

|  |  |
| --- | --- |
| МИНОБРНАУКИ РОССИИ | |
| *Федеральное государственное бюджетное образовательное учреждение*  *высшего образования*  ***«МИРЭА – Российский технологический университет»***  **РТУ МИРЭА** | |

Институт Информационных технологий (ИТ)

Кафедра Математического обеспечения и стандартизации информационных

технологий (МОСИТ)

**ПРАКТИЧЕСКАЯ РАБОТА №6**

**по дисциплине**

**«Тестирование и верификация программного обеспечения»**

Студенты группы ИКБО-20-21

Хитров Н.С.

Емельянов И.В.

Квашнин Ю.В.

Мухаметшин А.Р.

(подпись студента)

**Принял руководитель работы** Овчинникова М.А.

(подпись руководителя)

Практические работы выполнены « » 2023 г.

Зачтено « » 2023 г.

1. **Основные требования**

Хранение метаинформации и cookies на веб-сайте должно соответствовать современным стандартам безопасности и уважать приватность пользователей. Вот основные требования к хранению метаинформации и cookies:

1. Обеспечение конфиденциальности данных:

Используйте шифрование (например, протокол HTTPS) для передачи данных между пользователем и сервером, чтобы обеспечить конфиденциальность информации во время передачи.

1. Соблюдение законодательства о приватности:

Учитывайте местные и международные законы о защите данных и приватности пользователей, такие как GDPR в Европе или CCPA в Калифорнии.

1. Явное информирование пользователей:

Информируйте пользователей о том, какие данные собираются, обрабатываются и хранятся на сайте. Эта информация должна быть предоставлена в ясной и доступной форме, например, через политику конфиденциальности.

1. Согласие пользователя:

Получайте явное согласие от пользователей на использование cookies и сбор данных. Механизм получения согласия (cookie consent banner) должен быть прозрачным и легким в использовании.

1. Ограничение сроков хранения:

Устанавливайте ограниченные сроки хранения cookies и других данных. Собираемая информация должна быть актуальной и не храниться дольше необходимого для выполнения целей сбора данных.

1. Безопасность сессий:

Используйте безопасные методы управления сессиями, такие как уникальные идентификаторы сессий (session tokens) и механизмы предотвращения атак, таких как CSRF (Cross-Site Request Forgery) и XSS (Cross-Site Scripting).

1. Защита от атак:

Принимайте меры для предотвращения атак, таких как инъекции данных, взлом сессий и других видов злоупотреблений.

1. Политика отказа от ответственности (Disclaimer):

Включите четкую политику отказа от ответственности, определяющую, какие данные собираются, как они используются, и как пользователи могут управлять своей конфиденциальной информацией.

1. Возможность отказа от отслеживания:

Предоставьте пользователям возможность отказаться от отслеживания (Do Not Track) в соответствии с их предпочтениями.

1. Мониторинг и обновления:

Регулярно мониторьте безопасность сайта, а также следите за изменениями в законодательстве и обновляйте политики и механизмы согласия в соответствии с новыми требованиями.

Соблюдение этих требований поможет улучшить безопасность взаимодействия пользователя с веб-сайтом и защитить их приватность.

1. **Выбор веб-сайта**

Для анализа был выбран веб-сайт "Спортмастер". Он представляет крупную российскую розничную компанию, специализирующуюся на продаже спортивных товаров и экипировки. Сайт "Спортмастер" выполняет несколько основных функций:

**Онлайн-магазин:**

* + Пользователи могут просматривать и заказывать спортивные товары через интернет, включая одежду, обувь, инвентарь, электронику для занятий спортом, аксессуары и другие товары.

**Информационный ресурс:**

* + Сайт предоставляет информацию о продаваемых товарах, включая описания, технические характеристики, цены и отзывы покупателей. Также может содержать советы и статьи о здоровом образе жизни, фитнесе и других темах, связанных со спортом.

**Акции и скидки:**

* + "Спортмастер" регулярно проводит акции и предоставляет скидки на свои товары. Сайт предоставляет информацию о текущих акциях, специальных предложениях и скидках.

**Личный кабинет:**

* + Зарегистрированные пользователи могут создать личные кабинеты, где могут отслеживать статус своих заказов, сохранять предпочтения, управлять персональной информацией и получать персонализированные рекомендации.

**Поиск и фильтрация:**

* + Сайт предоставляет инструменты для удобного поиска и фильтрации товаров в соответствии с различными параметрами, такими как бренд, вид спорта, размер и другие.

**Информация о магазинах:**

* + Пользователи могут получить информацию о физических магазинах "Спортмастер", включая их расположение, часы работы и контактные данные.

**Блог и новости:**

* + На сайте могут размещаться блоги, статьи и новости о мире спорта, событиях, трендах и других темах, которые могут быть интересными для целевой аудитории.

