Состояние	Завершены
Тест начат	суббота, 6 декабря 2025, 18:35
Завершен	суббота, 6 декабря 2025, 18:47
Затраченное время	12 мин. 3 сек.
Баллы	46,00/46,00
Оценка	**10,00** из 10,00 (**100**%)

Вопрос 1

Верно

Баллов: 1,00 из 1,00

Что из перечисленного НЕ является особенностью Blind SSRF?

a. a) Нет прямого ответа от сервера
b. d) Используется DNS OAST или анализ времени ответа
c. c) Легко обнаруживается стандартными сканерами ✓
d. b) Требует использования Out-of-Band методов для подтверждения

Вопрос 2

Верно

Баллов: 1,00 из 1,00

Какой из вариантов соответствует примеру SSRF-атаки через Redis с использованием gopher://?

a. b) GET /index.html
b. a) SET mykey myvalue ✓
c. d) DELETE /cache
d. c) POST /containers/json

Вопрос 3

Верно

Баллов: 1,00 из 1,00

В чем заключается опасность SSRF-атаки на облачные метаданные?

a. a) Получение временных учетных данных и ролей облака ✓
b. b) Нарушение целостности базы данных
c. c) Превышение квот по трафику
d. d) Взлом браузера пользователя

Вопрос 4

Верно

Баллов: 1,00 из 1,00

Какая из следующих функций чаще всего становится точкой внедрения SSRF?

a. c) Интеграция с внешними API
b. b) Загрузка изображений
c. d) Все перечисленные ✓
d. a) Модуль предпросмотра ссылок

Вопрос 5

Верно

Баллов: 1,00 из 1,00

SSRF часто используется в связке с другими уязвимостями. Какую уязвимость чаще всего используют для превращения Blind SSRF в видимую (чтобы получить результат запроса)?

a. d) RCE (удаленное выполнение кода)
b. a) XSS (межсайтовый скриптинг)
c. c) Open Redirect (открытое перенаправление) ✓
d. b) XXE (XML External Entity)

Вопрос 6

Верно

Баллов: 1,00 из 1,00

Перед вами уязвимый параметр: ?url=https://api.trusted.com/data. Разрешены только домены *.trusted.com. Как можно попытаться достичь http://169.254.169.254?

a. d) Это невозможно обойти при корректно реализованном whitelist.
b. c) Использовать схему file://169.254.169.254
c. a) Найти Open Redirect на api.trusted.com, например: ?url ✓
d. b) Использовать URL: ?url
e. http://169.254.169.254
f. http://169.254.169.254.trusted.com
g. https://api.trusted.com/redirect?to

Вопрос 7

Верно

Баллов: 1,00 из 1,00

Чем Blind SSRF отличается от обычного SSRF?

- a. a) В Blind SSRF атакующий не получает ответ от сервера, но может косвенно понять, был ли выполнен запрос. ✓
- b. c) Blind SSRF менее опасен, чем обычный.
- c. b) В Blind SSRF сервер возвращает полный ответ.
- d. d) Для Blind SSRF нужен открытый редирект.

Вопрос 8

Верно

Баллов: 1,00 из 1,00

Какой из вариантов не является стандартной URL-схемой, но может использоваться в SSRF?

- a. a) gopher:// ✓
- b. c) ftp://
- c. b) https://
- d. d) ws://

Вопрос 9

Верно

Баллов: 1,00 из 1,00

Как можно использовать open redirect для обхода whitelist доменов?

- a. c) Использовать нестандартный протокол
- b. a) Перенаправить с доверенного домена на внутренний IP ✓
- c. d) Взломать прокси-сервер
- d. b) Зашифровать URL в параметрах

Вопрос 10

Верно

Баллов: 1,00 из 1,00

В чем ключевая опасность SSRF в облачных средах (AWS, Azure)?

- a. c) Доступ к сервисам метаданных (Metadata API), ведущий к компрометации учетных данных и ролей. ✓
- b. b) Кража сессионных куков пользователей.
- c. a) Возможность DDoS-атак на внешние сервисы.
- d. d) Дефейс главной страницы приложения.

Вопрос 11

Верно

Баллов: 1,00 из 1,00

Как SSRF-атака может использоваться для атаки на Redis?

- a. a) Отправлять команды через gopher:// протокол ✓
- b. b) Загружать вредоносные скрипты
- c. c) Использовать SQL-инъекции
- d. d) Подделывать cookies пользователей

Вопрос 12

Верно

Баллов: 1,00 из 1,00

SSRF редко используется изолированно. Какова ее наиболее типичная роль в многоэтапной атаке?

