PENGUJIAN KEAMANAN BASIS DATA SISTEM INFORMASI BERBASIS WEB

Andria[1], Wahyu Ambar Ningrum[2], Iqbal Mubarok[3]
[1,2,3]Universitas PGRI Madiun
e-mail : [1]andria@unipma.ac.id, [2]wahyumasif@gmail.com, [3]iqballmoe06@gmail.com

ABSTRACT

The database has a very important role in a web-based information system. In its function as a data storage area which can then be managed into necessary information as needed, of course its safety is necessary. In ensuring the security of a database, a test of the database is needed whose results can be used as a measure of the level of security and if a security gap or vulnerability is found, what actions need to be done appropriately so that the database security testing can also be used as a preventive effort and to minimize the risk of a vulnerability gap that is prone to abuse by irresponsible parties. Based on the results of database security testing for web-based information systems, it was found that there were vulnerabilities in the database layer. The occurrence of errors or deficiencies in the development of information systems on the aspect of data security could have the potential for SQL Injection attacks that allow hackers to access the database on a web server, so that the privacy of user data or sensitive information in it is very risky to be misused so that preventive efforts are needed as a precautionary measure. in securing an information system. Efforts that can be made to prevent or improve the SQL Injection Bug include providing encryption at the database layer, validating input, hiding error notifications or error messages and manipulating Web URLs.

Keywords : *Databases, Information Systems, Security Testing, SQL Injection, Website*

INTISARI

Basis data memiliki peranan yang sangat penting pada suatu sistem informasi berbasis web. Dalam fungsinya sebagai tempat penyimpanan data yang kemudian dapat dikelola menjadi suatu informasi yang diperlukan sesuai kebutuhan tentu perlu dipastikan keamanannya. Dalam memastikan keamanan suatu basis data diperlukan suatu pengujian terhadap basis data yang hasilnya dapat digunakan sebagai tolak ukur sejauh mana tingkat keamanannya dan apabila ditemukan adanya celah keamanan atau kerentanan maka tindakan seperti apa yang perlu dilakukan secara tepat sehingga dari pengujian keamanan basis data tersebut juga dapat dijadikan sebagai upaya preventif dan meminimalisir resiko dari adanya celah kerentanan yang rawan disalahgunakan oleh pihak yang tidak bertanggung jawab. Berdasarkan hasil pengujian keamanan basis data sistem informasi berbasis web ditemukan adanya celah kerentanan pada lapisan basis data. Terjadinya kesalahan atau kekurangan dalam pengembangan sistem informasi pada aspek keamanan data dapat berpotensi adanya serangan SQL Injection yang memungkinkan peretas dapat mengakses basis data pada suatu web server, sehingga privasi data pengguna atau informasi sensitif didalamnya sangat beresiko untuk disalahgunakan sehingga perlu adanya upaya preventif sebagai langkah antisipasi dalam mengamankan suatu sistem informasi. Upaya yang dapat dilakukan untuk pencegahan maupun perbaikan terhadap Bug SQL Injection diantaranya memberikan enkripsi pada lapisan basis data, melakukan validasi terhadap input, menyembunyikan notifikasi kesalahan atau pesan error dan melakukan manipulasi URL Web.

Kata kunci : *Basis Data, Injeksi SQL, Pengujian Keamanan, Sistem Informasi, Situs Web*

