# 7 историй из пентестов

Василий Кравец Начальник отдела ИИТ «Перспективный мониторинг»





#### Пентест или не пентест

1 Пентест

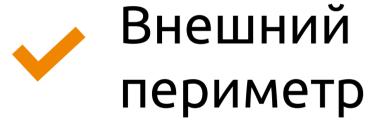
3 Аудит

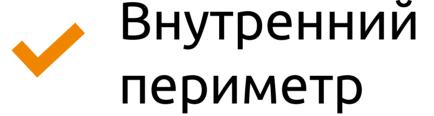
2 Анализ защищенности

4 Редтиминг



#### А что можно проверять?













#### Кто в лес, кто по дрова

```
FOLDERS
                                  public function imadeploy()
                                     SPR = Product::select('id', 'image', 'mirror')->whereIn('cat_id', [156,162])->where('color_id', 13);
                                     sbar = new ProgressBar(Sthis->output, SPR->count());
                                     Sbar->setFormat('deb---
                                                                   ---(1->setBarkidth(50)->start();
                                                . sproduct->imau
                                      contents(config('app.ur)
                                                                                          'enuz/min/" . Sproduct->image);
                                   ublic_path('imgs/products/vi
                                                                                             's/min/' . Sproduct->image):
                                                                                              tt-simage, Sfile_min);
                              params->unique('name') as $par
                                                                                                V" . Sproduct⇒inage);
                                                                                                V* . Sproduct⇒image);
                                                                                                image, Stile_min);
                              nts->where('id', $par->pivot->
  .local.env
                               t' => $var=>sort, 'name' => $v
  123.php
   ide helper.php
                                    'unique('name') as $par) {
                                                                                           Aderbits
                                       i->where('id', $par->pivot
                                            '$var->sort, 'name' =
                                                                                     ot-everient_id) (
                                                                                  riants->uhere('id', $variant_id)->first();
                                              Svariant = Sthis->model->categories->first();
                                               Sgender = Svariant->gender;
                                           return (object)['mame' --- Sname, 'gender' --- Sthis--petGender(Sgender), 'ma_param' --- Sthis--model--categories-->first()->no_param|;
                                        } catch (\Exception Se) {
                                           return (object)['mame' => "'];
```

#### Поиск черной кошки





## Обязательная история про вертолет







Человек, который очень хотел в интернет



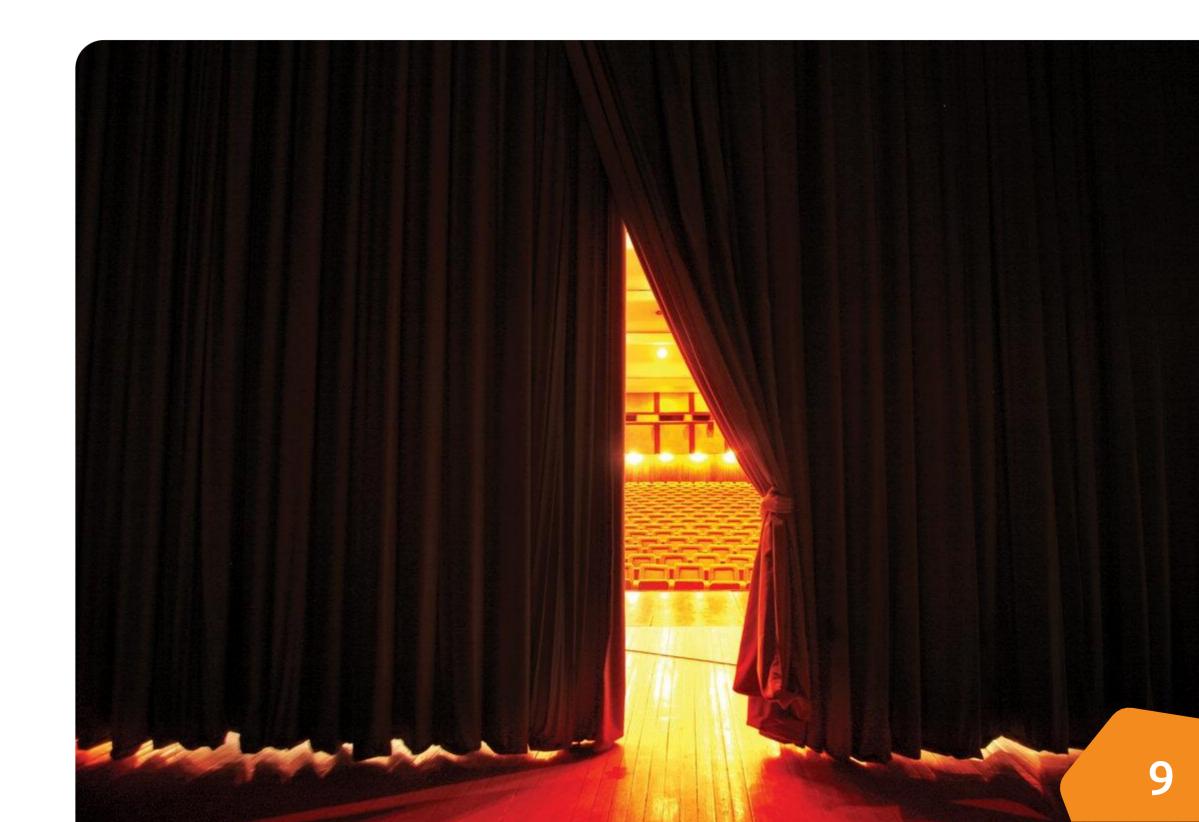


#### Универсальный пропуск





#### Театральные страсти





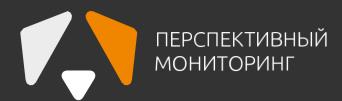
### Фишинге в фишинге





#### Выводы

- 1. Работы должны быть консистентны!
- 2. Слушайте обратную связь!
- 3. Проводите обучение сотрудников!
- 4. Обсуждайте с сотрудниками защищаемые данные!
- 5. Сотрудники должны знать кто и зачем может их проверять!



## Спасибо за внимание!

Кравец Василий Васильевич

Начальник отдела ИИТ

+7 (495) 737-61-97
Vasily.Kravets@amonitoring.ru