EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

Evidenčné číslo: 103004/B/2022/36124048425180676

ANALÝZA WEB STRÁNOK Z HĽADISKA BEZPEČNOSTI

Bakalárska práca

2022 **Ľuboš Bridiš**

EKONOMICKÁ UNIVERZITA V BRATISLAVE

FAKULTA HOSPODÁRSKEJ INFORMATIKY

ANALÝZA WEB STRÁNOK Z HĽADISKA BEZPEČNOSTI

Bakalárska práca

Študijný program: Hospodárska informatika

Študijný odbor: Hospodárska informatika

Školiace pracovisko: Katedra aplikovanej informatiky

Vedúci záverečnej práce: RAKOVSKÁ, Eva, RNDr., PhD.

Bratislava 2022 **Ľuboš Bridiš**

Čestné vyhlásenie

Čestne vyhlasujem, že som túto záverečnú prácu vypracoval samostatne na základe vlastných poznatkov, a že som uviedol všetku použitú literatúru.

Dátum:

.....

Ľuboš Bridiš

Poďakovanie

Touto cestou by som rád poďakoval vedúcej mojej bakalárskej práce Eve Rakovskej, RNDr., PhD. za jej ochotu, rady a venovaný čas pri vypracovávaní tejto bakalárskej práce.

ABSTRAKT

BRIDIŠ, Ľuboš: *ANALÝZA WEB STRÁNOK Z HĽADISKA BEZPEČNOSTI*– Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; Katedra aplikovanej informatiky. – RAKOVSKÁ, Eva, RNDr., PhD. – Bratislava: FHI EU, 2022, 49s

Cieľom záverečnej (habilitačnej) práce je analýza rizík a slabých miest konkrétnych webových stránok z rôznych pohľadov. Práca obsahuje teoretickú a praktickú časť a je rozdelená do troch kapitol. Obsahuje 6 tabuliek a 6 obrázkov. Prvá kapitola je venovaná teoretickej časti. Venuje sa informáciám o základných technických pojmoch, normách a certifikáciách, ktoré súvisia s danou problematikou. V ďalšej časti sa charakterizuje hlavný cieľ, metodiku práce a metódy skúmania tejto záverečnej práce. Výsledkom riešenia danej problematiky je úspešná analýza rizík a slabých miest na konkrétnych webových stránkach z viacerých pohľadov.

Kľúčové slová: bezpečnosť webových stránok, analýza rizík, analýza slabých miest

ABSTRACT

BRIDIŠ, Ľuboš: *WEB PAGE ANALYSIS FROM SECURITY VIEW*- University of Economics in Bratislava. Faculty of Economics Informatics; Department of Applied Informatics. – Consultant: RAKOVSKÁ, Eva, RNDr., PhD. – Bratislava: FHI EU, 2022, 49p

The aim of the final (habilitation) thesis is to analyze the risks and weaknesses of specific websites from different perspectives. The work contains a theoretical and practical part and is divided into three chapters. It contains 6 tables and 6 pictures. The first chapter is devoted to the theoretical part. It deals with information on basic technical concepts, standards and certifications related to the issue. The next part characterizes the main goal, methodology of work and methods of examining this final work. The result of solving the problem is a successful analysis of risks and vulnerabilities on specific websites from several perspectives.

Keywords: website security, risk analysis, vulnerability analysis

O B S A H

Zoznam Skratiek

BGP – „Border Gateway Protocol“ protokol brány, ktorý umožňuje internetu vymieňať si informácie o smerovaní medzi autonómnymi systémami

CA – „Certification authority“ certifikačná autorita

CAPTCHA – „Completely Automated Public Turing test to tell Computers and Humans Apart“ autentifikácia, ktorá testuje či sa prihlasuje človek alebo robot

CSFR – „Cross Site Request Forgery“ typ útoku, ktorý využíva falošné požiadavky

CSS – „Cascading Style Sheets“ kaskádové štýly používané vo webových stránkach

DDoS – „Distributed denial-of-service“ distribuované odmietnutie služby

DH – „Diffie-Hellman key exchange“ algoritmus výmeny kľúčov

DNS – „Domain Name System“ Systém názvov domén

DOM – „Document Object Model“ Objektový model dokumentu

EÚ – Európska únia

FORM – „Formulár“

GDPR – „General Data Protection Regulation“ všeobecné nariadenie na ochranu osobných údajov

HIPAA – „Health Insurance Portability and Accountability Act „ zákon o prenosnosti a zodpovednosti v zdravotnom poistení

HTML – „HyperText Markup Language“ Hypertextový značkový jazyk

HTTP – „HyperText Transfer Protocol“ komunikačný protokol používaný na pripojenie k webovým serverom na internete alebo v lokálnej sieti

HTTPS – „Hypertext Transfer Protocol Secure“ je kombinácia HTTP s SSL

ID – „Identifikátor“

IPsec – „Internet protocol security“ definuje pridanie bezpečnostného mechanizmu do štandardnej IP vrstvy.

ISMS – „Information security management system“ Systém riadenia informačnej bezpečnosti

ISO/IEC – Medzinárodný štandard pre informačnú bezpečnosť

IT – informačné technológie

JCB – „Japan Credit Bureau“ platobná karta od japonskej spoločnosti

NCSA – „The National Center for Supercomputing Applications“ Národné centrum pre superpočítačové aplikácie

OWASP – „Open Web Security Project“ nezisková charitatívna organizácia zameraná na zlepšenie bezpečnosti softvéru a webových aplikácií

PC – „Personal Computer“ osobný počítač

PCI DSS – „Payment Card Industry Data Security Standard“ štandard bezpečnosti dát platobných kariet

PHP – „Hypertext Preprocessor“ – skriptovací jazyk

PKI – „Public key infrastructure“ infraštruktúra verejných kľúčov

RSA – „Rivest–Shamir–Adleman“ je kryptosystém s verejným kľúčom, ktorý je široko používaný na bezpečný prenos dát

SAN – „Subject Alternative Name“ Alternatívny názov predmetu

SEO – „Search engine optimalization“ optimalizácia webu pre vyhľadávače

SHA – „Secure hash algoritm“ kryptografické hašovacie algoritmy používané na vytváranie digitálnych podpisov, ktoré overujú integritu údajov

SQL – „Structured Query Language“ Štruktúrovaný databázový programovací jazyk

SR – Slovenská republika

SSH – „Secure Shell Protocol“ kryptografický sieťový protokol na bezpečné prevádzkovanie sieťových služieb cez nezabezpečenú sieť

SSL - „Secure Sockets Layer „ protokol, ktorý poskytuje zabezpečenie komunikácie šifrovaním a autentizáciou

TLS – „Transport Layer Security „ “ kryptografický protokol, ktorý slúži na šifrovanie dát

URL – „Uniform Resource Locator“ jednotný vyhľadávač prostriedku

USA – „Spojené štáty americké“

WWW – „World Wide Web“ celosvetová sieť

XSS – „Cross Site Scripting“ typ útoku, ktorý sa zameriava na skripty vložené do stránky

Úvod

V dnešnej dobe sa používanie internetu a navštevovanie rôznych webových stránok stalo súčasťou života mnohých z nás. Vďaka webovým stránkam môžeme chodiť na sociálne siete, nakupovať rôzne tovary, zdieľať a pozerať videá a obrázky, dohľadať si informácie o čomkoľvek, počúvať hudbu, písať si s blízkymi, využívať elektronické bankovníctvo, sledovať „stream“ služby (živé vysielanie videí/zvuku) a mnohé ďalšie činnosti. Pri aktívnom navštevovaní webových stránok určite nejedného z nás napadlo, či sú naše údaje, ktoré sme poskytli danej stránke v bezpečí. Poprípade ak sme majiteľom nejakej webovej stránky napr. internetový obchod, firemná webová stránka a rôzne ďalšie, môžeme premýšľať ako je náš webový priestor odolný a chránený voči rôznym útokom.

V tejto práci sa budeme presne tejto problematike bezpečnosti webových stránok venovať. Budeme sa snažiť najskôr zaoberať základnými pojmami a potom normami a certifikáciami, ktoré sú zamerané na bezpečnosť na internete. Vymenujeme si bezpečnostné riziká a najčastejšie metódy, ktoré sa používajú pri útokoch. Následne si povieme ako sa čo najlepšie chrániť voči týmto konkrétnym útokom, a taktiež ako si všeobecne zabezpečiť svoje údaje a vyvarovať sa ich krádeži.

Ďalej sa budeme venovať analýze konkrétnych webových stránok z hľadiska ich bezpečnosti. Analýzu budeme vykonávať pomocou vybraných softvérov alebo aplikácií. Výsledky týchto analýz si popíšeme a nakoniec si ich porovnáme medzi sebou.

1. Súčasný stav riešenej problematiky doma a v zahraničí

V tejto kapitole sa oboznámime so základnými technickými pojmami, normami a certifikáciami, ktoré sú zamerané na našu problematiku. Bližšie si charakterizujeme rôzne metódy útokov a následne si vymenujeme ako si zabezpečiť svoj webový priestor. Tieto informácie a poznatky ďalej využijeme pri následnej analýze v tretej kapitole.

1.1. Technické pojmy

1.1.1. História webových stránok

Webové stránky tu sú s nami už viac ako štvrťstoročie. Stali sa každodenným a všadeprítomným zdrojom informácií u mnohých ľudí žijúcich po celom svete. Britský vedec Tim Berners-Lee vynašiel „World Wide Web“ (WWW) v roku 1989. Webový priestor bol pôvodne navrhnutý a vyvinutý tak, aby uspokojil dopyt po automatizovanom zdieľaní informácií medzi vedcami na univerzitách a inštitútoch kdekoľvek na svete. Základnou myšlienkou "World Wide Web“ bolo zlúčiť vyvíjajúce sa technológie počítačov, dátových sietí a „hypertextu“ do výkonného a jednoducho použiteľného globálneho informačného systému. V decembri 1991 bol spustený prvý webový server v USA. V tejto fáze existovali v podstate len dva druhy prehliadačov. Jednou z nich bola pôvodná vývojová verzia, ktorá bola prepracovaná, no dostupná len na strojoch od spoločnosti NeXT. Druhým bol prehliadač v „riadkovom režime“, ktorý sa dal jednoducho nainštalovať a spustiť na ľubovolnej platforme, ale s obmedzeným výkonom. Začiatkom roku 1993 Národné centrum pre superpočítačové aplikácie (NCSA) na „University of Illinois“ vydalo prvú verziu svojho prehliadača Mosaic. Tento softvér bežal v prostredí „X Window System“, populárnom vo výskumnej komunite a ponúkal jednoduchú interakciu v okne. Krátko nato NCSA vydala verzie aj pre prostredia PC a Macintosh. V roku 1994 sa správy o webovom priestore dostali do médií a vďaka tomu mal do konca toho roku webový priestor okolo 10 000 serverov a 10 miliónov užívateľov. A tak sa webový priestor postupne začal rozrastať až na dnešné pomery. [2] [3]

1.1.2. Webový portál a webová stránka

Ľudia sa často domnievajú, že webová stránka a webový portál je tá istá vec. Opak je však pravdou, pretože medzi portálom a stránkou sú značné rozdiely a je potrebné ich rozlišovať. Rozdiel medzi webovým portálom a webovou stránkou si ďalej popíšeme v tejto podkapitole.

