *Information gathering, Configuration and Deployment Management Testing, Identity Management Testing, Input Validation Testing, Testing For Error Handling, Business Logic Testing* dan *Client Side Testing.*

1. Berikut rangkuman kerentanan yang telah ditemukan dalam kelompok tahapan :

   a. Information Gathering

   Information gathering yang dilakukan menggunakan teknik *Fingerprint Web Server* dengan *tools* Burp *Suite*, ditemukan versi PHP 8.0.19 dan *server* yang digunakan yaitu *Litespeed.*

   b. Configuration and Deployment Management Testing

   Configuration and Deployment Management Testing yang dilakukan menggunakan teknik *Review Old Backup and Unreferenced Files for Sensitive Information* dengan *tools dirb,* ditemukan URL yang seharusnya bersifat *private* seperti halaman *log in admin, cpanel, webmail, file web.config* yang dapat didownload dan halaman yang tidak digunakan atau belum diimplementasikan.

   c. *Identity Management Testing*

   Identity Management Testing yang dilakukan menggunakan teknik *Test User Registration Process* dengan *tools* Burp *Suite*, tidak dapat membuat akun, memverifikasi *e-mail* dan bahkan meminta mengirim kembali *e-mail* verifikasi tidak dapat dilakukan.

   d. *Input validation Testing*

   Input validation Testing yang dilakukan menggunakan *tools* Burp *Suite,* dengan teknik *Testing For Stored Cross Site Scripting* dapat membuat akun dengan menggunakan *e-mail* palsu atau salah.

   e. *Testing For Error Handling*

Testing For Error Handling yang dilakukan menggunakan teknik *Testing For Improper Error Handling* dengan *tools* Burp *Suite* terdapat pengendalian *error* yang kurang baik.

f. *Business Logic Testing*

Business Logic Testing yang dilakukan menggunakan *tools* Burp *Suite,* dengan teknik *Register Tanpa Checklist*, pengguna *website* dapat melakukan *registe*r tanpa mencentang syarat dan ketentuan. Tidak ada validasi input, pengguna *website* dapat melakuan sembarang input pada *field box* yang disediakan oleh *website*. *Question* wizard, *responden* dapat melewati pertanyaan pertama ke pertanyaan yang diinginkan sebelum menjawab pertanyaan yang *mandatory*.

2. Berikut rangkuman rekomendasi untuk mengatasi kerentanan yang telah ditemukan dalam kelompok tahapan:

a. Information Gathering

Information gathering, rekomendasi yang diberikan yaitu sebaiknya mengatur *web server* untuk mengobfuskasi informasi yang terdapat didalam *headers,* menggunakan *server reverse proxy* untuk menciptakan lapisan keamanan tambahan dan memastikan perangkat lunak menggunakan versi terbaru.

b. Configuration and Deployment Management Testing

Configuration and Deployment Management Testing, rekomendasi yang diberikan yaitu sebaiknya secara rutin memeriksa laman yang terekspos ke publik, memperhatikan laman yang bersifat internal, memperhatikan kode yang menangani *error* dan menutup laman yang masih dalam tahap pengembangan.

c. *Identity Management Testing*

Identity Management Testing, rekomendasi yang diberikan yaitu sebaiknya periksa kembali pada *backend deployment laravel* dan *autentikasi* SMTP *Server.*

d. Input validation *Testing*

Input validation Testing, rekomendasi yang diberikan yaitu sebaiknya periksa kembali pada bagian *backend* dan tambahkan fungsi *validation e-mail.*

e. *Testing For Error Handling*

Testing For Error Handling, rekomendasi yang diberikan yaitu sebaiknya menggunakan *error handling* yang lebih pantas dengan tidak menampilkan kode *error* internal dari *website* XYZ.

f. *Business Logic Testing*

Business Logic Testing, rekomendasi yang diberikan yaitu sebaiknya menggunakan *strict validation* sehingga responden tidak dapat membuat akun sebelum mencentang syarat dan ketentuan, tidak dapat membuat akun dengan mengisi sembarang pada *field box* dan tidak dapat melewati pertanyaan tanpa menjawab pertanyaan yang *mandatory*.

5.2 Saran

Berdasarkan hasil penelitian *penetrasi testing* pada *website* XYZ diperlukan melakukan pengujian celah keamanan rutin yang lebih mendalam dan detail guna mencari kelemahan terbaru atau tidak disadari oleh pihak pengembang *website* XYZ. Adapun saran untuk penelitian selanjutnya yaitu mengujicoba metode yang belum diterapkan sehingga dapat mengetahui celah secara keseluruhan. Berikut adalah saran untuk celah yang ditemukan pada *website* XYZ :

a. Terhadap *admin website* XYZ :
   1. Sebaiknya menerapkan dan memelihara protokol keamanan yang baik dan benar sehingga dapat mengamankan *website* XYZ.
   2. Sebaiknya memastikan keamanan dan privasi *website* XYZ baik internet maupun intranet yang ada pada *website* XYZ.

b. Terhadap pengembang :
   1. Sebaiknya menerapkan, menguji dan megoperasikan teknik keamanan *website* XYZ.
   2. Sebaiknya melakukan *quality test* pada *website* XYZ.

c. Terhadap piham instansi pemilik *website* :
   1. Sebaiknya memantau dan meningkatkan keamanan *website* XYZ.

2. Sebaiknya mempekerjakan *pentester* untuk mengetahui tingkat keamanan dari *website* XYZ.
3. Sebaiknya mengelola dan memastikan *website* XYZ tetap aman dengan melakukan pemeriksaan keamanan secara berkala.