## LAMPIRAN

Hasil s*ecurity assessment* pada web aplikasi Perguruan Tinggi XYZ.

### 1. Tabel Kerentanan

Di bawah ini akan dijelaskan mengenai temuan celah keamanan pada aplikasi web MoU Perguruan Tinggi XYZ menggunakan *tool* Nessus *Vulnerability Scanner*.

| No | Jenis Kerentanan | Tingkat | Deskripsi |
|---|---|---|---|
| 1 | CGI Generic SQL Injection | *High* | url web aplikasi bisa menerima parameter yang bisa disisipi kueri sql *injection* |
| 2 | CGI Generic Cookie Injection Scripting | *Medium* | Dengan memanfaatkan masalah ini, seorang penyerang mungkin mampu melakukan *cookies injection*. Tergantung pada struktur aplikasi web jenis serangan yang bisa dilakukan *session fixation* |
| 3 | Web Application SQL Backend Identification | *Medium* | *database* yang diidentifikasi berupa mysql |
| 4 | CGI Generic XSS | *Medium* | Remote *web server host* CGI gagal untuk membersihkan *request string* dari *javascript* yang berbahaya. Serangan yang mungkin terjadi penyerang menjalan kan *javascript* pada web tersebut |
| 5 | CGI Generic HTML Injections | *Medium* | Remote *web server host* CGI gagal untuk membersihkan *request string* dari *javascript* yang berbahaya. Serangan yang mungkin terjadi penyerang menjalan kan *javascript* pada web tersebut |

| No | Jenis Kerentanan | Tingkat | Deskripsi |
|---|---|---|---|
| 6 | Web Application Information Disclosure | *Medium* | web aplikasi yang ada di *remote* web server menunjukkan *physical path* ke direktori ketika mengirimkan *malformed* request |
| 7 | Web Application Potentially Vulnerable to Clickjacking | *Medium* | Remote web server tidak menetapkan X-Frame-Option response header. Serangan yang mungkin dilakukan adalah clickjacking |
| 8 | Web Server Transmits Cleartext Credentials | *Low* | Web server mengirimkan data kredensial dalam bentuk *cleartext* |
| 9 | Web mirroring | *Info* | Pada *link* berikut terdapat parameter yang bisa dilakukan web *miror* dan parameter ini juga bisa dieksploitasi untuk SQLInjection. |
| 10 | Nessus SYN scanner | *Info* | Terdapat *port* setengah terbuka: *port* 80, 25, 22, 8080 |
| 11 | Web Server Directory Enumeration | *Info* | Beberapa direktori pada *web server* bisa ditemukan |
| 13 | HyperText Transfer Protocol (HTTP) Information | *Info* | Informasi tentang konfigurasi http bisa dilihat seperti versi yang digunakan, http pipelining |
| 14 | CGI Generic Tests Load Estimation (all tests) | *Info* | Skrip untuk menghitung jumlah maksimal permintaan yang akan dilakukan oleh *generic web test* |
| 16 | CGI Generic Tests HTTP Errors | *Info* | Ditemukan eror ketika menjalankan serangan cgi |
| 17 | Web Application Potentially Sensitive CGI Parameter Detection | *Info* | Aplikasi menggunakan parameter cgi untuk mengontrol informasi penting |

| No | Jenis Kerentanan | Tingkat | Deskripsi |
|---|---|---|---|
| 18 | Web Server Allows Password Auto-Completion | *Info* | Attribute autocomplete tidak di non-aktifkan pada field *password* |
| 19 | CGI Generic Injectable Parameter | *Info* | Memungkinkan halaman web untuk membaca parameter yang berbahaya pada url |
| 21 | External URLs | *Info* | Terdapat *link* ke *website* eksternal ketika melakukan *crawl* pada *web server* |
| 22 | Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header | *Info* | Beberapa respons pada *web server* tidak menetapkan frame header CSP |
| 23 | Missing or Permissive X-Frame-Options HTTP Response Header | *Info* | Beberapa respons pada *web server* tidak menetapkan X-Frame-Options |
| 24 | Backported Security Patch Detection (PHP) | *Info* | *Security patch* pada *web server* dapat dilakukan backported tanpa mengganti nomor versinya. |
| 25 | Web Application Cookies Not Marked Secure | *Info* | HTTP *session cookies* dikirimkan dalam bentuk *cleartext* tanpa enkripsi |
| 26 | Web Application Sitemap | *Info* | *Web server* terhubung dengan konten yang bisa dieksploitasi dengan *crawl website* |

**2. Rancangan Penyerangan**

Rancangan penyerangan adalah skenario yang dibuat oleh peneliti untuk untuk melakukan simulasi serangan pada sistem web aplikasi MoU. Rancangan ini memanfaatkan dua celah keamanan. Penjelasan singkat mengenai rancangan penyerangan, akan dijabarkan pada tabel dibawah ini.

| No. | Jenis Kerentanan | Tingkat | Deskripsi |
|---|---|---|---|
| 1 | CGI Generic SQL Injection | High | url web aplikasi bisa menerima parameter yang bisa disisipi *kueri* SQL Injection |

### 3. Hasil Simulasi Penyerangan

Hasil yang didapatkan peneliti dari proses simulasi penyerangan yang dilakukan adalah sebagai berikut

| No | Celah yang Diuji | Dampak | Tool | Success/Un |
|---|---|---|---|---|
| 1 | CGI Generic SQL Injection | Url pada web MoU memiliki parameter yang bisa disisipi malicious code untuk membaca data penting yang terdapat pada database aplikasi seperti nama pengguna dan kata sandi. | SQL Injection | Success |