Webová stránka je zbierkou rôznych textových a grafických súborov a súvisiacich webových stránok. Tieto stránky sú prepojené s pomocou hypertextových odkazov. Každá webová stránka má názov domény na jej identifikáciu. Organizácia alebo jednotlivci sa môžu starať o svoje webové stránky, aby informovali zákazníkov o svojich službách alebo produktoch. Webová stránka umožňuje používateľom rôzne funkcie ako napríklad prihlásiť sa, registrovať sa, kontaktovať majiteľa stránky, objednávať rôzne produkty, vykonávať online transakcie, odosielať spätné väzby a tak ďalej. Okrem toho sú HTML, JavaScript ,CSS bežnými jazykmi na strane klienta, zatiaľ čo Python a PHP sa bežne používajú pre rozvoj „backendu“ webových stránok. [4] [5]

Webové stránky sú dostupné v rôznych kategóriách. „E-commerce“ (elektronické obchodovanie) webové stránky ako Alza alebo Wish sú podobné virtuálnym obchodom. Zákazníci si môžu z týchto webových stránok nakupovať produkty alebo si ich prehľadávať. Ďalej vzdelávacie webové stránky poskytujú študentom akademickú podporu. Poskytujú študijné materiály, ako sú učebné pomôcky alebo tutoriály, ktoré môžu byť v rozličných podobách napr. audio, video ale aj v textovom formáte. Sociálne siete ako Twitter a Instagram dávajú možnosť svojich používateľom vytvárať súkromné profily a komunikovať s ich priateľmi. Webové stránky slúžiace na zdieľanie médií umožňujú používateľom medzi sebou rozširovať rôzne mediálne súbory vrátane fotografií, obrázkov, videí, hudby a tak ďalej. [5]

Webový portál alebo jednoducho portál je webová stránka, ktorá jednotne a konzistentne zhromažďuje informácie z rôznych zdrojov. Každý zdroj informácií získa na stránke vyhradenú oblasť na zobrazenie informácií. Existujú rôzne druhy portálov, ako sú osobné, finančné, skladové, vyhľadávacie, zdravotnícke, vládne a podnikové protokoly. Rozlišujeme hlavne dva typy portálov a to interné a externé portály. [5]

Interné web portály používajú najmä organizácie a spoločnosti. Spoločnosť využíva interné portály na zabezpečenie komunikácie a poskytovanie služieb svojim zamestnancom. Obsahuje informácie o pripravovaných udalostiach, vydaniach produktov, podrobnostiach o stretnutiach a informácie týkajúce sa práce. V portáli si zamestnanci môžu navzájom vymieňať informácie aj prostredníctvom e-mailov alebo online „chatových“ správ. Tieto portály existujú v rámci privátnej siete. Preto k nej majú prístup len autorizovaní užívatelia. Užívateľ musí pre prístup k danému portálu zadať platné prihlasovacie údaje. [5]

Externý portál môže navštíviť a používať ktokoľvek. Funguje ako východiskový bod pre prehliadanie webu. Má odkazy na rôzne články, ktoré zjednodušujú proces prehliadania webového priestoru. Napríklad jeden z najznámejších externých portálov je Yahoo. Yahoo poskytuje odkazy na rôzne témy, ako sú aktuálne správy, športové udalosti, financie a najnovšie informácie z politiky. Postupné zlepšovanie internetových vyhľadávačov ako je napríklad Google minimalizovalo popularitu portálov. Aj keď je portál odlišný od vyhľadávača, portál má určité schopnosti vyhľadávačov. Preto sa Yahoo považuje za portál aj webový vyhľadávač zároveň. [5]

Hlavným rozdielom medzi webovou stránkou a portálom je, že a portál je unikátny druh webovej stránky, ktorý funguje ako brána k „world wide webu“ (WWW) pre poskytovanie rôznorodých služieb užívateľom a webová stránka je súborom súvisiacich webových stránok, ktoré sú adresované vo vzťahu k spoločnej adrese „uniform resource locator“ (URL). [5]

Portál je teda špeciálna webová stránka, ktorá ponúka služby a zdroje, ako sú emaily, diskusné fóra a má možnosti vyhľadávacích nástrojov. Poskytuje prístup k viacerým zdrojom, funkcionalite a obsahu špecifickým pre jednotlivé úlohy a zlepšuje spoluprácu. Webová stránka je voči tomu umiestnením na internete, ktoré smeruje na kolekciu webových stránok, ktoré sú adresované vzhľadom na spoločnú adresu URL. Webová stránka sa dostane k cieľovému publiku. Okrem toho má špeciálne zameraný obsah, vďaka ktorému eliminuje potrebu navštíviť iné webové stránky. [5]

1.2. Certifikácie a normy webových stránok

Norma (štandard) je definovaná ako smernica alebo súbor pravidiel, ktoré musí organizácia dodržiavať, aby získala právo na niektoré funkcie. Akými sú napríklad prijímanie platieb online, ukladanie údajov o pacientovi atď. Normy pozostávajú z niekoľkých základných pravidiel, ktoré musí organizácia dodržiavať, aby udržala súlad s niektorými normami kybernetickej bezpečnosti. Na základe požiadavky podniku alebo organizácie existuje niekoľko rôznych štandardov. Je verejne známe, že informácie sú a budú primárnym predmetom ochrany. Čím väčšiu hodnotu informácie majú, tým by sa im mala venovať väčšia pozornosť na ich zabezpečenie. Veľmi dôležitým aspektom kybernetickej bezpečnosti je ochrana pred krádežou identity. Pre vhodné nastavenie bezpečnosti informácií boli vytvorené normy. Napríklad technická norma presne stanovuje požadované vlastnosti, tvar, prevedenie alebo usporiadanie opakujúcich sa predmetov alebo spôsobov a postupov práce, prípadne vymedzuje všeobecne využívané technické pojmy. Normy v oblasti bezpečnosti informácií sa zaoberajú riadením, nastavením a posudzovaním bezpečnosti daných informácií. Normy kybernetické bezpečnosti boli vytvorené relatívne nedávno, pretože len v posledných rokoch pribúda veľký počet citlivých informácií uložených na diskoch počítačov, ktoré sú pripojené na internet. Inštitúcie a firmy majú zvýšenú potrebu na zaistenie informačnej bezpečnosti, pretože si potrebujú chrániť svoje obchodné tajomstvo, dôverné informácie a rôzne osobné údaje napríklad o ich zamestnancoch, partneroch ale aj zákazníkoch. [1]

1.2.1. Norma ISO 27001

ISO/IEC 27001:2013 (známa aj ako ISO 27001) je medzinárodný štandard pre informačnú bezpečnosť. Špecifikuje špecifikáciu systému riadenia informačnej bezpečnosti (ISMS). Prístup osvedčených postupov ISO 27001 pomáha organizáciám riadiť bezpečnosť informácií prostredníctvom vystavenia ľuďom, procesom a technológiám. Certifikácia ISO 27001 je celosvetovo uznávaná, čo znamená, že váš ISMS je v súlade s najlepšími postupmi v informačnej bezpečnosti. Norma ISO/IEC 27001 je vhodná pre všetky organizácie a spoločnosti, ktoré chcú chrániť svoje vysoko hodnotné informačné aktíva a minimalizovať tak škody spôsobené ich prípadným únikom. Pozostáva zo súboru postupov, ktoré špecifikujú pravidlá a požiadavky, ktoré musí organizácia splniť, aby získala certifikáciu prostredníctvom tejto normy. Podľa tohto štandardu by organizácie mali udržiavať všetky technológie aktuálne, servery by mali byť bez zraniteľných miest a organizácie musia byť auditované po stanovených časových intervaloch, aby zostali zostavené podľa tohto štandardu. V dôsledku toho sa osoby, ktoré narábajú s citlivými informáciami alebo osobnými údajmi, môžu vyhnúť finančným a právnym postihom vyplývajúcim z úniku informácií alebo neoprávneného spracovania osobných údajov používateľov. [1] [7]

1.2.2. PCI DSS

PCI DSS je skratka pre štandard bezpečnosti dát platobných kariet. Štandard zabezpečenia údajov v odvetví platobných kariet (PCI DSS) je súbor požiadaviek, ktorých cieľom je zabezpečiť, aby všetky spoločnosti, ktoré spracúvajú, uchovávajú alebo prenášajú informácie o kreditných kartách a ich majiteľoch, aby udržiavali bezpečné prostredie. Podniky, ktoré ukladajú údaje o používateľovi, ako sú ich meno a informácie o karte, musia prijať tento štandard vo svojej organizácii. Technológie používané organizáciou by mali byť aktuálne a ich systém by mal neustále podliehať hodnoteniu bezpečnosti, aby sa zabezpečilo, že nemá žiadnu závažnú zraniteľnosť alebo chybu. Bol spustený 7. septembra 2006 s cieľom spravovať bezpečnostné štandardy a zlepšovať bezpečnosť účtov počas celého procesu transakcie. Tento štandard bol vytvorený a je riadený nezávislým orgánom PCI Security Standards Council tvoreným spoločnosťami akými sú Visa, MasterCard, American Express, Discover a JCB. [8]

1.2.3. HIPAA

Skratka HIPAA znamená zákon o prenosnosti a zodpovednosti v zdravotnom poistení. Je platný na území Spojených štátov, u nás v Európe sa používa štandard GDPR. Táto norma sa zaoberá používaním a zverejňovaním informácií o zdravotnom stave jednotlivcov (známych ako „chránené informácie o zdraví“) subjektmi, na ktoré sa vzťahuje pravidlo ochrany osobných údajov. Títo jednotlivci a organizácie sa nazývajú „kryté subjekty“. Pravidlá ochrany osobných údajov tiež obsahujú normy pre práva jednotlivcov pochopiť, ako sa používajú informácie o ich zdravotnom stave. Hlavným cieľom pravidla ochrany súkromia je zabezpečiť, aby boli informácie o zdravotnom stave jednotlivcov náležite chránené, a zároveň umožniť tok zdravotných informácií potrebných na poskytovanie a podporu vysokej kvality zdravotnej starostlivosti a na ochranu zdravia a pohody verejnosti. Pravidlo ochrany osobných údajov vytvára rovnováhu, ktorá umožňuje dôležité používanie zdravotných informácií a zároveň chráni súkromie ľudí, ktorí potrebujú starostlivosť a ošetrenie. [9]

1.2.4. GDPR

Všeobecné nariadenie o ochrane údajov (GDPR) alebo všeobecné nariadenie o ochrane údajov je právny rámec, ktorý stanovuje usmernenia pre zhromažďovanie a spracúvanie osobných údajov od fyzických osôb s bydliskom v Európskej únii (EÚ). Keďže nariadenie platí bez ohľadu na to, kde sa server webovej stránky nachádza, všetky webové stránky, ktoré priťahujú európskych návštevníkov, musia byť v súlade s nariadením, a to aj v prípade, že občanom EÚ konkrétne nepredávajú tovar ani služby. GDPR vyžaduje, aby webové stránky poskytovali návštevníkom EÚ informácie a údaje, ktoré o nich webové stránky majú. Stránka musí tiež podniknúť kroky na podporu práv spotrebiteľov v EÚ, aby boli informovaní v prípade porušenia ochrany osobných údajov. Nariadenie bolo prijaté v apríli 2016 a plne implementované v máji 2018 po dvojročnom prechodnom období. [10]

