Don’t roll ~~your own~~ crypto

Криптографию сложно внедрять

- Ева знает алгоритм
- Ева может читать сообщения
- Ева может менять сообщения
- Ева сильный математик и программист

Что значит “своя” криптография

- Свой примитив
- Свой режим использования примитива
- Свой протокол
- Своё хранение и ротация ключей

Что значит “своя” криптография

- Свой примитив
- Свой режим использования примитива
- Свой протокол
- Своё хранение и ротация ключей

Case study: токены восстановления пароля

- При клике на “я забыл пароль” пользователю высылается ссылка вида

`http://site/reset.php?token=<token>`

- Байты `<token>` генерируется функцией `rand`

Case study: токены восстановления пароля

- Ева получает один токен (для своего аккаунта)
- Ева восстанавливает сид генератора
- Ева знает чужой токен

Что значит “своя” криптография

- Свой примитив
- Свой режим использования примитива
- Свой протокол
- Своё хранение и ротация ключей

Режим использования примитива

- Параметры алгоритма
- Модель атакующего

Case study: Primefaces EL injection

- Контент страницы передается через куки
- AES в режиме CBC
- Подставляется в Spring Expression Language

Case study: Primefaces EL injection

- Шифруем наш пейлоад через padding oracle
- Получаем RCE

Что значит “своя” криптография

- Свой примитив
- Свой режим использования примитива
- Свой протокол
- Своё хранение и ротация ключей

Case study: JWT “downgrade”

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

Case study: JWT “downgrade”

```
{
  "alg": "none",
  "typ": "JWT"
}
{
  "sub": "1234567890",
  "name": "Admin",
  "iat": 1516239022
}
```

Что значит “своя” криптография

- Свой примитив
- Свой режим использования примитива
- Свой протокол
- Своё хранение и ротация ключей

Большинство криптографических ключей не меняются вообще никогда

Case study: GitHub RCE

- Кука _gh_session - сериализованный (Marshal’ом) объект сессии
- Для подписи используется HMAC на SHA1

Case study: GitHub RCE

```
use Rack::Session::Cookie,
  :key           => "_gh_manage",
  :path          => "/",
  :expire_after => 1800, # 30 minutes in seconds
  :secret        => ENV["ENTERPRISE_SESSION_SECRET"]
|| "641dd6454584ddabfed6342cc66281fb"
```

Case study: GitHub RCE

- Секрет в переменной окружения
- Она нигде не выставлялась :)

Case study #2: Bitnami/Laravel

- Готовые пакеты для разных приложений
- Пуллим докер и всё работает

Case study #2: Bitnami/Laravel

- Ключ зашивается при генерации докера
- Пробуем ключи из последних N версий

http://crypto-hasher.sh.je/

http://crypto-hasher.sh.je/

- `hash` поддерживает не только криптографические функции
- `trim` обрезает не только пробелы
- crc(x)=crc(y) => crc(x.s)=crc(y.s)
- Поиск коллизий в crc тривиален

http://crypto-sha3er.sh.je/

- Сначала решите http://crypto-hasher.sh.je/
- Потом думайте

```
$secret = "FIN";
```