GOCE DELCEV UNIVERSITY, SHTIP, NORTH MACEDONIA

FACULTY OF ELECTRICAL ENGINEERING

ETIMA 2021

FIRST INTERNATIONAL CONFERENCE

19-21 OCTOBER, 2021

TECHNICAL SCIENCES APPLIED IN ECONOMY, EDUCATION AND INDUSTRY

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ” - ШТИП
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

UNIVERSITY „GOCE DELCHEV” - SHTIP
FACULTY OF ELECTRICAL ENGINEERING

ПРВА МЕЃУНАРОДНА КОНФЕРЕНЦИЈА
FIRST INTERNATIONAL CONFERENCE

ЕТИМА / ETIMA 2021

ЗБОРНИК НА ТРУДОВИ
CONFERENCE PROCEEDINGS

19-21 Октомври 2021| 19-21 October 2021

Главен и одговорен уредник / Editor in Chief
Проф.д-р Сашо Гелев
Prof.d-r Saso Gelev

Јазично уредување / Language Editor
Весна Ристова (Македонски) / Vesna Ristova (Macedonian)

Техничко уредување / Technical Editing
Доц.д-р Далибор Серафимовски / d-r Dalibor Serafimovski

Издавач / Publisher
Универзитет „Гоце Делчев" - Штип / University Goce Delchev - Stip
Електротехнички факултет / Faculty of Electrical Engineering

Адреса на организационен комитет / Adress of the organizational committee
Универзитет „Гоце Делчев" – Штип / University Goce Delchev - Stip
Електротехнички факултет / Faculty of Electrical Engineering
Адреса: ул. „Крсте Мисирков" бр. 10-А / Adress: Krste Misirkov, 10 - A
Пош. фах 201, Штип - 2000, С.Македонија / PO BOX 201, Stip 2000, North Macedonia
E-mail: conf.etf@ugd.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

62-049.8(062)
004-049.8(062)

МЕЃУНАРОДНА конференција ЕТИМА (1 ; 2021)
Зборник на трудови [Електронски извор] / Прва меѓународна конференција ЕТИМА 2021, 19-21 Октомври 2021 = Conference proceedings / First international conferece ETIMA 2021, 19-21 October 2021 ; [главен и одговорен уредник Сашо Гелев]. - Штип: Универзитет "Гоце Делчев", Електротехнички факултет = Shtip: University "Goce Delchev", Faculty of Electrical Engineering, 2021

Начин на пристапување (URL): https://js.ugd.edu.mk/index.php/etima. - Текст во PDF формат, содржи 358 стр.илустр. - Наслов преземен од екранот. - Опис на изворот на ден 15.10.2021. - Трудови на мак. и англ. јазик. - Библиографија кон трудовите

ISBN 978-608-244-823-7

1. Напор. ств. насл.
а) Електротехника -- Примена -- Собири б) Машинство -- Примена -- Собири
в) Автоматика -- Примена -- Собири г) Информатика -- Примена -- Собири

COBISS.MK-ID 55209989

Прва меѓународна конференција ЕТИМА
19-21 Октомври 2021
First International Conference ETIMA
19-21 October 2021

ОРГАНИЗАЦИОНЕН ОДБОР
ORGANIZING COMMITTEE

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Маја Кукушева Панева / Maja Kukuseva Paneva
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Весна Конзулова / Vesna Konzulova
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Прва меѓународна конференција ЕТИМА
19-21 Октомври 2021
First International Conference ETIMA
19-21 October 2021

ПРОГРАМСКИ И НАУЧЕН ОДБОР
SCIENTIFIC COMMITTEE

Со Ногучи / So Noguchi
Висока школа за информатички науки и технологии
Универзитет Хокаидо, Јапонија
Graduate School of Information Science and Technology
Hokkaido University, Japan

Дионис Гашпаровски / Dionýz Gašparovský
Факултет за електротехника и информациони технологии,
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Антон Белан / Anton Beláň
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Георги Иванов Георгиев / Georgi Ivanov Georgiev,
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Ивелина Стефанова Балабанова / Ivelina Stefanova Balabanova,
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Бојан Димитров Карапенев / Boyan Dimitrov Karapenev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Влатко Чингоски / Vlatko Cingoski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Божо Крстајиќ / Bozo Krstajic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Милован Радуловиќ / Milovan Radulovic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Гоце Стефанов / Goce Stefanov
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Мирјана Периќ / Mirjana Peric
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Ана Вучковиќ / Ana Vuckovic
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Мирослава Фаркаш Смиткова / Miroslava Farkas Smitková
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Петер Јанига / Peter Janiga
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Јана Радичова / Jana Raditschová,
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Александар Туџаров / Aleksandar Tudzarov
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Владимир Талевски / Vladimir Talevski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

