УДК 004.056

УЯЗВИМОСТИ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Романова М.П.

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Насонова Н.В. – доктор техн. наук, доцент

Аннотация. В статье рассматриваются вопросы реализации и уязвимости одно- и многофакторной аутентификации. Проведён практический анализ возможностей эксплуатации механизмов многофакторной аутентификации на веб-сайтах с использованием специализированного ПО Burpsuite. В заключении автор предлагает несколько рекомендаций по внедрению многофакторной аутентификации на веб-сайтах для предотвращения возникновения описанных уязвимостей.

Ключевые слова: Аутентификация, уязвимости, эксплуатация.

Многофакторная аутентификация (multi-factor authentication, MFA) — расширенная аутентификация, метод контроля доступа, в котором пользователю для получения доступа к

информации необходимо предъявить более одного «доказательства механизма аутентификации». Среди всех рекомендаций по обеспечению безопасности доступа, многофакторная аутентификация, безусловно является одной из наиболее часто встречающихся [1].

Уязвимости аутентификации оказывают серьёзное влияние на безопасность информационного ресурса. Если злоумышленник обходит аутентификацию и получает доступ к учётной записи другого пользователя, он получает доступ ко всем данным и функциям, которыми обладает скомпрометированная учётная запись. Если удаётся скомпрометировать учётную запись с высоким уровнем привилегий, например, учётную запись системного администратора, они могут получить полный контроль над всем приложением и потенциально получить доступ к внутренней инфраструктуре.

Многие веб-сайты полагаются исключительно на однофакторную аутентификацию с использованием пароля для аутентификации пользователей. Однако она является небезопасной, поскольку пароли могут быть скомпрометированы различными способами. Например, согласно исследованию Verizon Data Breach Investigations Report за 2023 год, 82% утечек данных были связаны с человеческим фактором, включая использование слабых или украденных паролей [2]. Эффективным способом повысить защищенность процесса аутентификации является внедрение многофакторной аутентификации. Хотя проверка биометрических факторов может быть нецелесообразна для большинства веб-сайтов, все чаще встречается как обязательная, так и необязательная двухфакторная аутентификация (2FA), основанная на комбинации факторов «что вы знаете» (пароль) и «что у вас есть». Обычно это включает ввод традиционного пароля и временного кода проверки, полученного с физического устройства, находящегося во владении пользователя.

Большинство уязвимостей в механизмах аутентификации проявляются в одном из двух способов: механизмы аутентификации слабы, потому что они не могут адекватно защитить от атак методом перебора или же есть логические недостатки или ошибки реализации, которые позволяют злоумышленнику полностью обойти механизмы аутентификации. Иногда это называется «нарушенной аутентификацией».

Несмотря на то, что иногда злоумышленник может получить один фактор, основанный на знаниях, например, пароль, возможность одновременного получения другого фактора из внешнего источника значительно менее вероятна [3]. По этой причине двухфакторная аутентификация более безопасна, чем однофакторная аутентификация. Однако, как и любая мера безопасности, она безопасна настолько, насколько безопасна её реализация. Плохо реализованную двухфакторную аутентификацию можно обойти или даже полностью обойти, так же как и однофакторную аутентификацию.

Иногда реализация двухфакторной аутентификации несовершенна до такой степени, что её можно полностью обойти. Если пользователю сначала предлагается ввести пароль, а затем ввести код подтверждения на отдельной странице, пользователь фактически находится в состоянии «вошёл в систему» до того, как он ввёл код подтверждения. В этом случае стоит проверить, сможете ли вы напрямую перейти к страницам «только для входа в систему» после завершения первого шага аутентификации. Иногда вы можете обнаружить, что веб-сайт на самом деле не проверяет, выполнили ли вы второй шаг перед загрузкой страницы.

Уязвимости многофакторной аутентификации, связанные с ошибочной логикой процесса.

Например, если после того, как пользователь завершил первый этап входа в систему, веб-сайт не проверяет должным образом, что тот же пользователь завершает второй этап аутентификации.

