



















# Отчет по скану в режиме PenTest (белый ящик)

## Легенда

-  нет уязвимостей
-  доступна информация
-  низкий уровень
-  средний уровень (подозрение)
-  средний уровень
-  высокий уровень (подозрение)
-  высокий уровень
-  критический уровень (подозрение)
-  критический уровень
-  заблокированный сервис
-  недоступный сервис
-  неидентифицированный сервис
-  необработанный сервис
-  узел не проверялся
-  узел проверен не полностью (снят с ошибкой)
-  узел проверен не полностью (прервано пользователем)
-  ограничение лицензии
-  ограничение прав

Описание вектора CVSS, версия 2

<b>A:C</b>	при успешной эксплуатации злоумышленник может сделать систему полностью недоступной
<b>A:N</b>	эксплуатация уязвимости не влияет на доступность системы
<b>A:P</b>	эксплуатация уязвимости ведет к сбоям в доступности системы или к уменьшению производительности
<b>AC:H</b>	для эксплуатации уязвимости нужны особые условия, или уязвимая конфигурация редко встречается на практике
<b>AC:L</b>	для эксплуатации уязвимости не требуются особые условия
<b>AC:M</b>	для эксплуатации уязвимости нужна дополнительная информация или нестандартная конфигурация уязвимого ПО
<b>Au:M</b>	для эксплуатации уязвимости злоумышленник должен несколько (два и более) раз пройти аутентификацию
<b>Au:N</b>	для эксплуатации уязвимости проходить аутентификацию не требуется
<b>Au:NR</b>	для эксплуатации уязвимости проходить аутентификацию не требуется
<b>Au:S</b>	для эксплуатации уязвимости злоумышленник должен пройти аутентификацию в системе
<b>AV:A</b>	для успешной эксплуатации уязвимости злоумышленник должен иметь доступ к соседней сети
<b>AV:L</b>	для успешной эксплуатации уязвимости злоумышленник должен иметь физический доступ к системе или локальную учетную запись
<b>AV:N</b>	данная уязвимость может эксплуатироваться удаленно
<b>AV:R</b>	данная уязвимость может эксплуатироваться удаленно
<b>B:N</b>	веса угроз одинаковы
<b>C:C</b>	эксплуатация уязвимости влечет полное разглашение конфиденциальных данных
<b>C:N</b>	эксплуатация уязвимости не затрагивает конфиденциальные данные системы
<b>C:P</b>	эксплуатация уязвимости влечет существенное разглашение конфиденциальных данных
<b>E:F</b>	для данной уязвимости доступен эксплойт, который может быть применен в большинстве ситуаций
<b>E:H</b>	данную уязвимость можно эксплуатировать с помощью легко переносимого, автономного кода, или эксплойт не нужен
<b>E:ND</b>	данная метрика не влияет на оценку
<b>E:P</b>	доступен "Proof of Concept" код (эксплойт, описывающий концепцию эксплуатации), или существует стратегия атаки, которая неприменима в большинстве систем.
<b>E:POC</b>	доступен "Proof of Concept" код (эксплойт, описывающий концепцию эксплуатации), или существует стратегия атаки, которая неприменима в большинстве систем. Для использования этого эксплойта требуется внести в него значительные изменения, чтобы требует соответствующих навыков от злоумышленника.
<b>E:U</b>	эксплуатация уязвимости возможна теоретически
<b>I:C</b>	эксплуатация уязвимости влечет полное нарушение целостности системы
<b>I:N</b>	эксплуатация уязвимости не затрагивает целостность системы
<b>I:P</b>	эксплуатация уязвимости ведет к частичному нарушению целостности системы
<b>RC:C</b>	данная уязвимость подтверждена производителем или автором технологии эксплуатации уязвимости
<b>RC:ND</b>	данная метрика не влияет на оценку
<b>RC:UC</b>	достоверность наличия данной уязвимости не подтверждена
<b>RC:UR</b>	сообщения о данной уязвимости предоставлены несколькими неофициальными источниками
<b>RL:ND</b>	данная метрика не влияет на оценку
<b>RL:O</b>	доступно официальное обновление или исправление от производителя
<b>RL:OF</b>	для данной уязвимости доступно официальное обновление или исправление от производителя
<b>RL:T</b>	для данной уязвимости доступно официальное временное обновление
<b>RL:TF</b>	для данной уязвимости доступно официальное временное обновление
<b>RL:U</b>	для данной уязвимости обновление или исправление недоступно или не может быть применено
<b>RL:W</b>	для данной уязвимости доступно неофициальное решение, которое предоставлено третьей стороной

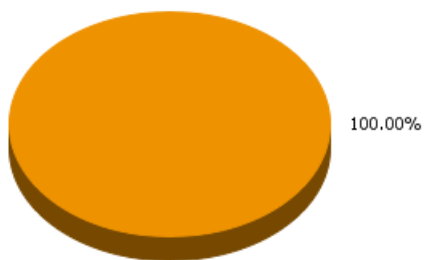
Описание вектора CVSS, версия 3

<b>A:H</b>	Полная потеря доступности. Злоумышленник способен вызвать полный отказ в доступе к ресурсам атакуемого компонента; этот отказ является либо устойчивым (длится, пока злоумышленник продолжает атаку), либо постоянным (сохраняется даже после завершения атаки).
------------	--