1.2.5. SSL a TLS certifikácie

„Secure Sockets Layer“ (SSL) a „Transport Layer Security“ (TLS) sú štandardy pre zabezpečenie internetových transakcií v bankovníctve, e-mailov a elektronických obchodov (e-commerce). Pozdĺž s infraštruktúrou verejných kľúčov (PKI) poskytuje SSL dôveryhodné identity prostredníctvom certifikačných reťazcov a súkromnej komunikácie cez šifrovanie. Ústredným bodom týchto záruk sú súkromné kľúče používané v SSL. Súkromné kľúče nie sú kompromitované tretími stranami, takže certifikáty založené na týchto súkromných kľúčoch musia byť znovu vydávané a odvolané, aby sa zabezpečilo, že tretie strany so zlým úmyslom sa nemôžu zamaskovať za nejaký dôveryhodný subjekt. Dôležité je, že PKI používa predvolený platný model, kde potenciálne kompromitované certifikáty zostávajú v platnosti až do ich vypršania alebo do ich odvolania. Zrušenie je však proces, ktorý si vyžaduje manuálny zásah vlastníkov certifikátov a spoluprácu od klientov, ktorí používajú ich certifikáty. Výsledkom je praktická bezpečnosť PKI v závislosti od rýchlosti, s akou vlastníci certifikátov a klienti SSL aktualizujú svoje zoznamy odvolaní. Sú to operácie, ktoré sa uskutočňujú v ľudských časových intervaloch (hodiny alebo dni) namiesto rýchlych počítačových intervalov (sekundy alebo minúty). [6]

Zabezpečené pripojenia SSL šifrujú všetky prenášané údaje, ako sú platobné informácie alebo vašu online komunikáciu. SSL však okrem bezpečnosti prináša aj ďalšie výhody, ako napríklad vyššie skóre SEO z pohľadu vyhľadávačov. Pridaná hodnota však spočíva aj v predchádzaní základným typom kybernetických útokov (najmä útoky typu „man-in-the-middle“) či pri budovaní dôvery. Vo väčšine prehliadačov sú webové stránky s platnými certifikátmi SSL označené zelenou adresou URL a ikonou zámku. Hovoria o svojej bezpečnosti a motivujú návštevníkov, aby sa uistili, že ich pripojenie na stránku je bezpečné. Nevyhnutnou súčasťou každej webovej stránky by preto mal byť platný a správne nastavený SSL certifikát zodpovedný za bezpečnosť seba a svojich návštevníkov. [6] [11]

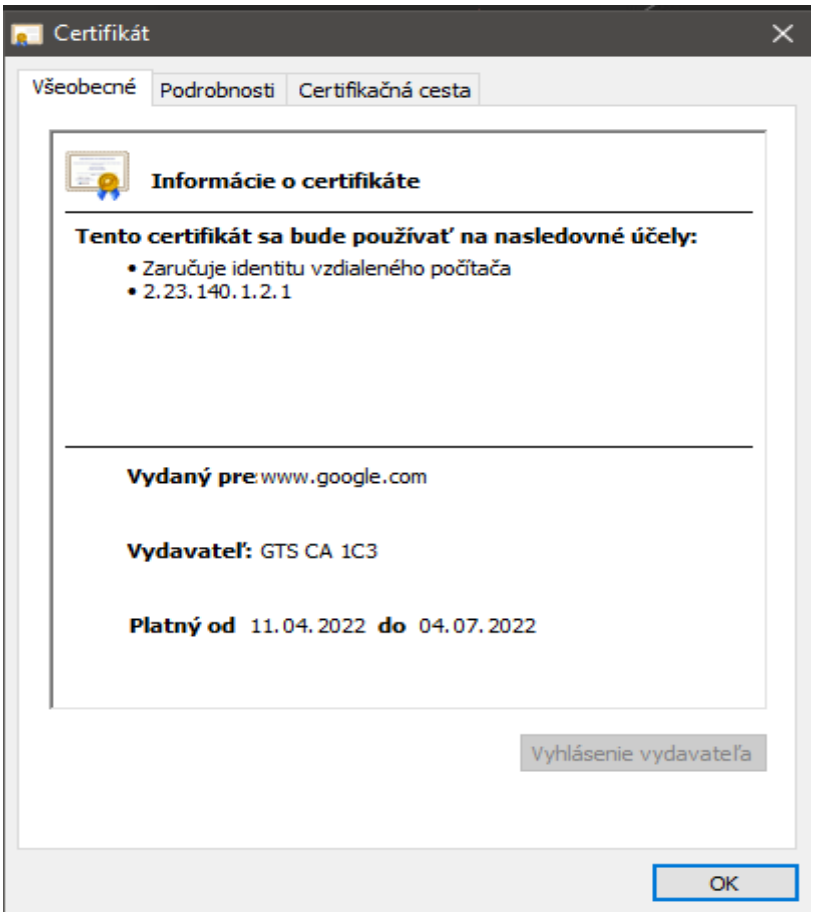
SSL spojenie sa nadviaže medzi serverom (webstránkou) a vašim prehliadačom pomocou procesu “SSL handshake”. Pri tvorbe šifrovaného spojenia sa používajú tri digitálne kľúče, a to nasledovným spôsobom: [11]

- Server pošle prehliadaču kópiu svojho asymetrického verejného kľúča.
- Internetový prehliadač vytvorí jednorazový symetrický kľúč relácie (symmetric session key) a zašifruje ním asymetrický verejný kľúč servera, a ten následne odošle späť na server.
- Server dešifruje prijatý kľúč použitím svojho privátneho asymetrického kľúča a tým získa symetrický kľúč relácie.
- Server a internetový prehliadač nadviažu spojenie a všetky odoslané a prijaté dáta šifrujú/dešifrujú pomocou vytvoreného symetrického kľúča relácie. Ten sa používa len počas jednej relácie a po jej skončení sa už naďalej nepoužíva.

Pri šifrovanej komunikácii sa tak používa jednorazový symetrický kľúč šifrovania, ktorý pozná len váš internetový prehliadač a daný server, s ktorým komunikuje. To zabezpečuje ochranu všetkých prenášaných dát pred treťou osobou. [6] [11]

Platný certifikát SSL musí momentálne obsahovať nejaké informácie. Základné informácie sú o vydavateľovi SSL certifikátu, ktorého vo všeobecnej terminológii nazývame Certifikačná autorita (CA). Mala by to byť organizácia, ktorej návštevníci dôverujú. Certifikát by mal okrem informácií o certifikačnej autorite obsahovať aj jej sériové číslo, dátum exspirácie (spravidla majú certifikáty platnosť jeden až tri roky), kópiu verejného kľúča držiteľa certifikátu a digitálny podpis certifikačnej autority. [6] [11]

O úrovni bezpečnosti certifikátu môžu hovoriť viaceré parametre. Napríklad je to štandard, ktorým bol vytvorený X.509, úroveň šifrovania komunikácie, ktorú používa (napr. 256-bitová šifra), kryptografický spôsob tvorby kľúčov (napr. RSA SHA-2 s 256-bitovým hashom) a spôsob šifrovania kľúčov (napr. 2048-bitová šifra). [6] [11]



Obrázok 1 - Ukážka SSL certifikátu

Rozlišujeme tri typy SSL certifikátov na základe počtu domén a subdomén, ktoré potrebujete chrániť: [11]

- „Single-name“ SSL certifikát zabezpečuje šifrované spojenie pre jednu doménu/subdoménu.
- „Wildcard“ SSL certifikát zabezpečuje šifrované spojenie pre jednu doménu a ľubovoľný počet jej subdomén.
- „Multi-domain“ (SAN – „Subject Alternative Name“) SSL certifikát takýto typ certifikátu umožňuje organizácii chrániť až sto rôznych domén v jej vlastníctve.

1.3. Možné bezpečnostné riziká na webových stránkach

Takmer polovica všetkých webových stránok na internete má značné bezpečnostné slabiny, z ktorých mnohé sú jednoduché na opravu a často sú aj so starými chybami, o ktorých sa predpokladalo, že sú zapísané dávno do histórie. Navyše takéto zraniteľnosti znamenajú, že viac ako polovica organizácií nespĺňa požiadavky na súlad s PCI (payment card industry). [12]

OWASP alebo „Open Web Security Project“ je nezisková charitatívna organizácia zameraná na zlepšenie bezpečnosti softvéru a webových aplikácií. Organizácia zverejňuje zoznam najvýznamnejších slabín zabezpečenia webových stránok a portálov na základe údajov od rôznych bezpečnostných organizácií. Nižšie si uvedieme a povieme niečo o najčastejších bezpečnostných rizikách a chybách na webových stránkach. [12] [13]

Obrázok 2 - top 10 bezpečnostných rizík webových stránok podľa OWASP, Zdroj [17]

1.4. Metódy, ktoré útočníci používajú na získanie citlivých informácií pomocou web stránok

1.4.1. SQL Injection

„SQL Injection“ je typ útoku, ktorý vďaka bezpečnostným chybám umožňuje útočníkovi zmeniť „backendové“ SQL príkazy pomocou manipulácie s údajmi poskytnutými používateľom. Samotný „SQL injection“ útok nastane, keď sa používateľský vstup odošle „interpreterovi“ ako súčasť príkazu alebo dotazu a oklame „interpreter“, aby vykonal neúmyselné príkazy a poskytne prístup k neoprávneným údajom. Interpreter je špeciálny počítačový program, ktorý sa používa na priame vykonávanie programových inštrukcií napísaných pomocou ľubovoľného vysokoúrovňového programovacieho jazyka a následne transformuje tieto inštrukcie do iného jazyka strednej úrovne a v ňom ich vykoná. Príkaz SQL, ktorý ak je spustený webovou aplikáciou môže taktiež odhaliť aj „backendovú“ databázu. [13] [24]

Útok „SQL injection“ sa stal jedným z najstarších a najrozšírenejších útokov, ktorý je dodnes stále aktívne využívaný. Útočník využívajúci útok „SQL injection“ v podstate zneužíva slabinu zavedenú do aplikácie v dôsledku nesprávnych postupov vývoja webových aplikácií. To umožňuje útočníkom vložiť príkazy SQL napríklad do prihlásenia alebo vyhľadávacieho poľa. Následne im umožňuje získať neoprávnený prístup k uchovávaným údajom „backendovej“ databázy. SQL „injection“ útok je možný, keď sú vstupy buď nesprávne filtrované na únikové znaky alebo používateľský vstup nie je správne overený. Vďaka tomu môže útočník napríklad manipulovať SQL dotazy. Takéto slabiny v dizajne aplikácie poskytujú útočníkom schopnosť vytvárať škodlivé požiadavky pre webovú aplikáciu, čo sa efektívne môže využiť na spustenie príkazov SQL a dotazov priamo v databáze. [12]

Najrýchlejší a najjednoduchší spôsob ako skontrolovať, či je možné použiť „SQL Injection“ útok na webovej aplikácii, je zadať jednoduché alebo dvojité úvodzovky (bežne označované ako „zaškrtnutie“) v poli alebo v parametri, ktorým útočník skúša zahájiť útok. To spôsobí syntaktickú chybu v príkaze SQL a vedie SQL „interpreter“ k výpisu chybovej hlášky, ktorá väčšinou bude zobrazená na webovej aplikácii, toto jasne naznačuje, že pole je zraniteľné voči „SQL Injection“. Útočník potom s najväčšou pravdepodobnosťou vyrobí konkrétne požiadavky, aby databáza zverejnila informácie o sebe v chybových hláseniach. Útočník môže použiť tieto informácie na identifikáciu typu používanej databázy (tento proces sa zvyčajne označuje ako „snímanie odtlačkov prstov“), týmto spôsobom zostaví schému databázy a získa údaje z rôznych tabuliek v databáze. [12]

Zhrnutie: [13]

- Útočník môže vložiť škodlivý obsah do zraniteľných oblastí.
- Z databázy je možné čítať citlivé údaje, ako sú používateľské mená, heslá atď.
- V databáze je možné vykonávať administráciu operácií.
- Údaje databázy je možné upravovať (vložiť/aktualizovať/vymazať).

