Techart

Консалтинг, цифровая трансформация,
интеграция бизнес-процессов, маркетинга и оргразвития

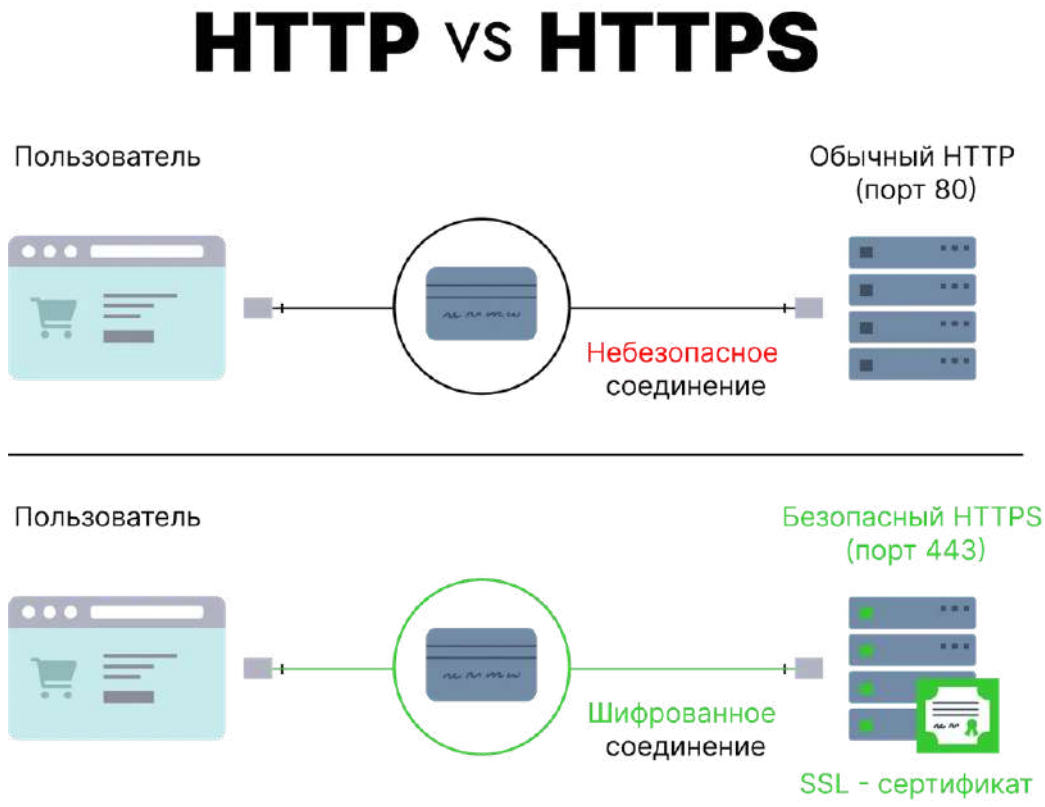
Безопасность сайта: основные угрозы и решения

06.04.2023

techart.ru | web.techart.ru

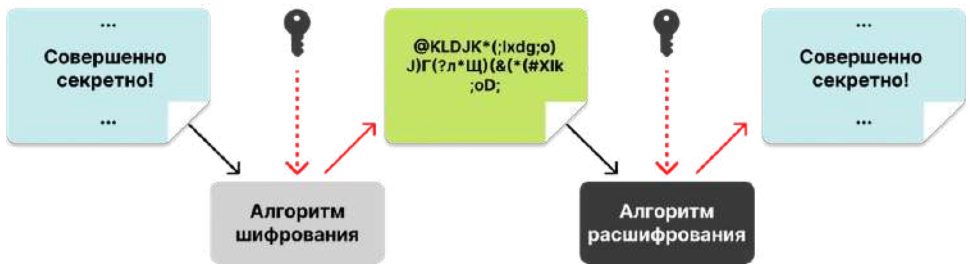
1999 2023

Что такое HTTPS?

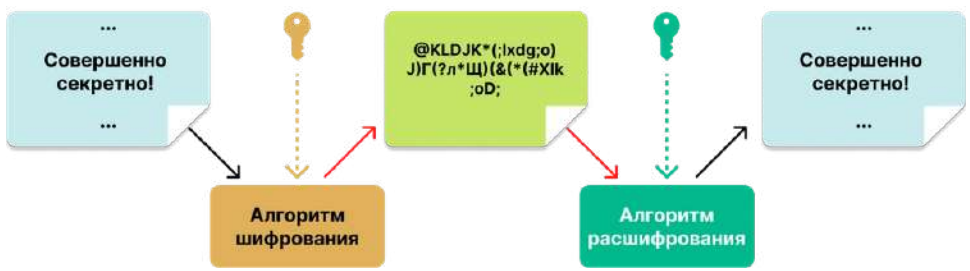


Симметричное и ассиметричное шифрование

Симметричное шифрование - один ключ



Асимметричное шифрование - пара ключей: открытый и приватный



SSL-сертификаты

По типу валидации:

- Сертификаты, которые подтверждают только доменное имя
- Сертификаты, которые подтверждают домен и организацию
- Сертификаты с расширенной проверкой

По свойствам:

- Обычные
- Wildcard сертификаты
- SAN сертификаты
- IDN сертификаты

Как вы храните пароли?

