Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 2, 842 16 Bratislava 4

Pokrok dosiahnutý na deviatom šprinte

Tímový projekt

Tím č. 19

Vypracoval: Jakub Perdek
Vedúci projektu: Ing. Pavol Helebrandt Phd.

Pokrok dosiahnutý na deviatom šprinte

Na konci deviateho šprintu sa začalo používateľské testovanie. V priebehu tohto testovania sme identifikovali množstvo chýb pomocou vlastného logera s názvom Sentry a na základe zozbieranej spätnej väzby od používateľov. Používatelia siahali po používateľskej príručke a identifikovali nedostatky, ktoré sa ani po našom tímovom testovaní nepodarilo identifikovať. Očakávania boli rôzne. Aj napriek použitiu príručky používatelia očakávali viac logických problémov väčšiu zložitosť a viac scenárov. Ďalej by uvítali zahrnúť do používateľskej príručky aj konfiguráciu k BurpSuite nástroju. Aplikácia sa im aj napriek problémom páčila a posmeľujú k jej vylepšeniu.

Zabezpečiť plynulý chod pri testovaní bolo nevyhnutné. Logy sme pravidelne sledovali v Sentry a rovnako aj mailovú komunikáciu na ktorú sme pohotovo reagovali. Okrem samotných docker obrazov sme nakoniec sprístupnili aj pôvodný repozitár po jeho vyžiadaní. Väčšina emailov zahŕňala spätnú väzbu. Tú sme spracovali do excel dokumentu rozdelením na časť s identifikovanými chybami, ďalej na časť s pocitmi používateľov, návrhmi na vylepšenie a chválenú funkcionalitu. Podľa logov a spätnej väzby používatelia väčšinu scenárov úspešne dokončili.

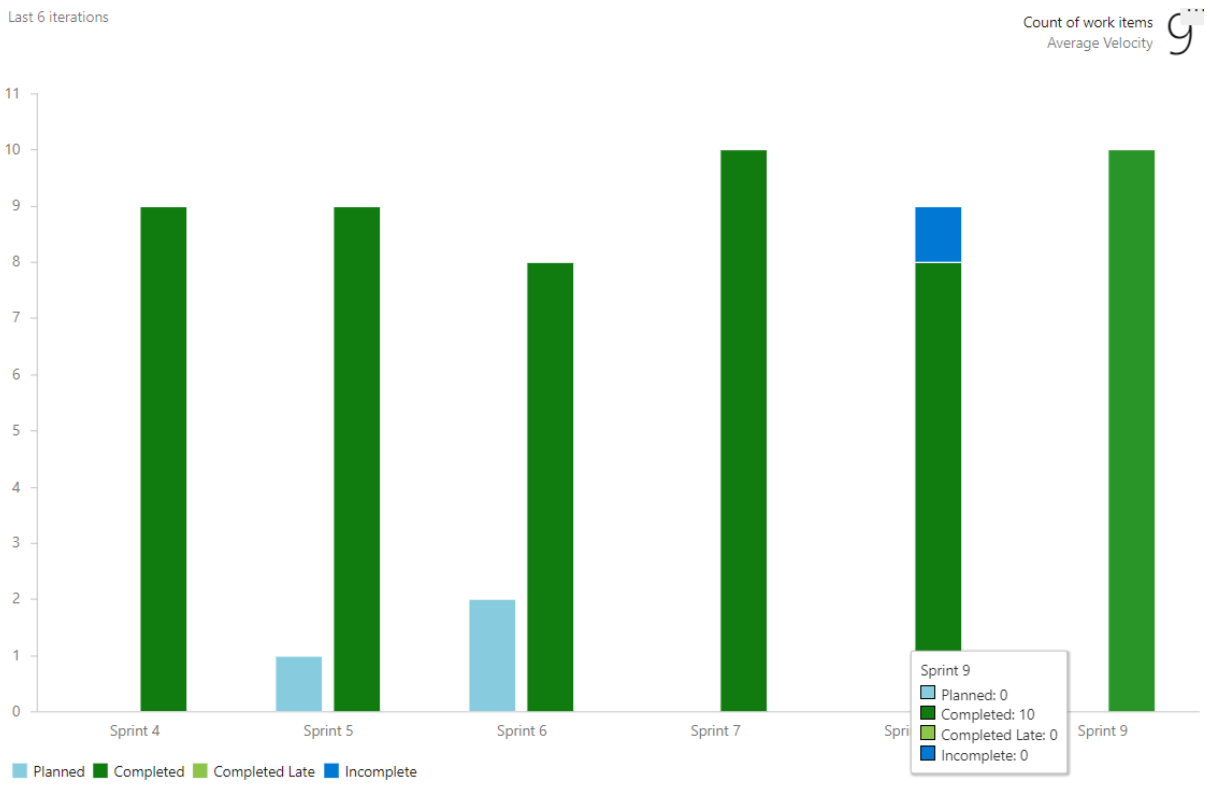
V šprinte sme pokračovali na vylepšeniach aplikácií. Konkrétne sme analyzovali možné vloženie referencie security eshopu do whois záznamov pre našu Whois aplikáciu. Lokálne nasadenie bolo znovu problematické. Docker compose na základe zistení neumožnil vygenerovať jedinečný identifikátor pre novú doménu, ale sa dal vložiť len ako premenná, buď pri volaní docker-compose alebo z .env súboru, prípadne iným spôsobom. Druhý problém bol závažnejší. Lokálne nasadenie pri zmene domény vyžaduje nastavenie domény v host súbore konkrétneho používateľa. Používateľ by tím vedel akú doménu bude vyhľadávať a bol by ešte viac zaťažený inštaláciou. Ďalším riešením je reverse proxy, ale aj to vyžaduje pluginy do prehliadača. Doména preto zostáva localhost a vo whois aplikácii bude potrebné zťažiť prístup k nej.