- a. b) Трамплин (pivot) для доступа к изолированной внутренней сети и взаимодействия с непредназначенными для внешнего доступа сервисами. ✓
- b. a) Финальная цель — кража денег.
- c. d) Инструмент для DDoS-атак.
- d. c) Средство для дефейса сайта.

Вопрос 13

Верно

Баллов: 1,00 из 1,00

Приложение имеет защиту от SSRF: blacklist внутренних IP-адресов и схема file:// заблокированы. Какая комбинация техник может помочь обойти эту защиту?

- a. d) Все вышеперечисленное. ✓
- b. b) Использовать альтернативное представление IP-адреса (например, шестнадцатеричное).
- c. a) Использовать доменное имя, которое резолвится во внутренний IP (DNS Rebinding).
- d. c) Использовать открытое перенаправление на доверенном домене.

Вопрос 14

Верно

Баллов: 1,00 из 1,00

Что такое «OAST» в контексте Blind SSRF?

- a. b) Протокол шифрования запросов.
- b. a) Способ обнаружения SSRF без прямого ответа. ✓
- c. d) Инструмент мониторинга трафика.
- d. c) Метод обхода фильтров URL.

Вопрос 15

Верно

Баллов: 1,00 из 1,00

Какая из техник помогает обнаружить SSRF-атаку?

a. a) Мониторинг DNS-запросов на неизвестные домены ✓
b. d) Увеличение размера сессии пользователя
c. c) Анализ cookie-файлов
d. b) Проверка валидности email-адресов

Вопрос 16

Верно

Баллов: 1,00 из 1,00

Какой порт обычно прослушивает Docker API, доступный локально?

a. d) 3306
b. c) 80
c. b) 9200
d. a) 2375 ✓

Вопрос 17

Верно

Баллов: 1,00 из 1,00

Что из следующего является признаком успешной SSRF-атаки?

a. a) Исходящий запрос к внутреннему IP, зафиксированный в логах ✓
b. d) Повышение нагрузки на базу данных
c. b) Отсутствие ошибок 404 в логах
d. c) Превышение времени ответа сервера

Вопрос 18

Верно

Баллов: 1,00 из 1,00

Какой инструмент часто используется для автоматического поиска и эксплуатации SSRF?

a. d) Metasploit
b. c) Nmap
c. a) SSRFmap ✓
d. b) Wireshark

Вопрос 19

Верно

Баллов: 1,00 из 1,00

Что из перечисленного — пример точки внедрения SSRF в веб-приложении?

a. c) Страница контактов с формой обратной связи
b. b) Модуль аутентификации по паролю
c. d) Система логирования
d. a) Функция предпросмотра ссылок ✓

Вопрос 20

Верно

Баллов: 1,00 из 1,00

Какой IP-адрес используется для доступа к AWS Metadata API через SSRF?

a. b) 192.168.0.1
b. c) 169.254.169.254 ✓
c. d) 10.0.0.1
d. a) 127.0.0.1

Вопрос 21

Верно

Баллов: 1,00 из 1,00

Какие из URL-схем могут быть опасными в SSRF?

a. d) Все перечисленные ✓
b. c) gopher://
c. b) file://
d. a) http://

Вопрос 22

Верно

Баллов: 1,00 из 1,00

Какая схема URL часто используется для чтения локальных файлов в SSRF?

a. a) http://
b. c) file:// ✓
c. d) mailto://
d. b) ftp://

Вопрос 23

Верно

Баллов: 1,00 из 1,00

Вы обнаружили, что приложение принимает URL для предпросмотра и проверяет, что домен находится в whitelist (например, *.example.com). На одном из разрешенных поддоменов есть открытое перенаправление. Как можно использовать это для атаки на внутренний сервис http://192.168.1.1?

a. http://192.168.1.1 — домен evil.com не в whitelist.
b. c) Использовать URL: https://trusted.example.com/redirect?url ✓
c. b) Использовать URL: http://evil.com?redirect
d. d) Использовать схему file:// для чтения локальных файлов.
e. a) Использовать URL: http://192.168.1.1 — он не в whitelist, поэтому не сработает.
f. http://192.168.1.1 — сначала проходит whitelist, затем перенаправляет на внутренний адрес.

Вопрос 24

Верно

Баллов: 1,00 из 1,00

Как DNS Rebinding помогает обходить whitelist при SSRF?

a. b) Перенаправляет трафик через прокси.
b. a) Меняет IP внутри TTL, резолвя домен сначала в внешний IP, затем во внутренний. ✓
c. d) Блокирует домены вне whitelist.
d. c) Кодирует IP в DNS-запросах.

