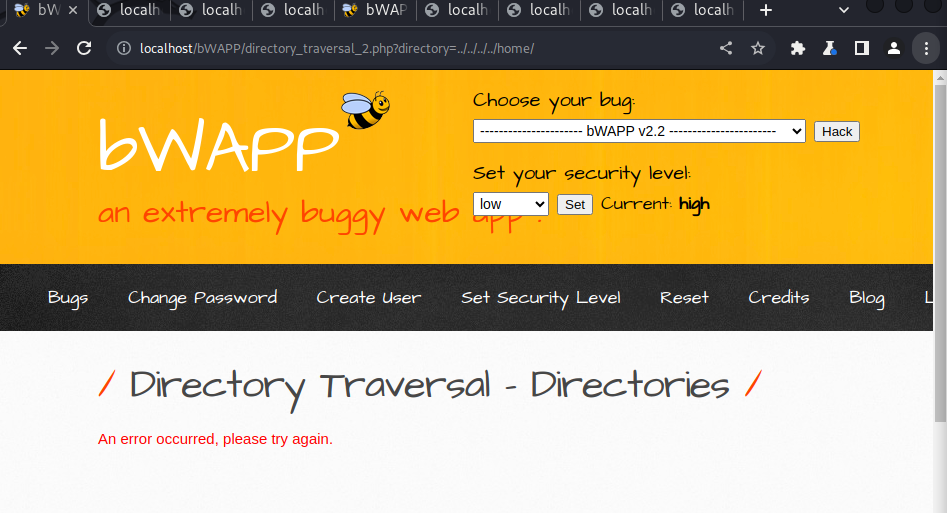
**A7 BWAPP**

**Шестаков Егор Павлович 11ИСП-211**

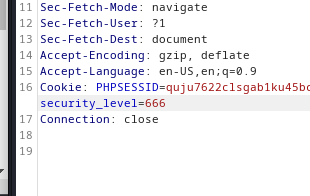
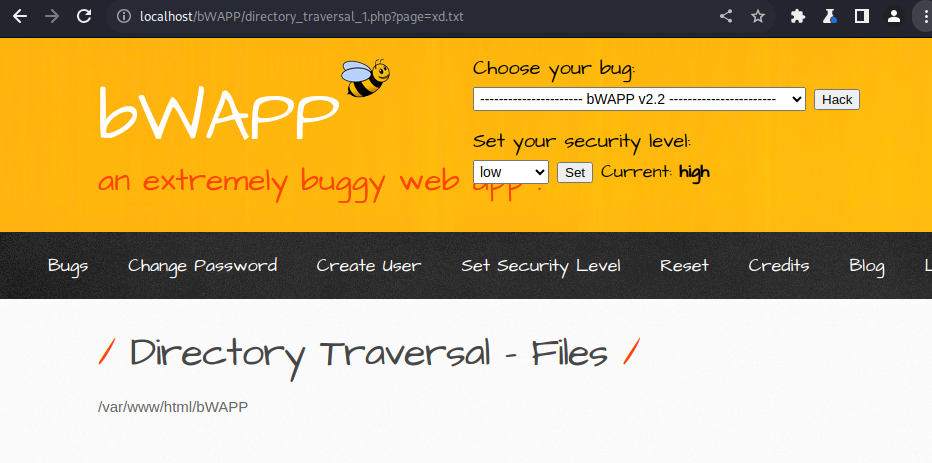
1. Directory Traversal

Функционал представляет GET запрос с параметром директории, которая просматривается и выдает содержимое. В запросе мы передали домашнюю директорию, что выдало ошибку.



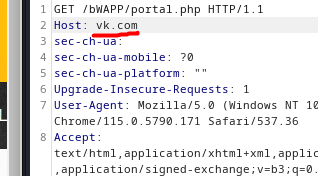
1. Directory Traversal Files

В аргументе теперь у нас page в значение вставляем путь к файлу и он выведется.

В php файле также обнаружена сложность «666», которую можно ввести во время отправки http запроса. Также если мы сбросим в Cookies security\_level то нас перекинет на Set Security level

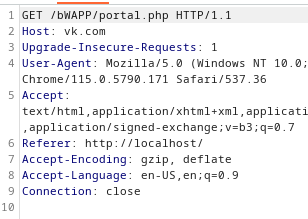
1. Host Header Attack (Cache Poisoning) (Reset Poisoning не работает из-за отсутствия SMTP сервера)