<b>A:L</b>	Происходит снижение производительности или перебои в доступности ресурса. Хотя возможна многократная эксплуатация уязвимости, злоумышленник не способен вызвать полный отказ в обслуживании законных пользователей.
<b>A:N</b>	Воздействие на доступность атакуемого компонента отсутствует.
<b>AC:H</b>	Успех атаки зависит от условий, находящихся вне контроля злоумышленника.
<b>AC:L</b>	Не существует специальных условий доступа и особых обстоятельств. Злоумышленник может рассчитывать на успешное повторение атаки в отношении уязвимого компонента.
<b>AV:A</b>	Уязвимый компонент также привязан к сетевому стеку, но атака ограничена той же совместно используемой физической (например, Bluetooth, IEEE 802.11) или логической (например, локальной IP-подсетью) сетью и не может быть произведена через границы уровня 3 модели OSI (например, маршрутизатор).
<b>AV:L</b>	Уязвимый компонент не привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через возможности чтения/записи/выполнения.
<b>AV:N</b>	Уязвимый компонент привязан к сетевому стеку, а маршрут проникновения злоумышленника пролегает через уровень 3 (сетевой уровень) модели взаимосвязи открытых систем (OSI).
<b>AV:P</b>	Уязвимость может эксплуатироваться при физическом доступе, и злоумышленнику для достижения своей цели необходимо физическое взаимодействие с уязвимым компонентом.
<b>C:H</b>	Полная потеря конфиденциальности, приводящая к тому, что все ресурсы атакуемого компонента становятся доступными злоумышленнику.
<b>C:L</b>	Возможен доступ к некоторой информации для ограниченного пользования, но злоумышленник не имеет контроля над тем, какую именно информацию он получит, или масштабы потерь невелики либо их последствия не носят массового характера.
<b>C:N</b>	Потеря конфиденциальности в атакуемом компоненте нет.
<b>E:F</b>	Доступен функциональный код эксплойта, применимый в большинстве ситуаций, где существует уязвимость.
<b>E:H</b>	Существующий функциональный автономный код или эксплойт не требуется (запуск производится вручную), и детали широко известны. Код эксплойта работает в любой ситуации или его активная доставка осуществляется автономным агентом (например, червем или вирусом).
<b>E:P</b>	Доступен код эксплойта, доказывающий правильность концепции, или существует демонстрация атаки, неприменимая в большинстве систем.
<b>E:U</b>	Код эксплойта не доступен или эксплуатация возможна лишь теоретически.
<b>E:X</b>	Присвоение этого значения показателю не влияет на оценку.
<b>I:H</b>	Полная потеря целостности или защиты.
<b>I:L</b>	Возможно изменение данных, но злоумышленник не имеет контроля над последствиями изменения или масштабы изменения ограничены.
<b>I:N</b>	Потеря целостности в атакуемом компоненте нет.
<b>PR:H</b>	Злоумышленник должен быть авторизован и располагать привилегиями, предоставляющими значительный (например, административный) контроль над уязвимым компонентом, который может затрагивать настройки и файлы в масштабе всего компонента.
<b>PR:L</b>	Злоумышленник должен быть авторизован и располагать ограниченными привилегиями, предоставляющими базовые пользовательские возможности, которые в нормальном случае распространяются только на настройки и файлы самого пользователя.
<b>PR:N</b>	Злоумышленник может не иметь авторизации перед атакой и, соответственно, не нуждается в доступе к каким-либо настройкам или файлам для ее осуществления.
<b>RC:C</b>	Имеются подробные сообщения или уязвимость функционально воспроизводима (например, существуют функциональные эксплойты).
<b>RC:R</b>	Опубликованы существенные подробности, но исследователи либо не уверены до конца в первопричине, либо не имеют доступа к исходному коду, чтобы окончательно подтвердить все взаимодействия, которые могут привести к рассматриваемому результату.
<b>RC:U</b>	Имеются сообщения о фактах воздействия на системы, указывающие на существование уязвимости.
<b>RC:X</b>	Присвоение этого значения показателю не влияет на оценку.
<b>RL:O</b>	Доступно полноценное решение от разработчика, который либо выпустил официальное исправление, либо предоставил обновление.
<b>RL:T</b>	Доступно официальное временное исправление. Например, разработчик выпустил оперативное исправление или временное программное средство либо опубликовал обходной прием.
<b>RL:U</b>	Решение либо недоступно, либо его невозможно применить.
<b>RL:W</b>	Доступно неофициальное решение, которое предоставлено третьей стороной.
<b>RL:X</b>	Присвоение этого значения показателю не влияет на оценку.
<b>S:C</b>	Эксплуатируемая уязвимость может воздействовать на ресурсы за рамками привилегий, предусмотренных уязвимым компонентом. В этом случае уязвимый и атакуемый компоненты различаются.
<b>S:U</b>	Эксплуатируемая уязвимость может воздействовать только на ресурсы под контролем того же субъекта авторизации. В этом случае уязвимый и атакуемый компоненты совпадают.
<b>UI:N</b>	Существует возможность эксплуатации уязвимой системы без взаимодействия с каким-либо пользователем.
<b>UI:R</b>	Для успешной эксплуатации этой уязвимости требуются те или иные действия со стороны пользователя.

Параметры отчета	
Тип отчета	Информация
Тип данных	Уязвимость PenTest
Исходные данные	По скану
Состав описания уязвимостей	Все
Количество строк в рейтинге:	10
Достоверность результатов	Любая (все результаты)
Включить уязвимости, помеченные как ложное срабатывание	Нет
Ограничение количества строк, отображаемых в результатах	50
Разбивать отчет на части	Не разбивать отчет
Содержание отчета	Легенда; Проверенные узлы; Уязвимые службы/ПО; Все службы/ПО; Уязвимость узлов; Состояние транспортных

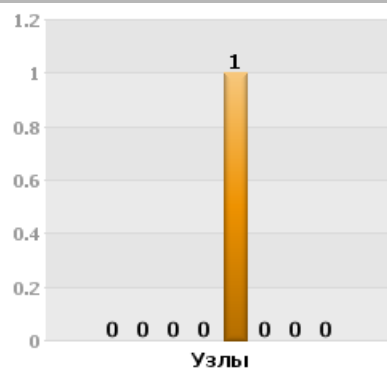
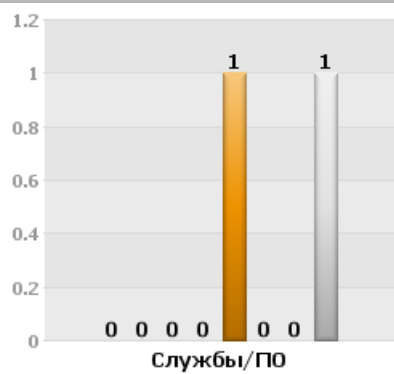
Данные, включенные в отчет		
задача	узлов	сканов
Задача_Pentest_web_scan_полное сканирование (белый ящик)	1	1
Итого:	1	1