Вопрос 25

Верно

Баллов: 1,00 из 1,00

Какая из следующих техник НЕ относится к методам обхода фильтров SSRF?

a. a) URL-кодирование
b. b) Использование альтернативных IP-представлений
c. c) Легитимный прокси
d. d) Использование Content-Security-Policy (CSP) ✓

Вопрос 26

Верно

Баллов: 1,00 из 1,00

Принцип "Zero Trust" (Нулевое доверие) в контексте защиты от SSRF предполагает:

a. d) Шифрование всего трафика с помощью TLS, даже внутри одного хоста.
b. c) Обязательное использование только whitelist доменов.
c. b) Что даже запросам из внутренней сети к внутренним же сервисам (например, к metadata API, Kubernetes API) требуется аутентификация и авторизация. ✓
d. a) Полное запрещение любых исходящих HTTP-запросов.

Вопрос 27

Верно

Баллов: 1,00 из 1,00

Что из перечисленного является примером безопасной архитектурной практики против SSRF в Kubernetes?

a. d) Отключение HTTP в кластере
b. a) Использование whitelist для pod'ов
c. c) Размещение всех подов в одной сети
d. b) Ограничение IAM ролей по принципу наименьших привилегий ✓

Вопрос 28

Верно

Баллов: 1,00 из 1,00

Какие шаги включают построение SSRF-атаки?

a. b) Установка вируса, получение root-доступа, отправка спама
b. a) Поиск уязвимых точек, обход фильтров, подтверждение успешности, эксплуатация ✓
c. c) Фишинг, получение cookies, XSS
d. d) Шифрование трафика, оптимизация запросов, повышение пропускной способности

Вопрос 29

Верно

Баллов: 1,00 из 1,00

Какой из методов позволяет передать данные из внутренней сети атакующему при Blind SSRF?

a. d) Изменение Referer
b. SECRET)
c. b) Запрос к контролируемому атакующим домену с данными в URL (например, http://attacker.com/?data ✓
d. a) Передача через User-Agent
e. c) Установка куки

Вопрос 30

Верно

Баллов: 1,00 из 1,00

Какое архитектурное решение наиболее эффективно блокирует SSRF-атаки на облачные metadata-сервисы в AWS?

a. c) Включение IMDSv2 (Instance Metadata Service v2) с обязательным PUT-токеном и Hop-Limit ✓
b. a) Whitelist доменов 169.254.169.254 в WAF.
c. 1.
d. d) Использование только IAM пользователей вместо ролей.
e. b) Запретить весь исходящий трафик через Security Group.

Вопрос 31

Верно

Баллов: 1,00 из 1,00

Почему blacklist IP-адресов считается ненадежной защитой от SSRF?

a. c) DNS Rebinding позволяет обходить списки
b. a) Множество форматов IP-адресов позволяют обходить фильтры
c. b) Постоянно появляются новые внутренние сети
d. d) Все вышеперечисленное ✓

Вопрос 32

Верно

Баллов: 1,00 из 1,00

Какова основная задача egress-фильтрации для защиты от SSRF?

a. d) Ускорить сетевой трафик
b. c) Запретить входящие соединения
c. b) Ограничить исходящие соединения к надежным адресам ✓
d. a) Разрешить все исходящие соединения

Вопрос 33

Верно

Баллов: 1,00 из 1,00

Какой заголовок может привести к SSRF, если сервер использует его для построения целевого URL?

a. b) User-Agent
b. c) Accept-Language
c. d) Cookie
d. a) X-Forwarded-For ✓

Вопрос 34

Верно

Баллов: 1,00 из 1,00

Как может использоваться gopher:// в SSRF-атаке?

a. a) Для отправки произвольных TCP-запросов (например, к Redis или Docker) ✓
b. b) Для загрузки файлов с локального диска
c. d) Для атаки на браузер пользователя
d. c) Для получения HTTP-ответов с сервера

Вопрос 35

Верно

Баллов: 1,00 из 1,00

Что такое pivoting в контексте SSRF?

a. a) Перемещение из скомпрометированного сервера в другую внутреннюю систему через SSRF. ✓
b. b) Атака на браузер пользователя.
c. d) Обход WAF.
d. c) Использование XSS для SSRF.

