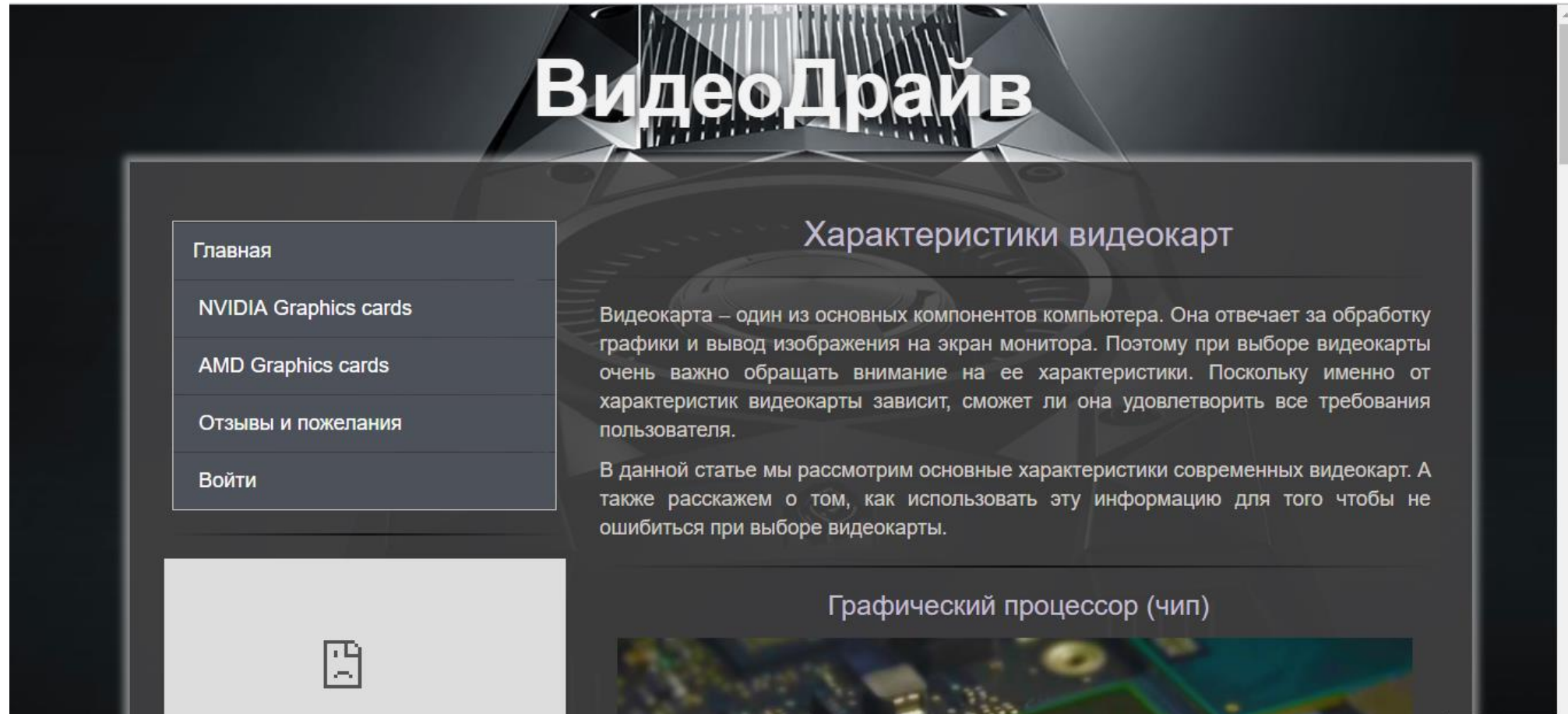


Cardviewer service

By Obi-Wan Kenobi

Сайт с информацией о видеокартах

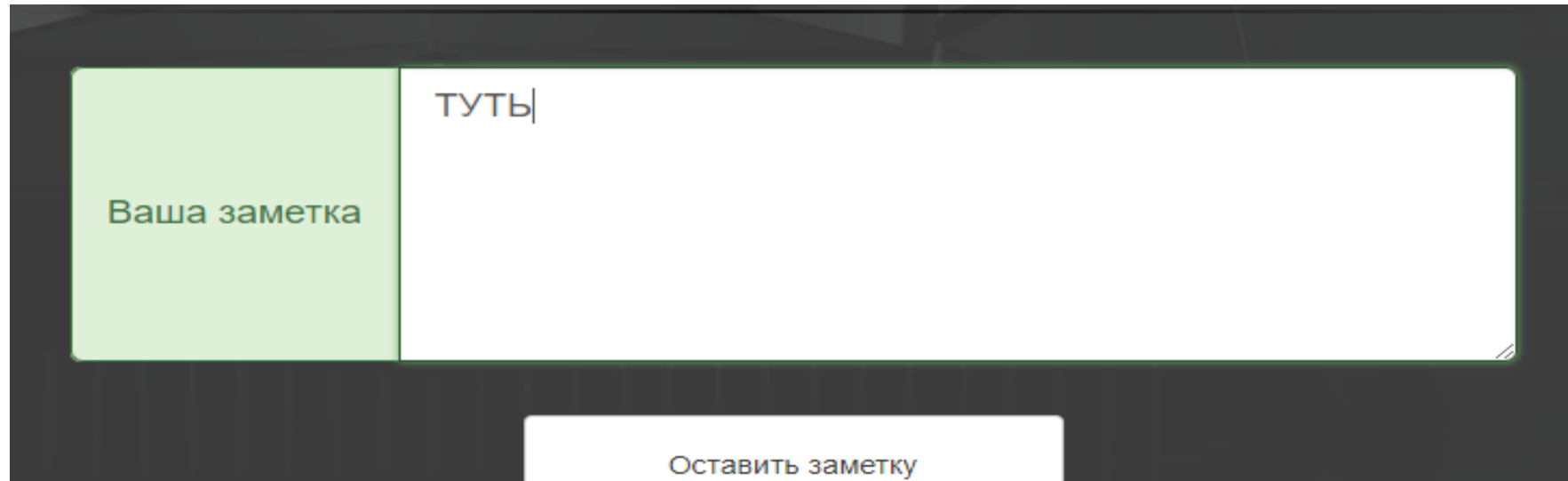


Написан на связке apache+php(framework yii2)+mysql
Сколько на сайте было уязвимостей?

А где флаги?

Таблица ▾

- ☐ auth_assignment
- ☐ auth_item
- ☐ auth_item_child
- ☐ auth_rule
- ☐ category
- ☐ comments
- ☐ migration
- ☐ notes
- ☐ products
- ☐ reviews
- ☐ users



Ваша заметка

ТУТЬ|

Оставить заметку

Таблица с заметками пользователей о пользователях.

Основное количество уязвимостей было связано с возможностью авторизоваться от лица другого пользователя и посмотреть его заметку о другом

Формы на сайте

- Регистрация
- Авторизация
- Обратная связь
- Личный кабинет
- Комментарий
- Заметка о пользователе!!!

Угадайте что помечено красным

Самое очевидное

ВидеоДрайв

Авторизация

Логин admin


Пароль

Войти

Нет аккаунта? [Зарегистрируйтесь!](#)

Вход с любым паролем

Причина



```
161      * @param string $password password to validate
162      * @return bool if password provided is valid for current user
163      */
164      public function validatePassword($password)
165      {
166          $MAX_PASSWORD_LENGTH = $GLOBALS['max_password_lenght'];
167          $pass=substr($password, start: 0, $MAX_PASSWORD_LENGTH);
