KEMENTERIAN
PENDIDIKAN DAN KEBUDAYAAN

RISK ASSESSMENT VULNERABILITY REPORT

Nama	: Gede Ananda
Phone no	: 085896873540
Email	: gedeananda03@gmail.com
Endpoint	: https://pkb.galerikejuruan.bbppmpvbmti.kemdikbud.go.id/home?
Date Report	: 12 Juni 2024

Contents

INTRO

SQL Injection

Description

Impact

References

Step to reproduce:

1. *Step 1 – Mengunjungi halaman*
2. *Step 2 – Memeriksa scope di burpsuite*
3. *Step 3 – Test SQL Injection*

Screnshoots/Logs:

System/Environment Detail:

Severity:

Recommendation/Fix

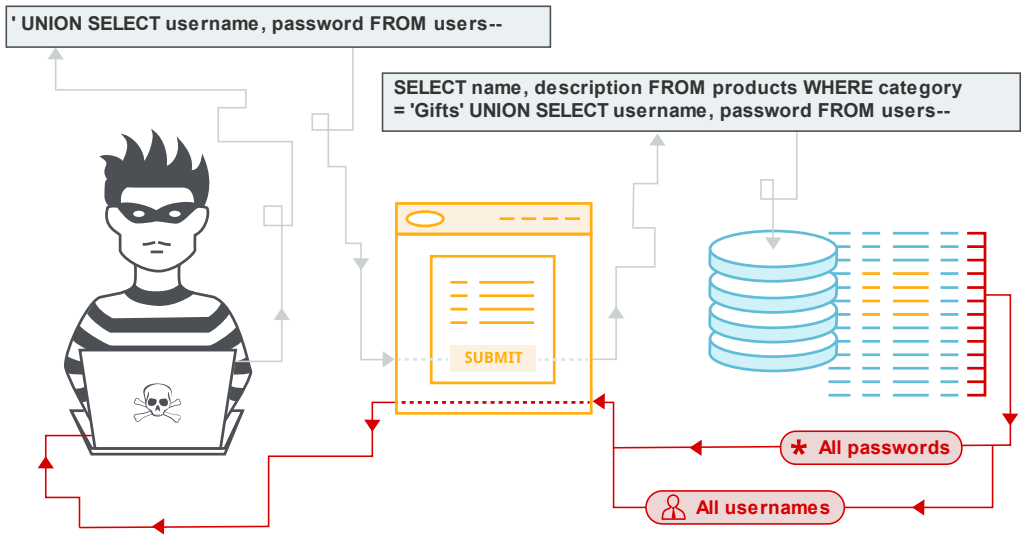
INTRO

Assalamu'alaikum Wr. Wb. Shalom, Om Swastiastu, Namo Budaya, Salam Kebajikan. Selamat Sejahtera bagi kita semua.

Yth.Bapak/Ibu

Perkenalkan nama saya Gede Ananda pada tanggal 12 juni 2024 , Jam 21.13 WIB saya ingin melaporkan kerentanan pada website https: https://pkb.galerikejuruan.bbppmpvbmti.kemdikbud.go.id/

SQL Injection



Description

SQL Injection adalah jenis serangan keamanan pada aplikasi web yang terjadi ketika penyerang menyisipkan atau "menyuntikkan" perintah SQL yang tidak sah ke dalam query yang dijalankan oleh database aplikasi tersebut. Serangan ini memanfaatkan kelemahan dalam validasi input pengguna, memungkinkan penyerang untuk mengakses, memanipulasi, atau bahkan menghancurkan data dalam database.

