**Отчет по сканированию проекта b24.reaspekt.ru**

Сканирование проведено при помощи OpenVAS. Использовалась готовая сборка на базе docker образа mikesplain/openvas. С отчетом приложен docker-compose.yml для воспроизведения той же самой сборки.
В качестве цели сканирования использовалось небольшое приложение https://b24.reaspekt.ru/ (предназначено для подсчета выработки специалистов внутри компании).
Обнаружено 7 уязвимостей, которые приведены в отчете report-1.pdf.

**Уязвимость №1. NVT: SSL/TLS: Missing `secure` Cookie Attribute**

Рекомендация по решению: установить атрибут `session.cookie_secure` в php.ini, либо в коде приложения использовать

```
ini_set('session.cookie_secure',1);
```

Статус: решено.

**Уязвимость №2. NVT: Missing `httpOnly` Cookie Attribute**

Рекомендация по решению: установить атрибут `session.cookie_httponly` в php.ini, либо в коде приложения использовать

```
ini_set('session.cookie_httponly',1);
```

Статус: решено.

**Уязвимость №3. NVT: FTP Unencrypted Cleartext Login**

Приложение размещено на shared хостинге, поэтому исправить не представляется возможным.

Рекомендация по решению: сервер на базе Linux, поэтому необходимо закрыть через правила iptables (firewall) 21 порт и использовать для

соединения sftp (на 22 порту). На данный момент хостинг не требует дополнительных настроек для работы по sftp.

Статус: не решено.

**Уязвимость №4. NVT: Missing `httpOnly` Cookie Attribute**

Аналогично Уязвимости №2.

Статус: решено.

**Уязвимость №5. NVT: SSH Weak Encryption Algorithms Supported**
Приложение размещено на shared хостинге, поэтому исправить не представляется возможным.

Рекомендация по решению: отключить слабые алгоритмы шифрования для соединений по ssh. В зависимости от системы это может быть конфиги вида `/etc/sysconfig/sshd`.

Статус: не решено

**Уязвимость №6. NVT: SSH Weak MAC Algorithms Supported**
Приложение размещено на shared хостинге, поэтому исправить не представляется возможным.

Рекомендация по решению: отредактировать конфиг ssh, чтобы выключить слабый MAC алгоритм. Для этого открыть файл `/etc/ssh/sshd_config` и в нем удалить алгоритм `hmac-sha1`. После этого перезапустить сервис sshd, например:

```
service sshd restart
```

Статус: не решено.

**Уязвимость №7. NVT: TCP timestamps**

Приложение размещено на shared хостинге, поэтому исправить не представляется возможным.

Рекомендация по решению: отключить TCP timestamps, для этого в конфиге `/etc/sysctl.conf` установить параметр ядра (добавить строку)

```
net.ipv4.tcp_timestamps = 0
```

После этого применить параметр ядра командой

```
sctl -p
```

Статус: не решено.

**Заключение**

Настройки, которые было возможно исправить — исправлены и проведено повторное сканирование.
Отчет сканирования приложен в файле report-2.pdf.