168          return md5($pass,$this->password);
169      }
```

Функция возвращает строку, которая в коде всегда приводится к **true**

Как победить?

```
public function validatePassword($password)
{
    $MAX_PASSWORD_LENGTH = $GLOBALS['max_password_lenght'];
    $pass=substr($password, start: 0,$MAX_PASSWORD_LENGTH);
    return md5($pass)=== $this->password;
}
```

Менее очевидное

Регистрация

Логин

admin\\

Пароль

....

Повторите пароль

....

Картинка

Выберите файл Файл не выбран

О себе

Сейчас мы будем хекать|

Зарегистрироваться

Добро пожаловать в ваш личный кабинет!

Здесь вы можете изменить свои данные

admin

Сейчас мы будем хекать

Логин

admin

Причина



```
59     ];  
60 }  
61  
62 /**  
63  * Registers user  
64  *  
65  * @return User|null the saved model or null if saving fails  
66  * @throws \yii\base\Exception  
67  */  
68 public function register()  
69 {  
70     if (!$this->validate()) {  
71         return null;  
72     }  
73  
74     $this->login=str_replace(["\\", "/", "'", "\\"], replace: "", $this->login);  
75  
76     if (!$user = User::findByLogin($this->login))  
77         $user = new User();  
78 }
```

Функция проверяет поле на уникальность, а потом стирает спецсимволы.
Это приводит к замене уже существующего пользователя.

