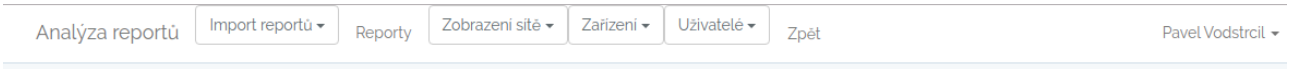
Příloha 2 – Stručný návod k ovládání aplikace

Po úspěšném rozbalení a zprovoznění celé aplikace má uživatel před sebou (po přihlášení) uživatelské menu, které je dostupné z kterékoliv části aplikace.



Popis položek menu:

- Import reportů
  - Obsahuje formuláře pro nahrání reportů (souborů .csv)
- Reporty
  - Obsahuje výpis reportů – níže popsáno
- Zobrazení sítě
  - Zobrazení dle sítí
    - Umožňuje uživateli postupně procházet celou síť
  - Zobrazení dle skupin
    - Zobrazení dle uživatelem definovaných skupin (nutno vytvořit ve správě skupin)
    - Jedno zařízení může být v neomezeně skupinách
  - Zobrazení dle typu zařízení
    - Funguje pouze pro uložená zařízení, funguje na základě uložené hodnoty v aktivech
  - Zobrazení dle kritičnosti
    - Funguje pouze pro uložená zařízení, funguje na základě uložené hodnoty v aktivech
  - Zobrazit všechny zařízení
    - Výpis všech uložených zařízení
  - Vyhledávání
    - Jednoduché vyhledávání – možnost hledat podle CVE, IP nebo části názvu řádku
  - Zobrazení dle hodnot
    - Funkce, která umožňuje zobrazit uživatelem definované rozpětí hodnot
  - Správa skupin zařízení
    - Jednoduchá správa skupin pro funkci „Zobrazení dle skupin“
- Zařízení
  - Zde má uživatel možnost spravovat aktiva.
  - Přidávat, editovat a mazat
  - Zde se vyplňují enviromentální hodnoty
- Uživatelé
  - Skupina funkcí pro přidání a jednoduchou správu uživatelů
  - Zde si může uživatel změnit svoje heslo
- Tlačítko zpět
- V pravé části je zobrazen právě přihlášený uživatel
  - možnost odhlášení a změna hesla právě přihlášeného uživatele