1. PENDAHULUAN

Adanya Kejahatan Siber (*cybercrime*) telah menjadi ancaman di berbagai kehidupan manusia, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet. Hal ini merupakan akibat dari pesatnya perkembangan teknologi informasi, sehingga setiap perkembangan pada hakikatnya membawa dampak yang positif maupun negatif. Salah satu dampak negatifnya adalah adanya penyalahgunaan data dan informasi pribadi. Kelemahan dunia siber tidak terlepas dari kurangnya pengaturan atau belum adanya regulasi mengenai keamanan siber dan perlindungan data pribadi, sehingga menimbulkan kerancuan ditengah-tengah anggota masyarakat (Aswandi, 2020). Banyaknya kasus peretasan data menjadi suatu ancaman dalam penerapan dan pemanfaatan suatu sistem informasi berbasis web. Dilansir dari situs *cyberthreat.id*, terdapat beragam kasus peretasan data terbesar sepanjang masa yang menimpa di sejumlah perusahaan besar di dunia dan beberapa marketplace ternama tanah air (Suud, 2020). Basis data memiliki peranan yang sangat penting pada suatu sistem informasi. Dalam fungsinya sebagai tempat penyimpanan data yang kemudian dapat dikelola menjadi suatu informasi yang diperlukan sesuai kebutuhan tentu perlu dipastikan keamanannya. Dalam memastikan keamanan suatu basis data diperlukan suatu pengujian terhadap basis data yang hasilnya dapat digunakan sebagai tolak ukur sejauh mana tingkat keamanannya dan apabila ditemukan

adanya celah keamanan atau kerentanan maka tindakan seperti apa yang perlu dilakukan secara tepat sehingga dari pengujian keamanan basis data tersebut juga dapat dijadikan sebagai upaya preventif sekaligus meminimalisir resiko dari adanya celah kerentanan yang rawan disalahgunakan oleh pihak yang tidak bertanggung jawab.

Adapun penelitian sebelumnya yang berjudul "Audit Keamanan *Website* Menggunakan *Uniscan* di *Kali Linux"*, penelitian ini membahas evaluasi berupa *audit* sistem keamanan *website* sebagai upaya preventif terhadap adanya suatu aksi peretasan yang dapat merugikan. Pada penelitian ini, *tool* yang digunakan adalah *Uniscan* yang merupakan alat scanner kerentanan aplikasi *web* yang sudah tersedia pada sistem operasi *Kali Linux*. Penelitian ini bertujuan untuk menganalisis adanya kerentanan pada suatu *website* sehingga dapat membantu para pengelola web dalam mengaudit sistem keamanan pada websitenya. (Andria, 2020a)

Adapula penelitian dengan judul "Analisis Celah Keamanan *Website* Menggunakan *Tools WEBPWN3R* di *Kali Linux*", menjelaskan bahwa adanya celah keamanan (*bug*) pada suatu website tentu memerlukan perhatian serius agar tidak dieksploitasi oleh pihak yang tidak bertanggung jawab. Berdasarkan hal tersebut, tentunya diperlukan adanya upaya preventif diantaranya dengan melakukan analisis terhadap kemungkinan adanya celah keamanan pada suatu website. Pada penelitian tersebut, *tools* yang digunakan adalah *WEBPWN3R* yang merupakan *Web Applications Security Scanner*, *tool open source* ini dapat menganalisa, mendeteksi adanya *bug* dari suatu website. Pengujian dilakukan menggunakan perangkat komputer bersistem operasi *Kali Linux*. Penelitian tersebut bertujuan untuk menganalisa adanya celah keamanan pada suatu website dan membantu administrator atau pengelola web untuk dapat mengetahui adanya kemungkinan celah keamanan pada suatu website, sehingga dapat segera dilakukan perbaikan dengan tepat berdasarkan temuan kerentanan atau celah keamanan yang terdapat pada website tersebut (Andria, 2020b).

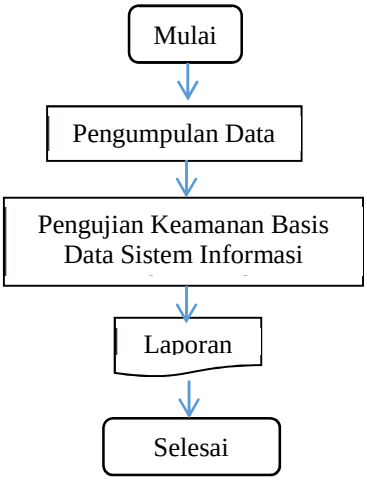
Adapun tujuan dari penelitian ini adalah melakukan pengujian keamanan basisdata pada suatu sistem informasi berbasis web dengan melakukan simulasi pada situs web yang memiliki celah kerentanan menggunakan media perangkat *Smartphone* bersistem operasi *Android* dengan bantuan aplikasi *Termux* yang didalamnya di *install tool SQLMap*, sehingga dengan ditemukan adanya celah kerentanan tersebut maka dapat dijadikan pedoman bagi pemilik atau pengelola web untuk dapat melakukan tindakan pengamanan secara tepat sebagai upaya preventif dalam mengamankan data dan aset digitalnya, sehingga resiko peretasan data oleh pihak yang tidak bertanggung jawab dapat diminimalisir dan dicegah sedini mungkin.