Изменяем хост для переадрисации

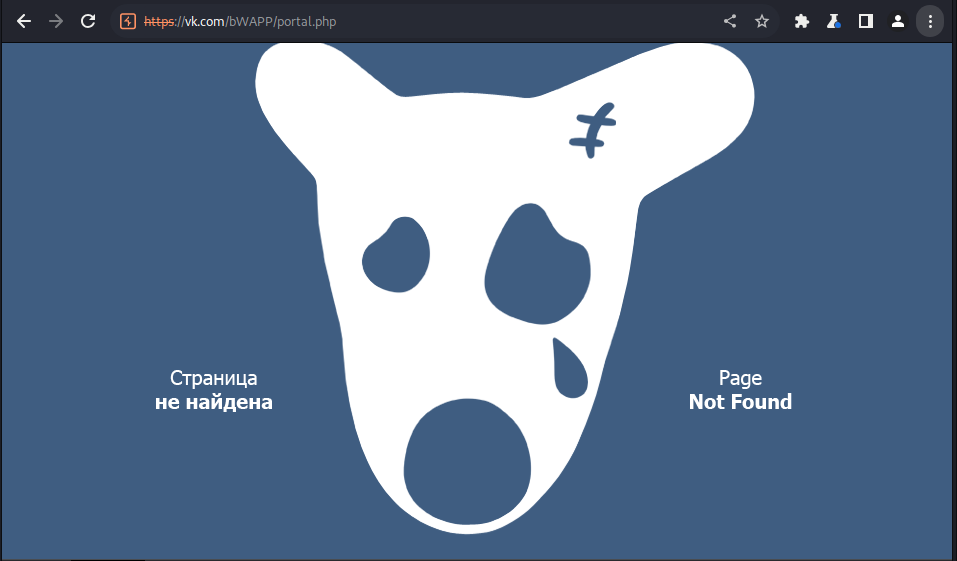


И затем страница «сломается» и будет считать какое-то время что её хост это “vk.com”.

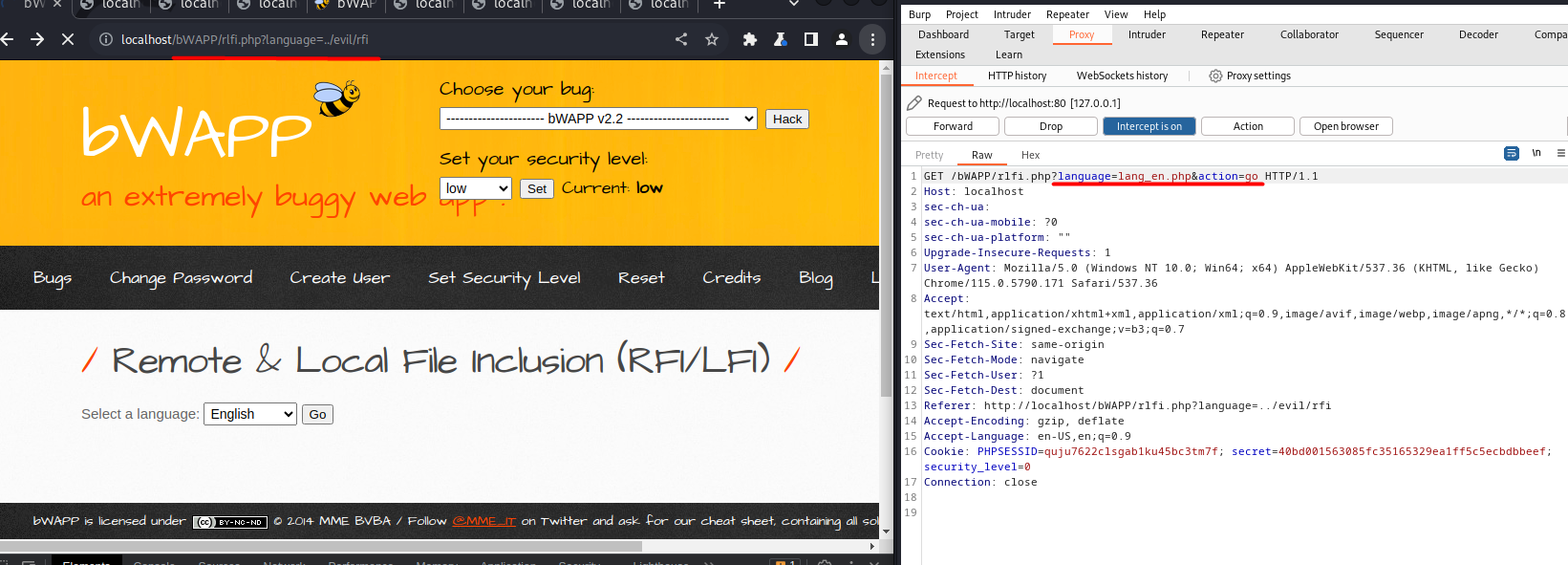




И потом и вовсе переадресует нас на vk.com



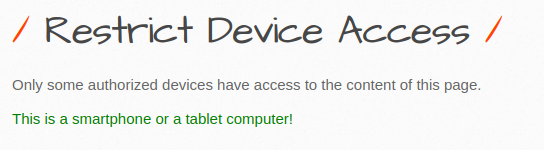
1. Remote n Local File Inclusion



1. Restrict Device Access

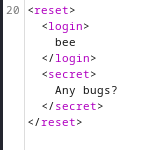
Необходимо добавить заголовок http запрос, чтобы указать что мы якобы мобильное устройство





1. XML Attack

XML атака в http запросе, также возможно поменять логин-секрет

­­­­