Уровень	Количество уязвимостей	Доля уязвимостей
Критический уровень	0	0.00%
Критический уровень (подозрение)	0	0.00%
Высокий уровень	0	0.00%
Высокий уровень (подозрение)	0	0.00%
Средний уровень	1	100.00%
Средний уровень (подозрение)	0	0.00%
Низкий уровень	0	0.00%
Итого:	1	100%



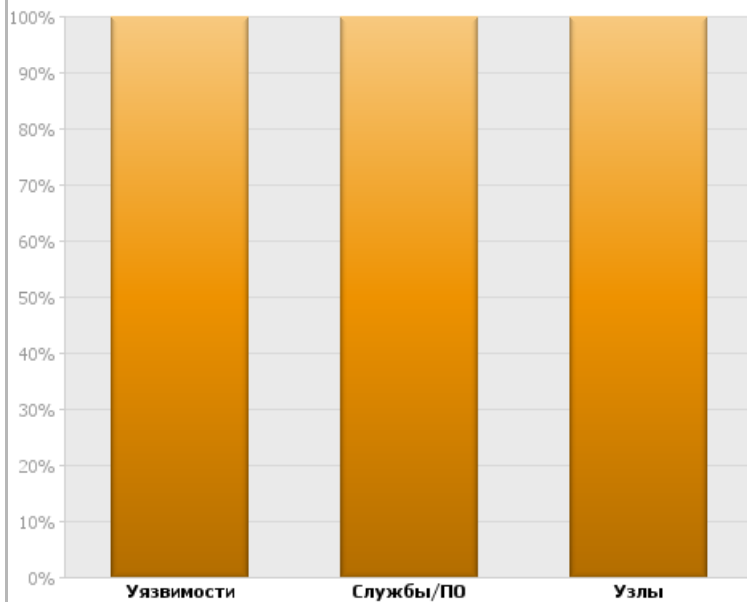
## Уязвимость объектов



Уровень	Службы / ПО	Узлы
Критический уровень	0	0
Критический уровень (подозрение)	0	0
Высокий уровень	0	0
Высокий уровень (подозрение)	0	0
Средний уровень	1	1
Средний уровень (подозрение)	0	0
Низкий уровень	0	0
нет уязвимостей	1	0
Итого:	2	1



## Распределение уровней опасности



Уровень	Уязвимости	Службы/ПО *	Узлы *
Критический уровень	0	0	0
Критический уровень (подозрение)	0	0	0
Высокий уровень	0	0	0
Высокий уровень (подозрение)	0	0	0
Средний уровень	1	1	1
Средний уровень (подозрение)	0	0	0
Низкий уровень	0	0	0
Итого:	1	1	1

\* Отображается количество служб/ПО, узлов, в которых данный уровень уязвимости максимальный.



## Проверенные узлы



узел	начало	конец	время	интегральная уязвимость
10.1.1.3	30.07.2025 16:35:38	30.07.2025 16:48:18	00:12:40	<div><div></div></div> 3

**Интегральная уязвимость** определяется по формуле:  $N7 * 7 + N5 * 5 + N3 * 3 + N6 + N4 + N2 + N1$ , где:

**N7** - количество уязвимостей критического уровня

**N6** - количество подозрений на уязвимость критического уровня

**N5** - количество уязвимостей высокого уровня

**N4** - количество подозрений на уязвимость высокого уровня

**N3** - количество уязвимостей среднего уровня



**N2** - количество подозрений на уязвимость среднего уровня

**N1** - количество уязвимостей низкого уровня



## Рейтинг уязвимых узлов





узел	начало	конец	время	задача	интегральная уязвимость
 10.1.1.3	30.07.2025 16:35:38	30.07.2025 16:48:18	00:12:40	Задача_Pentest_web_s cap_полное сканирование (белый ящик)	 3





## Рейтинг уязвимых служб/ПО



задача	Имя	узел	интегральная уязвимость
 Задача_Pentest_web_scan_полное сканирование (белый ящик)	443/TCP - HTTP SSL	10.1.1.3	 3

<div>  <span>Рейтинг уязвимостей</span>  </div>		
Уязвимость	CVE	Количество
 Некорректный сертификат		 1

Перечень уязвимых служб/ПО

IP-адрес

10.1.1.3

Имя из задачи

10.1.1.3

Служб и ПО:

1

443/TCP - HTTP SSL

Имя сервера:

nginx - Bitrix Site Manager

Состояние:

302 (Found)

Имя сервера (определено эвристикой):

Nginx HTTP Server

Информация об имени приложения подтверждена эвристическим методом



Перечень неуязвимых служб/ПО





IP-адрес

10.1.1.3

Имя из задачи

10.1.1.3

Служб и ПО:

1



80/TCP - HTTP

Имя сервера:

nginx



Состояние:

301 (Moved Permanently)

Имя сервера (определено эвристикой):

Nginx HTTP Server

Информация об имени приложения подтверждена эвристическим методом

	<b>Перечень неопределенных служб</b>	
Нет данных		

Перечень уязвимостей узлов

IP-адрес

10.1.1.3

Имя из задачи

10.1.1.3

Уязвимых  
служб/ПО :

1

Завершение сканирования:

30.07.2025 16:48:18

Задача:

Задача\_Pentest\_web\_scan\_полное сканирование (белый ящик)

Версия сканера:

40948

Имя сканера:

Default Scanner on SECURITY-NPIART

Время сканирования:

00:12:42

Начало сканирования:

30.07.2025 16:35:36

Достоверность сканирования:

высокая

Распределение уровней опасности

0

0

0

0

1

9

443/TCP - HTTP SSL

Имя сервера:

nginx - Bitrix Site Manager

Состояние:

302 (Found)

Имя сервера (определено эвристикой):

Nginx HTTP Server

Информация об имени приложения подтверждена эвристическим методом

Уязвимость

Некорректный сертификат

ID: 7029

Описание

Имя и альтернативные имена субъекта сертификата не соответствуют доменному имени узла. Возможно, данный сертификат используется некорректно.