2. METODE PENELITIAN

Tahap-tahap yang dilakukan untuk menemukan celah keamanan pada aplikasi berbasis web meliputi *scope, reconnaissance, vulnerability detection, information analysis & planning* dan *penetration testing*. Pada proses *vulnerability detection* di dalamnya terdapat metode *DAST (Dynamic Application Security Testing)* dalam menemukan celah keamanan pada *website* dengan bantuan aplikasi, misalnya *Acunetic* (Wicaksono, 2020). Penelitian ini menggunakan metode *Research and Development (R&D). Research and Development (R&D)* merupakan suatu proses atau langkah-langkah untuk mengembangkan suatu produk baru atau menyempurnakan produk yang telah ada, yang dapat dipertanggungjawabkan (Sukmadinata, 2009). Objek penelitian ini menggunakan situs web yang dirancang khusus untuk keperluan simulasi pengujian keamanan sistem informasi berbasis web yang beralamatkan di http://testphp.vulnweb.com/. Adapun bahan dan alat yang digunakan terdiri dari:

a. 1 unit *smartphone* bersistem operasi *Android* (peneliti menggunakan *Android versi 7)*
b. Aplikasi *Termux* sebagai *terminal Android* yang juga merupakan *environtment Linux.*
c. *SQLMap Tool* untuk mendeteksi dan melakukan *exploit* pada *bug SQL injection* secara otomatis

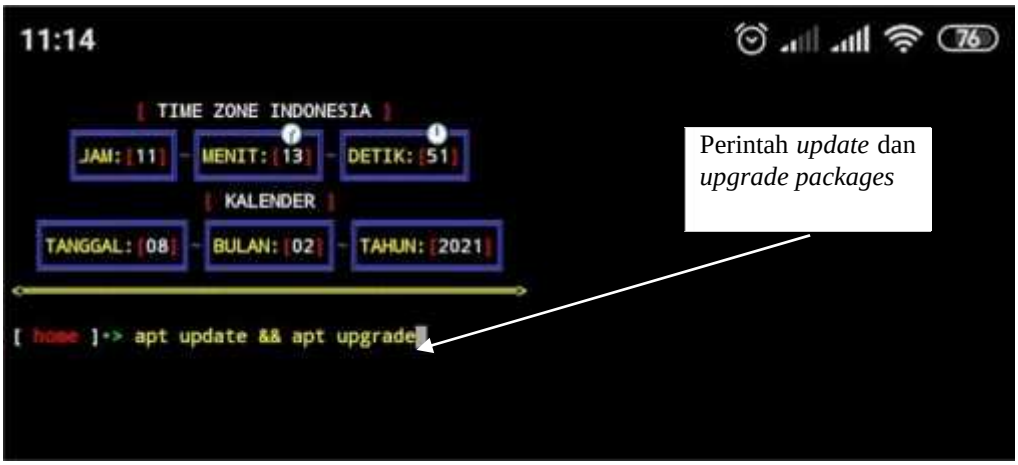
Waktu penelitian ini dilakukan selama 3 bulan bertempat di UPT Komputer UNIPMA. Adapun metode pengumpulan data dengan melakukan *Information Gathering* pada situs web tersebut dengan cara membuka tautan pada menu yang tersedia dan melakukan identifikasi *URL Address* yang memungkinkan terdapat adanya celah kerentanan. Alur penelitian untuk lebih jelasnya ditunjukkan pada Gambar 1 sebagai berikut.