Как победить?

```
public function register()
{
    if (!$this->validate()) {
        return null;
    }

    $this->login=str_replace(["\\", "/", "'", "\""], replace: "", $this->login);

    if (!$user = User::findByLogin($this->login))
        $user = new User();
}
```

Удалить эти строки...

Чистка поля не нужна – фреймворк справляется с угрозой инъекций сам.

А при регистрации обязательно должен создаваться новый пользователь.

Удивительное рядом

Но при регистрации
username:username войти можно под данными:

username:usern

username:userna

username:usern

username:user

username:usernamee

И т.д.

Почему?

Причина

```
SiteController.php x Users.php x
118     return static::findOne(['login' => $login]);
119 }
120
121 /**
122  * @inheritdoc
123  */
124 public function getId()
125 {
126     return $this->getPrimaryKey();
127 }
128
129 public function generatePasswordHash($pass)
130 {
131     $MAX_PASSWORD_LENGTH = $GLOBALS['max_password_length'];
132     $pass=substr($pass, start: 0,$MAX_PASSWORD_LENGTH);
133     try {
134         return md5($pass);
135     } catch (Exception $e) {
136     }
137 }
138
139

SiteController.php x Users.php x index.php x Application.php x
368 public function setBasePath($path)
369 {
370     parent::setBasePath($path);
371     Yii::setAlias( alias: '@app', $this->getBasePath());
372 }
373
374 /**
375  * Runs the application.
376  * This is the main entrance of an application.
377  * @return int the exit status (0 means normal, non-zero values mean abnormal)
378  */
379 public function run()
380 {
381     $GLOBALS['max_password_length']=Yii::$app->params['max_password_length'];

SiteController.php x Users.php x index.php x Application.php x params.php x
1 <?php
2
3 return [
4     'adminEmail' => 'admin@example.com',
5     'max_password_length' => '4'
6 ];
7
```

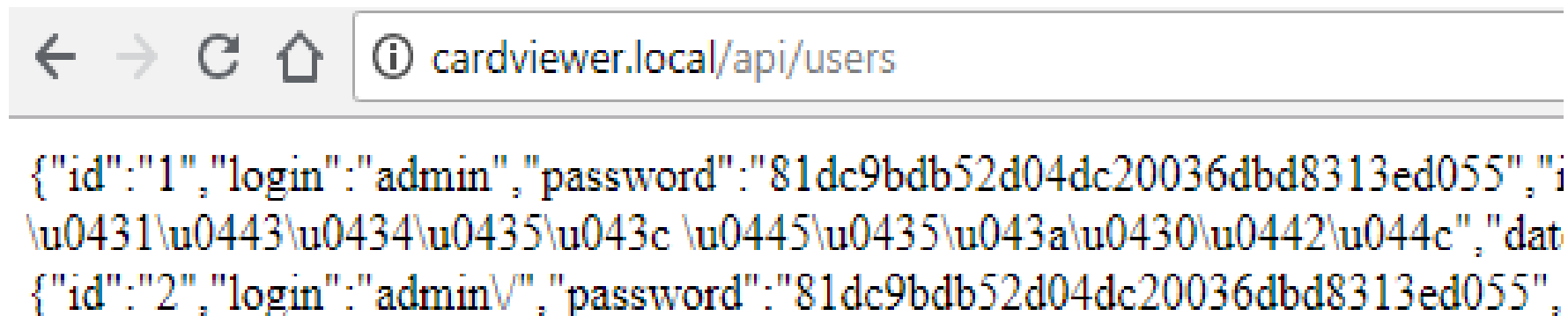
Весь клубок ведет к тому, что от реального пароля остается 4 символа, которые можно достаточно просто сбрутить.

Как победить?