Zraniteľné objekty: [13]

- Vstupné polia
- URL pracujúce s databázou

Prevencia: [13]

- Použitie bielej listiny („white list“) na vstupné polia
- Vyhnite sa zobrazovaniu podrobných chybových správ, ktoré sú užitočné pre útočníka.

1.4.2. Cross Site Scripting (XSS)

Útok Cross Site Scripting, tiež známy ako XSS sa zameriava na skripty vložené do stránky, ktoré sa spúšťajú na strane klienta, t. j. v prehliadači používateľa a nie na strane servera. Tieto chyby sa môžu vyskytnúť, keď aplikácia vezme nedôveryhodné údaje a odošle ich do webového prehliadača bez riadneho overenia. Útočníci môžu použiť XSS na spúšťanie škodlivých skriptov pre útok na používateľov, v tomto prípade v prehliadačoch obetí. Keďže prehliadač nemôže vedieť, či je skript dôveryhodný alebo nie, skript sa spustí a útočník môže ukradnúť relácie súborov „cookie“, znehodnotiť webové stránky alebo presmerovať používateľa na nechcené a škodlivé webové stránky. XSS je útok, ktorý umožňuje útočníkovi spúšťať skripty v prehliadači obete. [13]

XSS možno použiť rôznymi spôsobmi a môže spôsobiť vážne problémy. Jedným z tradičných a nebezpečných použití XSS je schopnosť útočníka ukradnúť relácie súborov „cookie“, ktoré umožňujú útočníkovi vydávať sa za obeť. Je používaný na spôsobenie chaosu na sociálnych sieťach, šírenie malvéru, phishing pre získanie údajov a dokonca sa používajú v spojení s technikami sociálneho inžinierstva a môžu eskalovať k ničivejším útokom. Skriptovanie medzi stránkami možno klasifikovať do troch hlavných kategórií – uložené XSS, Zrkadlené XSS a XSS založené na DOM. [12]

Zhrnutie: [13]

- Pomocou tejto bezpečnostnej chyby môže útočník vložiť skripty do aplikácie, môže ukradnúť relácie súborov „cookie“, znehodnotiť webové stránky a spustiť malvér na počítačoch obetí.

Zraniteľné objekty: [13]

- Vstupné polia
- URL adresa

Prevencia: [13]

- Použitie bielej listiny („white list“) na vstupné polia
- Správne vstupno-výstupné kódovanie [13]

1.4.3. Broken Authentication and Session Management

Nedostatočná autentifikácia a zlá správa relácií súborov „cookie“ vo webových aplikáciách sa dá zneužiť na napadnutie webových stránok. Webové stránky zvyčajne vytvárajú relácie súborov „cookie“ a ID relácie pre každú platnú reláciu. Tieto súbory „cookie“ obsahujú citlivé údaje, ako je používateľské meno, heslo atď. Keď sa relácia ukončí buď odhlásením alebo náhlym zatvorením prehliadača, tieto súbory by sa mali zmazať, a to znamená, že pre každú reláciu by sa mal vytvoriť nový súbor „cookie“. Ak nedôjde k zrušeniu platnosti súborov „cookie“, citlivé údaje budú v systéme naďalej uložené. Napríklad používateľ, ktorý používa verejný počítač má súbory „cookie“ zraniteľného webu umiestnené v danom systéme a sú vystavené potencionálnemu útočníkovi. Taktiež ak útočník po určitom čase používa rovnaký verejný počítač ako používateľ, jeho citlivé dáta sú ohrozené. Ďalším spôsobom zneužitia tejto metódy môže byť, ak používateľ, ktorý používa verejný počítač namiesto odhlásenia náhle zatvorí internetový prehliadač. Útočník má potom jednoduchý prístup k informáciám, ak otvorí tú istú zraniteľnú webovú stránku alebo portál a zobrazí sa mu predchádzajúca relácia obete. Útočník môže robiť čokoľvek, odcudziť informácie o profile, informácie o kreditnej karte atď. Preto by sa mala vykonať kontrola, vďaka ktorej vieme zistiť silu autentifikácie a správy relácií súborov „cookie“. Kľúče, tokeny relácie, súbory „cookie“ by mali byť implementované správne bez ohrozenia hesiel. Token je veľmi bezpečný formát používaný na prenos citlivých informácií medzi dvoma stranami kompaktným a samostatným spôsobom. Tokeny sa často používajú na posilnenie procesov autentifikácie, či už v rámci webovej lokality alebo aplikácie. [12] [13] [25]

Zhrnutie: [13]

- Využitím tejto zraniteľnosti môže útočník ukradnúť reláciu súborov „cookie“, a tak získať neoprávnený prístup do systému
- Relácie môžu byť zablokované pomocou ukradnutých súborov „cookie“ alebo ukradnutých relácií súborov „cookie“ pomocou XSS útoku.

Zraniteľné objekty: [13]

- ID relácií ak sú zverejnené v URL adrese.
- ID relácií ak sú rovnaké pred a po odhlásení a prihlásení na webovej aplikácii.

- Ak nie sú správne implementované časové limity relácie.
- Ak aplikácia priraďuje rovnaké ID relácie pre každú novú reláciu.
- Reláciu môže znova použiť používateľ s nízkymi právami.

Prevencia: [13]

- Všetky požiadavky na autentifikáciu a správu relácie by mali byť definované podľa štandardu overovania bezpečnosti aplikácií OWASP.
- Nikdy nezverejňujte osobné informácie v adresách URL alebo ich neukladajte v logoch webovej aplikácie.
- Veľké úsilie by sa malo vynaložiť aj na to, aby sa predišlo útokom XSS, ktoré možno použiť na ukradnutie ID relácií.

1.4.4. Nezabezpečené priame odkazy na objekt

Vyskytuje sa, keď vývojár odkryje odkaz na interný implementačný objekt, ako je súbor, adresár alebo kľúč databázy vo forme URL alebo ako parameter FORM. Útočník môže použiť tieto informácie na prístup k iným objektom a môže vytvoriť budúci útok na prístup k neoprávneným údajom. [13]

Zhrnutie: [13]

- Pomocou tejto zraniteľnosti môže útočník získať prístup k neoprávneným interným objektom, môže upravovať údaje alebo kompromitovať aplikáciu.

Zraniteľné objekty: [13]

- URL adresa

Prevencia: [13]

- Implementujte kontroly pre kontroly prístupu.
- Vyhnite sa odhaleniu odkazov na objekty v adresách URL.
- Overte autorizáciu pre všetky referenčné objekty.

1.4.5. Cross Site Request Forgery

Cross Site Request Forgery v skratke CSFR, je metóda útoku, ktorá využíva falošné požiadavky. CSRF útok je útok, ku ktorému dochádza, keď škodlivá webová stránka, e-mail alebo program spôsobí, že prehliadač používateľa vykoná nechcenú akciu na dôveryhodnej lokalite, pre ktorú je používateľ momentálne overený. Útok CSRF prinúti prehliadač prihlásenej obete odoslať sfalšovanú požiadavku HTTP vrátane relácie súborov „cookie“ obete a akýchkoľvek ďalších automaticky zahrnutých overovacích informácií do zraniteľnej webovej aplikácie. Útočník odošle odkaz obeti, a potom keď obeť (používateľ) po prihlásení na pôvodnú webovú stránku klikne na dané URL, jeho údaje budú z webovej stránky odcudzené. [13]

Zhrnutie: [13]

- Použitie tejto zraniteľnosti môže zmeniť informácie o používateľskom profile, zmeniť stav, vytvoriť nového používateľa v mene správcu atď.

Zraniteľné objekty: [13]

- Stránka profilu používateľa
- Formuláre používateľských účtov
- Stránka obchodnej transakcie

Prevencia: [13]

- Nariadiť používateľovi prítomnosť pri vykonávaní citlivých akcií.
- Implementujte mechanizmy ako CAPTCHA, opätovné overenie a jedinečné tokeny požiadavky.

1.4.6. Nesprávna konfigurácia zabezpečenia

Konfigurácia zabezpečenia musí byť definovaná a nasadená pre aplikáciu, rámce, aplikačný server, webový server, databázový server a platformu. Ak nie sú správne nakonfigurované, útočník môže mať neoprávnený prístup k citlivým údajom alebo funkciám. Niekedy takéto chyby vedú k úplnému ovládnutiu systému. Udržiavanie softvéru najnovšími aktualizáciami je tiež dobrým preventívnym zabezpečením. [13]

Zhrnutie: [13]

- S využitím tejto zraniteľnosti môže útočník vymenovať informácie o základnej technológii a verzii aplikačného servera, informácie o databáze a získať informácie o aplikácii, aby mohol vykonať niekoľko ďalších útokov.

Zraniteľné objekty: [13]

- URL adresa
- Polia formulára
- Vstupné polia

Prevencia: [13]

- Silná aplikačná architektúra, ktorá poskytuje dobré oddelenie a bezpečnosť medzi komponentmi.
- Zmena predvolených používateľských mien a hesiel.
- Zakázanie zoznamov adresárov a implementovanie kontroly riadenia prístupu.

1.4.7. Nezabezpečené kryptografické úložisko

Nezabezpečené kryptografické úložisko je bežnou zraniteľnosťou, ktorá sa vyskytuje, keď citlivé údaje nie sú uložené dostatočne bezpečne. Prihlasovacie údaje používateľa, informácie o profile, podrobnosti o zdravotnom stave, informácie o kreditnej karte atď. patria na webovej lokalite medzi citlivé údaje. Tieto údaje sú následne uložené v databáze danej aplikácie. Ak sú tieto údaje uložené nesprávne, pretože napríklad nepoužívajú šifrovanie alebo hashovanie, budú zraniteľné voči útočníkom. Hashovanie je transformácia znakov reťazca na kratšie reťazce pevnej dĺžky alebo kľúča. Na dešifrovanie reťazca by mal byť k dispozícii algoritmus použitý na vytvorenie kľúča. [13]

Zhrnutie: [13]

- Použitím tejto zraniteľnosti môže útočník ukradnúť alebo upraviť slabo chránené údaje, aby mohol páchať krádež identity, podvody s kreditnými kartami alebo iné trestné činy.

Zraniteľné objekty: [13]

- Databáza aplikácie.

Prevencia: [13]

- Zabezpečte použitie silných štandardných algoritmov. Nevytvárajte vlastné kryptografické algoritmy. Používajte iba schválené verejné algoritmy, ako sú AES, kryptografia s verejným kľúčom RSA a SHA-256.
- Uistite sa, že zálohy mimo lokality vašich databáz sú šifrované a tiež kľúče sa spravujú a zálohujú oddelene.

1.4.8. Zlyhanie pri obmedzení prístupu na adresu URL

Webové aplikácie kontrolujú prístupové práva URL pred vykreslením chránených odkazov a tlačidiel. Aplikácie musia vykonávať podrobné kontroly riadenia prístupu pri každom prístupe na tieto stránky. Vo väčšine aplikácií by sa privilegované stránky, miesta a zdroje nemali zobrazovať neprivilegovaným používateľom. Ale pomocou inteligentného odhadu alebo náhode môže útočník získať prístup k stránkam s právami. Útočník môže pristupovať k citlivým stránkam, vyvolať rôzne funkcie aplikácie a zobraziť dôverné informácie. [13]

Zhrnutie: [13]

- Využitím tejto zraniteľnosti môže útočník získať prístup k neoprávneným adresám URL bez toho, aby sa prihlásil do aplikácie a zneužil túto zraniteľnosť. Útočník môže pristupovať k citlivým stránkam a tým získať dôverné informácie.

