Universidade do Minho

Mestrado Integrado em Engenharia Informática

Engenharia de Segurança

Aula 3 - 02/Mar/2020

João de Macedo
A76268

João Aloísio
A77953

Nelson Gonçalves
A78173

9 de Março de 2020

1 Pergunta P1.1

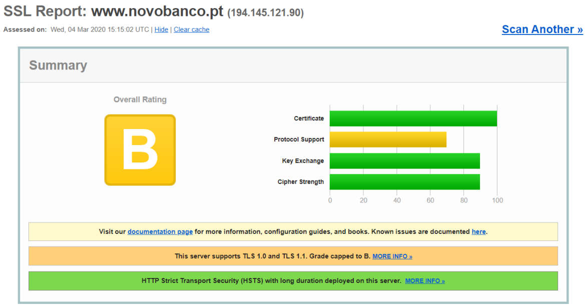
Os ficheiros com o código alterado encontram-se na pasta *Pergunta1*.

2 Pergunta P2.1

Os dois bancos escolhidos foram o BPI(https://www.bancobpi.pt/particulares) e o Novo banco(https://www.novobanco.pt/site)

2.0.1 i)

Nas seguintes imagens podemos ver o rating referente ao site do novo banco e do BPi respectivamente.



SSL Report: www.novobanco.pt (194.145.121.90)

Assessed on: Wed, 04 Mar 2020 15:15:02 UTC | Hide | Clear cache

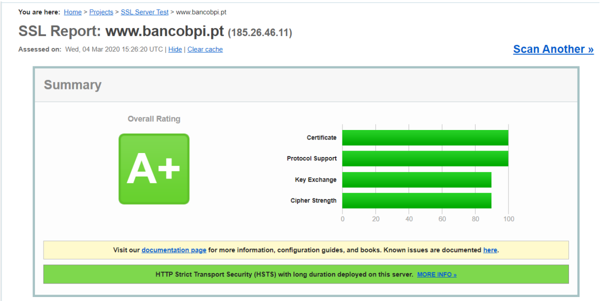
Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Figura 1



You are here: Home > Projects > SSL Server Test > www.bancobpi.pt

SSL Report: www.bancobpi.pt (185.26.46.11)

Assessed on: Wed, 04 Mar 2020 15:26:20 UTC | Hide | Clear cache

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Figura 2

2.0.2 ii)

O o bancom o pior rating é o novo Banco, a principal diferença a nivel de rating para o outro banco escolhido é o Protocol Support. Em que o site suporta TLS 1.0 e TLS 1.1, uma das principais causas para o site suportar este tipo de protocolos (mais antigos) é a compatibilidade, ou seja, aplicações utilizadas pelo banco ou para o banco em que utilizam estes tipos de protocolos.

2.0.3 iii)

O *Downgrade attack prevention* é um ataque de tentativa de regressão de versão, em que o atacante tenta "negociar"com o servidor o uso de versões de serviços inferiores com mais vulnerabilidades conhecidas de modo a tentar exploralas. Por exemplo, foi encontrado no OpenSSL que permitia ao invasor negociar o uso de uma versão inferior do TLS entre o cliente e o servidor.

3 Pergunta 3

3.1 Pergunta P3.1

As duas empresas comerciais de Paris escolhidas foram:

- OVH SAS: empresa que fornece servidores dedicados sob a lei francesa;
- Microsoft Azure: é uma plataforma destinada à execução de aplicativos e serviços, baseada nos conceitos da computação em nuvem.