**Обратная связь и поддержка:**

* + Пользователи могут обращаться в службу поддержки для получения помощи, задавать вопросы и оставлять отзывы о продуктах и обслуживании.

1. **Анализ данных**

Провести анализ данных на выбранном веб-сайте при помощи инструментального средства EditThisCookie. Предоставить результаты работы инструмента, а также сделать выводы о полученных результатах.

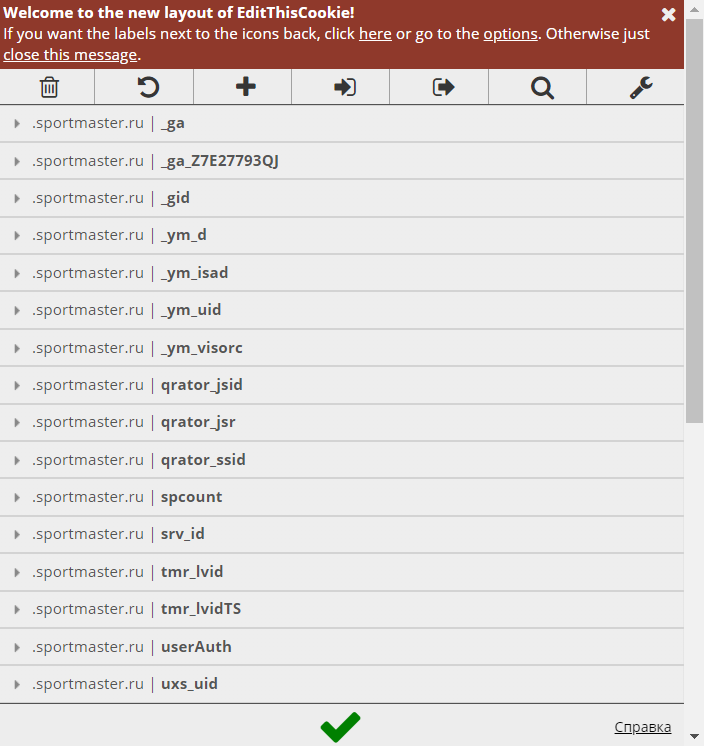


Рисунок 1 – Список куки, связанных с сайтом sportmaster.ru

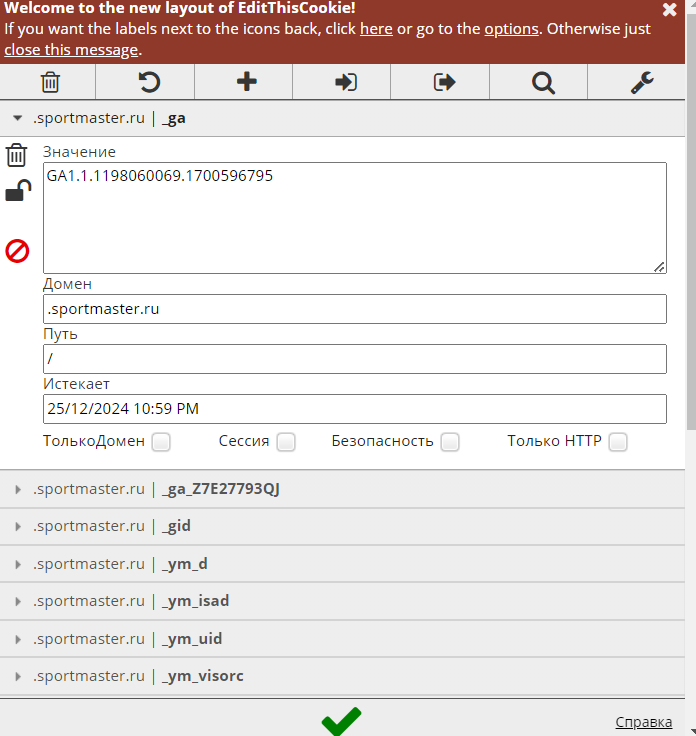


Рисунок 2 – Куки - идентификатор клиента

Куки, которая является идентификатором клиента, привязанным к конкретному пользователю, который посещает веб-сайт и использует Google Analytics для отслеживания его активности и поведения на сайте.

1. **GA1.1:** Это обозначение для Google Analytics и версии протокола. Значение **1.1** указывает на формат данных, который используется для отправки информации о событиях и взаимодействии пользователя на веб-сайте.
2. **1198060069:** Это идентификатор клиента (Client ID). Этот уникальный идентификатор присваивается пользователю при первом посещении веб-сайта и сохраняется в куках браузера. Это позволяет Google Analytics отслеживать поведение пользователя на протяжении его визитов к сайту.
3. **1700596795:** Это временная метка (Timestamp). Представляет собой количество секунд с начала эпохи (обычно 1970 года), когда была установлена кука. В данном случае, **1700596795** означает, что кука была установлена около 24 января 2023 года (если принять начало эпохи в 1970 году).