В открытом виде:

Login:	**admin**
Password:	**qwerty123**

Как вы храните пароли?

В зашифрованном виде:

Login:	**admin**
Password:	**gRD7%SN@8R**

Как вы храните пароли?

Хеш:

Login:	**admin**
Password:	**$2y$10$Kgbn2m1/8nlj9xFxsFj4fu9nXgvF6U085kyQ0ivQ/e4she5W/NSUK**

IDOR-уязвимость

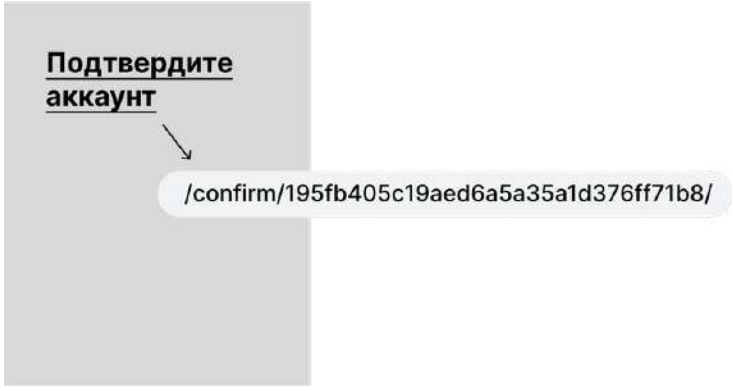
Insecure direct object reference

/images/passport-scans/563.jpg — **Id-пользователя**
можно изменить и получить непредназначенный для вас контент

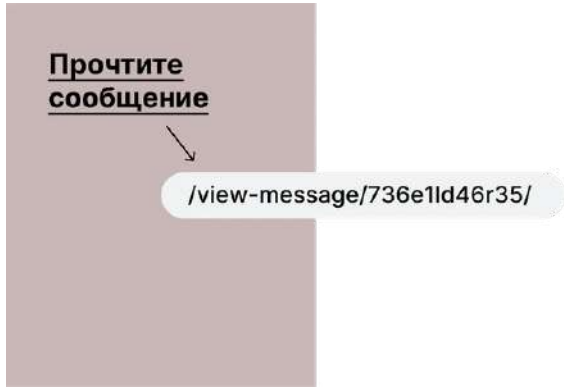
/images/passport-scans/8eefcfdf5990e441f0fb6f3fad709e21.jpg — **Зашифрованное Id-пользователя**
можно изменить и ничего не получить (но это не точно)

Когда допустимо использовать "секретные" ссылки

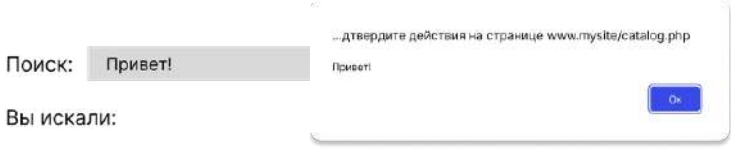
Одноразовые ссылки:



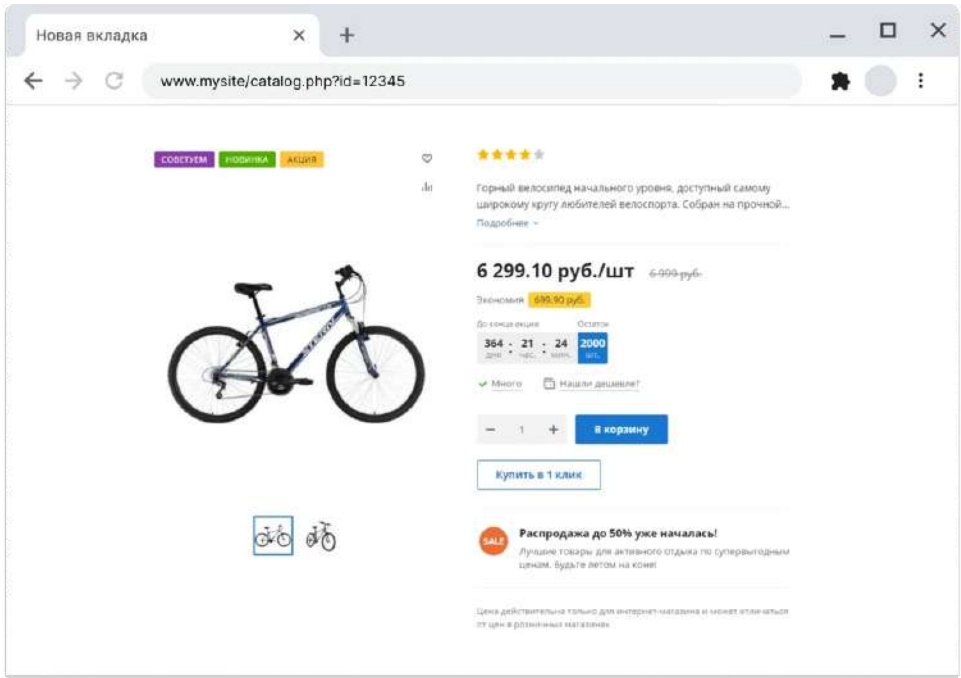
Не очень важная информация:



