Отчет Сябрюк Никита 28.2

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. **strip_tags()** - данная функция удаляет из строки аргумента только сами теги, причем второй аргумент служит для указания исключений, которые не нужно удалять. Через нее спокойно проходят строки**: , < img**.

```
foreach ($res as $el) {
  $values['fio']=strip_tags($el['fio']);
  $values['email']=strip_tags($el['email']);
  $values['year']=strip_tags($el['year']);
  $values['gender']=strip_tags($el['gender']);
  $values['limbs']=strip_tags($el['limbs']);
  $values['biography']=strip_tags($el['biography']);
}
```

2)**SQL Injection** - один из распространённых способов взлома сайтов, работающих с базами данных. Способ основан на внедрении в запрос произвольного SQL-кода. Внедрение SQL позволяет хакеру выполнить произвольный запрос к базе данных (прочитать содержимое любых таблиц, удалить, изменить или добавить данные). На этапе подготовки формируется SQL-запрос, где на месте значений будут находиться знаки вопроса — плейсхолдеры. Эти плейсхолдеры в дальнейшем будут заменены на реальные значения. Шаблон запроса отправляется на сервер MySQL для анализа и синтаксической проверки.

```
$stmt = $db->prepare("INSERT INTO application SET fio = ?, email = ?, year = ?, pol = ?, limb, biography = ?");
$stmt -> execute([$_POST['fio'], $_POST['email'], $_POST['year'], $_POST['gender'], $_POST['limbs'], $_POST['biography']]);

$id = $db->lastInsertId();
$stmt = $db->prepare("INSERT INTO baza SET id = ?, login = ?, password = ?");
$stmt -> execute([$id, $login, md5($password)]);
```

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 (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника). Добавила, ранее не было **$ _SESSION ['token']** содержит наш токен. Здесь он и устанавливается для дальнейшей авторизации. Добавил

```
// Начинаем сессию.
session_start();
if (empty($_SESSION['token']))
$_SESSION['token']=bin2hex(random_bytes(64));
```

4) **Include, Upload** - Отсутствуют, нет возможности загружать и скачивать файлы.