Zraniteľné objekty: [13]

- URL adresy

Prevencia: [13]

- Implementujte kontroly pre kontroly prístupu.
- Zásady autentizácie a autorizácie by mali byť založené na rolách.

- Obmedzte prístup pre nechcené adresy URL.

1.4.9. Nedostatočná ochrana transportnej vrstvy

Zaoberá sa výmenou informácií medzi klientom a serverom. Aplikácie často prenášajú citlivé informácie, ako sú overovacie údaje, informácie o kreditných kartách a tokeny relácie cez sieť. Používaním slabých algoritmov alebo používaním exspirovaných alebo neplatných certifikátov alebo nepoužívaním SSL môže byť komunikácia vystavená nedôveryhodným používateľom, čo môže ohroziť webovú aplikáciu alebo budú odcudzené citlivé informácie. [12] [13]

Zhrnutie: [13]

- Využitím tejto chyby zabezpečenia webu môže útočník odchytiť poverenia legitímneho používateľa a získať prístup k aplikácii.
- Útočník môže ukradnúť informácie o kreditnej karte.

Zraniteľné objekty: [13]

- Údaje odoslané cez sieť.

Prevencia: [13]

- Povoliť zabezpečený HTTP a vynútiť prenos poverení iba cez HTTPS.
- Uistite sa, že váš certifikát je platný a jeho platnosť nevypršala.

1.4.10. Neoverené presmerovania

Webová aplikácia používa niekoľko metód na presmerovanie používateľov na iné webové stránky na určený účel. Ak pri presmerovaní na iné stránky nedôjde k náležitému overeniu, útočníci to môžu využiť a môžu presmerovať obete na „phishingové“ alebo „malvérové“ webové stránky alebo použiť presmerovanie na prístup k neoprávneným stránkam. [13]

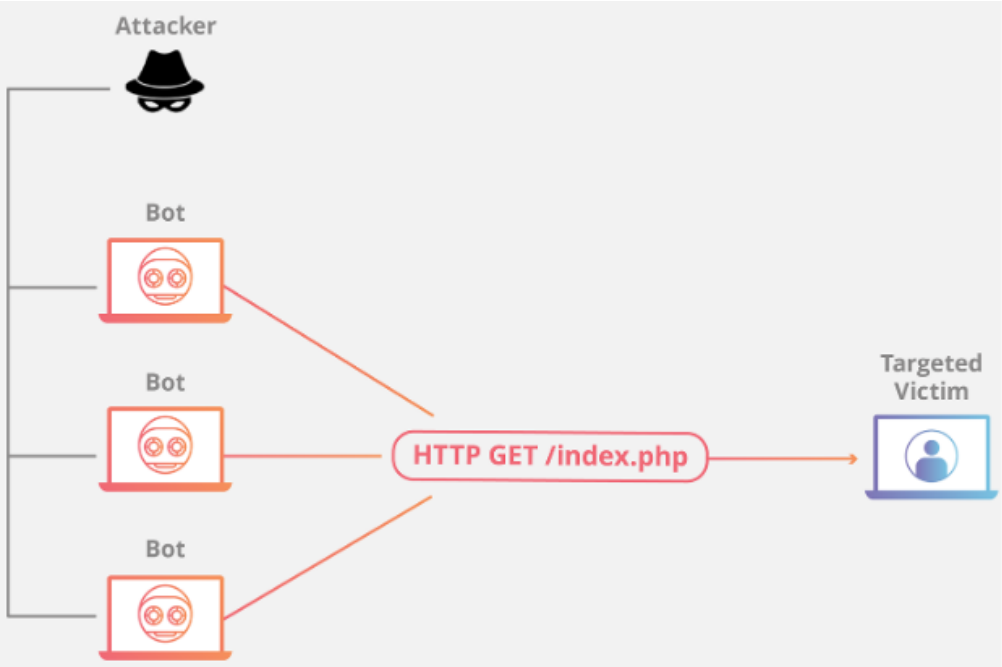
Prevencia: [13]

- Vyhnite sa používaniu presmerovaní v aplikácii.
- Ak sa presmerovaniu nedá vyhnúť dbajte na dôsledné overovanie a zabezpečenie.

1.4.11. DDoS útok

Distributed denial-of-service v skratke DDoS nie je určený na získavanie informácií ale na zabránenie prístupu užívateľov na webové stránky. Útok distribuovaného odmietnutia služby je pokus narušiť normálnu prevádzku cieľového servera, služby alebo siete zaplavením cieľa alebo jeho okolitej infraštruktúry veľkým objemom internetovej prevádzky. DDoS útoky dosahujú svoju efektivitu využívaním viacerých infikovaných počítačových systémov ako zdroja útočnej návštevnosti. Používané stroje môžu zahŕňať počítače a iné sieťové zdroje, ako sú zariadenia internetu vecí. [16]

DDoS útoky sa vykonávajú pomocou siete počítačov pripojených na internet. Tieto siete pozostávajú z počítačov infikovaných malvérom a iných zariadení, ako sú zariadenia internetu vecí, ktoré môžu útočníci ovládať na diaľku. Tieto jednotlivé zariadenia sa nazývajú boti (alebo zombie) a skupina botov sa nazýva botnet. Po vytvorení botnetu môže útočník nasmerovať útok odoslaním vzdialených príkazov každému botovi. Keď sa botnet zameria na server alebo sieť obete, každý bot odošle požiadavku na adresu IP cieľa, čo môže spôsobiť preťaženie servera alebo siete, čo má za následok odmietnutie služby. Keďže každý bot je legitímne internetové zariadenie, môže byť náročné odlíšiť útok od bežnej návštevnosti. [16]



Obrázok 3 - Ukážka schémy DDoS útoku, Zdroj [16]

1.5. Ako zabezpečiť webovú stránku

V tejto kapitole si vymenujeme niekoľko postupov ako si zabezpečiť svoju webovú stránku tak, aby bola čo najmenšia šanca na úspešný útok na ňu.

1.5.1. Nainštalovanie SSL certifikácie

Najjednoduchší spôsob ako si zabezpečiť svoju webovú stránku je inštalácia SSL certifikácie. Tá nám šifruje komunikáciu medzi webom a používateľom. Ako táto certifikácia funguje sme si už vysvetlili v predošlých podkapitolách

Pre ešte väčšiu bezpečnosť sa odporúča používať „Always-On“ SLL. Väčšina webových stránok používa šifrovanie SSL napríklad len na prihlasovacích stránkach alebo pri internetových obchodoch v nákupných košíkoch, resp. tam, kde sa pravdepodobne nachádzajú a vymieňajú dôverné údaje . To znamená, že niektoré interakcie návštevníkov s webovou stránkou nie sú šifrované a návštevník medzi nimi prepína a to ohrozuje ich bezpečnosť ale aj bezpečnosť webovej stránky. [14]

„Always-On“ SSL bojuje proti tomuto riziku šifrovaním všetkého od okamihu, keď návštevník príde na vašu stránku, až do momentu ich opustenia webstránky. Vďaka nemu je oveľa bezpečnejšie vyhľadávať, zdieľať a nakupovať online. Zákazníci vidia vo svojom prehliadači zelený visiaci zámok so šifrovaním SSL počas celej ich návštevy, čím dokážete, že vám záleží na bezpečnosti svojich návštevníkov webovej lokality ale aj na dobrom mene a dôveryhodnosti vašej webovej stránky. [14]

1.5.2. Používajte antimalvérový softvér

Mnoho predajcov a certifikačných autorít ponúka skenovanie zraniteľnosti a malvéru pre webové stránky. Napríklad niektorí poskytovatelia SSL certifikátov ponúkajú bezplatné skenovanie malvéru na vašom webe, keď si od nich kúpite certifikáty SSL. [14]

1.5.3. Udržujte svoj web aktuálny

Servery vašich webových stránok sú rovnako ako vaše osobné počítače pripojené na internet alebo do nejakej firemnej siete. Preto je veľmi dôležité pravidelne aktualizovať softvér na serveroch. Samotné servery majú operačný systém. Potom tam je aplikačný softvér, ktorý zobrazuje webové stránky na lokalite návštevníkov. Mnohé webové stránky navyše využívajú systémy na správu obsahu, ktoré umožňujú menej technicky zdatným používateľom vytvárať a upravovať webové stránky. Taktiež je veľmi dôležité mať správne nastavený firewall. [14] [19]

1.5.4. Minimalizácia prístupu

Je potrebné dbať na fyzickú bezpečnosť vašich serverov. Ak má, napríklad nejaký váš nespokojný zamestnanec fyzický prístup k serverom, môže na web nahrať škodlivý malvér alebo zjednodušiť prístup hackerom dostať sa na správu webu. Preto sa odporúča chrániť prístup priamo k serverom napr. dvojfázovou autentifikáciou. To znamená, že okrem použitia kľúčov je potrebné aj zadať heslo na klávesnici alebo použiť čítačku zamestnaneckých kariet. Taktiež je potrebné zamedziť prístup k sieti. To znamená, že ak útočníkom sa podarí preniknúť na váš web, celá vaša firemná sieť nebude odhalená. [14]

1.5.5. Pravidelné zálohovanie

Vytváranie záloh vášho webu zaisťuje, že ak by došlo k najhoršiemu, stále budete mať k dispozícii najnovšiu verziu vášho webu uloženú v bezpečí a pripravenú na opätovné spustenie. Záloha je v podstate kópia všetkých údajov z vašej webovej stránky, ako sú súbory, obsah, médiá a databázy. Ak máte komplikovanú webovú stránku, na uloženie všetkých údajov budete potrebovať väčšie množstvo záložného úložiska. [14]

1.5.6. Používajte neprelomiteľné heslá

Silné a neprelomiteľné heslo je také heslo, ktoré je nemožné uhádnuť, je aspoň pätnásť znakov dlhé, používa rôzne špeciálne znaky aby bolo takmer nemožné ho získať pomocou útoku hrubou silou. Je veľmi dôležité, aby ste heslá pravidelne menili. Ak by vaše heslo bolo prelomené, útočník by mal prístup k vášmu webu a ku všetkým citlivým dátam. [26]

1.6. Nástroje na analýzu bezpečnosti webových aplikácií

V tejto práci použijeme ako nástroj na analýzu SSL Server Test. Je voľne dostupný na webovej adrese: https://www.ssllabs.com/ssltest/ . Ďalej v tejto kapitole si povieme čo všetko analyzuje tento nástroj, a ako funguje.