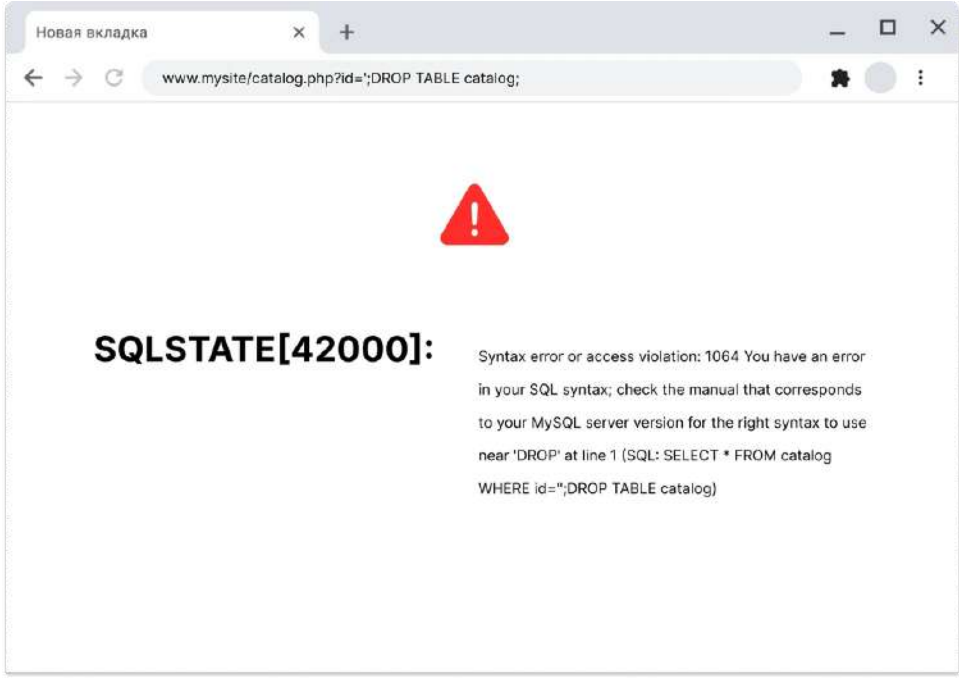
XSS-уязвимость

Вы вводите запрос - Привет!	Злоумышленник вводит запрос: <script>alert('Привет!');</script>	
 Вы искали: **Привет!**		
Так работает строка поиска	**Не защищенный сайт**	**Защищенный сайт**