Vloženie záznamu o security eshope vyžadovalo aj zverejnenie nejakých zraniteľností. Boli preto vytvorené ďalšie tri tabuľky umožňujúce mapovať zraniteľnosti s ľahkým pridaním ďalšej a zmeny stupnice pre ich mieru nebezpečnosti. Po tvorbe záznamu Jakub pre ne pridal 2 záznamy o zraniteľnostiach v podobe nickov dvoch používateľov a upozornenie na únik citlivých údajov. Zároveň používateľ by mal byť motivovaný agregovať si doménu s najväčším počtom zraniteľností pomocou zložitej SQL injekcie, ktorú bude možné realizovať v hlavnom

vyhľadávacom okne. Funkcionalita ale umožňuje vrátenie len jedného záznamu, čo bude používateľ musieť pri SQL injekcii dodržať. Prístupná pre tento scenár bude aj schéma databázy, ktorou sa aplikácia na jednej obrazovke aj pochváli. Navrhli sme a vytvorili tak ďalší scenár a reagovali tak na požiadavku používateľov žiadajúcich scenáre nútiace rozmýšľať a vynájsť sa pri ich riešení. Vymyslenú doménu budeme ešte musieť v texte whois záznamu namapovať na aktuálny security eshop informáciou o zmene domény na localhost.

Peter analyzoval spätnú väzbu z google formulárov a aj ju spracoval do inžinierskeho diela. Zároveň sa venoval aj rozpracovanej session, ktorú sme ale do šprintu nezahrnuli. Pravdepodobne ju dokončí v nasledujúcom šprinte. Podarilo sa dokončiť aj funkcionalitu na backende implementujúcu riadenie prístupu na základe rolí, ktoré používateľ má. Jej tvorcom bol Viktor Matovič. Nikola sa snažil otestovať aplikáciu pomocou OWASP nástroja, ale pre nemožnosť zmeniť port z 8080 sa mu to nepodarilo.

V šprinte sme boli výkonní aj napriek tomu, že sme čakali na prvú spätnú väzbu od používateľov. Tú sme nielen zdokumentovali ale následne z nej aj vyriešili veľké množstvo problémov. Naša velocity bola preto jedna z najlepších doposiaľ dosiahnutých. Zobrazuje ju obrázok 1. Výkonnosť v šprinte zobrazuje obrázok 2.