3.1.1 Pergunta P3.1.1

Resultados de ssh-audit para OVH SAS:

```
# general
(gen) banner: SSH-2.0-OpenSSH_6.2p2 Ubuntu-6ubuntu0.4
(gen) software: OpenSSH 6.2p2
(gen) compatibility: OpenSSH 6.2-6.6, Dropbear SSH 2013.62+ (some functionality from 0.5
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) ecdh-sha2-nistp256                    -- [fail] using weak elliptic curves
        ‘- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp384                    -- [fail] using weak elliptic curves
        ‘- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp521                    -- [fail] using weak elliptic curves
```

```
        `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) diffie-hellman-group-exchange-sha256  -- [warn] using custom size modulus (possibl
        `- [info] available since OpenSSH 4.4
(kex) diffie-hellman-group-exchange-sha1    -- [fail] removed (in server) since OpenSSH
        `- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 2.3.0
(kex) diffie-hellman-group14-sha1           -- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 3.9, Dropbear SSH 0.53
(kex) diffie-hellman-group1-sha1            -- [fail] removed (in server) since OpenSSH
        `- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
        `- [warn] using small 1024-bit modulus
        `- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28

# host-key algorithms
(key) ssh-rsa                               -- [info] available since OpenSSH 2.5.0, Dro
(key) ssh-dss                               -- [fail] removed (in server) and disabled (
        `- [warn] using small 1024-bit modulus
        `- [warn] using weak random number generator could reveal the key
        `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28

# encryption algorithms (ciphers)
(enc) aes128-ctr                            -- [info] available since OpenSSH 3.7, Dropb
(enc) aes192-ctr                            -- [info] available since OpenSSH 3.7
(enc) aes256-ctr                            -- [info] available since OpenSSH 3.7, Dropb
(enc) arcfour256                            -- [fail] removed (in server) since OpenSSH
        `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        `- [warn] using weak cipher
        `- [info] available since OpenSSH 4.2
(enc) arcfour128                            -- [fail] removed (in server) since OpenSSH
        `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        `- [warn] using weak cipher
        `- [info] available since OpenSSH 4.2
(enc) aes128-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes256-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes128-cbc                            -- [fail] removed (in server) since OpenSSH
        `- [warn] using weak cipher mode
        `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28
(enc) 3des-cbc                              -- [fail] removed (in server) since OpenSSH
        `- [warn] using weak cipher
        `- [warn] using weak cipher mode
        `- [warn] using small 64-bit block size
        `- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
(enc) blowfish-cbc                          -- [fail] removed (in server) since OpenSSH
        `- [fail] disabled since Dropbear SSH 0.53
        `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        `- [warn] using weak cipher mode
        `- [warn] using small 64-bit block size
        `- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
(enc) cast128-cbc                           -- [fail] removed (in server) since OpenSSH
        `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        `- [warn] using weak cipher mode
        `- [warn] using small 64-bit block size
        `- [info] available since OpenSSH 2.1.0
(enc) aes192-cbc                            -- [fail] removed (in server) since OpenSSH
        `- [warn] using weak cipher mode
        `- [info] available since OpenSSH 2.3.0
(enc) aes256-cbc                            -- [fail] removed (in server) since OpenSSH
        `- [warn] using weak cipher mode
        `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.47
(enc) arcfour                               -- [fail] removed (in server) since OpenSSH
        `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        `- [warn] using weak cipher
        `- [info] available since OpenSSH 2.1.0
(enc) rijndael-cbc@lysator.liu.se           -- [fail] removed (in server) since OpenSSH
        `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        `- [warn] using weak cipher mode
        `- [info] available since OpenSSH 2.3.0

# message authentication code algorithms
(mac) hmac-md5-etm@openssh.com              -- [fail] removed (in server) since OpenSSH
        `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        `- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 6.2
(mac) hmac-sha1-etm@openssh.com             -- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 6.2
(mac) umac-64-etm@openssh.com               -- [warn] using small 64-bit tag size
        `- [info] available since OpenSSH 6.2
(mac) umac-128-etm@openssh.com              -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256-etm@openssh.com         -- [info] available since OpenSSH 6.2
```

```
(mac) hmac-sha2-512-etm@openssh.com         -- [info] available since OpenSSH 6.2
(mac) hmac-ripemd160-etm@openssh.com        -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [info] available since OpenSSH 6.2
(mac) hmac-sha1-96-etm@openssh.com          -- [fail] removed (in server) since OpenSSH
        ‘- [warn] using weak hashing algorithm
        ‘- [info] available since OpenSSH 6.2
(mac) hmac-md5-96-etm@openssh.com           -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using weak hashing algorithm
        ‘- [info] available since OpenSSH 6.2
(mac) hmac-md5                              -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using encrypt-and-MAC mode
        ‘- [warn] using weak hashing algorithm
        ‘- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-sha1                             -- [warn] using encrypt-and-MAC mode
        ‘- [warn] using weak hashing algorithm
        ‘- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) umac-64@openssh.com                   -- [warn] using encrypt-and-MAC mode
        ‘- [warn] using small 64-bit tag size
        ‘- [info] available since OpenSSH 4.7
(mac) umac-128@openssh.com                  -- [warn] using encrypt-and-MAC mode
        ‘- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256                         -- [warn] using encrypt-and-MAC mode
        ‘- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha2-512                         -- [warn] using encrypt-and-MAC mode
        ‘- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-ripemd160                        -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using encrypt-and-MAC mode
        ‘- [info] available since OpenSSH 2.5.0
(mac) hmac-ripemd160@openssh.com            -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using encrypt-and-MAC mode
        ‘- [info] available since OpenSSH 2.1.0
(mac) hmac-sha1-96                          -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using encrypt-and-MAC mode
        ‘- [warn] using weak hashing algorithm
        ‘- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.47
(mac) hmac-md5-96                           -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using encrypt-and-MAC mode
        ‘- [warn] using weak hashing algorithm
        ‘- [info] available since OpenSSH 2.5.0

# algorithm recommendations (for OpenSSH 6.2)
(rec) -diffie-hellman-group14-sha1          -- kex algorithm to remove
(rec) -diffie-hellman-group-exchange-sha1   -- kex algorithm to remove
(rec) -diffie-hellman-group1-sha1           -- kex algorithm to remove
(rec) -ecdh-sha2-nistp256                   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp521                   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384                   -- kex algorithm to remove
(rec) -ssh-dss                              -- key algorithm to remove
(rec) -arcfour                              -- enc algorithm to remove
(rec) -rijndael-cbc@lysator.liu.se          -- enc algorithm to remove
(rec) -blowfish-cbc                         -- enc algorithm to remove
(rec) -3des-cbc                             -- enc algorithm to remove
(rec) -aes256-cbc                           -- enc algorithm to remove
(rec) -arcfour256                           -- enc algorithm to remove
(rec) -cast128-cbc                          -- enc algorithm to remove
(rec) -aes192-cbc                           -- enc algorithm to remove
(rec) -arcfour128                           -- enc algorithm to remove
(rec) -aes128-cbc                           -- enc algorithm to remove
(rec) -hmac-sha2-512                        -- mac algorithm to remove
(rec) -hmac-md5-96                          -- mac algorithm to remove
(rec) -hmac-md5-etm@openssh.com             -- mac algorithm to remove
(rec) -hmac-sha1-96-etm@openssh.com         -- mac algorithm to remove
(rec) -hmac-ripemd160-etm@openssh.com       -- mac algorithm to remove
(rec) -hmac-md5-96-etm@openssh.com          -- mac algorithm to remove
(rec) -hmac-sha2-256                        -- mac algorithm to remove
(rec) -hmac-ripemd160                       -- mac algorithm to remove
(rec) -umac-128@openssh.com                 -- mac algorithm to remove
(rec) -hmac-sha1-96                         -- mac algorithm to remove
(rec) -umac-64@openssh.com                  -- mac algorithm to remove
(rec) -hmac-md5                             -- mac algorithm to remove
(rec) -hmac-ripemd160@openssh.com           -- mac algorithm to remove
(rec) -hmac-sha1                            -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com            -- mac algorithm to remove
```

```
(rec) -umac-64-etm@openssh.com              -- mac algorithm to remove
```

