Дипломная работа по профессии «Специалист по информационной безопасности»

1. OSINT

Согласно задания необходимо просканировать приложение находящиеся по адресу **87.249.53.182**.

**Используемый инструментарий и ПО:** WireShark, nmap, OWASP ZAP, Burp Suite Pro, XSpider, Google Chrome

Был произведен поиск информации в сети интернет указанного адреса. Удалось выяснить адрес имеет 2 открытых порта **22** и **8060**. При сканировании с помощью **Nmap** удалось найти **22** порт.

Было проведено сканирование с помощью **shodan.io.** По его данным, было найдено:

* **Hostnames**: 608477-cg36175.tmweb.ru
* **Domains**: TMWEB.RU
* **Country**: Russian Federation
* **City**: Saint Petersburg
* **Organization**: TimeWeb Ltd.
* **ISP**: TimeWeb Ltd.
* **ASN**: AS9123
* **Operating System**: Ubuntu
* **22 port**: SSH-2.0-OpenSSH\_8.2p1 Ubuntu-4ubuntu0.2

С помощью **wireshark** удалось выяснить сто приложение взаимодействует с адресами **10.0.2.15**, **216.58.210.163 (Скрин 31)**

Приложение по адресу **87.249.53.182:8060** взаимодействует с приложением **87.249.53.182:7799**.

1. **Scanning**

С помощью программы **XSpider** сканировал адрес **87.249.53.182**. Программа показала следующие уязвимости: В Режиме Safe scan (Скрин 32, 33, 34, 35, 36), В режиме PCI DSS (Скрин 38-96)

С помощью **Owasp ZAP** было просканировано приложения **NetologyVuinApp.com (87.249.53.182:8060) и 87.249.53.182:7799**. Также по этим приложениям было проведено сканирование в **Burp Suite Pro**, которое показало аналогичные уязвимости. По данным уязвимостям была сделана проверка на False Positive срабатывания и проведен пентест.   
Удалось обнаружить уязвимости:

**87.249.53.182:8060**

|  |  |  |
| --- | --- | --- |
| **CWE** | **Описание** | **False Positive** |
| CWE-79 | Отсутствие мер по очистке входных данных, позволяющая нарушителю осуществлять межсайтовые сценарные атаки | Нет |
| CWE-22 | «Обход пути» | Да |
| CWE-541 | Включение конфиденциальной информации во включаемый файл | Да |
| CWE-89 | Непринятие мер по защите структуры запроса SQL (атаки типа "внедрение SQL") | Нет |
| CWE-311 | Отсутствует шифрование конфиденциальных данных | Нет |
| CWE-91 | XML-инъекция | Да |
| CWE-693 | Сбой механизма защиты | Нет |
| CWE-1021 | Неверное ограничение визуализируемых слоев или фреймов пользовательского интерфейса | Нет |
| CWE-352 | Подделка межсайтовых запросов (CSRF) | Нет |
| CWE-548 | Предоставление информации через список каталогов | Нет |
| CWE-20 | Неправильная проверка ввода | Нет |
| CWE-540 | Включение конфиденциальной информации в исходный код | Да |
| CWE-1004 | Конфиденциальный файл cookie без флага «HttpOnly» | Нет |
| CWE-1275 | Файл cookie с неправильным атрибутом SameSite | Нет |
| CWE-200 | Раскрытие информации | Нет |
| CWE-524 | Использование кэша, содержащего конфиденциальную информацию | Да |

**87.249.53.182:7799**

|  |  |  |
| --- | --- | --- |
| **CWE** | **Описание** | **False Positive** |
| CWE-79 | Отсутствие мер по очистке входных данных, позволяющая нарушителю осуществлять межсайтовые сценарные атаки | Нет |
| CWE-78 | Неправильная нейтрализация специальных элементов, используемых в команде ОС («Внедрение команды ОС») | Нет |
| CWE-22 | «Обход пути» | Нет |
| CWE-89 | Непринятие мер по защите структуры запроса SQL (атаки типа "внедрение SQL") | Нет |
| CWE-1021 | Неверное ограничение визуализируемых слоев или фреймов пользовательского интерфейса | Нет |
| CWE-829 | Включение функциональности из недоверенной сферы управления | Нет |
| CWE-693 | Сбой механизма защиты | Нет |
| CWE-190 | Целочисленное переполнение или перенос | Да |
| CWE-749 | Незащищенный опасный метод или функция | Нет |
| CWE-200 | Раскрытие информации | Нет |
| CWE-524 | Использование кэша, содержащего конфиденциальную информацию | Да |
| CWE-352 | Подделка межсайтовых запросов (CSRF) | Нет |