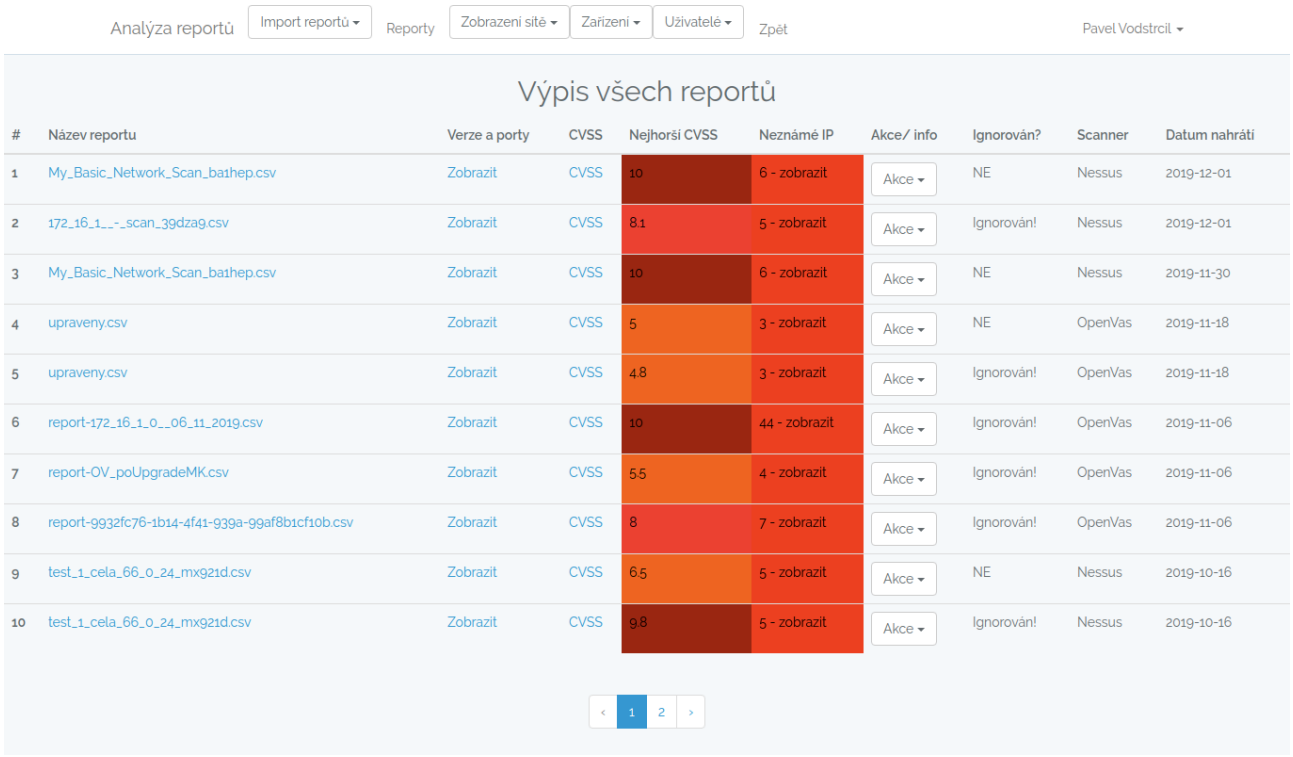
Nahrání reportu

Po zvolení správného formuláře (OpenVAS nebo Nessus) se zobrazí jednoduchý formulář ve kterém stačí vybrat soubor k nahrání. Musí být ve formátu .cvs (probíhá kontrola, ostatní formáty jsou odmítnuty).

Po nahrání automaticky započne dohledávání vektorů CVSS a výpočet. Tato operace je velmi náročná. Po celou dobu zpracování není uživatel nijak informován o stavu zpracování. Pouze na konci bude vypsána informativní hláška.

Po nahrání lze s reportem dále pracovat přes funkci reporty.

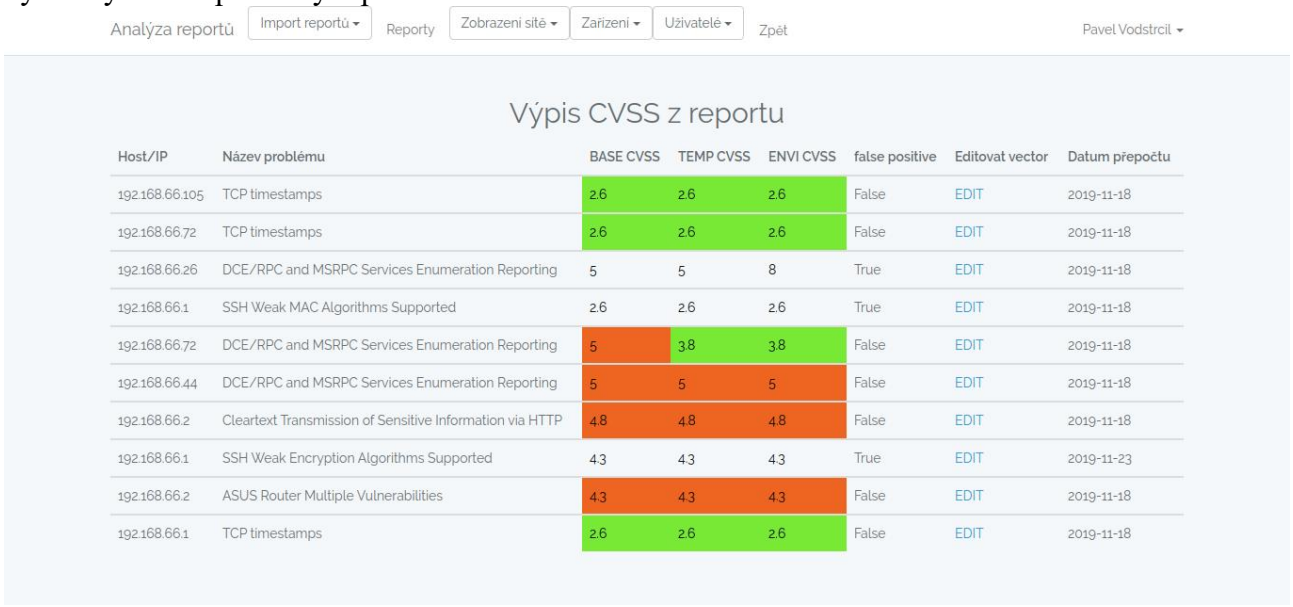
Funkce Reporty – zobrazení nahraných reportů



