# Semestrální práce – kontrolní otázky

Dle potřeby upravte velikost jednotlivých polí.

## Základní údaje:

|  |  |
| --- | --- |
| 1. Jméno kontrolovaného serveru
 |  |
| 1. Správce serveru – student, který instaloval aplikace
 |  |
| 1. Auditor – Vaše jméno
 |  |
| 1. Datum kontroly
 |  |
| 1. Název hlavní aplikace
 |  |
| 1. Stručný popis aplikace:
 |

## Funkční požadavky

|  |  |
| --- | --- |
| 1. Zobrazí se po zadání [http://bis*xxx*.vse.cz/](http://bisxxx.vse.cz/) úvodní stránka aplikace?
 |  |
| 1. Je hlavní aplikace funkční – lze se přihlásit a provádět základní činnosti (např. vkládat příspěvky/obrázky, …)?
 |  |
| 1. Jsou běžní uživatelé hlavní aplikace uloženi v LDAPu?
 |  |
| 1. Má uživatel hlavní aplikace možnost změnit své heslo[[1]](#endnote-1) ?
 |  |
| 1. Když změníte uživateli heslo v LDAPu, může se uživatel s novým heslem přihlásit do aplikace[[2]](#endnote-2)?
 |  |
| 1. Jsou aplikace funkční po restartu operačního systému[[3]](#endnote-3)? Pokud ne, tak vypište, které nefungují.
 |  |

## Bezpečnost operačního systému

|  |  |
| --- | --- |
| 1. Jsou nainstalovány poslední aktualizace pro operační systém[[4]](#endnote-4)? Pokud ne, kolik aktualizací je připraveno k instalaci?
 |  |
| 1. Instalují se bezpečnostní aktualizace automaticky[[5]](#endnote-5)?
 |  |
| 1. Vypište zbytečně spuštěné síťové služby – čísla portů, názvy aplikací[[6]](#endnote-6).
 |  |
| 1. Hesla – jsou na serveru uživatelé bez hesel? Pokud ano, vypište je.[[7]](#endnote-7)
 |  |
| 1. Sudo – je potřeba zadat heslo uživatele?[[8]](#endnote-8)
 |  |
| 1. Jaké je skóre programu lynis?[[9]](#endnote-9)
 |  |
| 1. Lze se ptát LDAP serveru přes síť bez zabezpečení[[10]](#endnote-10)?
 |  |

## Zabezpečení SSH

|  |  |
| --- | --- |
| 1. SSH – je zakázáno přihlašování pod uživatelem root? Pokud se může uživatel root přihlásit pouze z omezené sítě, tak ji vypište[[11]](#endnote-11).
 |  |
| 1. SSH – je zakázáno přihlašování pomocí hesla[[12]](#endnote-12)? Přihlašování pomocí hesla může být povoleno pro některé uživatele či z části sítě – pokud ano, tak rozepište kdo a odkud.
 |  |
| 1. SSH – je omezeno přihlašování pouze pro vybraná uživatelská jména či vybrané skupiny[[13]](#endnote-13)? Pokud ano, tak vypište uživatele/skupiny.
 |  |
| 1. SSH – loguje se konkrétní klíč, který uživatel použil pro přihlášení[[14]](#endnote-14)?
 |  |
| 1. SSH – vypište jednotlivé typy a délky klíčů, kterými se autentizuje SSH server. Splňují požadavek na 128bitovou sílu zabezpečení? [[15]](#endnote-15)?
 |  |

## HTTP/HTTPS

|  |  |
| --- | --- |
| 1. Jsou přesměrovány všechny http://bisxxx.vse.cz požadavky na https? Pokud ne, tak pro které je výjimka? [[16]](#endnote-16)
 |  |
| 1. Jaké je hodnocení https serveru v testu na SSLLabs[[17]](#endnote-17)?
 |  |
| 1. Jsou v HTTPS zakázány protokoly TLS 1.0 a TLS 1.1[[18]](#endnote-18)?
 |  |
| 1. Je nastaven HTTP Strict Transport Security?[[19]](#endnote-19)
 |  |
| 1. Je certifikát platný? Od které veřejné certifikační autority? [[20]](#endnote-20)
 |  |
| 1. Podporuje server OCSP stapling?[[21]](#endnote-21)
 |  |
| 1. Podporuje webserver protokol HTTP/2[[22]](#endnote-22)
 |  |
| 1. Je aplikace dostupná přes nešifrované spojení při zadání IP adresy (např. [http://146.102.54*.nn*](http://146.102.54.nn) či [*http://146.102.54.nn/aplikace*](http://146.102.54.nn/aplikace)*)*)? [[23]](#endnote-23)

