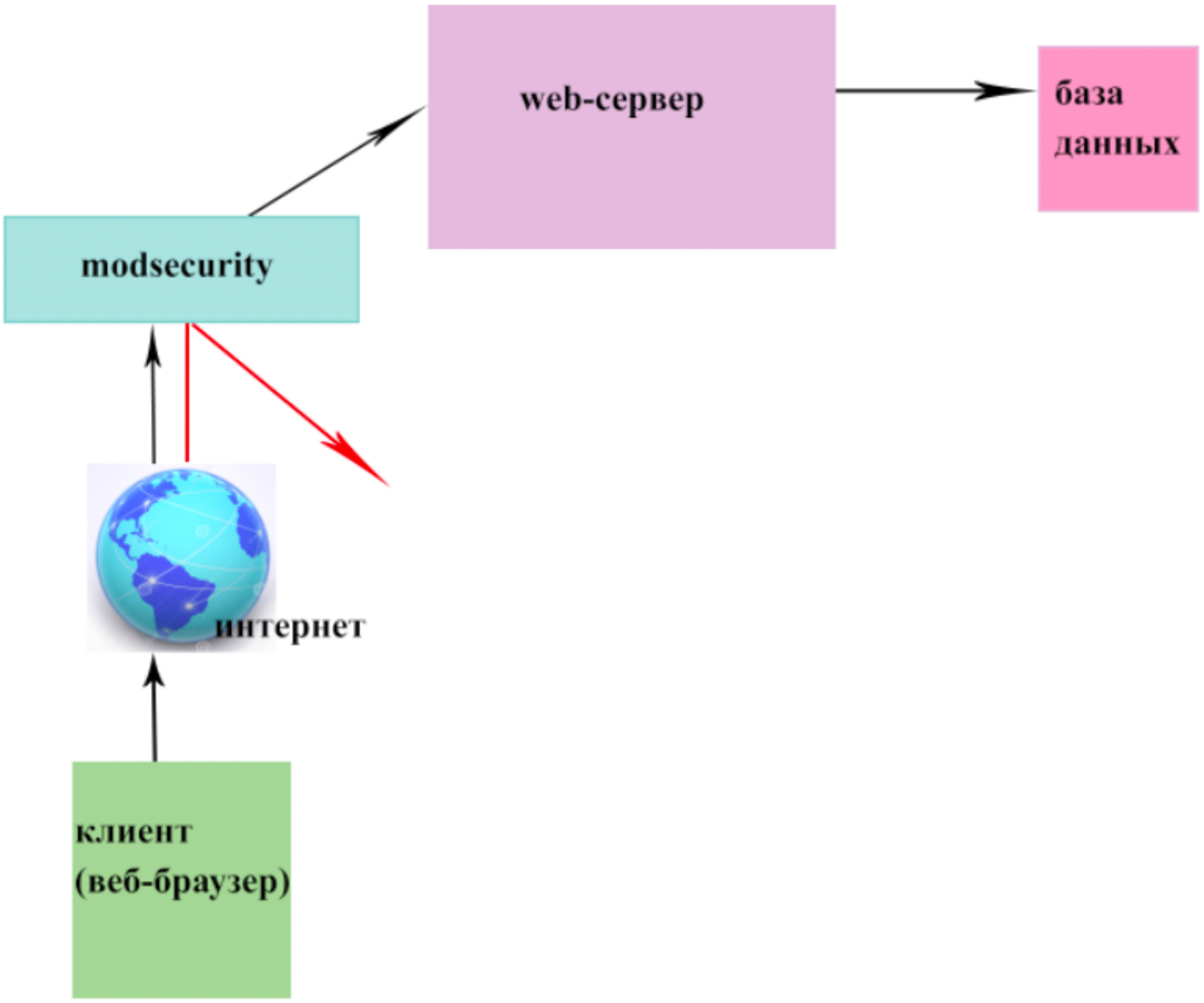
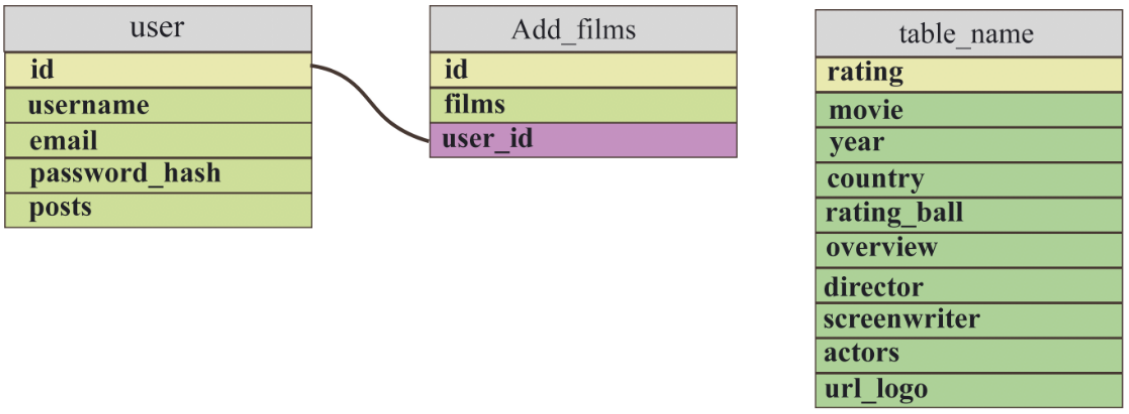
Структура работы веб-приложения