Gambar 1. Alur Penelitian

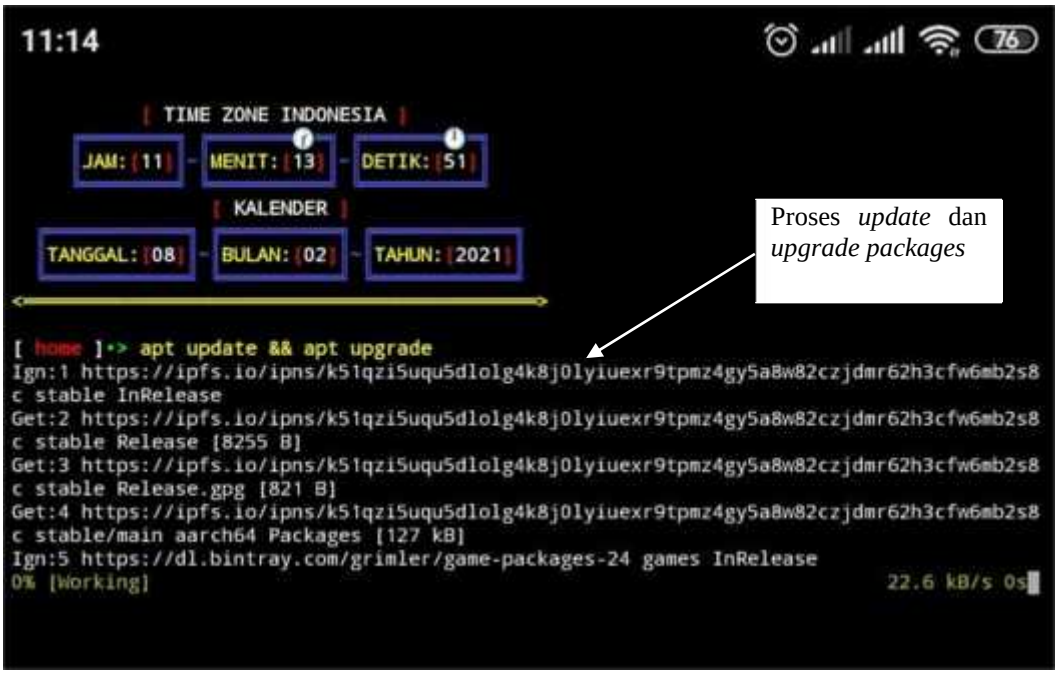
3. HASIL DAN PEMBAHASAN

Langkah awal yang perlu dilakukan yaitu melakukan instalasi aplikasi *Termux* di *smartphone* bersistem operasi *Android*, aplikasi *Termux* tersebut dapat diunduh secara gratis melalui *Play Store.* Selanjutnya setelah terinstall maka diperlukan *update* dan *upgrade packages* atau paket-paket yang dibutuhkan dengan mengetikkan perintah atau *command* di dalam aplikasi *Termux*. Perintah *update* dan *upgrade* paket di *termux* ditunjukkan pada Gambar 2.



Gambar 2. Perintah *Update* dan *Upgrade* Paket di *Termux*

Termux merupakan *emulator terminal Android* yang juga merupakan *environtment Linux*. Aplikasi ini dapat dijalankan secara langsung tanpa harus dilakukan *rooting* sehingga dapat langsung di *install* dan digunakan. Pada Gambar 3 ditunjukkan proses *update* dan *upgrade packages* yang sedang berjalan.



Gambar 3. Proses *Update* dan *Upgrade Packages* Berjalan

Kegunaan aplikasi *Termux* diantaranya dapat dijadikan media untuk melakukan pengujian keamanan terhadap kemungkinan adanya celah kerentanan pada suatu sistem informasi dan jaringan. Apabila proses *update* dan *upgrade packages* selesai maka tampilannya seperti yang ditunjukkan pada Gambar 4.