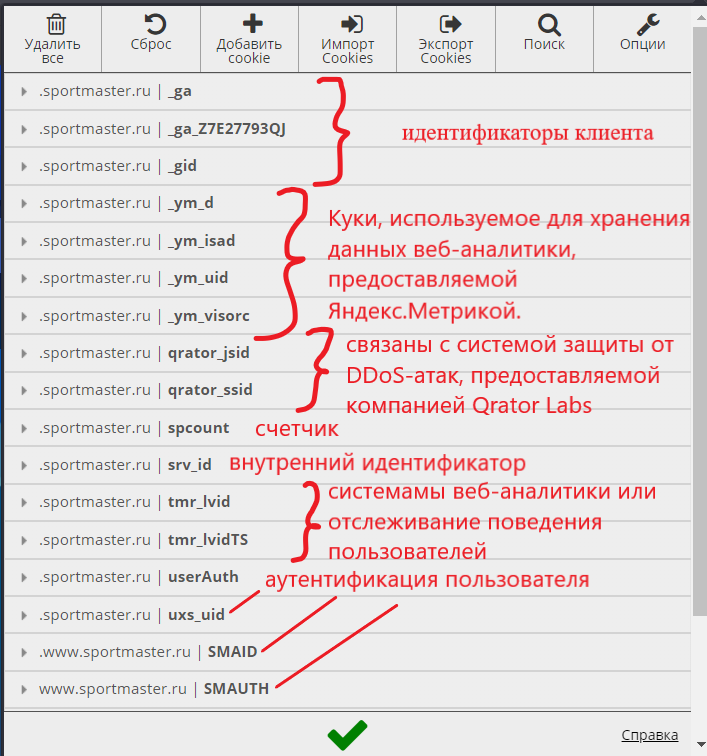


Рисунок 3 – Назначение остальных куки на сайте

Выводы:

**Аутентификация пользователя:**

* + Присутствие куки с именем "userAuth" может указывать на то, что на сайте используется механизм аутентификации для идентификации пользователей.

**Веб-аналитика:**

* + Куки, такие как "\_ym\_d", "GA1.1.1198060069.1700596795", "GA1.2.890753414.1700596795", "tmr\_lvid", "tmr\_lvidTS", "uxs\_uid" и другие, могут быть связаны с системами веб-аналитики (например, Яндекс.Метрика, Google Analytics). Они используются для отслеживания поведения пользователей и сбора статистики.

**Защита от DDoS-атак:**

* + Куки типа "qrator\_jsid" и "qrator\_ssid" могут указывать на то, что на сайте используется защита от DDoS-атак, предоставляемая компанией Qrator Labs.

**Идентификация сессии и пользователя:**

* + Куки, содержащие идентификаторы сессии и пользователя, такие как "SMAID" и "uxs\_uid", могут использоваться для отслеживания конкретных сеансов и идентификации пользователей.

**Временные метки:**

* + Некоторые из куки, например, "tmr\_lvidTS" и "GA1.1.1198060069.1700596795", содержат временные метки, которые могут указывать на время создания или обновления куки.

1. **Анализ информационной безопасности и оценки уязвимостей при помощи программного продукта FOCA.**

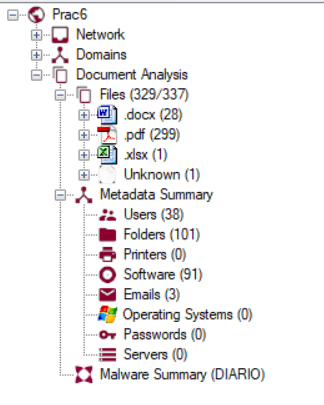


Рисунок 4 – Сводка метаданных

FOCA извлекает следующие данные: пользователи, папки, принтеры, программное обеспечение, электронная почта, операционные системы, пароли и серверы. Просматривая наши конкретные документы, мы обнаружили: было найдено 28 текстовых документов, 299 PDF-файлов, 1 файл xlsx и 1 неизвестный файл, в которых содержатся 38 пользователей, 101 папка, 3 электронных почты и 91 тип программного обеспечения.



Рисунок 5 – Имена пользователей



Рисунок 6 – Категории программного обеспечения

В метаданных сайта sportmaster.ru были найдены ФИО и должности работников организации, которые можно использовать для более детального изучения их деятельности или для связи с ними.

Объединив все точки данных (программное обеспечение, пользователи, пути к документам, информацию о документе), полученные в результате быстрого поиска FOCA, мы можем получить довольно хорошее представление о компании или организации изнутри, а также множество опорных точек, на основе которых можно построить дополнительные социальные сети, резюме и корпоративную разведку.

Список использованной литературы

* 1. Лекции Петренко А.А. по дисциплине «Тестирование и верификация программного обеспечения». МИРЭА, 2023 (Дата обращения 22.11.2023);