Имя субъекта

www.mile.by

Альтернативные имена субъекта

Тип	Значение
DNS	mile.by
DNS	www.mile.by

Идентификаторы узла

Тип	Значение
IP-адрес	10.1.1.3
Имя из задачи	10.1.1.3

Как исправить

Необходимо установить корректный сертификат для данного сервиса.

CVSS v2

Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Информация

Версии протокола SSL/TLS

ID: 8337

Краткое описание

Определены версии протокола SSL/TLS, поддерживаемые сервером

TLsv1.2

Информация

Информация об HTTP-заголовках

ID: 8375

Краткое описание

Перечисление HTTP-заголовков в ответе сервера, полученного на GET-запрос.

14

## HTTP-заголовки

HTTP-заголовок	Значение
CACHE-CONTROL	NO-STORE, NO-CACHE, MUST-REVALIDATE
CONNECTION	CLOSE
CONTENT-LENGTH	0
CONTENT-TYPE	TEXT/HTML; CHARSET=UTF-8
DATE	WED, 30 JUL 2025 13:42:17 GMT
EXPIRES	THU, 19 NOV 1981 08:52:00 GMT
LOCATION	HTTPS://MILE.BY/
P3P	POLICYREF="/BITRIX/P3P.XML", CP="NON DSP COR CUR ADM DEV PSA PSD OUR UNR BUS UNI COM NAV INT DEM STA"
PRAGMA	NO-CACHE
SERVER	NGINX
SET-COOKIE	PHPSESSID=8R3OYXPJYHNETBFBQ9QQ5K5Y5QNUJZYT; PATH=/; HTTPONLY; SAMESITE=LAX
VARY	HTTPS
X-CONTENT-TYPE-OPTIONS	NOSNIFF
X-FRAME-OPTIONS	SAMEORIGIN
X-POWERED-CMS	BITRIX SITE MANAGER (0DC0F0B1EBFF060F8A69CF39B628A7F7)

## Ссылки

<https://www.ietf.org/rfc/rfc2616.txt>



Информация  
**Наборы шифров SSL**  
ID: 7030

## Описание

в скобках указана длина ключа в битах.

## Шифры высокой стойкости (длина ключа >= 128 бит)

Версия	Название	Обмен ключами	Аутентификация	Шифрование	Целостность
TLSv1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH	RSA	AESGCM(128)	AEAD
TLSv1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH	RSA	AESGCM(256)	AEAD
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	RSA	AESGCM(128)	AEAD
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	RSA	AESGCM(256)	AEAD

## Ссылки

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>



Информация  
**Поддержка возобновления сессий**  
ID: 8353

## Краткое описание

Включена поддержка возобновления сессий на основе идентификатора сессии.

## Описание

При создании нового подключения сервер генерирует идентификатор сессии и отправляет его клиенту. При последующих соединениях клиент будет отправлять этот идентификатор в сообщении ClientHello, сообщая серверу о намерении возобновить предыдущую сессию. Если в локальном кэше сервера имеется данный идентификатор, то этап обмена зашифрованными данными между сервером и клиентом пропускается. Если злоумышленник скомпрометирует сервер и получит хранящиеся на нем сессионные ключи, то он сможет использовать их для расшифровки предыдущих, а также последующих сессий.

## Ссылки

<https://tools.ietf.org/html/rfc5077>

[https://wiki.mozilla.org/Security/Server\\_Side\\_TLS#Session\\_Resumption](https://wiki.mozilla.org/Security/Server_Side_TLS#Session_Resumption)

[https://www.openssl.org/docs/man1.0.1/ssl/SSL\\_set\\_generate\\_session\\_id.html](https://www.openssl.org/docs/man1.0.1/ssl/SSL_set_generate_session_id.html)

<https://hpbm.co/transport-layer-security-tls/#tls-session-resumption>



Информация

## Расширение ALPN для TLS

ID: 8354

### Краткое описание

Удаленный узел раскрыл поддерживаемые протоколы в ALPN расширении в TLS.

### ALPN расширение

Протокол
HTTP/1.1
HTTP/2.0



Информация

## Цепочка сертификатов

ID: 7027

Количество:

3

### 1. globalsign

Тип сертификата: Корневой сертификат CA

### SSL Сертификат





```

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    45:e6:bb:03:83:33:c3:85:65:48:e6:ff:45:51
  Signature Algorithm: sha384WithRSAEncryption
  Issuer: OU=GlobalSign Root CA - R6, O=GlobalSign, CN=GlobalSign
  Validity
    Not Before: Dec 10 00:00:00 2014 GMT
    Not After : Dec 10 00:00:00 2034 GMT
  Subject: OU=GlobalSign Root CA - R6, O=GlobalSign, CN=GlobalSign
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (4096 bit)
    Modulus:
      00:95:07:e8:73:ca:66:f9:ec:14:ca:7b:3c:f7:0d:
      08:f1:b4:45:0b:2c:82:b4:48:c6:eb:5b:3c:ae:83:
      b8:41:92:33:14:a4:6f:7f:e9:2a:cc:c6:b0:88:6b:
      c5:b6:89:d1:c6:b2:ff:14:ce:51:14:21:ec:4a:dd:
      1b:5a:c6:d6:87:ee:4d:3a:15:06:ed:64:66:0b:92:
      80:ca:44:de:73:94:4e:f3:a7:89:7f:4f:78:63:08:
      c8:12:50:6d:42:66:2f:4d:b9:79:28:4d:52:1a:8a:
      1a:80:b7:19:81:0e:7e:c4:8a:bc:64:4c:21:1c:43:
      68:d7:3d:3c:8a:c5:b2:66:d5:90:9a:b7:31:06:c5:
      be:e2:6d:32:06:a6:1e:f9:b9:eb:aa:a3:b8:bf:be:
      82:63:50:d0:f0:18:89:df:e4:0f:79:f5:ea:a2:1f:
      2a:d2:70:2e:7b:e7:bc:93:bb:6d:53:e2:48:7c:8c:
      10:07:38:ff:66:b2:77:61:7e:e0:ea:8c:3c:aa:b4:
      a4:f6:f3:95:4a:12:07:6d:fd:8c:b2:89:cf:d0:a0:
      61:77:c8:58:74:b0:d4:23:3a:f7:5d:3a:ca:a2:db:
      9d:09:de:5d:44:2d:90:f1:81:cd:57:92:fa:7e:bc:
      50:04:63:34:df:6b:93:18:be:6b:36:b2:39:e4:ac:
      24:36:b7:f0:ef:b6:1c:13:57:93:b6:de:b2:f8:e2:
      85:b7:73:a2:b8:35:aa:45:f2:e0:9d:36:a1:6f:54:
      8a:f1:72:56:6e:2e:88:c5:51:42:44:15:94:ee:a3:
      c5:38:96:9b:4e:4e:5a:0b:47:f3:06:36:49:77:30:
      bc:71:37:e5:a6:ec:21:08:75:fc:e6:61:16:3f:77:
      d5:d9:91:97:84:0a:6c:d4:02:4d:74:c0:14:ed:fd:
      39:fb:83:f2:5e:14:a1:04:b0:0b:e9:fe:ee:8f:e1:
      6e:0b:b2:08:b3:61:66:09:6a:b1:06:3a:65:96:59:
      c0:f0:35:fd:c9:da:28:8d:1a:11:87:70:81:0a:a8:
      9a:75:1d:9e:3a:86:05:00:9e:db:80:d6:25:f9:dc:
      05:9e:27:59:4c:76:39:5b:ea:f9:a5:a1:d8:83:0f:
      d1:ff:df:30:11:f9:85:cf:33:48:f5:ca:6d:64:14:
      2c:7a:58:4f:d3:4b:08:49:c5:95:64:1a:63:0e:79:
      3d:f5:b3:8c:ca:58:ad:9c:42:45:79:6e:0e:87:19:
      5c:54:b1:65:b6:bf:8c:9b:dc:13:e9:0d:6f:b8:2e:
      dc:67:6e:c9:8b:11:b5:84:14:8a:00:19:70:83:79:
      91:97:91:d4:1a:27:bf:37:1e:32:07:d8:14:63:3c:
      28:4c:af
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Key Usage: critical
      Certificate Sign, CRL Sign
    X509v3 Basic Constraints: critical
      CA:TRUE
    X509v3 Subject Key Identifier:
      AE:6C:05:A3:93:13:E2:A2:E7:E2:D7:1C:D6:C7:F0:7F:C8:67:53:A0
    X509v3 Authority Key Identifier:
      keyid:AE:6C:05:A3:93:13:E2:A2:E7:E2:D7:1C:D6:C7:F0:7F:C8:67:53:A0

  Signature Algorithm: sha384WithRSAEncryption
    83:25:ed:e8:d1:fd:95:52:cd:9e:c0:04:a0:91:69:e6:5c:d0:
    84:de:dc:ad:a2:4f:e8:47:78:d6:65:98:a9:5b:a8:3c:87:7c:
    02:8a:d1:6e:b7:16:73:e6:5f:c0:54:98:d5:74:be:c1:cd:e2:
    11:91:ad:23:18:3d:dd:e1:72:44:96:b4:95:5e:c0:7b:8e:99:
    78:16:43:13:56:57:b3:a2:b3:3b:b5:77:dc:40:72:ac:a3:eb:
    9b:35:3e:b1:08:21:a1:e7:c4:43:37:79:32:be:b5:e7:9c:2c:
    4c:bc:43:29:99:8e:30:d3:ac:21:e0:e3:1d:fa:d8:07:33:76:
    54:00:22:2a:b9:4d:20:2e:70:68:da:e5:53:fc:83:5c:d3:9d:
    f2:ff:44:0c:44:66:f2:d2:e3:bd:46:00:1a:6d:02:ba:25:5d:
    8d:a1:31:51:dd:54:46:1c:4d:db:99:96:ef:1a:1c:04:5c:a6:
    15:ef:78:e0:79:fe:5d:db:3e:aa:4c:55:fd:9a:15:a9:6f:e1:
    a6:fb:df:70:30:e9:c3:ee:42:46:ed:c2:93:05:89:fa:7d:63:
    7b:3f:d0:71:81:7c:00:e8:98:ae:0e:78:34:c3:25:fb:af:0a:
    9f:20:6b:dd:3b:13:8f:12:8c:e2:41:1a:48:7a:73:a0:77:69:
    c7:b6:5c:7f:82:c8:1e:fe:58:1b:28:2b:a8:6c:ad:5e:6d:c0:
    05:d2:7b:b7:eb:80:fe:25:37:fe:02:9b:68:ac:42:5d:c3:ee:
    f5:cc:dc:f0:50:75:d2:36:69:9c:e6:7b:04:df:6e:06:69:b6:
    de:0a:09:48:59:87:eb:7b:14:60:7a:64:aa:69:43:ef:91:c7:
    4c:ec:18:dd:6c:ef:53:2d:8c:99:e1:5e:f2:72:3e:cf:54:c8:
    bd:67:ec:a4:0f:4c:45:ff:d3:b9:30:23:07:4c:8f:10:bf:86:
    96:d9:99:5a:b4:99:57:1c:a4:cc:bb:15:89:53:ba:2c:05:0f:
    e4:c4:9e:19:b1:18:34:d5:4c:9d:ba:ed:f7:1f:af:24:95:04:
    78:a8:03:bb:ee:81:e5:da:5f:7c:8b:4a:a1:90:74:25:a7:b3:
    3e:4b:c8:2c:56:bd:c7:c8:ef:38:e2:5c:92:f0:79:f7:9c:84:
    ba:74:2d:61:01:20:7e:7e:d1:f2:4f:07:59:5f:8b:2d:43:52:
    eb:46:0c:94:e1:f5:66:47:79:77:d5:54:5b:1f:ad:24:37:cb:
    45:5a:4e:a0:44:48:c8:d8:b0:99:c5:15:84:09:f6:d6:49:49:
    c0:65:b8:e6:1a:71:6e:a0:a8:f1:82:e8:45:3e:6c:d6:02:d7:
    0a:67:83:05:5a:c9:a4:10