1.6.1. SSL Server Rating metóda

SSL Server Rating slúži na ohodnotenie zabezpečenia webovej stránky špeciálnou metódou hodnotenia, ktorou umožňuje správcom spoľahlivo vyhodnotiť konfigurácie servera SSL bez toho, aby boli odborníkmi na SSL certifikáciu. Tento nástroj nám po úspešnom analyzovaní webu vypíše skóre a následne oznámkuje silu zabezpečenia webu. V následnej tabuľke môžeme vidieť stupnicu hodnotenia sily zabezpečenia webu. [15]

Skóre	Známka
>= 80	A
>= 65	B
>= 50	C
>= 35	D
>= 20	E
<20	F

Tabuľka 1 - Stupnica hodnotenia bezpečnosti webu podľa SSL Server Ratingu

Bodovanie funguje tak, že sa sledujú tri kategórie. Kategóriami sú podpora protokolov, výmena kľúčov a sila šifrovania. Následne sa sčíta skóre týchto troch kategórií do jednej známky. Percentuálne pomery bodovania môžeme vidieť v nasledujúcej tabuľke. [15]

Kategória	Skóre
Podpora protokolov	30%
Výmena kľúčov	30%
Sila šifrovania	40%

Tabuľka 2 - Percentuálne pomery bodovania podľa SSL Server Ratingu

Skóre prvej kategórie podpora protokolov sa vypočíta nasledovne. Najprv sa pozrie na protokoly podporované serverom SSL. Pretože server môže podporovať niekoľko protokolov, na dosiahnutie konečného skóre používa nasledujúci postup. Zoberie skóre najlepšieho protokolu, pripočíta k nemu skóre najhoršieho protokolu a výsledok vydelí číslom dva. [15]

Protokol	Skóre
SSL 2.0	0%
SSL 3.0	80%
TLS 1.0	90%
TLS 1.1	95%
TLS 1.2	100%

Tabuľka 3 - Stupeň hodnotenia kategórie podpora protokolov

Skóre druhej kategórie výmena kľúčov sa vypočíta nasledovne. Skratka DH znamená Diffie-Hellman key exchange algoritmus. [15]

Aspekt výmeny kľúčov	Skóre
Slabý kľúč (chyba Debian OpenSSL)	0%
Anonymná výmena kľúčov (bez autentifikácie)	0%
Sila kľúča alebo parametra DH < 512 bitov	20%
Exportovateľná výmena kľúčov (obmedzená na 512 bitov)	40%
Sila kľúča alebo parametra DH < 1024 bitov (napr. 512)	40%
Sila kľúča alebo parametra DH < 2048 bitov (napr. 1024)	80%
Sila kľúča alebo parametra DH < 4096 bitov (napr. 2048)	90%
Sila kľúča alebo parametra DH >= 4096 bitov (napr. 4096)	100%

Tabuľka 4 - Stupeň hodnotenia kategórie výmena kľúčov

Skóre tretej kategórie sila šifrovania sa vypočíta nasledovne. [15]

Sila šifrovania	Skóre
0 bitov (bez šifrovania)	0%
< 128 bitov (napr. 40, 56)	20%
< 256 bitov (napr. 128, 168)	80%
>= 256 bitov (napr. 256)	100%

Tabuľka 5 - Stupeň hodnotenia kategórie sila šifrovania

[15]

2. Cieľ práce, Metodika práce a metódy skúmania

V tejto kapitole si charakterizujeme hlavný cieľ práce a taktiež metodiku práce a metódy skúmania. Začneme cieľom práce a ďalej budeme pokračovať metodikou a metódami.

2.1. Cieľ práce

Práca si dáva za cieľ analyzovať riziká a slabé miesta konkrétnych webových stránok z rôznych pohľadov. Každá webová stránka, portál alebo webová aplikácia je vystavená možnému riziku útoku s cieľom poškodenia alebo ukradnutia dôležitých informácií a dát. Preto je veľmi dôležité dbať na ochranu a bezpečnosť webovej stránky pre čo najväčšie minimalizovanie ohrozenia. Okrem poukázania na riziká a slabé miesta je dôležité sa oboznámiť s normami a certifikáciami, ktoré súvisia s ochranou a bezpečnosťou internetových stránok. Vďaka týmto normám a certifikáciám, akými sú napríklad ISO 27001, PCI DSS, SSL, TLS a tak ďalej, vieme čo najlepšie zabezpečiť webové stránky. Ďalej je veľmi dôležité urobiť prehľad a vysvetlenie rôznych spôsobov, akými sú vykonávané útoky a následné opatrenia, ako sa im vieme čo najlepšie vyvarovať. Najčastejšie útoky sú SQL Injection, Cross Site Scripting (XSS), DDOS útoky atď. Následne pomocou webových nástrojov vieme vykonať podrobné analýzy slabých miest a rizík na ľubovoľných, nami zadaných URL adries webových stránok, portálov alebo aplikácií. Vzhľadom na nevhodnosť navrhovaného softvéru v anotácii sme urobili zmenu. Počas písania bakalárskej práce sa ukázalo, že navrhnutý softvér v anotácii nebol vhodný pre náš cieľ a teda sme zvolili iný prístup. Namiesto digitálneho WWW archívu „Wayback Machine“ sme použili metódu SSL Server Rating. Vďaka analýze vieme zistiť nedostatky, ktoré ak opravíme už nebudú znamenať hrozbu a nebudú slabinou pre možné útoky.

2.2. Metodika práce a metódy skúmania

Pre dosiahnutie cieľa tejto bakalárskej práce bolo potrebné získať poznatky z odbornej literatúry, ktorá je zameraná na bezpečnostné riziká a nedostatky na webových stránkach, taktiež certifikácie a normy, ktoré sa zaoberajú ochranou webových stránok a literatúru, ktorá popisuje rôzne spôsoby útokov, vďaka ktorým vieme pri analýze webstránok porovnávať ich bezpečnosť. Informácie o týchto problematikách sme čerpali z niekoľkých kníh ale najmä z literatúry získanej zo zahraničných internetových zdrojov a rôznych vedeckých štúdií, pretože v knižných podobách a to na internete a v SR bolo pre nás použiteľných zdrojov veľmi málo.

Na začiatku prvej kapitoly sme sa zamerali na krátku históriu webstránok a technické pojmy napr. rozdiel medzi webovou stránkou a portálom. Pokračujeme potom charakteristikou a vymenovaním noriem a certifikácií, ktoré sa zaoberajú bezpečnosťou internetových stránok. Pri certifikáciách sme sa zamerali hlavne na SSL a TLS certifikácie, ktoré sú veľmi dôležité pre správnych chod stránok v dnešnej dobe. Následne sme sa zaoberali možnými bezpečnostnými rizikami a chybami. Vymenovali sme si najčastejšie metódy útokov na webové stránky a potom ako si správne zabezpečiť svoje webstránky aby sme sa vyvarovali útokom. Nakoniec sme sa zaoberali nástrojmi na analýzu bezpečnosti a popísali sme si ako fungujú a následne ich použijeme v praktickej časti.

Praktická časť sa zaoberá analýzou konkrétnych webových stránok s využitím problematiky rizík a bezpečnostných chýb. V praktickej časti používame nástroje na analýzu bezpečnosti a to konkrétnu metódu SSL Server Rating. Vďaka ktorej následne porovnávame zabezpečenie rôznych stránok podľa stupňa ohodnotenia tejto metódy a prípadne čo by sa malo na nich zlepšiť. Túto metódu testovania sme si vybrali z dôvodu praktickosti a pretože sa zameriava na viaceré aspekty bezpečnosti, rizík a slabých miest na webových lokalitách a je teda pre náš cieľ ideálna.

3. Výsledky práce a diskusia

V tejto kapitole sa zameriavame na samotnú analýzu rizík a slabých miest webových stránok z hľadiska bezpečnosti. Taktiež si popíšeme podrobne protokoly a certifikácie, ktoré využíva metóda s ktorou budeme analyzovať webové stránky.

3.1. Rozdiel medzi SSL a TLS

Keď hovoríme o certifikátoch SSL/TLS, hovoríme o digitálnych súboroch X.509, ktoré umožňujú obsluhovať webové stránky cez HTTPS (použitím zabezpečeného protokolu TLS nad nezabezpečeným HTTP pripojením) pomocou šifrovania verejného kľúča. Štandard X.509 je založený na jazyku popisu rozhrania známom ako „Abstract Syntax Notation One“ (ASN.1) , ktorý definuje dátové štruktúry, ktoré možno serializovať a deserializovať naprieč rôznymi platformami. Formát certifikátu X.509 používa súvisiaci pár verejných a súkromných kľúčov na šifrovanie a dešifrovanie správy. [18] [27]

Možné dôvody, prečo ľudia označujú SSL a TLS za rovnaké certifikáty: [18]

- Obidva sú zabezpečené protokoly, ktoré vytvárajú šifrovanú komunikáciu medzi webovým serverom a klientom (prehliadačom) cez HTTPS.
- TLS je nástupcom protokolu SSL a keďže väčšina ľudí už dobre poznala protokol SSL, bolo jednoduchšie používať pojem SSL namiesto TLS.

Dôvodom, prečo sa líšia, je ten, že TLS je nástupcom protokolu SSL. Pri porovnaní SSL a TLS sa protokoly SSL a TLS líšia vo svojich funkciách, autentifikácii správ, výstražných správach, protokole záznamu a sile šifrovania. Líšia sa tiež najmä z hľadiska procesu, ktorý je známy ako „SSL/TLS handshake“. Tento proces sa vykonáva, keď obe strany (klient a server) navzájom komunikujú. „Handshake“ (v preklade podávanie rúk) je zodpovedný za určenie typu šifrovania, ktoré sa použije na zabezpečenie údajov počas transakcie, autentifikácii servera alebo oboch strán a generovanie a výmena kľúčov relácie, ktoré sa budú používať počas transakcie. [18]

Taktiež si musíme všimnúť rozdiel medzi tým, ako SSL a TLS nadväzujú pripojenia. Napríklad pri „handshake“ SSL vytvára explicitné spojenia cez port. TLS na druhej strane uľahčuje implicitné pripojenia prostredníctvom protokolu. Tento „handshake“ funguje na špecifických metódach/algoritmoch nazývaných „cipher suites (balíky šifier)“. Zásadný rozdiel medzi SSL a TLS spočíva v týchto balíkoch šifier, ktoré zohrávajú významnú úlohu v bezpečnosti pripojenia. Balíky šifier zahŕňa algoritmus výmeny kľúčov, algoritmus overovania/validácie, algoritmus hromadného šifrovania a algoritmus kódu na overenie správ (MAC). Každá verzia SSL/TLS má svoju vlastnú podporovanú sadu balíkov šifier a novšie verzie neustále prichádzajú s bezpečnejšími balíkmi šifier, ktoré zlepšujú bezpečnosť a výkon pripojenia. Tieto dva protokoly SSL a TLS sme si popísali ako fungujú, pretože ich používa metóda, s ktorou budeme analyzovať konkrétne webové lokality. [18]

3.2. SHA256 s podpisom RSA

SHA256 s podpisom RSA je efektívna metóda asymetrického šifrovania používaná v mnohých bezpečnostných API. Algoritmus najprv vypočíta jedinečný vstupný „hash“ pomocou algoritmu SHA256. „Hash“ sa používa na overenie, či údaje nie sú upravené, nemanipulované alebo poškodené. Inými slovami, môžeme overiť, či si údaje zachovali integritu. „Hash“ sa potom zašifruje súkromným kľúčom pomocou algoritmu RSA. Iba „hash“ šifrovanie je oveľa rýchlejšie vďaka svojej malej veľkosti. Generovanie kľúča pre algoritmus RSA je nasledovné: Vyberte dve rôzne prvočísla p a q. Z bezpečnostných dôvodov by celé čísla p a q mali byť vybrané náhodne a mali by mať podobnú veľkosť, ale mali by sa líšiť v dĺžke o niekoľko číslic, aby sa rozklad na súčiniteľov sťažil. Tento SHA256 s RSA sme si popísali, pretože sa bude často vyskytovať v analýzach našich konkrétnych webových stránok. [20] [28]