#	Název reportu	Verze a porty	CVSS	Nejhorší CVSS	Neznámé IP	Akce/ info	Ignorován?	Scanner	Datum nahrátí
1	My_Basic_Network_Scan_ba1hep.csv	Zobrazit	CVSS	10	6 - zobrazit	Akce	NE	Nessus	2019-12-01
2	172_16_1__-_scan_39dza9.csv	Zobrazit	CVSS	8.1	5 - zobrazit	Akce	Ignorován!	Nessus	2019-12-01
3	My_Basic_Network_Scan_ba1hep.csv	Zobrazit	CVSS	10	6 - zobrazit	Akce	NE	Nessus	2019-11-30
4	upraveny.csv	Zobrazit	CVSS	5	3 - zobrazit	Akce	NE	OpenVas	2019-11-18
5	upraveny.csv	Zobrazit	CVSS	4.8	3 - zobrazit	Akce	Ignorován!	OpenVas	2019-11-18
6	report-172_16_1_0__06_11_2019.csv	Zobrazit	CVSS	10	44 - zobrazit	Akce	Ignorován!	OpenVas	2019-11-06
7	report-OV_poUpgradeMK.csv	Zobrazit	CVSS	5.5	4 - zobrazit	Akce	Ignorován!	OpenVas	2019-11-06
8	report-9932fc76-1b14-4f41-939a-99af8b1cf10b.csv	Zobrazit	CVSS	8	7 - zobrazit	Akce	Ignorován!	OpenVas	2019-11-06
9	test_1_cela_66_0_24_mx921d.csv	Zobrazit	CVSS	6.5	5 - zobrazit	Akce	NE	Nessus	2019-10-16
10	test_1_cela_66_0_24_mx921d.csv	Zobrazit	CVSS	9.8	5 - zobrazit	Akce	Ignorován!	Nessus	2019-10-16