```

## 2. globalsign gcc r6 alphassl ca 2023

Тип сертификата: Промежуточный сертификат

## SSL Сертификат

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
7f:1f:2c:90:2e:83:d0:e3:b6:fb:3b:ee:47:8b:5e:80  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: OU=GlobalSign Root CA - R6, O=GlobalSign, CN=GlobalSign  
Validity  
Not Before: Jul 19 03:43:25 2023 GMT  
Not After : Jul 19 00:00:00 2026 GMT  
Subject: C=BE, O=GlobalSign nv-sa, CN=GlobalSign GCC R6 AlphaSSL CA 2023  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
Public-Key: (2048 bit)  
Modulus:  
00:d3:42:6f:93:90:03:a6:93:b4:ae:00:e7:8f:53:  
35:e1:72:1b:d3:7d:80:6a:ce:34:f4:92:45:01:bf:  
1c:52:38:a9:14:eb:61:ef:24:8b:75:a5:8b:7b:7b:  
3a:de:84:ac:e7:1d:de:5b:0c:d3:a5:7e:01:16:4c:  
d9:6f:14:f5:7a:82:52:1d:f4:f6:33:4c:19:e5:03:  
8f:70:22:23:b2:bf:98:07:c4:c0:bd:5d:b2:25:2c:  
aa:f9:e9:91:ac:df:c5:b6:00:92:4d:a5:97:48:9e:  
63:8a:95:bc:48:9f:d5:02:e5:cf:33:3b:80:3f:6c:  
98:a6:e3:dc:8e:34:39:1b:2a:ec:b0:35:e0:bb:e1:  
61:b5:8c:6a:c8:53:fb:05:2b:f1:f6:34:21:87:94:  
15:e7:38:4b:c9:cb:9a:9f:c9:fe:27:45:30:d3:d5:  
91:40:ae:89:19:0e:47:cc:36:50:8a:79:0d:7a:5f:  
9f:65:93:51:1b:58:04:f5:07:a1:fa:d1:c1:a6:5a:  
e4:6a:50:75:83:ce:6a:26:43:ce:27:b4:a8:12:f2:  
ac:98:39:1a:8e:08:24:fe:c4:aa:ec:d3:f2:cc:56:  
9a:fd:50:46:66:24:51:1b:e1:64:c4:20:67:88:60:  
f9:eb:5f:0f:43:8b:6b:73:01:f2:32:88:d2:14:e6:  
ce:1d  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
X509v3 Key Usage: critical  
Digital Signature, Certificate Sign, CRL Sign  
X509v3 Extended Key Usage:  
TLS Web Server Authentication, TLS Web Client Authentication  
X509v3 Basic Constraints: critical  
CA:TRUE, pathlen:0  
X509v3 Subject Key Identifier:  
BD:05:B7:F3:8A:93:3C:73:CB:79:FA:0F:85:12:A1:77:96:18:91:74  
X509v3 Authority Key Identifier:  
keyid:AE:6C:05:A3:93:13:E2:A2:E7:E2:D7:1C:D6:C7:F0:7F:C8:67:53:A0  
  
Authority Information Access:  
OCSP - URI:http://ocsp2.globalsign.com/rootr6  
CA Issuers - URI:http://secure.globalsign.com/cacert/root-r6.crt  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI:http://crl.globalsign.com/root-r6.crl  
  
X509v3 Certificate Policies:  
Policy: 2.23.140.1.2.1  
Policy: 1.3.6.1.4.1.4146.10.1.3  
  
Signature Algorithm: sha256WithRSAEncryption  
7c:c9:24:32:8e:60:e2:69:f5:7e:de:1d:e3:14:76:90:7c:d8:  
a4:3b:a4:84:2d:57:60:fc:1f:49:93:77:03:d9:c4:05:a7:63:  
74:a6:4c:1f:b8:ae:4b:5b:c5:f2:e4:9c:83:6e:bf:df:40:d1:  
3d:e9:f6:7c:54:6c:af:ae:b6:10:2c:94:09:1e:0e:7d:e8:a2:  
18:d7:68:42:f7:1e:b0:cf:57:a5:ec:37:1c:b4:0f:e2:a1:e0:  
fa:ce:fb:e2:13:4b:bc:64:43:e1:a2:92:2b:01:6a:2c:ca:dc:  
a8:2c:3a:b4:40:1f:5f:df:6d:15:6b:03:e2:3c:db:0b:a9:3c:  
b6:34:8b:cc:49:74:7d:35:25:7e:42:5a:5a:9b:cb:56:4a:60:  
f5:eb:7c:b4:3f:1d:e7:56:f2:98:28:39:27:a2:7a:c1:c5:e9:  
9a:c4:86:9e:4b:01:a1:b6:9c:d7:e9:d7:9a:00:7b:8d:00:bd:  
79:d5:3c:67:8d:45:16:8f:3b:05:5d:e4:0a:da:d6:5a:c7:64:  
41:ab:ce:6c:cb:17:50:f9:7f:00:ef:32:fe:33:ae:01:6c:f4:  
c3:2b:cf:9c:aa:26:fa:8e:96:e2:f2:83:63:af:fa:5c:fc:a9:  
35:d7:9b:38:9e:a6:8f:26:88:2e:9d:2a:ba:84:2f:86:3c:7c:  
ec:1c:c4:36:1e:6c:e7:b0:08:3b:22:06:a5:2d:2c:0c:40:a1:  
54:33:f3:2c:47:d1:b0:7d:85:27:cf:d6:e7:0a:05:d2:7b:ec:  
05:3a:9f:61:20:aa:6e:54:1b:1d:e0:c3:b4:28:fb:32:57:fc:  
25:fa:9a:32:ea:9c:6c:4e:2b:31:2c:9f:78:7c:82:75:94:30:  
9d:cf:eb:f6:e8:e7:b6:1e:bd:d4:02:61:c7:26:1e:08:cd:38:  
99:eb:49:21:ee:dc:07:a7:78:74:59:be:3d:de:5e:ae:f6:38:  
c7:7d:ab:d2:e4:35:43:4b:29:cb:55:63:36:a5:09:8e:eb:2c:  
62:e5:cd:c8:c9:85:1d:2b:8b:41:0e:8f:ad:e3:e6:1f:99:5c:  
48:c4:29:60:ac:fa:a0:3f:d1:88:d5:43:fc:f2:b4:3b:7b:ee:  
3b:9b:e1:de:8e:e8:29:bd:45:7f:3a:1a:9c:3b:05:15:3a:f0:  
d1:a2:ce:75:15:bf:b6:62:cf:59:53:55:94:06:fc:69:df:81:  
f3:46:09:b0:be:07:5d:89:d0:1b:cc:18:00:56:fc:2e:1c:12:  
0f:24:fd:bf:e0:b5:0b:59:5c:20:71:3b:9c:4d:00:02:9f:49:  
48:7c:43:62:c9:9a:f6:98:b8:83:43:e1:83:70:60:3a:6d:9e:  
b9:34:73:c3:b4:74:4b:35