1. **Testing**

С помощью **Owasp ZAP** было просканировано приложение **NetologyVuinApp.com (87.249.53.182:8060)**. По данным уязвимостям была сделана проверка на False Positive срабатывания и проведен пентест. Удалось обнаружить уязвимости:

1. **Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79) (скрин 1) (proof-of-concept скрины 114 и 115)**   
   **- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)   
   - Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 6,1)**

**Решение:**

Используйте стратегию проверки входных данных «принять заведомо исправные», т. е. Используйте разрешенный список допустимых входных данных, которые строго соответствуют спецификациям.

1. **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CWE-89) (Скрин 4, Скрин 5) (proof-of-concept скрины 116 и 117)   
   - Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)   
   - Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 5,6)  
   Решение:**

Не доверяйте набору ввода клиента, даже если на месте есть проверка на стороне клиента. Как правило, введите все данные на стороне сервера.

1. **Missing Encryption of Sensitive Data (CWE-311) (Скрин и proof-of-concept 6)   
   - Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N) |  
   - Уровень опасности уязвимости: Низкий (базовая оценка CVSS 3.0 составляет 3,7)  
   Решение:**

Настройте свой веб-сервер или сервер приложений для использования SSL (HTTPS).

1. **Protection Mechanism Failure (CWE-693) (proof-of-concept Скрин 8 Скрин 18, Скрин 20 )****- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N)**

**- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 5,8)  
Решение:**

Убедитесь, что ваш веб-сервер, сервер приложений, балансировщик нагрузки и т. д. настроены для установки заголовка Content-Security-Policy для достижения оптимальной поддержки браузера: «Content-Security-Policy»

1. **Improper Restriction of Rendered UI Layers or Frames (CWE-1021) (Скрин и proof-of-concept 9)   
   - Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)**

**- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 4,3)  
Решение:**

Современные веб-браузеры поддерживают Content-Security-Policy и заголовки HTTP X-Frame-Options. Убедитесь, что один из них установлен на всех веб-страницах, возвращаемых вашим сайтом/приложением.

1. **Cross-Site Request Forgery (CSRF) (CWE-352) (Скрин 10, Скрин 11)****- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)   
   - Уровень опасности уязвимости: Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,8)  
   Решение:**

* Создайте уникальный одноразовый номер для каждой формы, поместите одноразовый номер в форму и проверьте одноразовый номер после получения формы.
* Убедитесь, что одноразовый номер непредсказуем

1. **Exposure of Information Through Directory Listing (CWE-548) (Скрин 12) (proof-of-concept скрины 118)   
   - Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)**

**- Уровень опасности уязвимости: Высокий (базовая оценка CVSS 3.0 составляет 7,5)  
Решение:**

Отключить просмотр каталогов. Если это необходимо, убедитесь, что перечисленные файлы не представляют опасности.

1. **Improper Input Validation (CWE-20) (Скрин 13, Скрин 27) (proof-of-concept скрины 114 и 115)   
   - Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)**

**- Уровень опасности уязвимости: Критический (базовая оценка CVSS 3.0 составляет 9,8)  
Решение:**

Используйте заголовок HTTP-ответа Content-Type, чтобы злоумышленнику было сложнее заставить веб-браузер неверно интерпретировать тип содержимого ответа.

1. **Sensitive Cookie Without 'HttpOnly' Flag (CWE-1004) (Скрин и proof-of-concept 15) Критичность: 6.5 (CVSS v3)  
   Решение:**

Убедитесь, что для всех файлов cookie установлен флаг HttpOnly.

1. **Sensitive Cookie with Improper SameSite Attribute (CWE-1275) (Скрин и proof-of-concept 16) - Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)**

**- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 6,1)  
Решение:**

Убедитесь, что для атрибута SameSite установлено значение «слабый» ('lax') или в идеальном случае «строгий» (strict') для всех файлов cookie.

1. **Exposure of Sensitive Information to an Unauthorized Actor (CWE-200) (proof-of-concept Скрин 17, Скрин 19, Скрин 21, Скрин 22, Скрин 23, Скрин 28, Скрин 29)   
   - Базовый вектор уязвимости (CVSS 3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)**

**- Уровень опасности уязвимости: Средний уровень опасности (базовая оценка CVSS 3.0 составляет 5,5)  
Решение:**

Настройте сервер для предотвращения таких утечек информации. Например: В Tomcat это делается с помощью директивы «сервер» и реализации пользовательских страниц ошибок. В Apache это делается с помощью директив ServerSignature и ServerTokens.