Gambar 4. *Update* dan *Upgrade Packages* Selesai

Tahapan selanjutnya, instalasi *tool SQLMap* di aplikasi *Termux* yang akan digunakan sebagai alat pengujian keamanan pada basis data sistem informasi berbasis web. Adapun langkah instalasinya sebagai berikut:

1. Buka aplikasi *Termux* dan ketikkan perintah / *command*:
   $apt install python python2 –y
   Perintah tersebut berfungsi untuk menginstall bahasa pemrograman *python*
2. Kemudian ketikkan perintah / *command*:
   $apt install git
   Perintah tersebut untuk menginstall *git* agar bisa di *cloning*
3. Selanjutnya, ketikkan:
   $git clone https://github.com/sqlmapproject/sqlmap
   Perintah / *command* tersebut untuk *clone SQLMap Tool*
4. Berikutnya, ketikkan perintah atau *command* untuk masuk ke direktori SQLMap
   $cd sqlmap
5. Kemudian, ketikkan *command* atau perintah untuk menjalankan *SQLMap Tool* di *Termux*
   $python2 sqlmap.py –u *URL Web Vuln* - -dbs
   Bagian *URL Web Vuln* di isi dengan alamat situs web target yang akan dilakukan pengujian keamanan. Sebagai contoh pada penelitian ini situs web target adalah sebagai berikut:
   http://testphp.vulnweb.com/listproducts.php?cat=2, sehingga tampilan lebih *detail* di aplikasi *Termux* seperti ditunjukkan pada Gambar 5.

Gambar 5. Perintah untuk Pengujian Keamanan Basis Data Situs Web dengan *SQLMap Tool* di *Termux*

Pengujian keamanan basis data sistem informasi berbasis web ini terbagi menjadi 4 tahapan, yaitu:

1) *Information Gathering*

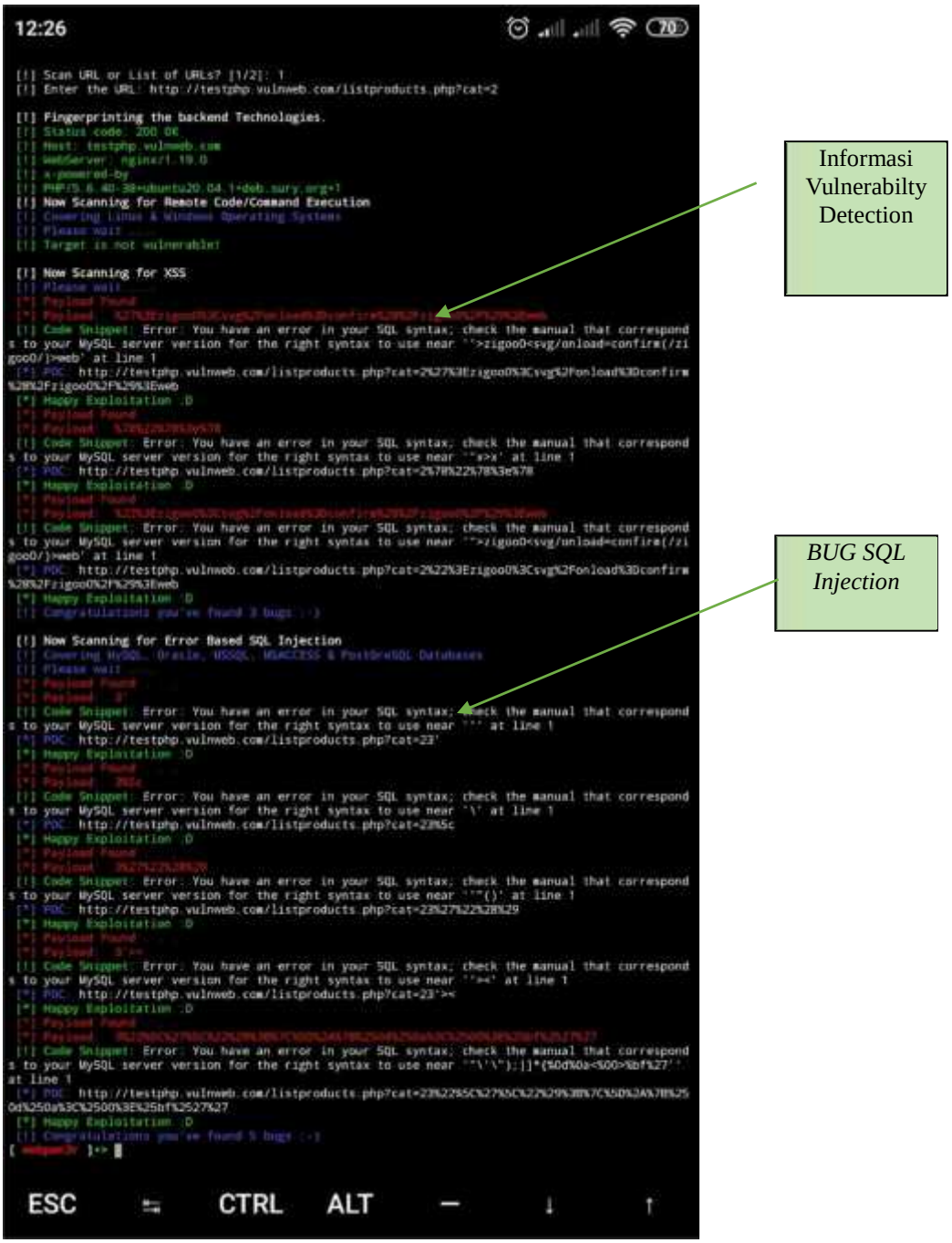
Tahapan ini mengumpulkan semua informasi, seperti *backend technology* yang digunakan dari situs web target. *Information Gathering* dilakukan dengan menggunakan *tool WebPwn3r*. Tampilan *Information Gathering* di *tool Webpwn3r* ditunjukkan pada Gambar 6.