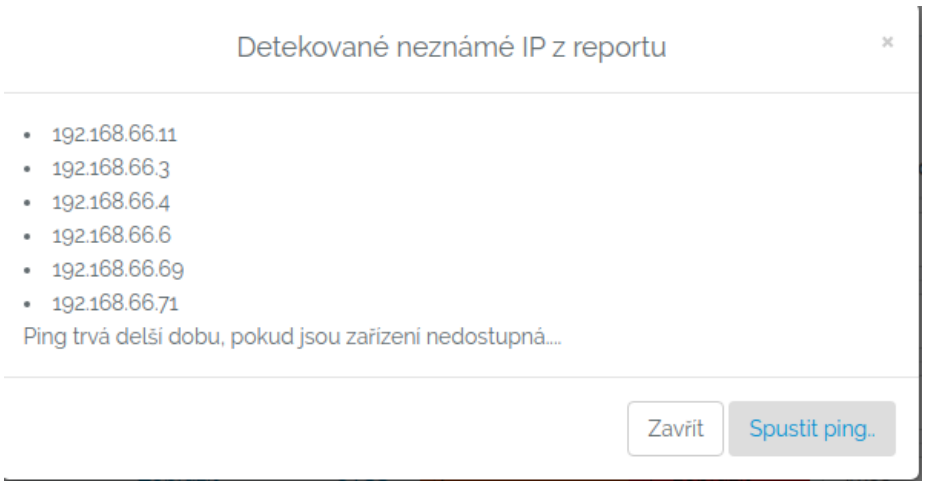
‹ 1 2 ›

Ve výpisu reportů má uživatel možnost, po kliknutí na název reportu, procházet jednotlivé reporty. Dále spustit detekci služeb a portů. Po kliknutí na odkaz CVSS se uživateli zobrazí nalezené výsledky CVSS pro daný report.



Host/IP	Název problému	BASE CVSS	TEMP CVSS	ENVI CVSS	false positive	Editovat vector	Datum přepočtu
192.168.66.105	TCP timestamps	2.6	2.6	2.6	False	EDIT	2019-11-18
192.168.66.72	TCP timestamps	2.6	2.6	2.6	False	EDIT	2019-11-18
192.168.66.26	DCE/RPC and MSRPC Services Enumeration Reporting	5	5	8	True	EDIT	2019-11-18
192.168.66.1	SSH Weak MAC Algorithms Supported	2.6	2.6	2.6	True	EDIT	2019-11-18
192.168.66.72	DCE/RPC and MSRPC Services Enumeration Reporting	5	3.8	3.8	False	EDIT	2019-11-18
192.168.66.44	DCE/RPC and MSRPC Services Enumeration Reporting	5	5	5	False	EDIT	2019-11-18
192.168.66.2	Cleartext Transmission of Sensitive Information via HTTP	4.8	4.8	4.8	False	EDIT	2019-11-18
192.168.66.1	SSH Weak Encryption Algorithms Supported	4.3	4.3	4.3	True	EDIT	2019-11-23
192.168.66.2	ASUS Router Multiple Vulnerabilities	4.3	4.3	4.3	False	EDIT	2019-11-18
192.168.66.1	TCP timestamps	2.6	2.6	2.6	False	EDIT	2019-11-18

Ve sloupci „Nejhorší CVSS“ je uživatel upozorňován na nejhorší vyhodnocené CVSS skóre z celého reportu (pokud je řádek v reportu označen jako falsePositive, je ignorován).



Po kliknutí na počet neznámých IP adres ve sloupci „Neznámé IP“ je uživateli zobrazeno okno s výčtem neznámých IP adres, které byly nalezeny v reportu a nejsou uložené v databázi aktiv.

Z tohoto dialogového okna má uživatel možnost spustit na všechny zobrazené IP adresy ping, aby mohl ověřit, že jsou opravdu v síti.

V nabídce Akce/info má uživatel informace o uživateli, který nahrál daný report, dále možnost tento report smazat a označit ho jako ignorovaný. Pokud uživatel označí report jako ignorovaný je ignorován v celé aplikaci pro vyhodnocování. Není tedy nutné starší reporty mazat, stačí jen označit jako ignorované. O stavu ignorování je uživatel informován v dalším sloupci.