Веб-приложение работает на flask, и имеет 2 базы данных
Использовался python 3

Структура БД веб-приложения



Что такое modsecurity?

Программа ModSecurity — это межсетевой экран с открытым исходным кодом Web-приложений. Продукт защищает от ряда атак, направленных на Web-приложения, позволяет осуществлять мониторинг HTTP-трафика и выполнять анализ событий в реальном времени. ModSecurity, или брандмауэры веб-приложений в целом, специализируется на HTTP-трафике (уровень 7 модели OSI) и выполняет действия в зависимости от содержимого HTTP-запроса и ответа.

Чтобы обнаружить и предотвратить атаки на веб-приложения, брандмауэр веб-приложений (ModSecurity) проверяет все запросы к вашему веб-серверу и соответствующие ответы сервера на соответствие своему набору правил. Если проверка пройдена, запрос передается сайту для получения контента. Если проверка не пройдена, выполняются заданные действия.

OWASP CRS может работать в двух режимах:

Автономный режим - Это традиционный режим, используемый в CRS v2.x. Если HTTP-запрос соответствует правилу, ModSecurity немедленно заблокирует HTTP-запрос и прекратит оценку оставшихся правил.

Режим оценки аномалий - Это режим по умолчанию, используемый в CRS v3.x. ModSecurity проверит HTTP-запрос на соответствие всем правилам и добавит оценку каждому подходящему правилу. При достижении порогового значения HTTP-запрос считается атакой и блокируется. Оценка по умолчанию для входящих запросов - 5, а для исходящих ответов - 4.

