

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

Whois aplikácia

*Vyhľadanie informácií o serveroch použitých v
scenároch*

Jakub Perdek

Študijný program: Informatika
Ročník: 4
Kružok: Str 14:00, DIGILAB
Predmet: Tímový projekt
Vedúci projektu: Ing. Pavol Helebrandt Phd.
Ak. rok: 2020/2021

1. Whois aplikácia pre vyhľadanie domény

Aplikácia slúži na vyhľadávanie informácií v databáze o konkrétnej doméne. Databáza je získaná z internetu a bude doplnená o ďalšie domény zahrnuté v scenároch. Dodatočne k informáciám o konkrétnej doméne môžu byť pridané aj potenciálne hrozby. Reprezentuje nástroj, na základe ktorého môže používateľ vyhľadať informácie o nájdených hrozbách a použiť ich pre potenciálny útok alebo obranu konkrétnej aplikácie. Zároveň sa predpokladá, že získa zručnosti pri práci s takýmto nástrojom. Navrhnutý dizajn má približovať meniacu sa sieť internetových prepojení.

2. Vyhľadanie domény

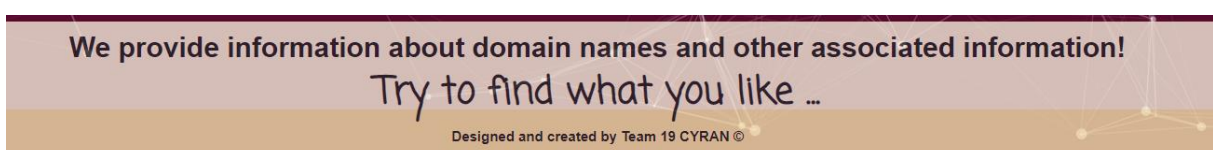
Používateľ po načítaní stránky vloží názov domény do okna v strede obrazovky a stlačí tlačidlo Search. Formulár je zobrazený na Obrázku 1. Reťazec je hľadaný v uprostred doménových mien. Výsledok môže obsahovať tento reťazec kdekoľvek v názve domény. Vrátenej je len jeden výsledok, preto by dopyt mal byť čo najpresnejší. Hlavnú stránku tvorí lista v hlavičke obsahujúce logo vľavo a menu tlačidlá na pravo. Lišta je zobrazená na Obrázku 2. Päta stránky informuje o možnostiach tohto webu. Na jej samom spodku sa nachádzajú informácie o tvorcach stránky. Päta je zobrazená na Obrázku 3.



