POSUDEK BAKALÁŘSKÉ PRÁCE

Autor:	Tomáš Klouček
Název:	Časté zranitelnosti webových aplikací Zabezpečení webových aplikací v jazyce PHP
Posudek vypracoval:	vedoucí práce RNDr. Ondřej Žára

Cílem bakalářské práce je analýza pěti vybraných kategorií bezpečnostních zranitelností, jejich vysvětlení, detekce a náprava. Autor za tímto účelem nejprve sestavil webovou aplikaci v jazyce PHP a zahrnul do ní zmíněné zranitelnosti. Dále naimplementoval penetrační nástroj, který dokáže přítomnost těchto zranitelností ověřit prostřednictvím automatizovaných HTTP dotazů. Na závěr popsal, jak se tyto problémy dají opravit. Tím dostává práce drobný didaktický přesah, neboť ji lze následně použít při praktických ukázkách v kontextu výuky informační bezpečnosti.

V oblasti typografie s ohledem na použití školní TEX-ové šablony téměř není co vytknout. Jazykově je práce na průměrné úrovni, objevují se občasné překlepy a neobratnosti (*standart* namísto *standard*, číslice místo diakritiky u Listingu 5.1). V textu věnujícím se bezpečnosti by autor v kontextu úschovy hesel rozhodně neměl používat termín *zašifrovaná podoba*. K práci s použitými zdroji a citacemi nemám připomínek.

Výsledná aplikace je implementována v PHP, využívá databázi MariaDB a je určena ke snadnému zprovoznění pomocí technologie Docker. Penetrační skript je napsán v jazyce Python. Jak aplikace, tak skript jsou vybaveny automaticky generovanou dokumentací, což hodnotím pozitivně. Naopak nepříjemný dojem si odnáším z kapitoly o zranitelnosti XSS, která demonstruje především autorovo zmatení v této oblasti. Listing 5.22 totiž ukazuje ochranu, která patří do předchozí kapitoly (5.3.1, SQL), zatímco správná ochrana proti XSS je zmíněna jen zběžně teoreticky a v žádné ukázce se vůbec neobjevuje.

Autor sestavil aplikaci dle zadání, popsal a vysvětlil požadované zranitelnosti, vytvořil detekční nástroj a doporučil, jak kód vylepšit. S ohledem na výše uvedené připomínky však výsledek není perfektní, a proto navrhuji ohodnotit předloženou bakalářskou práci známkou **B – velmi dobře**.

V Praze dne 4. června 2024 RNDr. Ondřej Žára