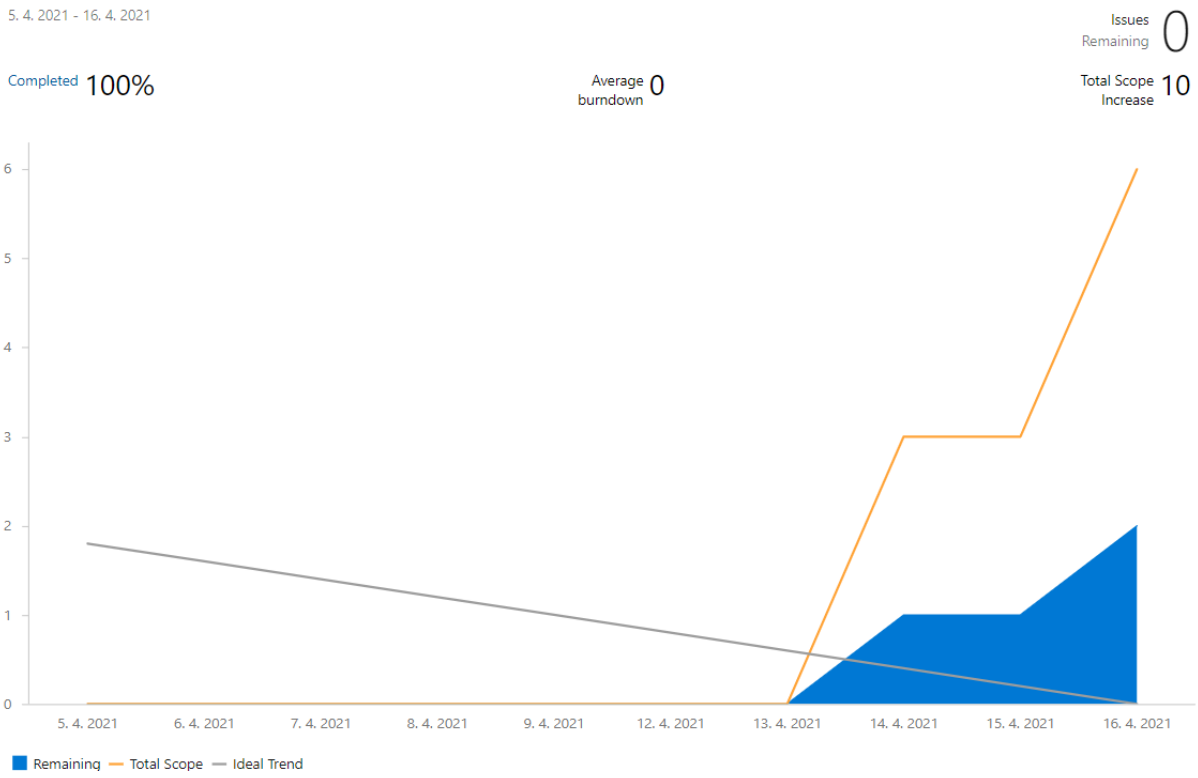


Obrázok 1: Velocity tímu v šprinte 9

V tomto šprinte sme realizovali úlohy zobrazené v tabuľke 1.

Pridelená úloha	Zodpovedný riešiteľ	Aktuálny stav rozpracovania (nedeľa 18. 04.)	Šprint
Implement role based access control	Viktor Matovič	dokončené	šprint č. 9
Create doc from user testing and sort information	Jakub Perdek	dokončené	šprint č. 9
Supply user testing - fixing fatal issues	Jakub Perdek Abd Alrahman Saleh	dokončené	šprint č. 9
Create scenario with Advanced SQL injection	Jakub Perdek	dokončené	šprint č. 9
Create tables for vurnerabilities and insert appropriate records	Jakub Perdek	dokončené	šprint č. 9
Create view with DB schema	Jakub Perdek	dokončené	šprint č. 9
Design SQL injection	Jakub Perdek	dokončené	šprint č. 9
Observe possibilities to change domain name for local deployed whois application	Jakub Perdek	dokončené	šprint č. 9
Create sprint progress and retrospective	Jakub Perdek	dokončené	šprint č. 9
Create user guide for advanced SQL injection scenario	Jakub Perdek	dokončené	šprint č. 9
Add local deployment parts and setup for BurpSuite to user guide	Jakub Perdek	dokončené	šprint č. 9
Analyse feedback from users	Peter Spusta	dokončené	šprint č. 9
Document user feedback from google forms	Peter Spusta	dokončené	šprint č. 9

Tabuľka 1: Úlohy z deviateho šprintu



Obrázok 2: Výkonnosť tímu v deviatom šprinte