Например, пользователь входит в систему со своими обычными учетными данными на

первом шаге следующим образом:

```
POST /login-steps/first HTTP/1.1
Host: vulnerable-website.com
...
username=carlos&password=qwerty
```

Затем им присваивается файл cookie, относящийся к их учетной записи, прежде чем они переходят ко второму этапу процесса входа в систему:

```
HTTP/1.1 200 OK
Set-Cookie: account=carlos

GET /login-steps/second HTTP/1.1
Cookie: account=carlos
```

При отправке кода подтверждения запрос использует этот файл cookie, чтобы определить, к какой учетной записи пользователь пытается получить доступ:

```
POST /login-steps/second HTTP/1.1
Host: vulnerable-website.com
Cookie: account=carlos
...
verification-code=123456
```

В этом случае злоумышленник может войти в систему, используя свои учетные данные, но затем изменить значение файла cookie на любое произвольное имя пользователя при отправке кода подтверждения. account

```
POST /login-steps/second HTTP/1.1
Host: vulnerable-website.com
Cookie: account=victim-user
...
verification-code=123456
```

Это чрезвычайно опасно, если злоумышленник затем сможет подобрать код верификации, поскольку это позволит ему входить в учетные записи произвольных пользователей, основываясь исключительно на их имени пользователя. Им даже не нужно будет знать пароль пользователя.

Уязвимости многофакторной аутентификации, связанные со слабыми механизмами.

Как и в случае с паролями, веб-сайты должны принимать меры для предотвращения подбора кода проверки 2FA. Это особенно важно, потому что код часто представляет собой простое 4 или 6-значное число. Без надёжной защиты от перебора взломать такой код несложно.

Некоторые веб-сайты пытаются предотвратить это, автоматически выходя из системы, если пользователь вводит определённое количество неправильных кодов подтверждения. На практике это неэффективно, потому что продвинутый злоумышленник может даже автоматизировать этот многоступенчатый процесс, создав макросы для Burp Intruder. Для этой цели также можно использовать удлинитель Turbo Intruder.

Подводя итоги, дадим некоторые рекомендации по внедрению многофакторной

аутентификации на веб-сайтах для предотвращения описанных уязвимостей. Итак, они включают выбор надёжных методов MFA, таких как FIDO2, приложения-аутентификаторы и push-уведомления с подтверждением номера, избегая менее предпочтительных вариантов вроде SMS-кодов и email-кодов, реализацию MFA с плавной интеграцией, простым процессом настройки, предложением нескольких вариантов и безопасных резервных методов, а также безопасное хранение секретных ключей и защиту от обхода MFA, обеспечение удобства использования через возможность запоминания устройств и адаптивную MFA, обучение и поддержку пользователей с информированием о важности MFA и предоставлением инструкций, а также постоянное совершенствование через мониторинг, регулярное обновление и аудит безопасности. Внедрение MFA помогает предотвратить атаки с использованием украденных учётных данных, фишинг, атаки типа "человек посередине", атаки на сеансы и внутренние угрозы, значительно повышая безопасность веб-сайта.

Список литературы

1. *За пределами MFA: почему пароли все еще играют ключевую роль в безопасности? [Electronic resource] / SecurityLab. – Mode of access :https://www.securitylab.ru/analytics/546198.php?ysclid=m8hadlgxes727904854&utm_referrer=https%3A%2F%2Fyandex.by%2F – Date of access : 21.02.2023.*

2. *Verizon Data Breach Investigations Report [Электронный ресурс] / Verizon. – Режим доступа : https://www.verizon.com/business/en-nl/resources/reports/dbir/2023/summary-of-findings/. – Дата доступа : 15.02.2024*

3. *Виды многофакторной аутентификации [Electronic resource] / Keeper. – Mode of access : https://www.keepersecurity.com/blog/ru/2023/06/27/types-of-multi-factor-authentication-mfa/. – Date of access : 27.06.2023.*

UDC 004.056

Multifactor Authentication vulnerabilities

Romanova M.P.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Nasonova N.V. – Doctor of Technical Sciences, Associate Professor

Annotation. The article discusses the implementation and vulnerability of single- and multi-factor authentication. A practical analysis of the possibilities of using multifactor authentication mechanisms on websites using specialized Burpsuite software has been carried out. In conclusion, the author offers several recommendations for implementing multi-factor authentication on websites to prevent the occurrence of the described vulnerabilities.

Keywords: Authentication, vulnerabilities, exploitation.