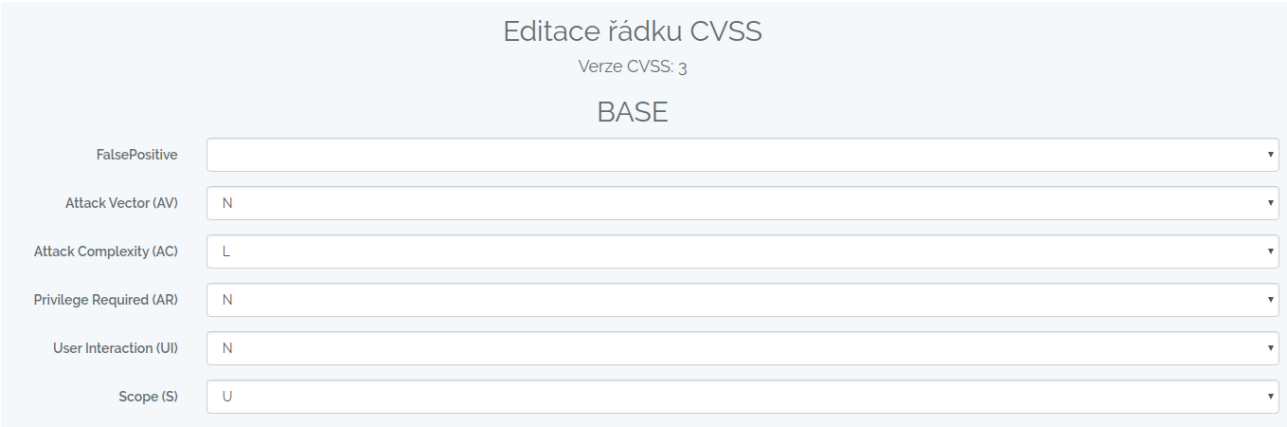
Editování vektoru pro výpočet CVSS

Po zpracování je složen pouze z vektoru, který byl nalezen v pluginu a enviromentálních hodnot aktiva (pokud jsou vyplněny).

Uživatel má stále možnost měnit jakoukoliv položku (i zkopírované z aktiv). K formuláři na změny je několik cest. Možnost je přímo ze zobrazení daného reportu, popřípadě z jakéhokoliv jiného zobrazení.

Formulář je obdobný pro oba skenery. Pouze formulář pro Nessus obsahuje položky CVSS verze 2 i 3. Hned v hlavičce je uživatel upozorněn na počítanou verzi. Pokud uživatel změní nebo vyplní položky, které nepatří do dané verze nebude aplikace s těmito hodnotami pracovat.

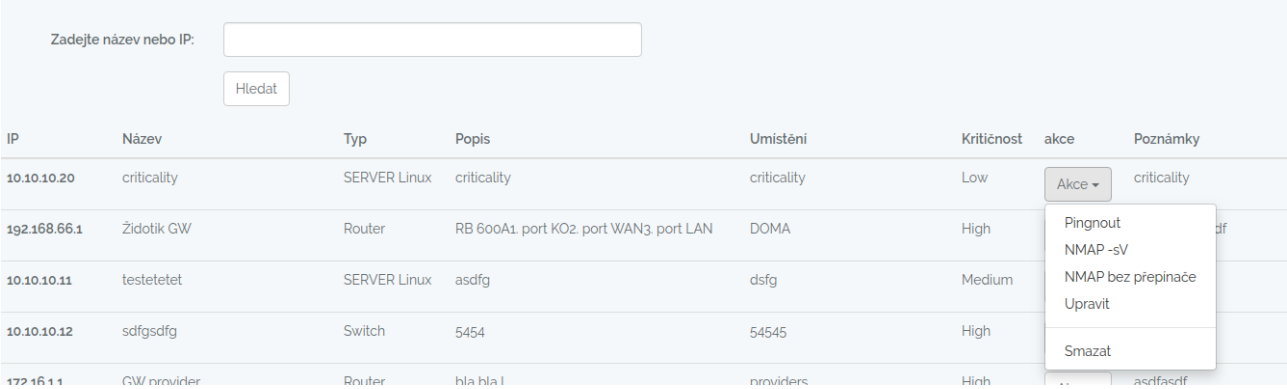
Po uložení se automaticky provede přepočet pro daný řádek a je uložen do databáze.



Ve formuláři jsou originální názvy, které jsou převzaty z dokumentace. Výsledný vektor není zobrazen, je uložen pouze výsledek do databáze.

Správa zařízení (aktiv)

Aplikace je vybavena jednoduchou správou zařízení. Ve správě zařízení je možné hledat zařízení podle názvu a IP adresy.