Pokud ano, napište URL, přes které je dostupná. Ověřte i případnou aplikaci pro změnu hesla (např. <http://146.102.54.nn/heslo/> ). |  |
| 1. Je nainstalována aplikace Ldap account manager? Pokud ano, jsou v ní změněna obě počáteční hesla pro správu[[24]](#endnote-24) ?
 |  |
| 1. Co se vrací při dotazu curl <http://146.102.54.xxx/lam/> z Vašeho serveru[[25]](#endnote-25)?

a) přesměrování na https,b) odkaz na aplikaci LAM,c) spojení se odmítá |  |
| 1. Je webová aplikace pro správu LDAPu dostupná z Internetu?[[26]](#endnote-26)
 |  |
| 1. Jaké je hodnocení úvodní stránky aplikace v testu na <https://securityheaders.com/> [[27]](#endnote-27)?
 |  |
| 1. Jaké je hodnocení úvodní stránky aplikace na <https://observatory.mozilla.org/> [[28]](#endnote-28)?
 |  |
| 1. Lze získat další certifikát od Let’s Encrypt [[29]](#endnote-29)?
 |  |
| 1. Splňuje certifikát serveru požadavek na 128 bitovou sílu zabezpečení [[30]](#endnote-30)?
 |  |

## Nadstandardní požadavky

|  |  |
| --- | --- |
| 1. Je nainstalováno ModSecurity?[[31]](#endnote-31). Jsou vidět v logách nějaké zachycené útoky?
 |  |
| 1. Je nainstalován fail2ban či aplikace crowdsec?[[32]](#endnote-32) Kolik IP adres se zablokovalo za poslední týden?
 |  |
| 1. SSH – používá se pro přihlášení vícefaktorová autentizace[[33]](#endnote-33)?
 |  |
| 1. Aplikace – musí se správce, popř. všichni uživatelé hlásit pomocí vícefaktorové autentizace?
 |  |
| 1. Lze stáhnout soubor security.txt z <https://bisxxx.vse.cz/.well-known/security.txt> [[34]](#endnote-34)?
* je podepsán pomocí PGP?
* lze stáhnout PGP veřejný klíč?
 |  |

## Vysvětlivky:

1. **Má uživatel hlavní aplikace možnost změnit své heslo?** Tj. zda se může přihlásit např. do aplikace Ldap Account Manager a v ní si změnit heslo. Změna hesla ve vlastní aplikaci nemusí být funkční a v 95% případů ani funkční nebude (skrz aplikaci obvykle nelze měnit hesla v LDAPu). [↑](#endnote-ref-1)
2. **Když změníte uživateli heslo v LDAPu, může se uživatel s novým heslem přihlásit do aplikace?** Toto je základní kontrola, že se uživatelé ověřují vůči LDAPu. [↑](#endnote-ref-2)
3. **Je aplikace funkční po restartu operačního systému**? Zkontrolujte, že se potřebné aplikace spustí i po restartu operačního systému. **Pozor!!! tento test dělejte jako poslední, neboť se může stát, že se server nespustí.** Restart se provede privilegovaným příkazem

 reboot

Po restartu je potřeba zkontrolovat, zda se přihlásíte přes SSH a zda jsou aplikace funkční.