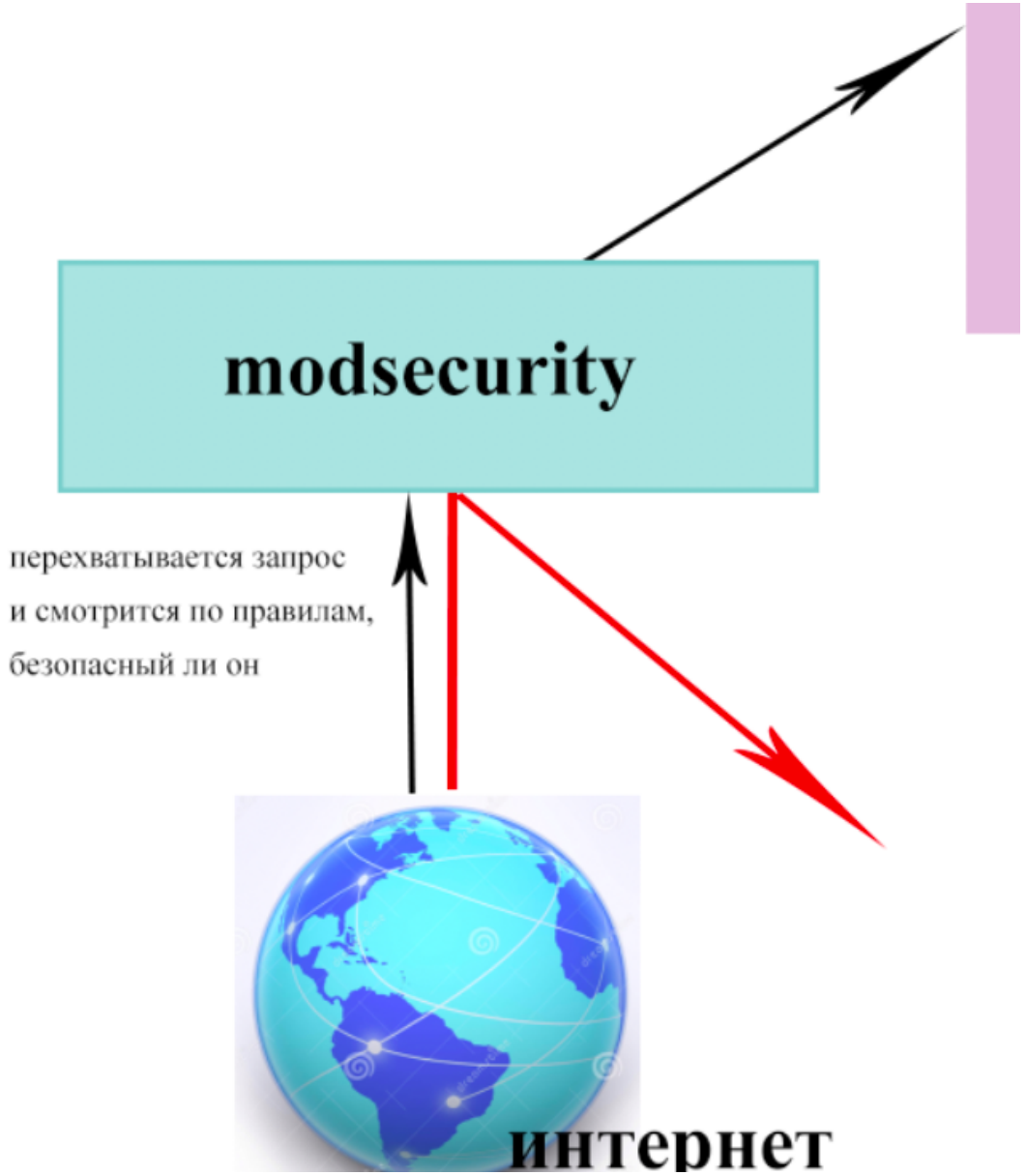
При работе в режиме оценки аномалий существует 4 уровня фильтрации:

- Paranoia level 1 (default)
- Paranoia level 2
- Paranoia level 3
- Paranoia level 4

С каждым повышением уровня фильтрации CRS включает дополнительные правила, обеспечивающие более высокий уровень безопасности. Однако более высокий уровень фильтрации также увеличивает вероятность блокировки некоторого валидного трафика из-за ложных тревог.

Индивидуальные правила CRS хранятся в /etc/apache2/modsecurity-crs/coreruleset-3.3.0/rules/ каталоге. Каждое правило сопоставления увеличивает оценку аномалии.

Схема работы :



перехватывается запрос и смотрится, не опасный ли он. Это делается по правилам. Если все хорошо - выполняем запрос к бд