3.3. Diffie-Hellman výmena kľúčov

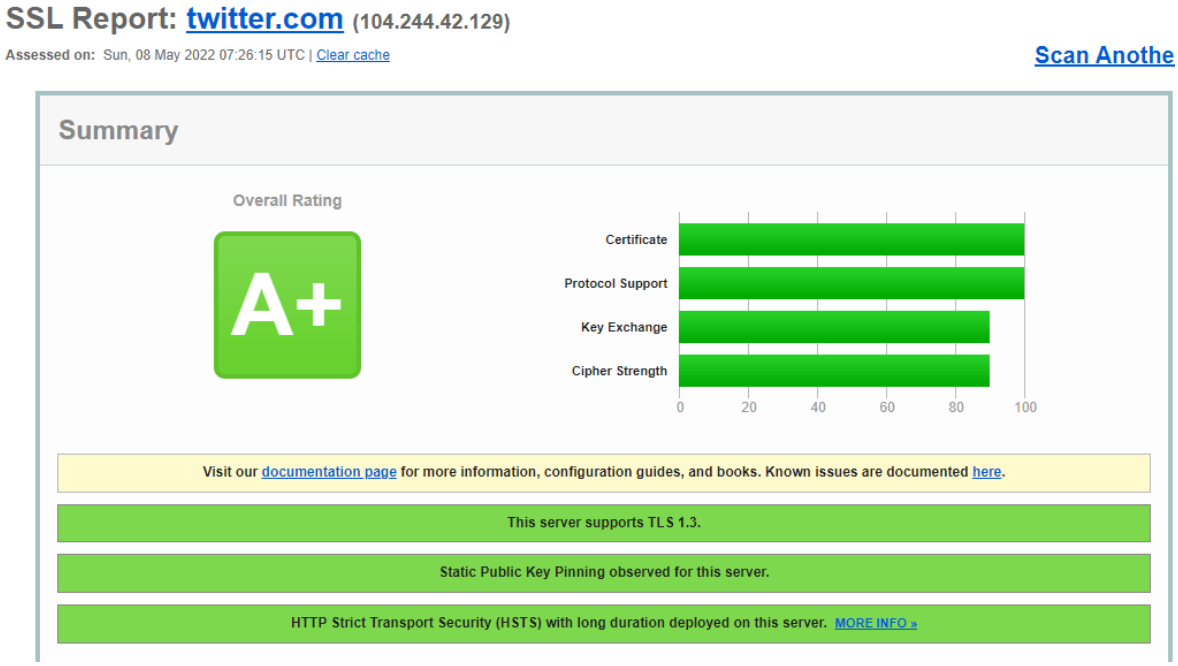
Výmena kľúčov Diffie-Hellman je jedným z najdôležitejších pokrokov v kryptografii s verejným kľúčom a dodnes sa často implementuje v rôznych bezpečnostných protokoloch. Hlavným účelom výmeny kľúčov Diffie-Hellman je bezpečne vyvinúť zdieľané tajomstvo, ktoré možno použiť na odvodenie kľúčov. Tieto kľúče potom možno použiť s algoritmami symetrických kľúčov na prenos informácií chráneným spôsobom. Symetrické algoritmy sa často používajú na šifrovanie väčšiny údajov, pretože sú efektívnejšie ako algoritmy verejného kľúča. Ako jedna z najbežnejších metód bezpečnej distribúcie kľúčov sa výmena kľúčov Diffie-Hellman zvyčajne implementuje v bezpečnostných protokoloch, ako sú TLS, IPsec, SSH atď. Vďaka tomu je neoddeliteľnou súčasťou našej bezpečnej komunikácie. [21]

3.4. Analýza bezpečnosti konkrétnych webových stránok

Táto podkapitola je zameraná na samotnú analýzu slabých miest a nedostatkov alebo naopak veľmi dobrej bezpečnosti. Pre porovnanie si spravíme analýzu troch rôznych webstránok popíšeme si ich nedostatky a nakoniec ich porovnáme medzi sebou. Vybrali sme si nakoniec tri webové lokality. Prvú sme si zvolili, pretože má ukážkové zabezpečenie. Ako druhú webovú lokalitu sme si zvolili známu sociálnu sieť, ktorú používa veľké množstvo z nás a chceme v analýze zistiť, ako dobre je zabezpečená. Poslednú tretiu webovú stránku sme si zvolili pre demonštrovanie veľmi zlého zabezpečenia a popisu rizík, náhodnú veľmi zle zabezpečenú webovú stránku.

3.4.1. Analýza prvej webovej stránky

Ako prvú webovú lokalitu sme si zvolili známu sociálnu sieť twitter. Spustíme si analýzu pomocou metódy SSL server test (ktorú sme si podrobne popísali v podkapitole 1.6.1) a po pár minútach máme výsledok. Na obrázku nižšie môžeme vidieť aké ohodnotenie táto webová stránka získala.



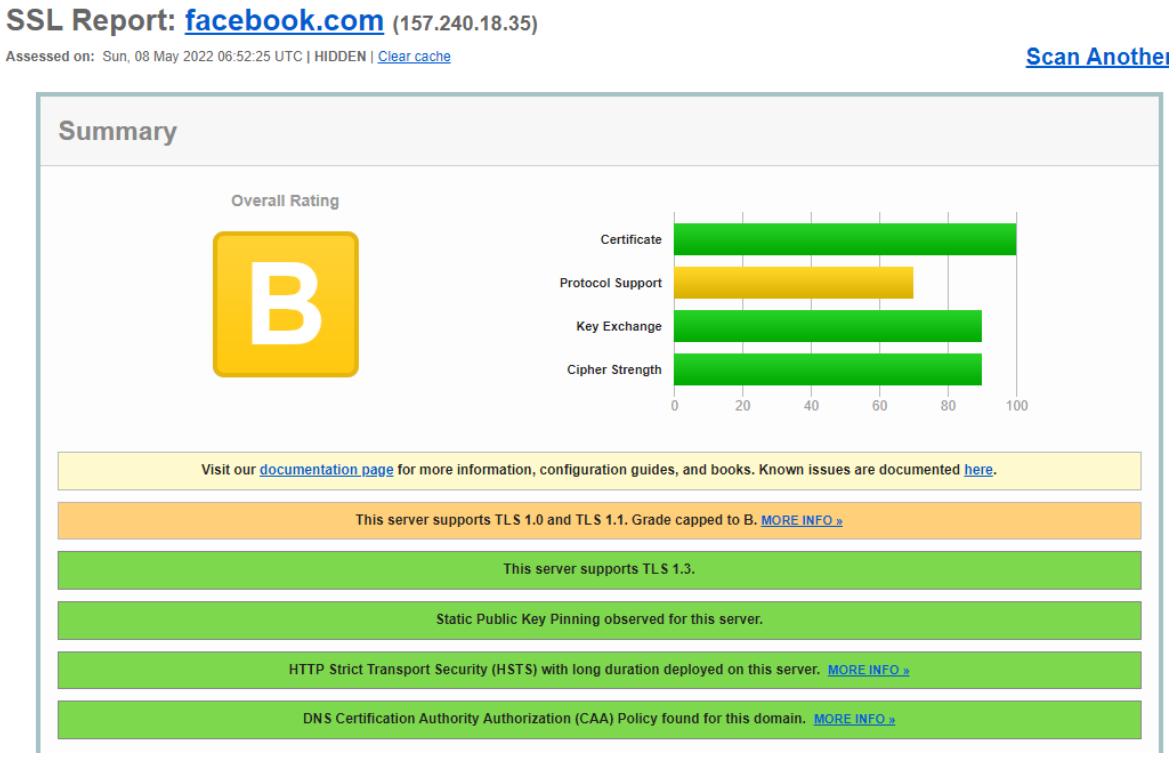
Obrázok 4 - Výsledok analýzy webstránky twitter.com

Môžeme pozorovať, že zabezpečenie tejto stránky získalo najvyššie možné hodnotenie. To znamená, že je chránená proti všetkým známym možným útokom. Môžeme teda vylúčiť útoky typu SQL Injection alebo Cross Site Scripting atď. Používa najaktuálnejšie TLS certifikácie a to verziu 1.3 a 1.2, ktoré sú zatiaľ neprelomené a nemajú známu chybu alebo slabinu. Na šifrovanie používa certifikát RSA 2048 bitový (SHA256 s RSA), ktorý je veľmi bezpečný.

Najväčšou hrozbou pre túto webstránku je teda DDoS útok. Posledný veľký útok, ktorý dokázal vyradiť twitter bol v roku 2016. Niekoľko veľkých DDoS útokov na Dyn, ktorý je poskytovateľ DNS zapríčinil výpadky niekoľkých veľkých stránok a medzi nimi bol aj twitter. [22]

3.4.2. Analýza druhej webovej stránky

Ako druhú webovú lokalitu sme si zvolili taktiež veľmi známu sociálnu sieť facebook. Spustíme si analýzu pomocou metódy SSL server test (ktorú sme si podrobne popísali v podkapitole 1.6.1) a po pár minútach máme výsledok. Na obrázku nižšie môžeme vidieť aké ohodnotenie táto webová stránka facebook získala.



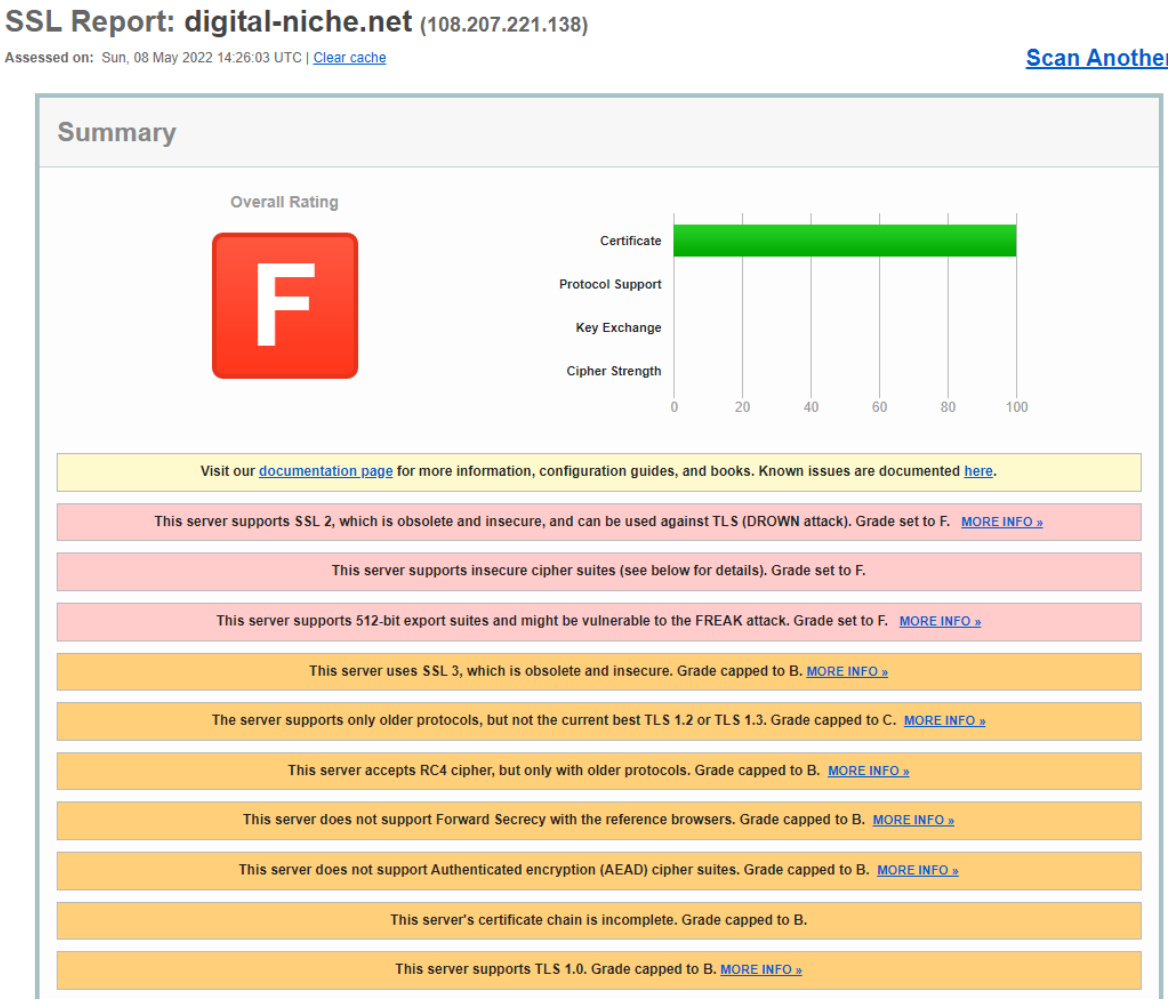
Obrázok 5 - Výsledok analýzy webstránky facebook.com

Oproti predchádzajúcej analýze tu môžeme vidieť nižšie hodnotenie. Dôvodom je okrem podpory najnovšej verzie certifikácie TLS 1.3, taktiež aj podporuje certifikácie TLS 1.0 a TLS 1.1, ktoré boli prelomené v roku 2020. Dôvodom prečo facebook podporuje tieto prelomené certifikácie je prístup na ich webstránku zo starších zariadení, napríklad smartfónov s Android verziou 4.3 alebo nižšie. Okrem tohto slabého miesta využíva na šifrovanie certifikát EC 256 bitový (SHA256 s RSA) na niektorých zariadeniach a na ostatných certifikát RSA 2048 bitový (SHA256 s RSA).