При сканировании приложения **87.249.53.182:7799** с помощью **OWASP ZAP** были выявлены уязвимости. По данным уязвимостям была сделана проверка на False Positive срабатывания и проведен пентест:

1. **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CWE-89) (Скрин 98) (proof-of-concept Скрины 121 и 122)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)   
- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 5,6)  
Решение:**

Не доверяйте набору ввода клиента, даже если на месте есть проверка на стороне клиента. Как правило, введите все данные на стороне сервера.

1. **Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78) (Скрин 99**) **(proof-of-concept Скрин 120)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)**

**- Уровень опасности уязвимости: Критический (базовая оценка CVSS 3.0 составляет 9,8)**

**Решение:**

* По возможности используйте вызовы библиотеки, а не внешние процессы, чтобы воссоздать желаемую функциональность.
* Запустите свой код в «тюрьме» или подобной среде песочницы, которая устанавливает строгие границы между процессом и операционной системой. Это может эффективно ограничить, к каким файлам можно получить доступ в конкретном каталоге или какие команды могут выполняться вашим программным обеспечением.

1. **Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79) (Скрин 100)** **(proof-of-concept Скрины 123 и 124)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)   
- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 6,1)**

**Решение:**

Используйте стратегию проверки входных данных «принять заведомо исправные», т. е. Используйте разрешенный список допустимых входных данных, которые строго соответствуют спецификациям.

1. **Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22) (Скрин 101)** **(proof-of-concept Скрин 125)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)**

**- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 6,5)  
Решение:**

Предположим, что весь ввод злонамерен. Используйте стратегию проверки входных данных «принять заведомо исправные», т. е. Используйте разрешенный список допустимых входных данных, которые строго соответствуют спецификациям. Отклоняйте любой ввод, который не строго соответствует спецификациям, или преобразуйте его во что-то, что соответствует.

1. **Protection Mechanism Failure (CWE-693) (Скрин и proof-of-concept 102, 109, 110)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N)**

**- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 5,8)  
Решение:**

Убедитесь, что ваш веб-сервер, сервер приложений, балансировщик нагрузки и т. д. настроены для установки заголовка Content-Security-Policy для достижения оптимальной поддержки браузера: «Content-Security-Policy»

1. **Improper Restriction of Rendered UI Layers or Frames (CWE-1021) (Скрин 103 и proof-of-concept)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)**

**- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 4,3)  
Решение:**

Современные веб-браузеры поддерживают Content-Security-Policy и заголовки HTTP X-Frame-Options.Убедитесь, что один из них установлен на всех веб-страницах, возвращаемых вашим сайтом/приложением.

1. **Cross-Site Request Forgery (CSRF) (CWE-352) (Скрин 104, Скрин 105)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)   
- Уровень опасности уязвимости: Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,8)**

**Решение:**

* Создайте уникальный одноразовый номер для каждой формы, поместите одноразовый номер в форму и проверьте одноразовый номер после получения формы.
* Убедитесь, что одноразовый номер непредсказуем

1. **Inclusion of Functionality from Untrusted Control Sphere (CWE-829) (Скрин и proof-of-concept 106)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)**

**- Уровень опасности уязвимости: Средний (базовая оценка CVSS 3.0 составляет 6,5)  
Решение:**

Обновите до последней версии jquery.

1. **Exposed Dangerous Method or Function (CWE-749) (Скрин и proof-of-concept 108)**

**- Базовый вектор уязвимости: (CVSS 3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)**

**- Уровень опасности уязвимости: Высокий (базовая оценка CVSS 3.0 составляет 8,8)  
Решение:**

Заменить используемый метод, либо предусмотреть права его вызова.

1. **Exposure of Sensitive Information to an Unauthorized Actor (CWE-200) (Скрин и proof-of-concept 111, 112)**

**- Базовый вектор уязвимости (CVSS 3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)**

**- Уровень опасности уязвимости: Средний уровень опасности (базовая оценка CVSS 3.0 составляет 5,5)  
Решение:**

* Убедитесь, что ваш веб-сервер, сервер приложений, балансировщик нагрузки и т. д. настроены на подавление заголовка «Сервер» или предоставление общих сведений.
* Просмотрите исходный код этой страницы.
* Реализуйте настраиваемые страницы ошибок.