Seznam automaticky spouštěných aplikací lze vypsat pomocí

 systemctl list-unit-files | grep enabled

Automatické spuštění aplikace appxxx se nastaví pomocí

 systemctl enable appxxx [↑](#endnote-ref-3)
4. **Jsou nainstalovány poslední aktualizace pro operační systém**? Nejdříve je potřeba zaktualizovat seznam dostupných verzí jednotlivých programů pomocí příkazu:

 apt update

Seznam dostupných aktualizací se vypíše příkazem:

 apt list --upgradable

Nainstalovat dostupné aktualizace lze pomocí příkazu

 apt upgrade [↑](#endnote-ref-4)
5. **Instalují se bezpečnostní aktualizace automaticky**? Viz [How to perform unattended upgrades](https://blog.sleeplessbeastie.eu/2015/01/02/how-to-perform-unattended-upgrades/) či [Using unattended-upgrades on Debian and Ubuntu](http://linux-audit.com/using-unattended-upgrades-on-debian-and-ubuntu/). Automatická aktualizace zajišťuje balíček unattended-upgrades a řídí se pomocí dvou souborů v adresáři /etc/apt/apt.conf.d. Soubor 10periodic:

APT::Periodic::Update-Package-Lists "1";

APT::Periodic::AutocleanInterval "7";

APT::Periodic::Unattended-Upgrade "1";

První řádek udává, že se každý den má provést aktualizace balíčků (v podstatě příkaz apt-get update), druhý řádek udává, že každý týden se má vyčistit disk od starých souborů, třetí řádek udává, že každý den se má provést apt-get upgrade. Které balíčky se mají upgradovat je popsáno v souboru 50unattended-upgrades – je nastaveno, že se mají upgradovat balíčky ze základní distribuce a bezpečnostní opravy. Historie aktualizací je v logu /var/log/apt/history.log. [↑](#endnote-ref-5)
6. **Vypište síťové služby, které nejsou potřeba**? Seznam otevřených síťových portů lze vypsat pomocí příkazu:

netstat –luntp

Následuje ukázkový výpis:

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:37194 0.0.0.0:\* LISTEN 455/rpc.statd

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN 446/rpcbind

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 474/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 595/master

tcp6 0 0 :::111 :::\* LISTEN 446/rpcbind

tcp6 0 0 :::22 :::\* LISTEN 474/sshd

tcp6 0 0 :::44855 :::\* LISTEN 455/rpc.statd

udp 0 0 0.0.0.0:43558 0.0.0.0:\* 455/rpc.statd

udp 0 0 0.0.0.0:68 0.0.0.0:\* 405/dhclient

udp 0 0 0.0.0.0:12113 0.0.0.0:\* 405/dhclient

udp 0 0 0.0.0.0:621 0.0.0.0:\* 446/rpcbind

udp 0 0 0.0.0.0:111 0.0.0.0:\* 446/rpcbind

udp 0 0 127.0.0.1:632 0.0.0.0:\* 455/rpc.statd

udp 0 0 0.0.0.0:46773 0.0.0.0:\* 244/systemd-timesyn

udp6 0 0 :::621 :::\* 446/rpcbind

udp6 0 0 :::111 :::\* 446/rpcbind

udp6 0 0 :::37533 :::\* 455/rpc.statd

udp6 0 0 :::9652 :::\* 405/dhclient

Ve výpisu lze vidět otevřené porty pro protokoly TCP a UDP (viz první sloupec, tcp a udp označují služby pouze pro IPv4, tcp6 a udp6 označují služby otevřené pro IPv6). Je potřeba se podívat do čtvrtého sloupce (Local Address), z kterého lze zjistit na jaké lokální adrese a jakém portu je služba otevřena. Pokud je to na adrese [127.0.0.1](http://en.wikipedia.org/wiki/Localhost), tak je služba dostupná pouze lokálně a ne ze světa. V posledním sloupci je číslo a jméno procesu.

K rušení služeb nelze přistupovat bez rozmyslu. Např. systemd-timesync je proces pro časovou synchronizaci, dhclient obsluhuje získávání IP adresy přes DHCP. [↑](#endnote-ref-6)
7. **Hesla – jsou na serveru uživatelé bez hesel? Pokud ano, vypište je.** Uživatelské účty operačního systému jsou uloženy v souboru /etc/passwd. Hesla jsou v souboru /etc/shadow – každý řádek obsahuje více údajů oddělených dvojtečkou. Druhá položka obsahuje heslo zahešované pomocí některého algoritmu (začátek $6$ označuje použití algoritmu SHA512). Pokud položka obsahuje znaky jako \* či !, tak se nelze přihlásit. Pokud je položka prázdná, tak uživatel nemá heslo a lze se přihlásit bez hesla. [↑](#endnote-ref-7)
8. **Sudo – je potřeba zadat heslo uživatele?** Konfigurace programu sudo je v souboru /etc/sudoers. Následující řádek říká, že členové skupiny sudo mohou spouštět libovolné příkazy:

%sudo ALL=(ALL:ALL) ALL

Pokud je na řádku parametr NOPASSWD:, tak nemusí zadávat heslo. Toto není doporučované nastavení. [↑](#endnote-ref-8)
9. Jaké je skóre programu lynis? [Lynis](https://cisofy.com/lynis/) je open source security auditing tool. Můžete ho nainstalovat pomocí

apt install lynis

Kontrola se spouští příkazem:

lynis audit system

V repozitářích Debianu je starší verze. Pokud chcete aktuální, tak se podívejte na https://packages.cisofy.com/community/. [↑](#endnote-ref-9)
10. **Je LDAP server dostupný nezabezpečeně přes síť?** LDAP server obsahuje uživatelská jména a hesla uživatelů. LDAP podporuje komunikaci přes nezabezpečený port (389) či přes implicitní TLS port (636). Port 389 by neměl být ze sítě dostupný, aby ani omylem se nestalo, že se přes nezabezpečené spojení budou přenášet autentizační údaje uživatelů. Port 389 může být otevřen na rozhraní loopback (IP adresa 127.0.0.1). Není nutné zprovoznit TLS komunikaci, tj. port 636. Vhodnější je komunikovat přes SSH tunel.

Zabezpečení ssh.

Nejdříve se aspoň zběžně seznamte s doporučeními ve článku Top 20 OpenSSH Server Best Security Practices - <http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html> [↑](#endnote-ref-10)
11. **SSH – je zakázáno přihlašování pod uživatelem root? Popř. může se uživatel root přihlásit pouze z omezené sítě?** Úplné zablokování přihlašování uživatele root přes ssh může komplikovat správu serverů – hlavně v situaci, kdy se spravuje velké množství serverů. Variantou úplného zákazu je omezení pouze na bezpečné IP adresy. Následuje ukázka zápisu v konfiguračním souboru /etc/ssh/sshd\_config:

PermitRootLogin no

Match address 146.102.0.0/16,2001:718:1e02::/48,127.0.0.1/32,::1/128

 PermitRootLogin without-password

Parametr Match začíná sekci – zadává se filtr, pro které klienty se mají parametry v sekci použít.. Všechny následující parametry patří pro uvedenou sekci a to i v případě, že nejsou uvozeny mezerami. Sekce končí buď dalším parametrem Match či koncem souboru. [↑](#endnote-ref-11)
12. **SSH – je zakázáno přihlašování pomocí hesla?** Mělo by být povoleno pouze přihlašování pomocí klíče, popř. pomocí tokenu od Kerberose. Přihlašování heslem se v konfiguraci /etc/ssh/sshd\_config zakáže řádkem:

 PasswordAuthentication no

Podívejte se do logu /var/log/auth.log (popř. do starších jako je auth.log.1, auth.log.2.gz, auth.3.log.gz) a spočítejte si, kolik bylo na serveru neoprávněných pokusů o přihlášení. [↑](#endnote-ref-12)
13. **SSH – je omezeno přihlašování pouze pro vybraná uživatelská jména?** Dobrou praxí je omezit v konfiguračním souboru uživatele či uživatelské skupiny, které se mohou přihlásit. Používají se k tomu následující direktivy v konfiguračním souboru:

AllowGroups

DenyGroups

AllowUsers

DenyUsers

Při instalaci serverů jsem omezil přihlašování pomocí následující direktivy:

AllowGroups root sudo users [↑](#endnote-ref-13)
14. **SSH – loguje se konkrétní klíč, který byl použit pro přihlášení?** V jednom souboru authorized\_keys může být více klíčů. Je poté více než vhodné logovat, který klíč byl použit pro přihlášení. Při standardní instalaci ssh to nelze zjistit, je potřeba nastavit úroveň logování na verbose (již nastaveno ode mne):

LogLevel VERBOSE

Přihlašování se loguje v souboru /var/log/auth.log.