Gambar 6. Tampilan *Information Gathering* di *Tool Webpwn3r*

Pada Gambar 6 dapat dijelaskan bahwa situs web target menggunakan *WebServer Nginx/1.19.01*, bahasa pemrograman *PHP/5.6.40, status code: 200 OK, host: testphp.vulnweb.com.*

2) *Vulnerabilty Detection*

Setelah mengetahui informasi tentang sistem target, pencarian celah keamanan masih dilakukan dengan *tool WebPwn3r* yang merupakan *tool* berbasis *open source*. Hasil *Vulnerabilty Detection* seperti yang ditunjukkan pada Gambar 7 sebagai berikut.



Gambar 7. Tampilan *Vulnerability Detection*

Pada Gambar 7 tersebut dapat dijelaskan bahwa berdasarkan informasi *vulnerability detection* yaitu pendeteksian adanya celah kerentanan pada situs web yang dikategorikan menjadi beberapa jenis pendeteksian ditemukan hasil adanya banyak *bug*, salah satunya yaitu *Bug SQL Injection* pada situs web target yang menjadi fokus pada penelitian ini. *Bug SQL Injection* merupakan celah kerentanan pada lapisan basis data dalam sebuah aplikasi. Informasi lebih jelasnya ditampilkan pada Tabel 1 sebagai berikut.