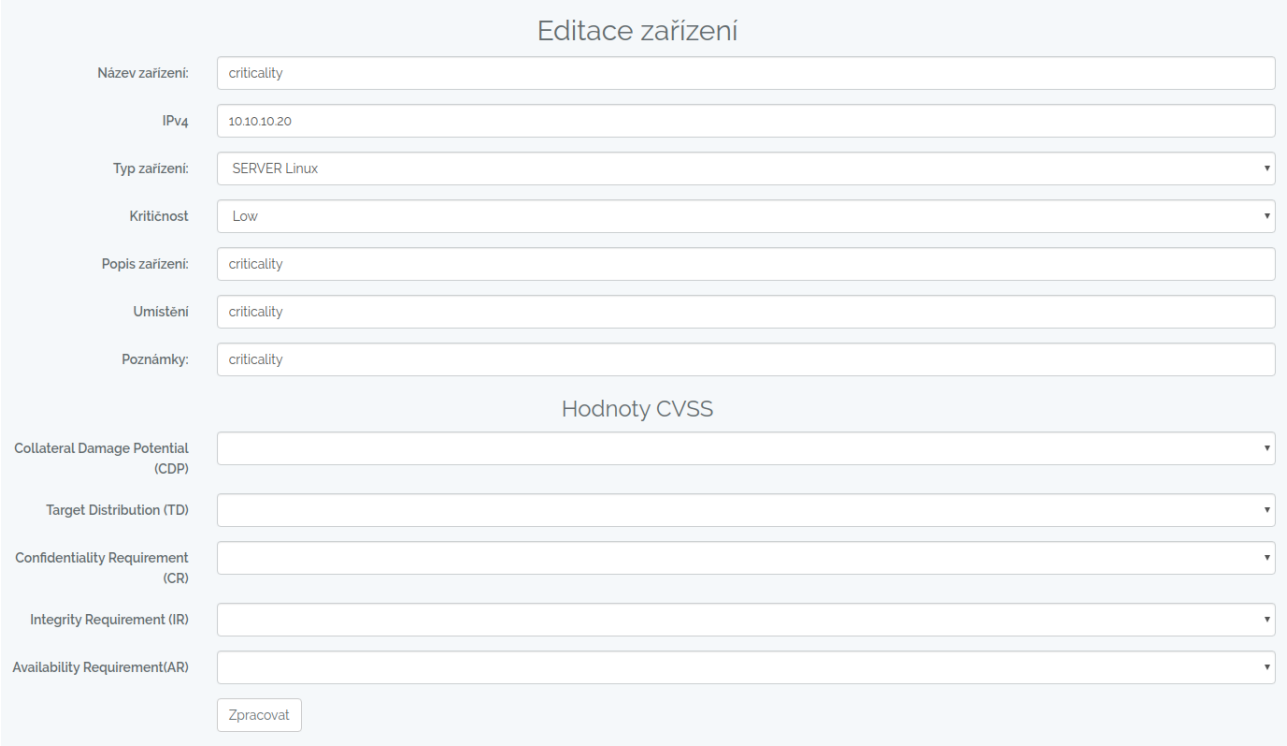


Pokud uživatel bude chtít přidat nové typy zařízení, musí tak učinit přímo v databázi, přidat záznam do tabulky „device_type“.

Pokud u zařízení nebude správně vyplněná IP adresa (pouze IPv4!) nebude správně fungovat doplňování enviromentálních hodnot při nahrání nového reportu.

Přidání a změna enviromentálních hodnot u uloženého zařízení

Pro změnu hodnot je nutné nejprve zařízení najít a poté přes menu akce → upravit přejít do editace daného zařízení.



Provedené změny hodnot se neprojeví v již nahraných reportech. Pokud uživatel chce, aby se tyto změny projevily, musí znova nahrát report, popřípadě udělat ručně změny u všech záznamů.