Popisy: [Log key fingerprints used to login via SSH](http://jpmens.net/2012/09/10/log-keys-used-to-log-in-via-ssh/)

[How to log history and logins from multiple ssh-keys under one user account](http://www.screenage.de/blog/2012/02/10/how-to-log-history-and-logins-from-multiple-ssh-keys-under-one-user-account-with-puppet/). [↑](#endnote-ref-14)
15. **SSH – – vypište jednotlivé typy a délky klíčů, kterými se autentizuje SSH server. Splňují požadavek na 128bitovou sílu zabezpečení?**

V konfiguračním souboru /etc/ssh/sshd\_config jsou uvedeny soubory s klíči pro server, např.

HostKey /etc/ssh/ssh\_host\_rsa\_key

HostKey /etc/ssh/ssh\_host\_ecdsa\_key

HostKey /etc/ssh/ssh\_host\_ed25519\_key

Pomocí programu ssh-keygen s parametry -l -f <file> si můžete vypsat informace o klíčích, např.

ssh-keygen -l -f /etc/ssh/ssh\_host\_rsa\_key

Nové klíče pro sshd se generují též pomocí programu ssh-keygen. Příkazy

ssh-keygen -t rsa -f /etc/ssh/ssh\_host\_rsa\_key -N ""

ssh-keygen -t ecdsa -f /etc/ssh/ssh\_host\_ecdsa\_key -N ""

ssh-keygen -t ed25519 -f /etc/ssh/ssh\_host\_ed25519\_key -N ""

Pomocí přepínače -b lze zadat délku v bitech (pouze pro RSA a ECDSA):

ssh-keygen -t rsa -b 3072 -f /etc/ssh/ssh\_host\_rsa\_key -N ""

ssh-keygen -t ecdsa -b 384 -f /etc/ssh/ssh\_host\_ecdsa\_key -N ""

|  |
| --- |
| **Další informace k zabezpečení SSH:** [Top 20 OpenSSH Server Best Security Practices](http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html) [Getting started with SSH security and configuration](https://www.ibm.com/developerworks/aix/library/au-sshsecurity/) [More Secure SSH Connections](http://www.linuxjournal.com/content/more-secure-ssh-connections) |

 [↑](#endnote-ref-15)
16. Jsou webové aplikace s přihlašováním dostupné pouze přes https? Přečtěte si [Transport Layer Protection Cheat Sheet](https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) na serveru owasp.org. Hlavně následující krátké odstavce:

Rule - Use TLS for All Login Pages and All Authenticated Pages

Rule - Use TLS on Any Networks (External and Internal) Transmitting Sensitive Data

Rule - Do Not Provide Non-TLS Pages for Secure Content

Rule - Do Not Mix TLS and Non-TLS Content [↑](#endnote-ref-16)
17. **Jaké je hodnocení https serveru v testu na SSLLabs?** Prostřednictvím SSLLabs otestujte nastavení https. Měli byste dosáhnout minimálně úrovně A. Pokud máte self-signed či neplatný certifikát, tak se Vám zobrazí hodnocení T a pod ním malým písmem hodnocení při ignorování problémů certifikátu. [↑](#endnote-ref-17)
18. **Jsou v HTTPS zakázány protokoly TLS 1.0 a TLS 1.1?**

Od začátku roku 2020 nebudou prohlížeče podporovat tyto dva staré protokoly z bezpečnostních důvodů. Server by je neměl nabízet. [↑](#endnote-ref-18)
19. **Je nastavena hlavička** [**HTTP Strict Transport Security**](http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security)**?** Pokud prohlížeč na webu zjistí příznak HSTS, tak již všechny své další požadavky bude posílat pouze na zabezpečení připojení (https) a to i v případě, že v html stránce bude odkaz pouze pomocí http. Informaci o nastavení HSTS si prohlížeč pamatuje do příště.

Popis nastavení pro apache najdete na [owasp.org](https://www.owasp.org/index.php/HTTP_Strict_Transport_Security) i [mnoha dalších stránkách](https://encrypted.google.com/search?q=HTTP+Strict+Transport+Security+apache&ie=utf-8&oe=utf-8&aq=t). [↑](#endnote-ref-19)
20. **Je certifikát platný? Je podepsán veřejnou certifikační autoritou?** Zkontrolujte, zda je certifikát platný, tj. obsahuje správné jméno, není prošlý, není na seznamu revokovaných certifikátů (ne pro selfsigned certifikáty). Zkontrolujte, zda je podepsaný nějakou certifikační autoritou, která je přítomna ve většině prohlížečů/operačních systémů. [↑](#endnote-ref-20)
21. **Podporuje OCSP stapling?** Server může posílat sám údaje pro ověření, že certifikát není revokován. Viz <https://en.wikipedia.org/wiki/OCSP_stapling>.