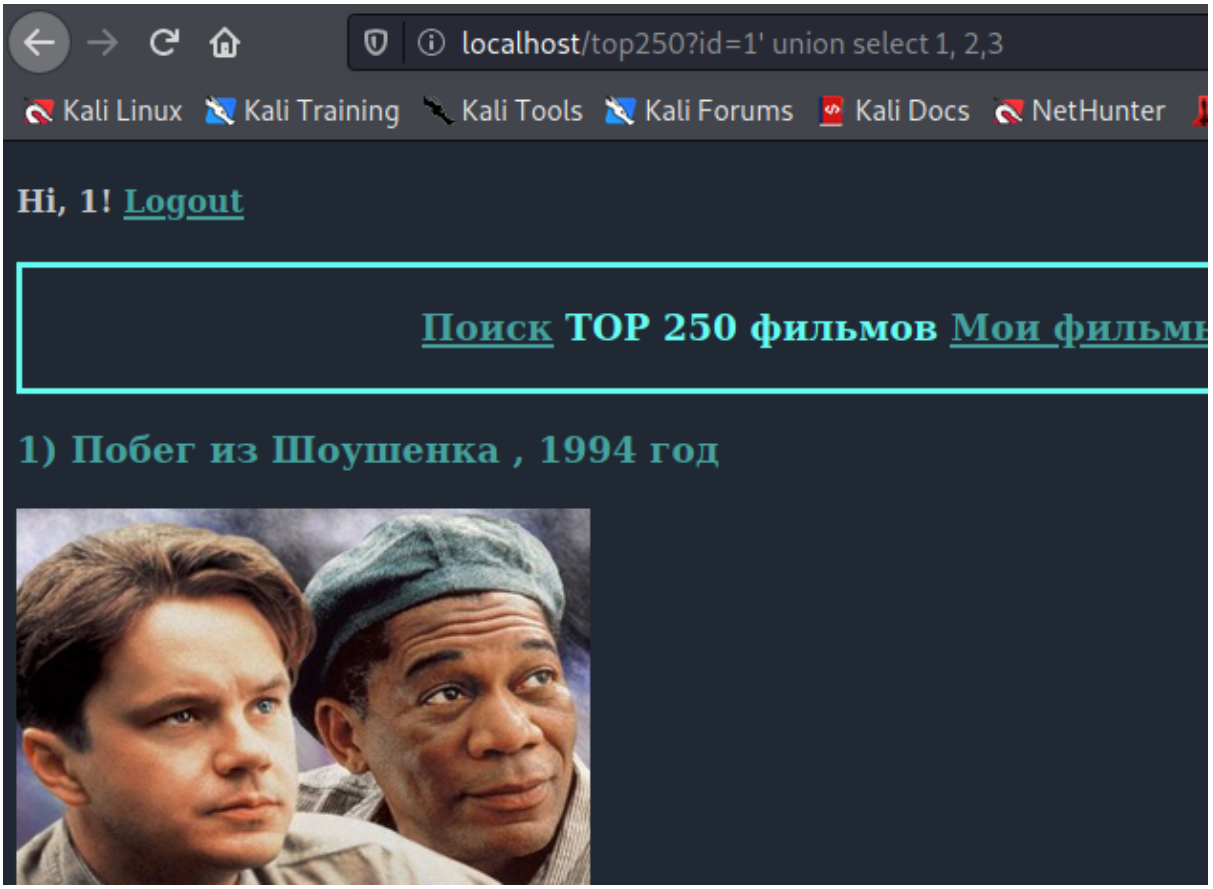
Тестирование

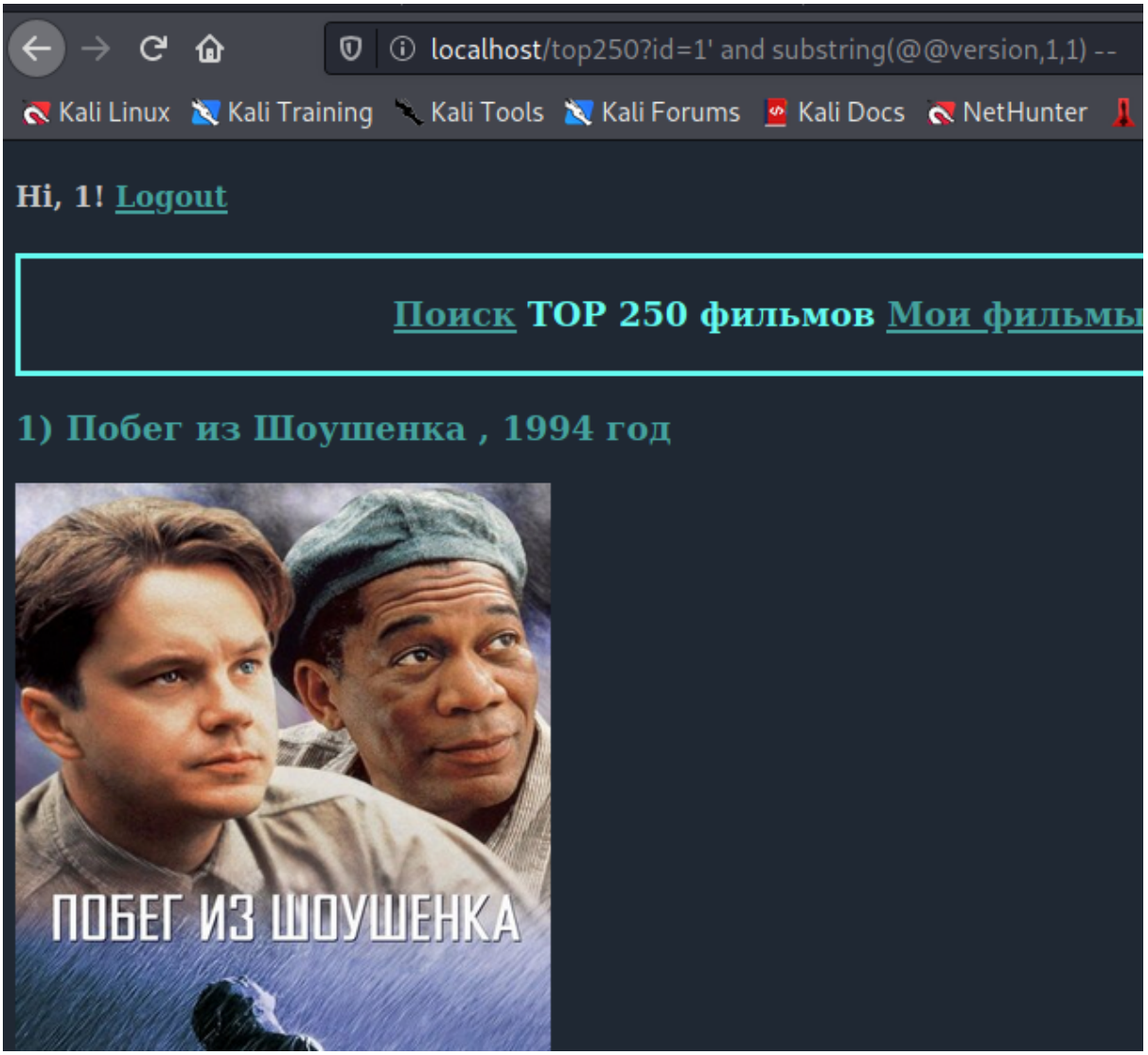
Проведем несколько sql-инъекций на сайт с выключенным modsecurity

```
        # following line enable
        # after it has been glo
        #Include conf-available
        SecRuleEngine Off
        SecRule ARGS:modsecpara
</VirtualHost>
```