Resultado para Microsoft Azure:

```
# general
(gen) banner: SSH-2.0-OpenSSH_7.4
(gen) software: OpenSSH 7.4
(gen) compatibility: OpenSSH 7.3+ (some functionality from 6.6), Dropbear SSH 2016.73+ (
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256                     -- [warn] unknown algorithm
(kex) curve25519-sha256@libssh.org          -- [info] available since OpenSSH 6.5, Dropb
(kex) ecdh-sha2-nistp256                    -- [fail] using weak elliptic curves
        `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp384                    -- [fail] using weak elliptic curves
        `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp521                    -- [fail] using weak elliptic curves
        `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) diffie-hellman-group-exchange-sha256  -- [warn] using custom size modulus (possibl
        `- [info] available since OpenSSH 4.4
(kex) diffie-hellman-group16-sha512         -- [info] available since OpenSSH 7.3, Dropb
(kex) diffie-hellman-group18-sha512         -- [info] available since OpenSSH 7.3
(kex) diffie-hellman-group-exchange-sha1    -- [fail] removed (in server) since OpenSSH
        `- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 2.3.0
(kex) diffie-hellman-group14-sha256         -- [info] available since OpenSSH 7.3, Dropb
(kex) diffie-hellman-group14-sha1           -- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 3.9, Dropbear SSH 0.53
(kex) diffie-hellman-group1-sha1            -- [fail] removed (in server) since OpenSSH
        `- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
        `- [warn] using small 1024-bit modulus
        `- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28

# host-key algorithms
(key) ssh-rsa                               -- [info] available since OpenSSH 2.5.0, Dro
(key) rsa-sha2-512                          -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256                          -- [info] available since OpenSSH 7.2
```

```
(key) ecdsa-sha2-nistp256                   -- [fail] using weak elliptic curves
        ‘- [warn] using weak random number generator could reveal the key
        ‘- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(key) ssh-ed25519                           -- [info] available since OpenSSH 6.5

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com         -- [info] available since OpenSSH 6.5
        ‘- [info] default cipher since OpenSSH 6.9.
(enc) aes128-ctr                            -- [info] available since OpenSSH 3.7, Dropb
(enc) aes192-ctr                            -- [info] available since OpenSSH 3.7
(enc) aes256-ctr                            -- [info] available since OpenSSH 3.7, Dropb
(enc) aes128-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes256-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes128-cbc                            -- [fail] removed (in server) since OpenSSH
        ‘- [warn] using weak cipher mode
        ‘- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28
(enc) aes192-cbc                            -- [fail] removed (in server) since OpenSSH
        ‘- [warn] using weak cipher mode
        ‘- [info] available since OpenSSH 2.3.0
(enc) aes256-cbc                            -- [fail] removed (in server) since OpenSSH
        ‘- [warn] using weak cipher mode
        ‘- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.47
(enc) blowfish-cbc                          -- [fail] removed (in server) since OpenSSH
        ‘- [fail] disabled since Dropbear SSH 0.53
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using weak cipher mode
        ‘- [warn] using small 64-bit block size
        ‘- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
(enc) cast128-cbc                           -- [fail] removed (in server) since OpenSSH
        ‘- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
        ‘- [warn] using weak cipher mode
        ‘- [warn] using small 64-bit block size
        ‘- [info] available since OpenSSH 2.1.0
(enc) 3des-cbc                              -- [fail] removed (in server) since OpenSSH
        ‘- [warn] using weak cipher
        ‘- [warn] using weak cipher mode
        ‘- [warn] using small 64-bit block size
        ‘- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28

# message authentication code algorithms
```

```
(mac) umac-64-etm@openssh.com               -- [warn] using small 64-bit tag size
        `- [info] available since OpenSSH 6.2
(mac) umac-128-etm@openssh.com              -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256-etm@openssh.com         -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-512-etm@openssh.com         -- [info] available since OpenSSH 6.2
(mac) hmac-sha1-etm@openssh.com             -- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 6.2
(mac) umac-64@openssh.com                   -- [warn] using encrypt-and-MAC mode
        `- [warn] using small 64-bit tag size
        `- [info] available since OpenSSH 4.7
(mac) umac-128@openssh.com                  -- [warn] using encrypt-and-MAC mode
        `- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256                         -- [warn] using encrypt-and-MAC mode
        `- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha2-512                         -- [warn] using encrypt-and-MAC mode
        `- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha1                             -- [warn] using encrypt-and-MAC mode
        `- [warn] using weak hashing algorithm
        `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28

# algorithm recommendations (for OpenSSH 7.4)
(rec) -diffie-hellman-group14-sha1          -- kex algorithm to remove
(rec) -ecdh-sha2-nistp256                   -- kex algorithm to remove
(rec) -diffie-hellman-group-exchange-sha256 -- kex algorithm to remove
(rec) -diffie-hellman-group1-sha1           -- kex algorithm to remove
(rec) -diffie-hellman-group-exchange-sha1   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp521                   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384                   -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256                  -- key algorithm to remove
(rec) -blowfish-cbc                         -- enc algorithm to remove
(rec) -3des-cbc                             -- enc algorithm to remove
(rec) -aes256-cbc                           -- enc algorithm to remove
(rec) -cast128-cbc                          -- enc algorithm to remove
(rec) -aes192-cbc                           -- enc algorithm to remove
(rec) -aes128-cbc                           -- enc algorithm to remove
(rec) -hmac-sha2-512                        -- mac algorithm to remove
(rec) -umac-128@openssh.com                 -- mac algorithm to remove
(rec) -hmac-sha2-256                        -- mac algorithm to remove
(rec) -umac-64@openssh.com                  -- mac algorithm to remove
(rec) -hmac-sha1                            -- mac algorithm to remove
```

```
(rec) -hmac-sha1-etm@openssh.com            -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com              -- mac algorithm to remove
```