Otestovat lze přes SSLLabs či pomocí příkazu:

openssl s\_client -connect bis.vse.cz:443 -servername bis.vse.cz –status

který musí vrátit „OCSP Response Data:“. [↑](#endnote-ref-21)
22. **Používá server HTTP/2**?

Cílem nové verze protokolu [HTTP/2](http://en.wikipedia.org/wiki/HTTP/2) (schválen v roce 2015) je urychlit načítání informací z webových serverů, hlavně při přístupu přes HTTPS. Apache v defaultní konfiguraci nemá zapnutu podporu protokolu HTTP/2.

Podporu HTTP/2 lze otestovat na stránce <https://tools.keycdn.com/http2-test> či pomocí aplikace curl ( curl –http2 https://bis.vse.cz/ ). [↑](#endnote-ref-22)
23. **Co se vrací při http dotazu přes IP adresu?**

Při zabezpečení serveru se občas zapomene na možnost přístupu přes IP adresu. Pokud někdo zkusí přístup přes IP adresu (tj. nezadá v http požadavku Host či zadá IP adresu či chybné jméno), tak by server měl mít jednu z následujících akcí:

odmítnout spojení (vrátit chybovou zprávu),

přesměrovat na https

Pokud vrátí cokoliv jiného, tak je to špatně – aplikace je obvykle dostupná přes http (a lze to zneužít např. v phishingových kampaních). Výjimkou jsou požadavky na ověření správy serveru při získávání certifikátu Let’s Encrypt.

Zkuste nejen úvodní stránku (<http://146.102.54.nn> – za nn doplňte příslušné číslo serveru, je to překlad doménového jména na IP adresu), ale i URL odpovídající adrese aplikace (např. <http://146.102.54.nn/aplikace> - odvoďte z URL pro aplikaci). Někdy prohlížeče blokují odkazy s IP adresou (závisí na antivirovém programu i nastavení prohlížeče), doporučuji testovat pomocí programu curl např. z Vašeho serveru či z bis.vse.cz (curl -i http://146.102.54.nn/). [↑](#endnote-ref-23)
24. **Je nainstalována aplikace Ldap account manager? Pokud ano, jsou v ní změněna obě počáteční hesla pro správu?**

Aplikace LAM se instaluje s heslem lam pro správu profilů a pro úpravy prvního profilu. Správce by měl tato počáteční hesla změnit, jinak kdokoliv může dělat úpravy. [↑](#endnote-ref-24)
25. **Co se vrací při dotazu curl http://146.102.54.xxx/lam/ z Vašeho serveru?**

Je to obdoba testu přes IP adresu o kousek výše – zde je ale zaměřena na konkrétní aplikaci. Vhodnou odpovědí je zablokování přístupu či přesměrování na https. [↑](#endnote-ref-25)
26. Ldap account manager (či jiné obdobné aplikace pro administraci) by měli být dostupné pouze ze školní sítě a ne obecně z Internetu pro různé útočníky. Pro apache 2.4 se filtrování nastavuje pomocí require – viz <https://httpd.apache.org/docs/2.4/howto/access.html>. Další příklady jsou na <http://www.the-art-of-web.com/system/apache-authorization/>.

Otestování je jednoduché – je potřeba vyzkoušet přístup ze školy a z Internetu. Můžete k tomu využít online proxy (např. <https://www.proxysite.com/>) či on-line testy webových stránek, např. https://www.webpagetest.org/. [↑](#endnote-ref-26)
27. **Jaké je hodnocení úvodní stránky aplikace v testu na** [**https://securityheaders.com/**](https://securityheaders.com/) **?**

Neměl by být problém dosáhnout hodnocení B či lepšího. Na webu jsou i popisy významu jednotlivých hlaviček i popisy jejich nastavení. [↑](#endnote-ref-27)
28. **Jaké je hodnocení úvodní stránky aplikace na** [**https://observatory.mozilla.org/**](https://observatory.mozilla.org/) **?**

Zde se hodnotí i kvalita nastavení hlavičky CSP či parametry u cookies. Měli byste dosáhnout minimálně hodnocení B. [↑](#endnote-ref-28)
29. **Lze získat další certifikát od Let’s Encrypt**? Certifikáty od Let’s Encrypt jsou platné 90 dní, obvykle po 70-75 dnech se certifikát aktualizuje. Konfigurace webového serveru musí umožnit aktualizaci certifikátu.

