1.XSS — тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода и взаимодействии этого кода с веб-сервером злоумышленника.Для защиты от XSS рекомендуется использовать фильтрацию входных данных и экранирование вывода. Пример кода:

```php
function F_Int_dt($input) {
  return htmlspecialchars(trim($input), ENT_QUOTES, 'UTF-8');
}
function F_Out_dt($output){
  return htmlentities($output, ENT_QUOTES, 'UTF-8');
}
```

2.Внедрение SQL-кода (SQL injection)— один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода.Для защиты от SQL Injection рекомендуется использовать подготовленные запросы и фильтрацию входных данных. Пример кода:

```php
$stmt = $db->prepare("UPDATE applications SET name = ?, email = ?, date = ?, pol = ?, konechn = ?, info = ? WHERE id =?");
$stmt -> execute(array(
  F_Int_dt($_POST['name']),
  F_Int_dt($_POST['email']),
  F_Int_dt($_POST['date']),
  F_Int_dt($_POST['pol']),
  F_Int_dt($_POST['konechn']),
  F_Int_dt($_POST['info']),
```

3.CSRF — вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер, осуществляющий некую вредоносную операцию.Для защиты от CSRF рекомендуется использовать токены CSRF и проверку referer. Пример кода:

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

```php
if ($_SESSION['csrf_token'] !== $_POST['token']) {
  die('Invalid CSRF token');
}
if (parse_url($_SERVER['HTTP_REFERER'], PHP_URL_HOST) !== 'u54997.kubsu-dev.ru') {
  die('Invalid referer');
}
  <form action="index.php"
    method="POST">
<input type="hidden" name="token" value="<?= $token; ?>">
```

4. Include - защита от включения вредоносного кода из внешних файлов, которые могут привести к краже данных пользователя. Для защиты от Include рекомендуется использовать только относительные пути и проверку наличия файла. Пример кода:

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

Upload - защита от загрузки вредоносных файлов на сервер, которые могут привести к краже данных пользователя. Для защиты от Upload рекомендуется проверять тип и размер загружаемого файла, а также использовать уникальные имена файлов.