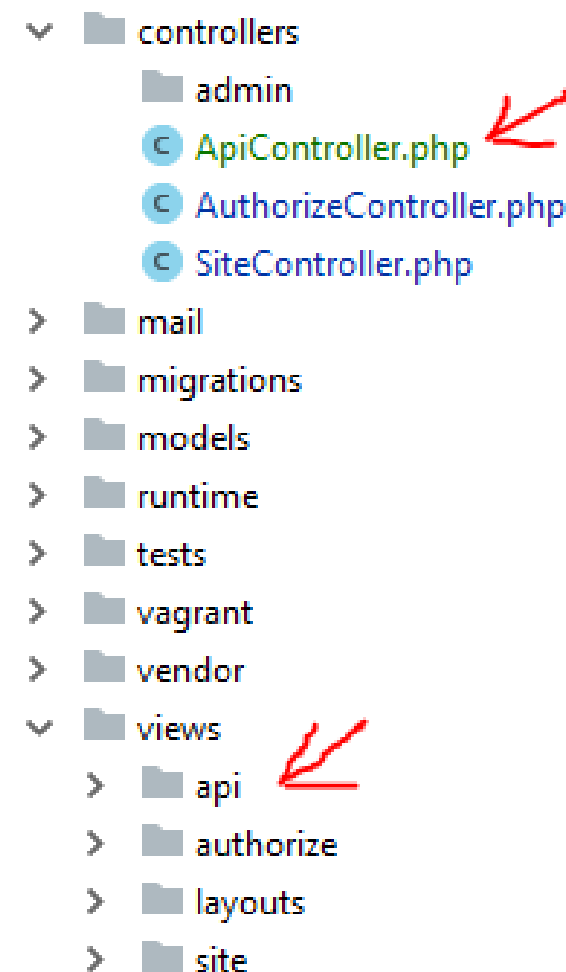
Увеличить число в параметрах, либо повсеместно удалить его.

А вы что думали?

То, что никто не заметил (Но это не точно)



На сайте было API , которое отображало последних 10 пользователей. Пароли – хэш md5, который так же легко сбрутить.



Причина

Ну, она просто была.

Для функционала сайта она не несла никакой пользы и смысла.

```
public function actionUsers()
{
    $users = User::find()->orderBy(['date_reg'=>SORT_DESC])->limit( limit: 10)->asArray()->all();

    return $this->render( view: "users", [
        'users'=>$users
    ]);
}
```

Как победить?

Вы не поверите, но можно(нужно) просто **удалить** весь этот функционал

То, что вы любите. SQL-injection

Ваша заметка

```
1') and sleep(5000) --|
```

Причина

```
ApiController.php x NotesForm.php x
47
48 if (Yii::$app->user->isGuest)
49     return false;
50
51 $notes = new Notes();
52 $oldNote = Notes::find()->where( condition: "id_user=" . $user->id .
53     " and id_owner=" . Yii::$app->user->id)->one();
54 if (!empty($oldNote))
55     $notes = $oldNote;
56
57
58 $notes->id_user = $user->id;
59 $notes->id_owner = Yii::$app->user->id;
60 $notes->text = $this->text;
61
62
63 if (empty($oldNote)) {
64     $query = Yii::$app->db->createCommand( sql: "INSERT INTO notes (id_owner,id_user,text) VALUES(:id_owner,:id_user,\"{$notes->text} \")", [
65         ':id_owner' => $notes->id_owner,
66         ':id_user' => $notes->id_user,
67     ]);
68 } else {
69     $query = Yii::$app->db->createCommand( sql: "UPDATE notes SET id_owner=:id_owner, id_user=:id_user, text=\"{$notes->text} \" WHERE id={$oldNote->id}", [
70         ':id_owner' => $notes->id_owner,
71         ':id_user' => $notes->id_user,
72     ]);
73 }
74
75 if ($query->execute()) {
```

Как победить?

Самая опасная уязвимость, которая позволяла полностью сливать все флаги.

Фиксить экранированием спец символов, либо использованием методов фреймворка

```
//      if (empty($oldNote)) {  
//          $query = Yii::$app->db->createCommand("INSERT INTO notes (id_owner,id_u  
//              ':id_owner' => $notes->id_owner,  
//              ':id_user' => $notes->id_user,  
//          });  
//      } else {  
//          $query = Yii::$app->db->createCommand("UPDATE notes SET id_owner=:id_ow  
//              ':id_owner' => $notes->id_owner,  
//              ':id_user' => $notes->id_user,  
//          });  
//      }  
$notes->save();  
  
//      if ($query->execute()) {  
//          return true;  
//      }  
//      return false;
```

Ну, вот так как-то.
И да пребудет с Вами Сила!