SQL-инъекция

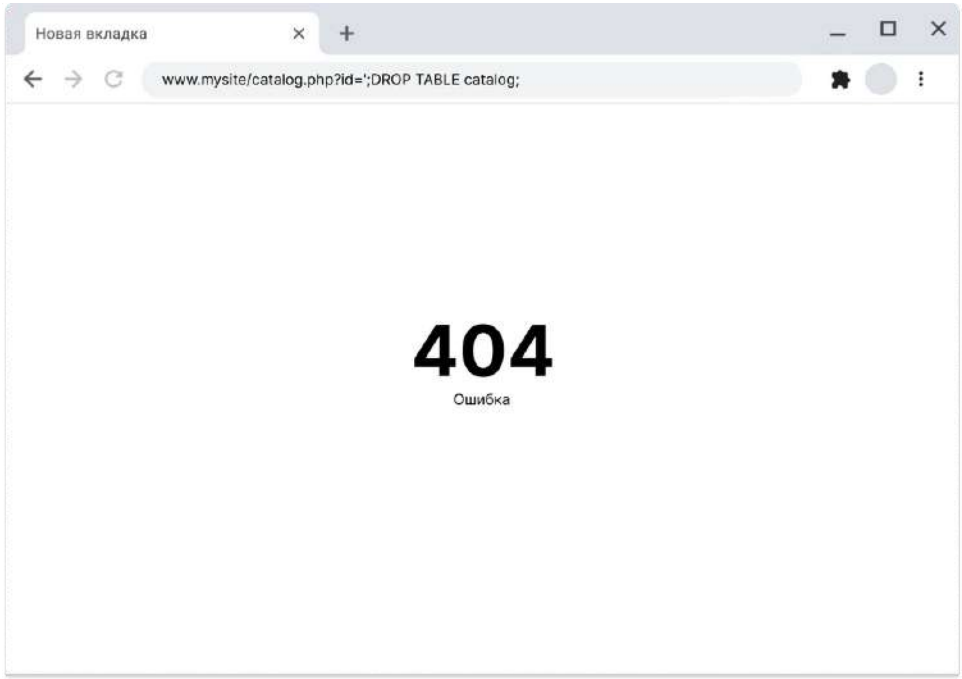


SQL-инъекция

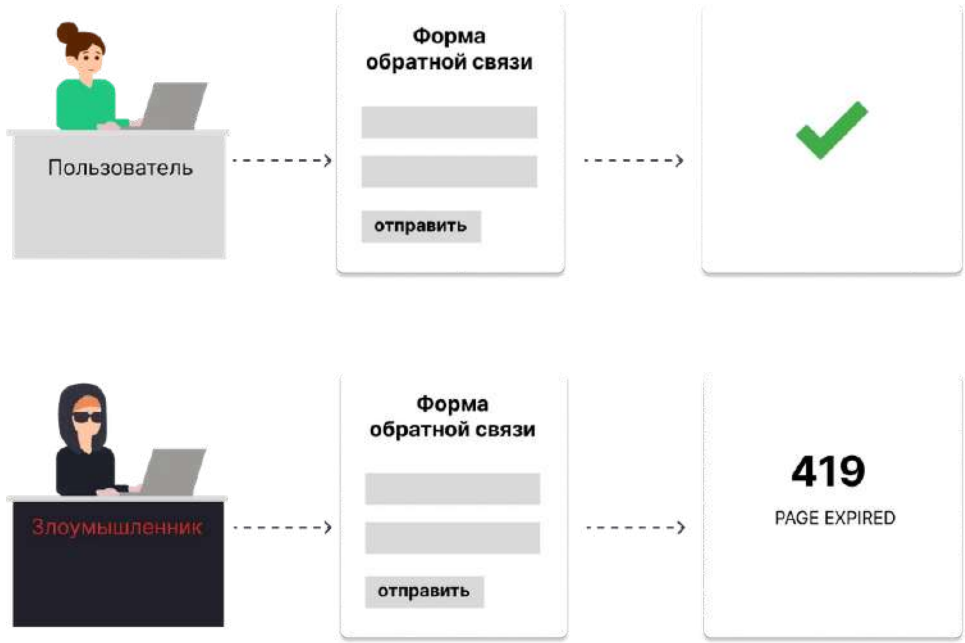


Неправильно

SQL-инъекция



CSRF-уязвимость



Сканеры уязвимости

Простые сканеры

Sucuri SiteCheck

Mozilla Observatory

Qualys SSL Labs

Тестирование посложнее:

Kali Linux

Утилиты:

fail2ban

Что делать?

- Не ищите дешевый хостинг
- Пользуйтесь проверенным ПО
- Обновляйте ПО
- Используйте проактивную защиту
- Делайте бэкапы
- Не пренебрегайте тестированием

Защита от DDoS-атак:

QRATOR LABS qrator.ru

StormWall stormwall.pro

kaspersky kaspersky

DDOS-GUARD ddos-guard

ГАРДА ТЕХНОЛОГИИ gardatech

Techart

Консалтинг, цифровая трансформация,
интеграция бизнес-процессов, маркетинга и оргразвития

Павел Гусев

Директор направления «IT-решения и веб-разработка»

gusev@techart.ru

Андрей Жмурин

Зам. директора направления «IT-решения и веб-разработка»

zhmurin@techart.ru

+7 495 790 75 91

techart.ru

web.techart.ru

info@techart.ru

Аналитика и бизнес-планирование
research.techart.ru

Интегрированный маркетинг и PR
promo.techart.ru

Дизайн-бюро
design.techart.ru

IT-решения и веб-разработка
web.techart.ru

Фотоагентство
photo.techart.ru

Работа в «Текарт»
hr.techart.ru

Авторский telegram-канал «Системное развитие бизнеса» t.me/techart_ru