Вопрос 36

Верно

Баллов: 1,00 из 1,00

Что из следующего НЕ является признаком SSRF в логах?

a. c) Запросы только к внешним адресам, не связанным с приложением ✓
b. a) Исходящие запросы к внутренним IP из внешнего приложения
c. d) Многочисленные запросы с одного и того же IP на нестандартные порты
d. b) Неожиданные DNS-запросы к неизвестным доменам

Вопрос 37

Верно

Баллов: 1,00 из 1,00

Как можно использовать SSRF для атаки на Docker?

a. d) Выполнять SQL-запросы к базе данных Docker
b. a) Отправлять команды через Docker API, слушающий на 2375 порту ✓
c. c) Использовать XSS уязвимости в Docker UI
d. b) Загружать вредоносные контейнеры из интернета

Вопрос 38

Верно

Баллов: 1,00 из 1,00

Как CRLF-инъекция может усилить SSRF-атаку?

a. c) Позволяет выполнить JavaScript в браузере.
b. a) Позволяет внедрять произвольные HTTP-заголовки в запрос, отправляемый сервером, что может обойти проверки на внутренних сервисах. ✓
c. b) Позволяет разбить ответ сервера на несколько частей.
d. d) CRLF-инъекция не связана с SSRF.

Вопрос 39

Верно

Баллов: 1,00 из 1,00

Какую из техник часто используют для подтверждения Blind SSRF?

a. c) Перехват сессии пользователя
b. d) Использование cookie
c. a) DNS OAST (out-of-band) ✓
d. b) Анализ содержимого HTTP-ответа

Вопрос 40

Верно

Баллов: 1,00 из 1,00

В каком формате можно представить IP-адрес для обхода фильтра, запрещающего 127.0.0.1?

a. c) 0177.0.0.1 (восьмеричный)
b. d) Все перечисленные ✓
c. a) 2130706433 (десятичный)
d. b) 0x7f000001 (шестнадцатеричный)

Вопрос 41

Верно

Баллов: 1,00 из 1,00

Какой подход является лучшим для защиты от SSRF?

a. c) Регулярное обновление серверного ПО
b. a) Сегментация сети и строгие egress-правила ✓
c. b) Использование только HTTPS
d. d) Запрет JavaScript в браузере пользователя

Вопрос 42

Верно

Баллов: 1,00 из 1,00

Что такое SSRF?

a. c) Межсайтовая подделка запроса (CSRF).
b. b) Подмена содержимого запроса клиента.
c. a) Атака, заставляющая сервер выполнять несанкционированные запросы к внутренним или внешним ресурсам. ✓
d. d) Механизм авторизации API.

Вопрос 43

Верно

Баллов: 1,00 из 1,00

Почему использование библиотек для HTTP-запросов без правильной нормализации URL увеличивает риск SSRF?

a. d) Используют только whitelisting
b. b) Неправильная нормализация может позволить обход фильтров, например, через URL-энкодинг или альтернативные представления IP ✓
c. c) Они уменьшают скорость обработки запросов
d. a) Библиотеки автоматически защищают от SSRF

Вопрос 44

Верно

Баллов: 1,00 из 1,00

Какие из следующих действий помогут снизить риск SSRF?

a. %33.33%b) Ограничение исходящих запросов с сервера
b. %33.33%d) Использование принципа наименьших привилегий для сервисов
c. c) Использование Content Security Policy (CSP)
d. %33.33%a) Валидация и нормализация входящих URL ✓

Вопрос 45

Верно

Баллов: 1,00 из 1,00

Какое поведение HTTP-библиотеки может привести к SSRF даже при валидации URL по whitelist доменов?

a. a) Автоматическое разрешение относительных путей (/etc/passwd).
b. c) Кэширование DNS-запросов на 24 часа.
c. b) Автоматическое следование редиректам (follow redirects) без повторной проверки целевого URL. ✓
d. d) Поддержка HTTP/2.

Вопрос 46

Верно

Баллов: 1,00 из 1,00

Предположим, уязвимое приложение использует белый список (whitelist) доменов и разрешает только домены, оканчивающиеся на .trusted.com. Какой из следующих подходов НЕ поможет обойти эту защиту?

a. c) Использование DNS Rebinding на домене rb.evil.com, который сначала резолвится в IP доверенного сервера, а затем во внутренний IP.
b. b) Регистрация домена eviltrusted.com (без точки) и использование его для атаки. ✓
c. d) Нахождение уязвимости поддомена, который разрешен (например, api.trusted.com), и использование его для проксирования запроса.
d. a) Использование открытого редиректа на поддомене legit.trusted.com, который перенаправляет на внутренний IP.

Служба поддержки сайта

Вы зашли под именем Новиков Виталий Сергеевич (Выход)