Impact

Kerentanan SQL Injection dapat dieksploitasi dengan mudah, tetapi dampak dari jenis serangan ini berpotensi menjadi menjadi bencana besar. Di bawah ini adalah beberapa cara SQL Injection dapat berdamapak pada kerahasiaan, Integritas, dan Ketersediaan data clint:

1. ***Pengambilalihan Akun*** – Penyerang dapat mencuri kredensial pengguna, seperti nama pengguna dan kata sandi, dengan menjalankan query yang mengakses tabel yang menyimpan informasi login. Ini dapat menyebabkan pengambilalihan akun pengguna yang sah, termasuk akun administratif, yang dapat memberikan akses penuh ke sistem aplikasi.
2. ***Pengungkapan Data Sensitif*** *– SQL Injection memungkinkan penyerang untuk mengakses informasi sensitif yang disimpan dalam database, seperti data pribadi (PII), data keuangan, atau informasi bisnis rahasia. Hal ini dapat menyebabkan pelanggaran privasi dan kerugian reputasi yang signifikan bagi organisasi.*
3. ***Manipilasi Data*** *– Penyerang dapat mengubah, menambahkan, atau menghapus data dalam database. Manipulasi data dapat menyebabkan ketidaksesuaian informasi, laporan yang salah, atau kerugian operasional. Misalnya, penyerang dapat mengubah saldo rekening atau data inventaris.*
4. ***Penghancuran Data -*** *Penyerang dapat menghapus data secara keseluruhan atau merusak tabel dalam database, yang dapat mengakibatkan hilangnya data yang berharga. Penghancuran data dapat menghentikan operasi bisnis, menyebabkan kerugian finansial, dan merusak reputasi perusahaan.*

References

- https://portswigger.net/sql-injection

Discovered Vulnerability Details

Vulnerability #1

SQL Injection

SEVERITY: ***STATUS:***

Hight ***Unsolved***

Endpoint:

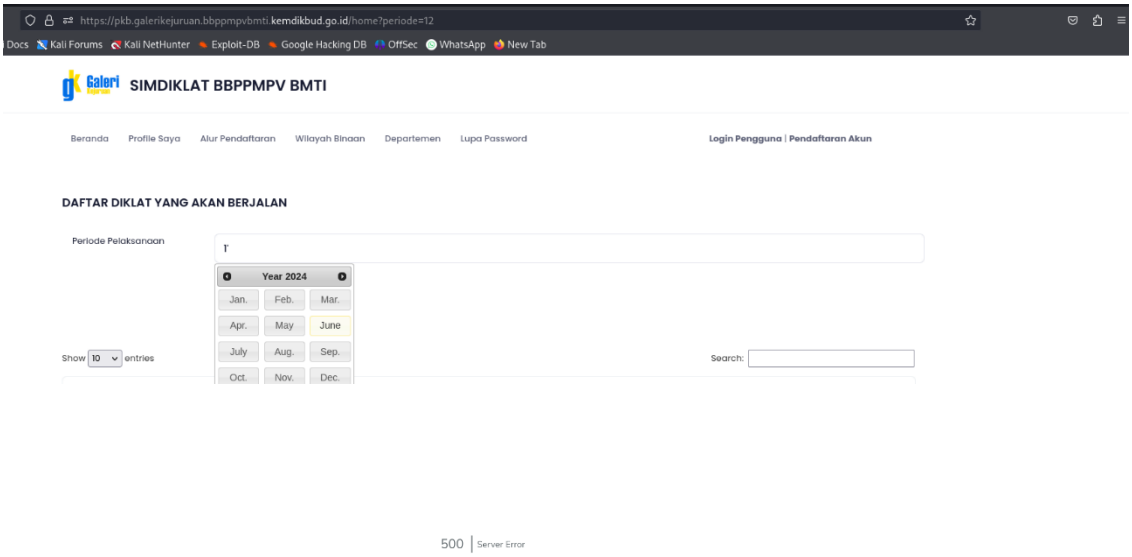
- https://pkb.galerikejuruan.bbppmpvbmti.kemdikbud.go.id/home?