Obrázok 1: Okno vyhľadávača



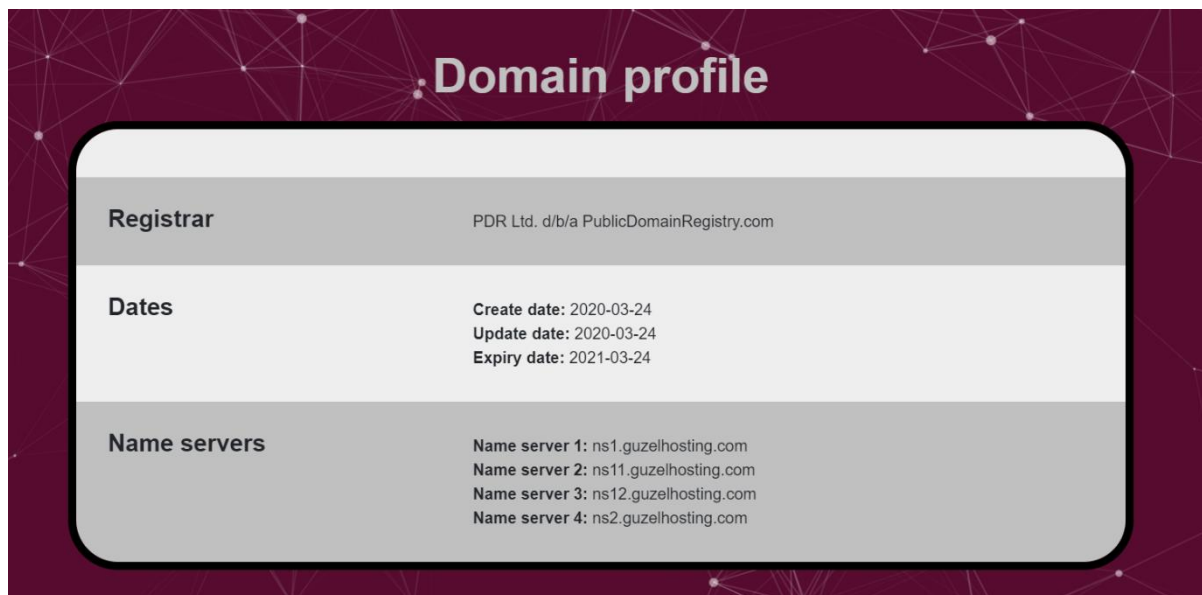
Obrázok 2: Navigácia vyhľadávača



Obrázok 3: Päta vyhľadávača

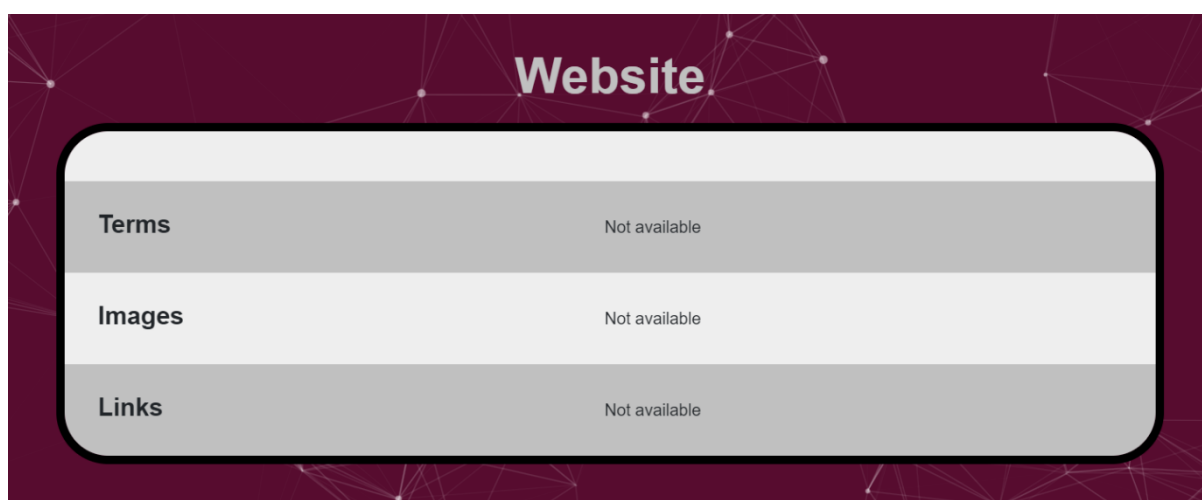
3. Informácie o vyhľadanej doméne

Pokiaľ bolo vyhľadanie úspešné zobrazia sa dostupné informácie o konkrétnej doméne. Zahŕňajú informácie o registračnej doméne, dátumoch vzniku, úpravy a doby platnosti. V základnom popise sú uvedené aj menné servery. Doménový profil je zobrazený na Obrázku 4.



Obrázok 4: Profil domény

Základné zozbierané informácie o stránke je možné uviesť a neskôr získať z časti pre informácie o stránke. Tvorí ju základná štatistika o výskyte termov, obrázkov a odkazov na stránke. V našom riešení tieto informácie neuvádzame ani nezberáme, ale v budúcnosti môže byť riešenie rozšírené o preliezač webu, ktorý získa tieto informácie. Táto časť je zobrazená na Obrázku 5.



Obrázok 5: Informácie o stránke

Whois Record

Domain: 01cukurovabims.com
Registrant:
Create date: 2020-03-24
Update date: 2020-03-24
Expiry date: 2021-03-24

Domain registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com
Domain registrar whois: whois.publicdomainregistry.com
Domain registrar url: http://www.publicdomainregistry.com

Registrant name: SELMAN SAGMEN
Registrant address: S.Cengiz KARACA Mah. 1048 Cad. 9/3
Registrant city: ANKARA
Registrant state: CANKAYA
Registrant zip: 06530
Registrant country: Turkey
Registrant email: frmseymen@gmail.com
Registrant phone: +90.5363013647

Obrázok 6: Podrobnejšie informácie

Administrative name: Guzel Hosting
Administrative company: GNET Internet Telekomunikasyon A.S.
Administrative address: Icerenkoy Mh. Ertac Sk. Ardil Is Merkezi No 4/2
Administrative city: Istanbul
Administrative state: Atasehir
Administrative zip: 34752
Administrative country: Turkey
Administrative email: alanadi@guzel.net.tr
Administrative phone: +90.908508850558

Technical name: Guzel Hosting
Technical company: GNET Internet Telekomunikasyon A.S.
Technical address: Icerenkoy Mh. Ertac Sk. Ardil Is Merkezi No 4/2
Technical city: Istanbul
Technical state: Atasehir
Technical zip: 34752
Technical country: Turkey
Technical email: alanadi@guzel.net.tr
Technical phone: +90.908508850558

