

ДЗ 5

1.

```
echo$_GET['username'];
```

в чем уязвимость

Хацкер передает данные через урлу по типу `http://some-site.ru/page.php?`

`username=<script>alert('XSS')</script>`

значение username будет выводиться без проверки и обработки

Выглядит как CWE-79 (XSS-уязвимости)

Исправить можно по типу

```
if (isset($_GET['username'])) {  
    echo htmlspecialchars($_GET['username'], ENT_QUOTES, 'UTF  
}
```

2.

CWE-284 - это уязвимость неправильного контроля доступа, те приложение не ограничивает доступ к ресурсам и функциям при необходимости. Это может повлечь к выполнению сценариев с вредным эффектом, на которые у пользователя прав нет.

Nasa Kodiak v1.0 имела уязвимость CWE-502 в функции обработки данных библиотек, это могло привести к удаленному выполнению кода. Так как ПО сугубо математическое и направлено на решения ОДУ и прочей тяжелой математики (а такие вещи обычно крутятся на мощных вычислительных кластерах), то это могло привести к захвату кластера и использованию мощностей, например, для майнинга криптовалюты или к заражению соседней инфраструктуры.