- ***Video PoC***
  https://drive.google.com/file/d/1XZheezzE3s1MZ-wpJEswOajHuzSfQRST/view?usp=sharing

Step to reproduce:

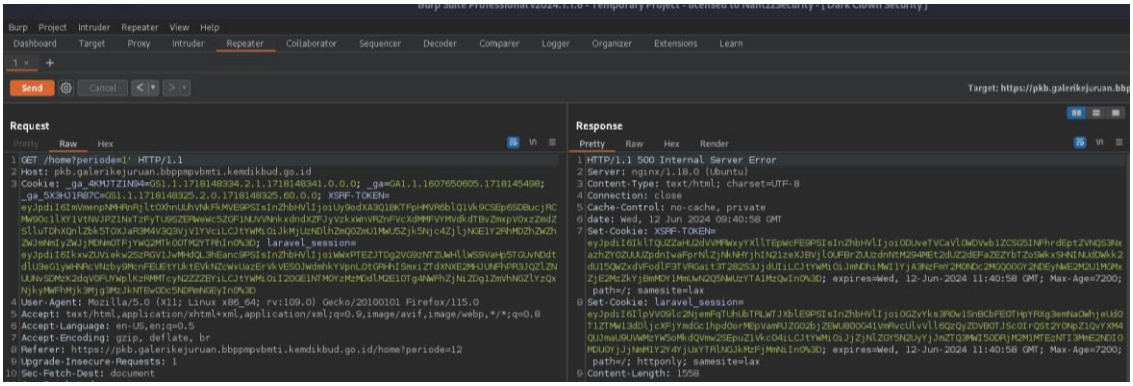
1. Step 1 – Mengunjungi halaman

   Saya mengunjungi web https://pkb.galerikejuruan.bbppmpvbmti.kemdikbud.go.id/home? Dan tertarik untuk memasukkan sebuah query pada kolom pencarian, dan terjadi Internal server error



2. Step 2 – Memeriksa Scope di Burpsuite

   Saya memeriksa bagian burpsuite pada https://pkb.galerikejuruan.bbppmpvbmti.kemdikbud.go.id/home? dan benar saja, ketika di search normal, scope tidak menemukan kejanggalan dan ketika di tambahkan string terjadi internal server error



3. Step 3 – Test SQL Injection
   Selanjutnya saya mencoba untuk melakukan sql injection dengan mengetikkan: sqlmap -u https://pkb.galerikejurusan.bbppmpvbmti.kemdikbud.go.id/home?periode=1 --random-agent --threads=10 --level= 5 --risk=3 -v 3 -dbs
   Dan hasilnya saya mendapatkan beberapa database seperti gambar di bawah

Screenshoot and log:

https://drive.google.com/drive/folders/1UWW0HyB8LRklrjz5XU2RJ2lM_5HQ4T0J?usp=sharing

Video Dokumentasi PoC untuk melengkapi dokumentasi laporan.

Recommendation/Fix

Memulikan Kerentanan SQL Injection

- Menggunakan prepared statements dan parameterized queries untuk semua interaksi dengan database. Teknologi ini membantu memastikan bahwa input pengguna diperlakukan sebagai data, bukan perintah SQL, sehingga mencegah penyisipan kode berbahaya.
- Validasi input yang ketat di sisi klien dan server. Input harus selalu diperiksa untuk memastikan bahwa sesuai dengan format yang diharapkan dan tidak mengandung karakter berbahaya. Gunakan whitelist (daftar karakter yang diizinkan) untuk memfilter input.
- Gunakan Object-Relational Mapping (ORM) untuk mengabstraksi interaksi dengan database. ORM menyediakan mekanisme keamanan bawaan yang dapat melindungi terhadap SQL Injection, sehingga mengurangi risiko.
- Pastikan bahwa semua input pengguna yang digunakan dalam query SQL di-escape dengan benar. Escaping input membantu memastikan bahwa karakter khusus dalam input diperlakukan sebagai data biasa, bukan sebagai bagian dari query SQL
- Gunakan stored procedures untuk semua operasi database yang kompleks. Stored procedures memungkinkan logika bisnis terpisah dari kode aplikasi, dan dapat membantu mencegah SQL Injection dengan membatasi jenis query yang dapat dijalankan.

Best Regards,
Gede Ananda