1. XSS – внедрение кода на веб-сайт для кражи данных пользователей. Для защиты от XSS используем фильтрацию данных.

```php
function input_data($input) {
  return htmlspecialchars(trim($input), ENT_QUOTES, 'UTF-8');
}
```

2. SQL Injection - уязвимость, которая позволяет атакующему использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для манипулирования базой данных и получения доступа к потенциально ценной информации. Для защиты будем проверять данные и подготовленные запросы.

```php
$upd=$db->prepare("UPDATE form SET name=:name, email=:email, year=:byear, pol=:pol, limbs=:limbs, bio=:bio WHERE id=:id");
$cols=array(
  ':name'=>$name,
  ':email'=>$email,
  ':byear'=>$year,
  ':pol'=>$pol,
  ':limbs'=>$limbs,
  ':bio'=>$bio
);
foreach($cols as $k=>&$v){
  $upd->bindParam($k,input_data($v));
}
```

3. CSRF — это вид атаки на сайт, которая производится с помощью мошеннического сайта или скрипта, который заставляет браузер пользователя выполнить нежелательное действие на доверенном сайте, на котором пользователь авторизован. Для защиты используем токены и проверки.

```php
if (!isset($_SESSION['csrf_token'])) {
    $_SESSION['csrf_token'] = bin2hex(random_bytes(32));
}
$token = $_SESSION['csrf_token'];
```

```php
if (parse_url($_SERVER['HTTP_REFERER'], PHP_URL_HOST) !== 'u52825.kubsu-dev.ru') {
  die('Invalid referer');
```

4. Include – угроза от включения вредоносного кода из внешних файлов. Для защиты от Include нужно сделать проверку файла.
   Upload - угроза от загрузки вредоносных файлов на сервер. Для защиты от Upload нужно сделать проверку файла на тип, размер и название.

```php
if (file_exists('form.php')) {
  include('form.php');
}
```