Что мы можем видеть:

Инъекции спокойно срабатывают



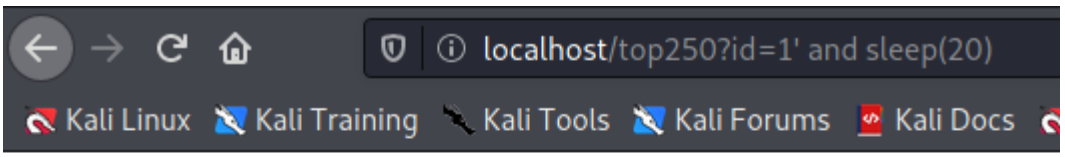

localhost/top250?id=1' and substring(@@version,1,1) --
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Hi, 1! Logout
Поиск TOP 250 фильмов Мои фильмы
1) Побег из Шоушенка , 1994 год
ПОБЕГ ИЗ ШОУШЕНКА

Для защиты сайта включим WAF

```
    # after it has been globa
    #Include conf-available/s
    SecRuleEngine On
    SecRule ARGS:modsecparam
irtualHost>
```

Перезагрузим апач

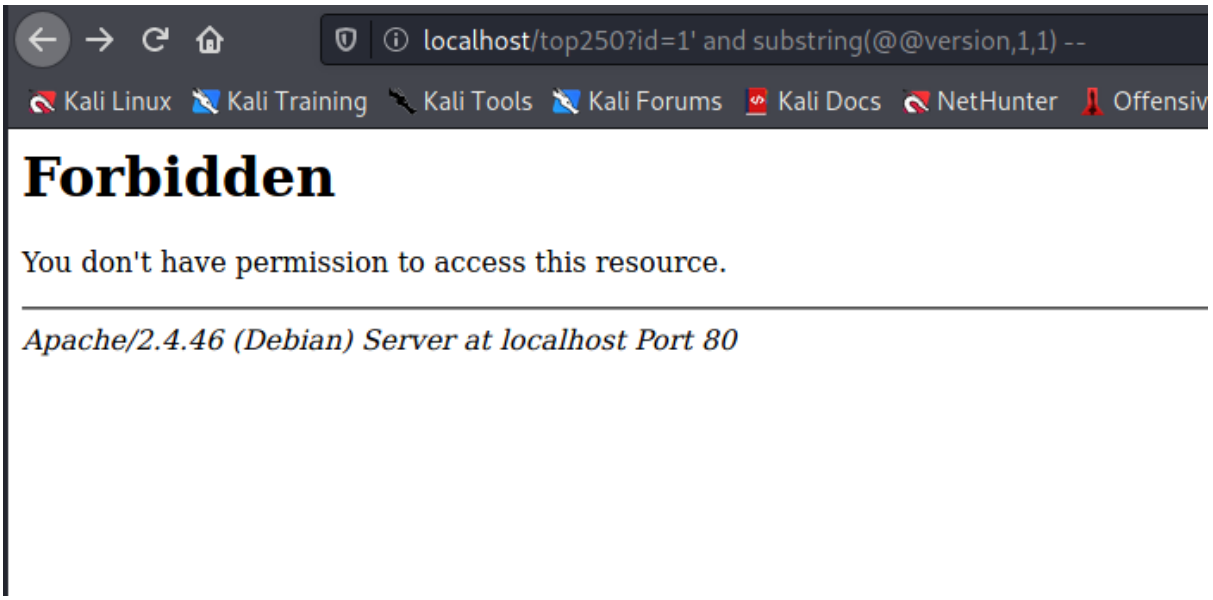
Попробуем снова провести sql-инъекции.
Waf не дает им сработать