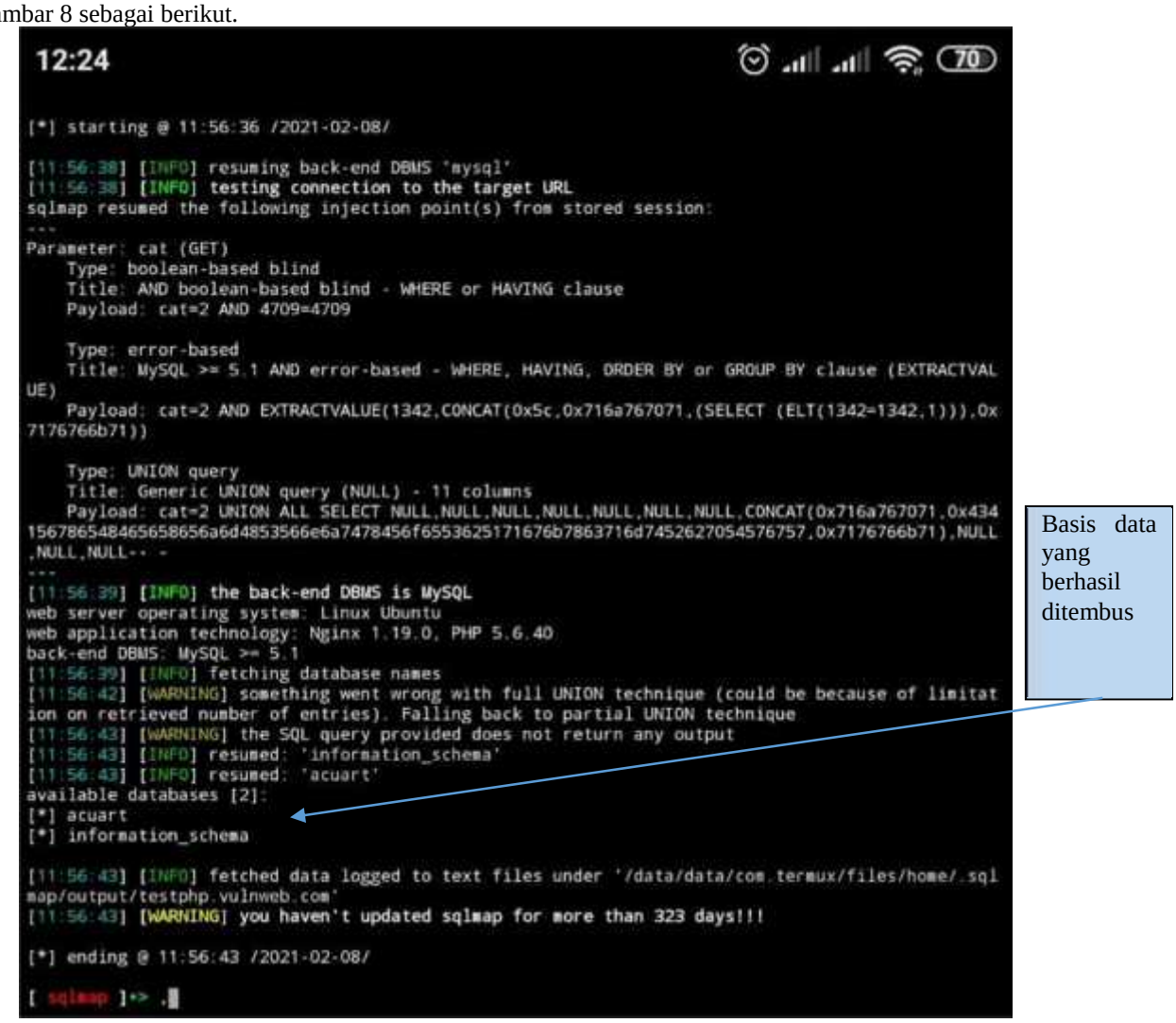
Tabel 1. Hasil *Vulnerabilty Detection*

No	Jenis Pendeteksian	Hasil
1	*Cross-Site Scripting (XSS)*	Terdapat 3 *bugs*
2	*SQL Injection*	Terdapat 5 *bugs*

3) *Exploitation*

Pada tahapan ini dilakukan eksploitasi dengan menggunakan *tool SQLMap* yang di install pada aplikasi *Termux* sebagai media pengujian keamanan basis data dengan menggunakan metode *SQL Injection*. Adapun kegunaan *tool SQLMap* yaitu dapat menganalisa, mendeteksi dan melakukan *exploit* (sebuah kode yang dapat menyerang

keamanan sistem komputer secara spesifik) pada *bug SQL Injection*. Hasil dari *exploitation* ditunjukkan pada Gambar 8 sebagai berikut.