3.1.2 Pergunta P3.1.2

Os softwares e versões usados pelos servidores são:

- **OVH SAS:** software "OpenSSH"com a versão 6.2p2;
- **Microsoft Azure:** software "OpenSSH"com a versão 7.4;

3.1.3 Pergunta P3.1.3

Recorrendo ao website *https://www.cvedetails.com/version-search.php* é possível observar que a versão 6.2p2 tem 5 vulnerabilidades conhecidas e a versão 7.4 tem 2 vulnerabilidades conhecidas. Assim sendo a versão 6.2p2 tem mais vulnerabilidades.

3.1.4 Pergunta P3.1.4

Observando os resultados obtidos no *CVE Details*, a vulnerabilidade mais crítica tem um CVSS Score 5 e pode ser encontrada em ambas as versões, sendo **CVE-2018-15919**.

3.1.5 Pergunta P3.1.5

A vulnerabilidade indicada na alínea anterior pode não ser considerada não grave porque esta somente afeta parcialmente a Confidencialidade, não afetando a Integridade e Disponibilidade do software. Mesmo assim, dado que é de um grau de complexidade baixa e não é necessária nenhuma autorização, esta tem que ser corrigida porque há um acesso a informação indevida. Uma solução para a resolução desta vulnerabilidade é o uso de um software mais atualizado.