Pokud se používá pro získávání certifikátů aplikace certbot, tak můžete ověřit možnost získání (tj. správnou konfiguraci) pomocí příkazu

certbot renew --dry-run

Aplikace certbot zkusí získat nový certifikát, na konci však neaktualizuje aktuální certifikát. **Pozor!!!** je omezen počet pokusů za den pro zkoušení získání certifikátů pro jeden server (odhadem 5 pokusů za den). [↑](#endnote-ref-29)
30. Splňuje certifikát serveru požadavek na 128 bitovou sílu zabezpečení?

Jen připomínám, že v případě RSA je potřeba délka klíče 3072 bitů, v případě ECDSA stačí 256 bitů.

Jak vygenerovat nový certifikát (přejít na jinou délku, přejít na ECDSA) je popsáno v dokumentaci certbot. Jen si dávejte pozor, pro jakou verzi certbot je konkrétní dokumentace. Pro verzi 1.12 je např. na

<https://www.interhacktive.de/certbot/using.html> [↑](#endnote-ref-30)
31. **Je nainstalováno ModSecurity**? ModSecurity je Web Application Firewall. Do verze 3.x to byl modul do Apache, od verze 3.x je to samostatná aplikace/knihovna s konektory z příslušných webových serverů (tj. rozšíření podpory na Nginx, Varnish, IIS, …). Není zatím kompletní, pro apache je doporučeno stále používat modul do apache z verze 2.x. V Debianu/Ubuntu se balíček jmenuje libapache2-mod-security2, postup instalace a konfigurace je např. na <https://www.linuxbabe.com/security/modsecurity-apache-debian-ubuntu>.

Modul nestačí nainstalovat, je nutné ho povolit a nakonfigurovat. Modul může fungovat v režimu detekce či v režimu blokování. Při blokování se může část webu/aplikace znepřístupnit. [↑](#endnote-ref-31)
32. **Je nainstalován fail2ban**? Fail2ban prochází logy (standardně logy od SSH), hledá pokusy o hádání hesel a pokud z nějaké adresy je v krátkém čase větší počet pokusů o hádání hesel, tak uvedenou IP adresu zablokuje (může zablokovat). Krátký popis instalace je např. na <https://www.a2hosting.com/kb/security/hardening-a-server-with-fail2ban>. Pro efektivní blokování je potřeba mít nakonfigurování firewall. V Debianu přichází použití nftables či nadstavby ufw. Méně problémová je instalace obdobná aplikace crowdsec. Poznámky k instalaci fail2ban i crowdsec je na https://bis.vse.cz/dokuwiki/doku.php/fail2ban. [↑](#endnote-ref-32)
33. **SSH a vícefaktorová autentizace**. Nakonfigurujte SSH server tak, aby bylo možné se přihlásit buď pomocí klíče nebo pomocí hesla doplněného o TOTP (Google Authenticator). Jak nastavit? Na google hledejte „ssh google authenticator debian“ či „ssh two-factor authentication debian“. Z bis.vse.cz by mělo být možné se přihlásit bez 2FA. [↑](#endnote-ref-33)
34. **Lze stáhnout soubor security.txt z**[**https://bisxxx.vse.cz/.well-known/security.txt**](https://bisxxx.vse.cz/.well-known/security.txt)? Soubor security.txt sdílí kontakty pro nahlášení zranitelností. Popis je na <https://securitytxt.org/>, popř. na <https://www.michalspacek.cz/k-cemu-je-soubor-security.txt>. Soubor by měl být stažen přes https (tj. u požadavku na http musí být přesměrování na https).

Soubor by měl být podepsán pomocí PGP (formát cleartext), v souboru by měl být odkaz na stažení klíče PGP pro ověření podpisu a pro poslání zašifrované zprávy (obvykle je to stejný PGP klíč). [↑](#endnote-ref-34)