Forbidden

You don't have permission to access this resource.

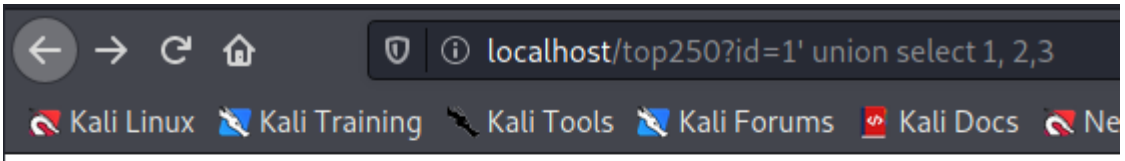
Apache/2.4.46 (Debian) Server at localhost Port 80



Forbidden

You don't have permission to access this resource.

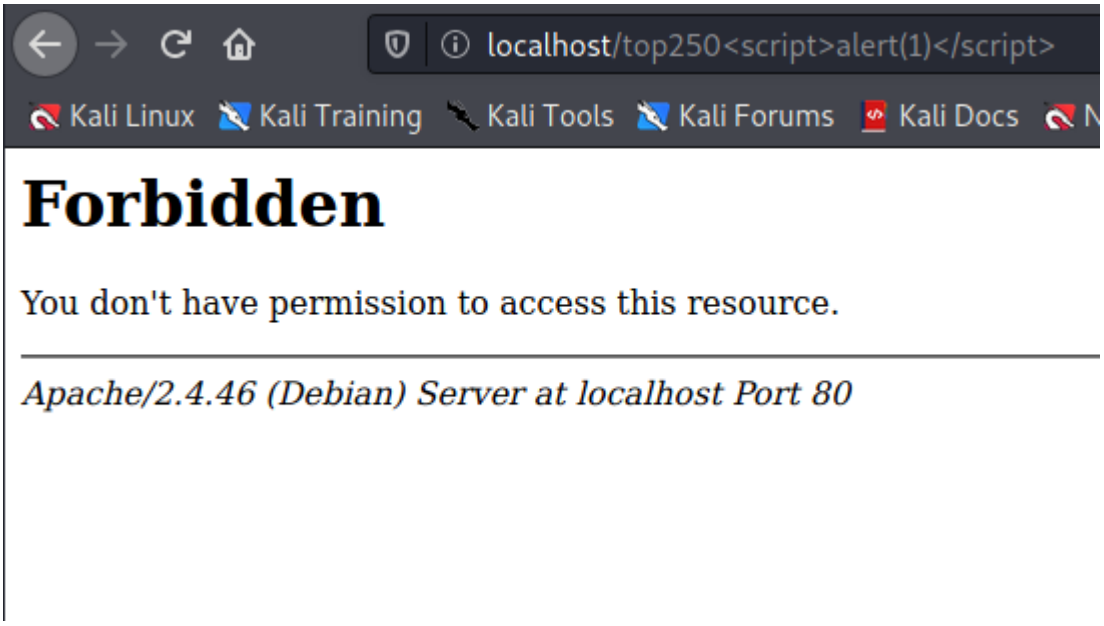
Apache/2.4.46 (Debian) Server at localhost Port 80



Forbidden

You don't have permission to access this resource.

Apache/2.4.46 (Debian) Server at localhost Port 80


localhost/top250<script>alert(1)</script>
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
Forbidden
You don't have permission to access this resource.
Apache/2.4.46 (Debian) Server at localhost Port 80