Gambar 8. Tampilan Eksploitasi *Bug SQL Injection* di *tool SQLMap*

Setelah mendapatkan akses ke basis data, maka langkah selanjutnya dapat dilakukan eksploitasi lebih lanjut dengan mengakses *table*, *column* hingga *record.*

4) *Reporting*

Tahapan pelaporan mengenai celah keamanan yang ditemukan serta usulan atau rekomendasi perbaikan kepada pengelola sistem. Umumnya, *penetration testing (pentesting)* atau pengujian keamanan sistem dilakukan atas dasar kerjasama antara pemilik *website* dengan *pentester* (pihak yang melakukan *pentesting)*, meskipun terdapat juga beberapa *pentester* yang sebelumnya tanpa ada kerjasama melakukan aktivitas pencarian celah keamanan sistem dan kemudian secara kooperatif melaporkan temuannya ke pemilik atau *admin web* agar diperbaiki, umumnya *pentester* tipe ini disebut dengan *bug hunter.*

Selama hal tersebut bertujuan baik dan tidak merugikan, justru akan sangat membantu bagi para pengelola website atau pemilik bisnis dalam mengamankan sistem informasinya. Pelaporan atas temuan *bug* atau celah keamanan sistem dapat dikemas dalam suatu dokumen yang disebut dengan *Proof of Concept (PoC)* yang memuat bukti dan penjelasan dari temuan celah kerentanan. Dokumen *PoC* tersebut biasanya dikirimkan melalui *email* kepada *owner* atau *admin web* untuk dilakukan pengecekan dan perbaikan.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan hasil penelitian sebagai berikut :

1) Penelitian dilakukan untuk menguji keamanan basis data pada sistem informasi berbasis web dan membantu *administrator* atau pengelola web untuk dapat memeriksa adanya celah keamanan basis data yang dapat dieksploitasi oleh peretas.

2) Dari hasil pengujian keamanan basis data sistem informasi berbasis web ditemukan adanya celah kerentanan pada lapisan basis data, seperti pada Tabel 1 bahwa terdapat 5 *bug SQL Injection.*
3) Terjadinya kesalahan atau kekurangan dalam pengembangan sistem informasi pada aspek keamanan data yang berpotensi adanya serangan *SQL Injection* dan memungkinkan peretas dapat mengakses basis data pada suatu *web server*, sehingga privasi data pengguna atau informasi sensitif didalamnya beresiko disalahgunakan. Upaya preventif perlu sebagai langkah antisipasi mengamankan suatu sistem informasi.
4) Upaya yang dapat dilakukan untuk pencegahan maupun perbaikan terhadap *Bug SQL Injection* diantaranya memberikan enkripsi pada lapisan basis data, melakukan validasi terhadap *input,* menyembunyikan notifikasi kesalahan atau pesan *error* dan melakukan manipulasi *URL Web.*

UCAPAN TERIMA KASIH

Penulis menyampaikan terimakasih banyak kepada Universitas PGRI Madiun melalui program LPPM Universitas PGRI Madiun yang telah memberikan dana hibah penelitian, terimakasih juga kepada rekan-rekan Program Studi Sistem Informasi Universitas PGRI Madiun yang telah banyak memberikan motivasi dan terimakasih kepada banyak pihak yang penulis tidak bisa sebutkan satu persatu.

DAFTAR PUSTAKA

Andria. (2020a). Audit Keamanan Website Menggunakan Uniscan di Kali Linux. *Seminar Nasional Inovasi Teknologi* (pp. 323-328). UN PGRI Kediri.

Andria. (2020b). Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux. *Generation Journal*, 4(2), 69-76.

Aswandi, R., Muchsin, P.R.N., Sultan, M. (2020). Perlindungan Data dan Informasi Pribadi Melalui *Indonesia Data Protection Sysrem (IDPS). LEGISLATIF (Lembaga Gagasan Mahasiswa yang Solutif dan Inovatif).* 3(2), 167-190.

Sukmadinata, N.S. (2009). *Metode Penelitian Pendidikan.* Bandung: Remaja Rosdakarya.

Wicaksono, B., Kusumaningsih, Rr., Y., R. (2020). Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik *Penetration Testing* dan *DAST (Dinamyc Application Security Testing). Jurnal JARKOM.* 8(1), 1-9.

Suud, Y.A. (2020). *13 Kasus Peretasan Data Terbesar Sepanjang Masa.* Diakses tanggal 4 Februari 2020, dari https://cyberthreat.id/read/6570/13-Kasus-Peretasan-Data-Terbesar-Sepanjang-Masa