Posledný veľký výpadok tejto webstránky bol v októbri 2021, keď údajne kvôli chybe pri konfigurácii BGP routerov ich spoločnosti prestalo fungovať DNS a užívatelia sa nemohli dostať na ich web, ale aj všetky ostatné aplikácie, ktoré vlastní rovnaká spoločnosť. [23]

3.4.3. *Analýza tretej webovej stránky*

Ako poslednú stránku sme si pre ukážku zlého zabezpečenia zvolili web digital-niche.net, ktorý má veľké nedostatky. Na obrázku nižšie môžeme vidieť aké ohodnotenie táto webová stránka získala.



Obrázok 6 - Výsledok analýzy webstránky digital-niche.net

Táto webstránka získala najhoršie možné ohodnotenie z analýzy. Podporuje certifikát SSL 2, ktorý je nebezpečný a dávno prelomený. Dôvodom podpory tohto certifikátu je podpora veľmi starých zariadení. Taktiež používa nedostatočné šifrovanie a len 512-bitové exportné balíky. Web je bezbranný proti útokom akými sú napr. drown alebo freak. Jediné pozitívum je použitie certifikátu RSA 2048-bitový (SHA256 s RSA). Najjednoduchším spôsobom ako opraviť tieto bezpečnostné chyby je zrušiť podporu certifikátu SSL 2 a prejsť len na najnovšie TLS 1.3 alebo TLS 1.2.

3.4.4. Porovnanie analýz

V tejto časti si nakoniec porovnáme všetky analýzy navzájom. V predchádzajúcich podkapitolách sme analyzovali tri konkrétne webstránky a rozpísali sme si ich potencionálne slabé miesta. Porovnanie môžeme vidieť v tabuľke nižšie.

	twitter.com	facebook.com	digital-niche.net
Certifikát	RSA 2048 bitový (SHA256 s RSA)	EC 256 bitový RSA 2048 bitový (SHA256 s RSA) – pre oboje	RSA 2048 bitový (SHA256 s RSA)
Podpora protokolov	100%	70%	0%
Výmena kľúčov	90%	90%	0%
Sila šifrovania	90%	90%	0%
Celkové ohodnotenie	A+	B	F

Tabuľka 6 - Porovnanie analýz

Z tohto porovnania nám vyplýva, že sme natrafili na veľmi dobre zabezpečený web ale aj na nezabezpečenú webovú stránku. Každá z týchto webových stránok má určité nedostatky v sile šifrovania a vo výmene kľúčov, zatiaľ čo prvé dve stránky majú len veľmi malé nedostatky pri poslednej sa jedná o závažné bezpečnostné chyby. Čo sa týka podpory protokolov sa pri prvej webovej stránke nemáme čím zaoberať. Druhá webstránka má nedostatky kvôli podpore prelomených protokolov TLS 1.0 a TLS 1.1. Tretia stránka podporuje zastaralý protokol a je v jej záujme zrušiť túto podporu.

Záver

V tejto bakalárskej práci sme sa venovali rizikám a slabým miestam na konkrétnych webstránkach a ich následnej analýze na špecifických príkladoch. Vymenovali sme si certifikácie, normy a protokoly, ktoré sa zameriavajú na túto problematiku. Ďalej sme si popísali riziká a najčastejšie metódy útokov na webových stránkach. Nakoniec sme si popísali ako si chrániť bezpečnosť webových stránok a vyvarovať sa chybám, nedostatkom a útokom na tieto internetové lokality. Naučili sme sa veľa spôsobov a metód, akými sú webové stránky ohrozené ale aj ako sa chrániť a používať bezpečnostné normy a certifikácie.

Pri metódach útokov sme si ich podrobne popísali. Čo sú tie útoky zač, ako fungujú a aké chyby využívajú na ich vykonanie. Nakoniec sme si povedali ako sa brániť proti týmto najčastejším metódam útokov podľa organizácie OWASP a tiež sme pridali ďalšie známe útoky akými sú napr. DDoS.

Ďalej sme si vypísali ako si správne zabezpečiť webovú stránku. Vymenovali sme si použitie bezpečnostných certifikácií a protokolov. Taktiež sme si povedali najpoužívanejšie praktiky a tipy, ktoré sú potrebné pre efektívnu ochranu webstránok. Naučili sme sa viacero praktických spôsobov, ako sa chrániť a vyvarovať proti útokom na webových lokalitách.

V praktickej časti sme začali s analýzou bezpečnosti konkrétnych webových stránok. Na túto analýzu sme použili aplikáciu a metódu SSL Server Test, ktorú sme si popísali v prvej kapitole ako funguje a čo to je. Následne sme si zvolili tri náhodné webové stránky a to twitter.com, facebook.com a digital-niche.net. Tie sme v menovanej aplikácií nechali analyzovať niekoľko minút a následne sme získali ohodnotenia bezpečnosti daných stránok. Tieto analýzy sme si rozobrali a nakoniec sme ich medzi sebou porovnali. V analýze sme dosiahli k záveru, že aj najväčšie a najpoužívanejšie webové stránky a portály majú riziká a slabé miesta.

Zoznam použitej literatúry

[1]. HRŮZA, P. et al. Kybernetická bezpečnost. . Brno: Univerzita obrany, 2012. ISBN 978-80-7231-914-5

[2]. Niels Brügger and Ralph Schroeder (eds.), The Web as History. London, UCL Press, 2017. ISBN: 978–1–911307–56–3

[3]. A short history of the Web [Online]

https://home.cern/science/computing/birth-web/short-historyweb#:~:text=Where%20the%20Web%20was%20born,and%20institutes%20around%20the%20world.

[4]. Bud E. Smith and Arthur Bebak, Creating Web Pages For Dummies, 7th Edition, Wiley Publishing, Inc., 111 River Street Hoboken, NJ 07030-5774 ISBN: 0-7645-7327-6

[5]. Aký je rozdiel medzi portálom a webovou stránkou [Online] https://sk.strephonsays.com/what-is-the-difference-between-portal-and-website

[6]. Zhang, Liang; Choffnes, David; Levin, Dave; Dumitras, Tudor; Mislove, Alan; Schulman, Aaron; Wilson, Christo (2014). [ACM Press the 2014 Conference - Vancouver, BC, Canada (2014.11.05-2014.11.07)] Proceedings of the 2014 Conference on Internet Measurement Conference - IMC '14 - Analysis of SSL certificate reissues and revocations in the wake of heartbleed. , (), 489–502. doi:10.1145/2663716.2663758

[7]. ISO 27001: The International Information Security Standard [Online] https://www.itgovernance.co.uk/iso27001

[8]. What is PCI Compliance? [Online] https://digitalguardian.com/blog/what-pci-compliance

[9]. Health Insurance Portability and Accountability Act of 1996 (HIPAA) [Online] https://www.cdc.gov/phlp/publications/topic/hipaa.html

[10]. General Data Protection Regulation (GDPR) [Online]

https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

[11]. Čo je SSL certifikát a prečo by ho mal mať aj váš web? [Online] https://www.digmia.com/sk/blog/co-je-ssl-certifikat-preco-ho-mal-mal-aj-vas-web/

[12]. Muscat, Ian (2016). Web vulnerabilities: identifying patterns and remedies. Network Security, 2016(2), 5–10. doi:10.1016/S1353-4858(16)30016-2

[13]. 10 Most Common Web Security Vulnerabilities [Online] https://www.guru99.com/web-security-vulnerabilities.html

[14]. John Wiley & Sons, Ltd, Website Security For Dummies, John Wiley & Sons, Ltd The Atrium Southern Gate Chichester West Sussex PO19 8SQ England, ISBN: 978-1-118-94830-9

[15]. SSL Server Rating Guide [Online] https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

[16]. What is a DDoS attack? [Online] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[17]. The OWASP Top 10 Has Been Updated and You Need to Read It [Online] https://www.goldsecurity.com/the-owasp-top-10-has-been-updated-and-you-need-to-read-it/

[18]. SSL vs TLS: Decoding the Difference Between SSL and TLS [Online] [Dátum 23.3.2020]

https://sectigostore.com/blog/ssl-vs-tls-decoding-the-difference-between-ssl-and-tls/#:~:text=SSL%20is%20a%20cryptographic%20protocol,the%20successor%20of%20SSL%20protocol.

[19]. Alena Kabelová a Libor Dostálek, Velký průvodce protokoly TCP/IP a systémem DNS, Computer Press, Brno 2008, ISBN 8025122365

[20]. What is RSA with SHA256? [Online] [Dátum 17.5.2020]

https://www.rampfesthudson.com/what-is-rsa-with-sha256/#:~:text=SHA256%20with%20RSA%20signature%20is,due%20to%20its%20small%20size.

[21]. What is the Diffie–Hellman key exchange and how does it work? [Online] [Dátum 23.3.2021] https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/

[22]. Large DDoS attacks cause outages at Twitter, Spotify, and other sites [Online] [Dátum 21.10.2016] https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

[23]. The Facebook Outage Wasn't a DDoS attack, but it Shines the Light on Digital Resilience Planning [Online] [Dátum 5.10.2021] https://www.a10networks.com/blog/the-facebook-outage-wasnt-a-ddos-attack-but-it-shines-the-light-on-digital-resilience-planning/

[24]. Interpreter [Online] [Dátum 12.8.2020]

https://www.techopedia.com/definition/7793/interpreter

[25]. Token-Based Authentication: How to Optimize your Website [Online] [Dátum 6.7.2020] https://swoopnow.com/token-based-authentication/

[26]. How to create a strong password [Online] [Dátum 15.8.2018] https://blog.avast.com/strong-password-ideas

[27]. What Is an X.509 Certificate & How Does It Work? [Online] [Dátum 7.1.2021]

https://sectigo.com/resource-library/what-is-x509-certificate

[28]. Hashing [Online] https://cybersecurityglossary.com/hashing/