Obrázok 7: Podrobnejšie informácie pokračovanie 1

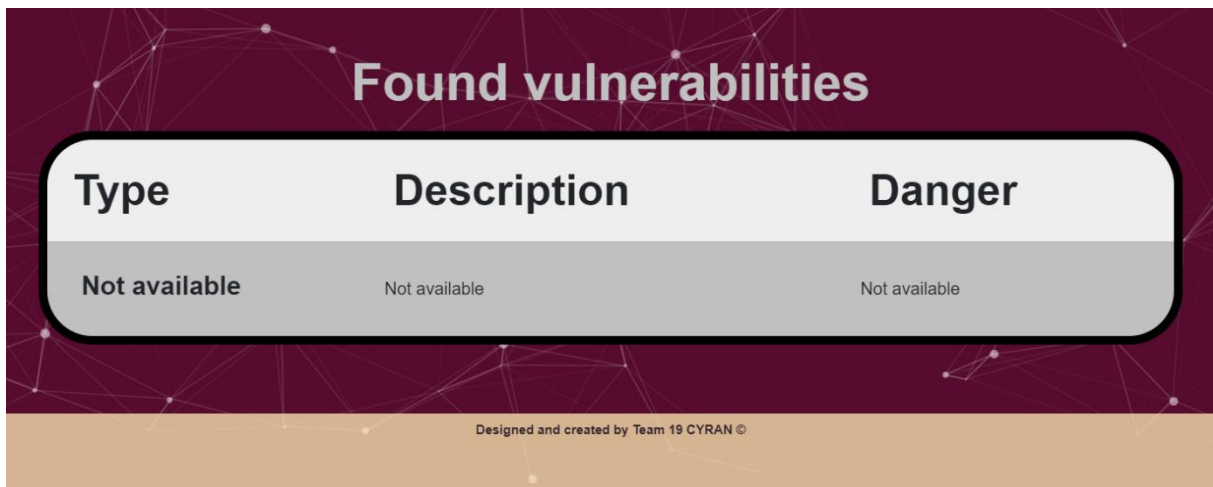
Name server 1: ns1.guzelhosting.com
Name server 2: ns11.guzelhosting.com
Name server 3: ns12.guzelhosting.com
Name server 4: ns2.guzelhosting.com

Domain status 1: clientTransferProhibited

Obrázok 8: Podrobnejšie informácie pokračovanie 2

Podrobnejšie informácie sme vložili do samostatného okna. Zobrazujeme tu všetky dostupné informácie z databázy pre konkrétnu doménu. Obsahom sú mailové adresy, telefónne čísla, adresy a ďalšie informácie o administratíve, platbách, prípadne o technickom stave pokiaľ sú k dispozícii. Pokiaľ niektorá informácia nebola nájdená alebo chyba v databáze, potom sa vo výslednom výpise nezobrazí. Ukážky výpisu pre doménu cukurovabims.com sú zobrazené na Obrázkoch 6 až 8.

Podstatným informačným obsahom pre penetračného testera alebo útočníka sú informácie o zraniteľnostiach. Vytvorili sme pre ne samostatnú tabuľku. V prípade scenára je možné poskytnúť používateľovi informáciu o zraniteľnostiach domény, na základe čoho by mal byť schopný dohľadať doplňujúce informácie a urobiť vhodnú akciu. Databáza whois ale informácie o zraniteľnostiach neobsahuje.



Type	Description	Danger
Not available	Not available	Not available

Designed and created by Team 19 CYRAN ©

Obrázok 9: Nájdené hrozby

4. Zhodnotenie

Vyhľadanie a zber informácií je podstatnou časťou penetračného testovania. Vytvorili sme preto aplikáciu pre vyhľadanie informácií o konkrétnej doméne. V rámci bezpečnostných scenárov by do databázy ktorú aplikácia využíva mali byť pridané informácie o doménach bežiacich v sandbexe, respektíve o webových objektoch bezpečnostných scenárov. Predpokladáme, že bežne dostupné whois servery tieto informácie nebudú mať, a to hlavne z dôvodu dostupnosti nami pridaných webových lokalít. Pridanie vlastných zraniteľností do informácií o doméne by malo vylepšiť hrateľnosť scenárov a podnietiť používateľa vyhľadať si informácie o nich. Rovnako pri vypnutí niektorých zraniteľností je zhotovené riešenie flexibilné, keďže je potrebné len zmeniť hodnotu uloženú v databáze.