### 3. www.mile.by

Тип сертификата: Сертификат данного узла

## SSL Сертификат

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      13:7f:d5:46:d2:72:fb:47:0e:6e:20:38
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign GCC R6 AlphaSSL CA 2023
    Validity
      Not Before: Mar 21 11:40:28 2025 GMT
      Not After : Apr 22 11:40:27 2026 GMT
    Subject: CN=www.mile.by
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        00:e3:dc:f5:d6:21:8d:15:37:d5:1b:22:e0:80:ec:
        fe:2f:a1:9f:cb:a8:62:7a:e7:e2:a2:eb:48:36:55:
        c3:0a:22:8a:33:23:fc:59:d5:a0:90:a4:e1:85:44:
        f0:f8:59:e6:be:12:fe:b6:88:36:a0:3a:90:1d:ed:
        6b:4c:13:5a:12:52:65:b2:97:d5:26:59:a3:cd:ca:
        c9:43:d8:0a:34:48:b9:df:8e:a1:7d:50:ee:50:98:
        36:26:85:fc:4c:af:64:54:c2:bc:29:af:05:23:16:
        cc:1a:1a:4e:33:54:a9:65:84:ae:fa:32:50:60:9e:
        76:ca:e1:95:ba:9e:94:ff:4e:10:1d:48:56:67:36:
        a4:c2:b6:30:7a:92:b1:e6:80:c0:c7:3a:b3:65:8b:
        de:05:6a:1c:e2:c9:6d:cc:26:08:45:f9:24:e7:cb:
        bb:0d:e4:9a:a0:7b:1e:f8:87:67:89:14:61:6e:f8:
        7b:a6:44:61:57:1a:fd:18:ae:06:37:ff:0a:48:d0:
        13:3b:52:5b:5d:a3:a8:57:f7:f6:dd:dc:3e:37:ba:
        dc:28:28:e9:cf:14:f7:b6:50:50:44:94:3c:6c:34:
        c9:94:65:e9:26:91:9b:3a:41:16:be:8a:f4:3e:e7:
        dc:05:4b:8f:aa:79:b9:25:43:6b:22:3c:5b:03:c4:
        15:f1:5d:76:0f:70:1b:fb:45:3f:c4:27:8e:3c:2e:
        59:a9:a8:bd:6c:c1:2a:c1:62:b7:2a:0b:22:34:49:
        40:f9:65:4b:3f:0f:73:85:de:7b:61:da:09:ed:d9:
        20:14:40:45:66:73:e1:10:05:e5:38:7e:2c:bc:ab:
        79:9f:b2:8d:51:52:66:b2:6f:cc:d8:55:08:c5:a0:
        76:a6:57:81:d8:e4:db:05:41:d9:65:73:8b:e6:0c:
        a3:87:b3:11:c9:c7:12:cc:bb:ce:ea:f0:35:0b:26:
        4b:75:41:12:62:dd:f5:eb:3e:bb:cd:d5:da:59:c1:
        6b:7e:d8:e8:aa:ff:e4:a6:2b:1d:e1:fa:a5:92:97:
        f6:96:c3:4b:75:aa:4d:cf:b0:53:23:af:df:17:7b:
        e5:25:42:03:40:46:59:c3:1e:13:fb:d4:0a:24:c8:
        f0:ba:db:45:96:af:6e:9a:19:53:e6:70:39:62:a8:
        93:bf:61:4b:f6:9a:99:0f:6e:33:2a:c9:be:21:7f:
        c5:6d:ff:35:4b:da:14:1d:73:94:8e:69:fb:93:0b:
        55:31:29:79:0f:84:af:bb:fe:68:87:c1:a8:7a:2c:
        8d:6e:d1:3d:80:5c:b5:b2:4d:87:e0:d9:97:dc:c1:
        a2:c6:46:63:89:d7:9b:a4:86:86:5e:c1:bd:43:9d:
        45:67:77
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
      X509v3 Basic Constraints: critical
        CA:FALSE
      Authority Information Access:
        CA Issuers - URI:http://secure.globalsign.com/cacert/gsgccr6alphasslca2023.crt
        OCSP - URI:http://ocsp.globalsign.com/gsgccr6alphasslca2023

      X509v3 Certificate Policies:
        Policy: 2.23.140.1.2.1
        Policy: 1.3.6.1.4.1.4146.10.1.3
        CPS: https://www.globalsign.com/repository/

      X509v3 CRL Distribution Points:

        Full Name:
          URI:http://crl.globalsign.com/gsgccr6alphasslca2023.crl

      X509v3 Subject Alternative Name:
        DNS:www.mile.by, DNS:mile.by
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
      X509v3 Authority Key Identifier:
        keyid:BD:05:B7:F3:8A:93:3C:73:CB:79:FA:0F:85:12:A1:77:96:18:91:74

      X509v3 Subject Key Identifier:
        53:04:4F:09:F6:A9:47:6F:78:75:FE:0E:1D:3C:2D:CB:C6:97:18:D7
    CT Precertificate SCTs:
      Signed Certificate Timestamp:
        Version : v1(0)
        Log ID : 64:11:C4:6C:A4:12:EC:A7:89:1C:A2:02:2E:00:BC:AB:
          4F:28:07:D4:1E:35:27:AB:EA:FE:D5:03:C9:7D:CD:F0
        Timestamp : Mar 21 11:40:32.921 2025 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
          30:45:02:21:00:AC:82:1B:5C:D9:60:53:1C:55:DE:7A:
          26:BA:AD:9C:DF:9B:9F:13:C4:6F:A8:9B:14:80:29:EA:
          E1:0A:3A:C6:8E:02:20:0F:EF:B7:1B:56:BA:01:EA:C5:
          05:3A:D3:11:69:74:8E:2E:1A:58:CF:03:94:9C:EB:5A:
          3E:7D:C7:F7:4E:9E:07
      Signed Certificate Timestamp:
        Version : v1(0)
        Log ID : 0E:57:94:BC:F3:AE:A9:3E:33:1B:2C:99:07:B3:F7:90:
          DF:9B:C2:3D:71:32:25:DD:21:A9:25:AC:61:C5:4E:21
        Timestamp : Mar 21 11:40:32.905 2025 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256

```

30:44:02:20:4F:21:C6:B5:E3:E4:74:86:6E:45:98:6D:  
55:60:75:65:FF:F9:5C:35:A2:AB:A3:8E:D6:59:11:11:  
56:D6:4C:B6:02:20:09:DC:C1:E6:69:CA:C4:34:05:82:  
3E:0A:06:5A:0B:D6:96:D9:32:35:60:80:A9:2A:2E:A5:  
C9:67:31:07:D0:69  
Signed Certificate Timestamp:  
Version : v1(0)  
Log ID : 49:9C:9B:69:DE:1D:7C:EC:FC:36:DE:CD:87:64:A6:B8:  
5B:AF:0A:87:80:19:D1:55:52:FB:E9:EB:29:DD:F8:C3  
Timestamp : Mar 21 11:40:32.945 2025 GMT  
Extensions: none  
Signature : ecdsa-with-SHA256  
30:45:02:21:00:BD:F0:21:48:64:28:57:AE:E9:C1:DF:  
28:5B:B1:AE:42:E5:2F:55:3D:0E:13:5A:9A:F0:67:4A:  
10:13:81:D2:74:02:20:45:3B:F8:B3:49:33:2E:70:17:  
C2:F8:2A:A0:99:77:AD:F7:7D:67:6B:8B:9D:60:73:27:  
BD:AD:21:27:CA:96:54

Signature Algorithm: sha256WithRSAEncryption  
b5:e5:1d:34:db:67:42:eb:ca:85:e6:c1:67:6a:36:88:1f:28:  
e7:55:52:b9:0b:2a:c1:9a:e6:32:41:e0:32:23:14:d5:79:f1:  
1a:ab:3e:6e:f7:99:81:c0:ed:63:62:b0:dc:31:c3:ee:e8:83:  
7e:e1:41:47:14:97:af:11:7d:be:6c:cb:08:9d:4e:05:16:63:  
1f:c1:88:6d:04:0a:f3:4b:63:d9:26:08:3d:da:cf:b5:6d:bf:  
6c:95:ad:c6:cc:7b:4b:16:b0:7c:32:5d:70:65:77:f3:4b:14:  
28:c3:73:a4:2f:f9:45:62:6f:0f:20:37:f2:97:c4:c3:10:67:  
e7:9e:47:5c:8c:22:86:28:8e:92:7d:42:39:59:a5:32:ea:ed:  
c5:dc:44:fa:f4:e7:a1:e5:6e:fd:ca:b3:5d:3b:78:24:6f:62:  
26:c0:cb:ee:65:9b:6c:35:c6:dd:72:91:ee:ac:eb:dd:9b:9c:  
2d:f3:9c:cc:28:bb:fc:fb:93:42:ce:eb:8c:98:a8:85:e3:43:  
63:32:21:7d:05:2d:3c:f5:15:30:2d:34:ce:d5:64:a4:52:b3:  
95:96:a3:ed:eb:83:3e:f9:f1:04:03:c8:68:65:c9:fc:4d:f1:  
2d:da:ba:cc:1e:3a:d7:fd:3c:86:7c:54:bb:2b:d7:bf:01:e5:  
d4:e8:78:7b

## 80/TCP - HTTP

Имя сервера:	nginx
Состояние:	301 (Moved Permanently)
Имя сервера (определено эвристикой):	Nginx HTTP Server
Информация об имени приложения подтверждена эвристическим методом	



Информация  
**Информация об HTTP-заголовках**  
ID: 8375

### Краткое описание

Перечисление HTTP-заголовков в ответе сервера, полученного на GET-запрос.

### HTTP-заголовки

HTTP-заголовок	Значение
CONNECTION	CLOSE
CONTENT-LENGTH	282
CONTENT-TYPE	TEXT/HTML; CHARSET=ISO-8859-1
DATE	WED, 30 JUL 2025 13:42:13 GMT
LOCATION	HTTPS://MILE.BY/
SERVER	NGINX
X-CONTENT-TYPE-OPTIONS	NOSNIFF
X-FRAME-OPTIONS	SAMEORIGIN

### Ссылки

<https://www.ietf.org/rfc/rfc2616.txt>

Конец отчета MaxPatrol (сборка 40948)  
© 2025 Positive Technologies