PREFACE

The Faculty of Electrical Engineering at University Goce Delcev (UGD), has organized the International Conference ***Electrical Engineering, Informatics, Machinery and Automation - Technical Sciences applied in Economy, Education and Industry-ETIMA*.**
ETIMA has a goal to gather the scientists, professors, experts and professionals from the field of technical sciences in one place as a forum for exchange of ideas, to strengthen the multidisciplinary research and cooperation and to promote the achievements of technology and its impact on every aspect of living. We hope that this conference will continue to be a venue for presenting the latest research results and developments on the field of technology.
Conference ETIMA was held as online conference where contributed more than sixty colleagues, from six different countries with forty papers.
We would like to express our gratitude to all the colleagues, who contributed to the success of ETIMA'21 by presenting the results of their current research activities and by launching the new ideas through many fruitful discussions.
We invite you and your colleagues also to attend ETIMA Conference in the future. One should believe that next time we will have opportunity to meet each other and exchange ideas, scientific knowledge and useful information in direct contact, as well as to enjoy the social events together.

The Organizing Committee of the Conference

ПРЕДГОВОР

Меѓународната конференција ***Електротехника, Технологија, Информатика, Машинство и Автоматика-технички науки во служба на економија, образование и индустрија-ЕТИМА*** е организирана од страна на Електротехничкиот факултет при Универзитетот Гоце Делчев.
ЕТИМА има за цел да ги собере на едно место научниците, професорите, експертите и професионалците од полето на техничките науки и да представува форум за размена на идеи, да го зајканува мултидисциплинарното истражување и соработка и да ги промовира технолошките достигнувања и нивното влијание врз секој аспект од живеењето. Се надеваме дека оваа конференција ќе продолжи да биде настан на кој ќе се презентираат најновите резултати од истражувањата и развојот на полето на технологијата.
Конференцијата ЕТИМА се одржа online и на неа дадоа свој допринос повеќе од шеесет автори од шест различни земји со четириесет труда.
Сакаме да ја искажеме нашата благодарност до сите колеги кои допринесоа за успехот на ЕТИМА'21 со презентирање на резултати од нивните тековни истражувања и со лансирање на нови идеи преку многу плодни дискусии.

Ве покануваме Вие и Вашите колеги да земете учество на ЕТИМА и во иднина. Веруваме дека следниот пат ќе имаме можност да се сретнеме, да разменime идеи, знаење и корисни информации во директен контакт, но исто така да уживаме заедно и во друштвените настани.

Организационен одбор на конференцијата

Содржина / Table of Contents

ASSESSING DIGITAL SKILLS AND COMPETENCIES OF PUBLIC ADMINISTRATION AND DEFINING THEIR PROFICIENCY LEVEL 12

PWM OPERATION OF SYNCHRONOUS PERMANENT MAGNET MOTOR 21

SPEED REGULATION OF INDUCTION MOTOR WITH PWM INVERTER 30

WI-FI SMART POWER METER 42

RF SENSOR SMART NETWORK 50

FREQUENCY SINUS SOURCE 62

MEASUREMENT ON COMPENSATION CAPACITANCE IN INDUCTIVE NETWORK BY MICROCONTROLLER 70

ИЗРАБОТКА НА ВЕШТ НАОД И МИСЛЕЊЕ ОД ОБЛАСТА НА ЕЛЕКТРОТЕХНИЧКИТЕ НАУКИ 79

SIMULATION OF AN INDUSTRIAL ROBOT WITH THE HELP OF THE MATLAB SOFTWARE PACKAGE 86

BATTERY ENERGY STORAGE SYSTEMS AND TECHNOLOGIES:A REVIEW .. 95

POWER-TO-X TECHNOLOGIES 105

NEW INNOVATIVE TOURISM PRODUCT FOR REANIMATING RURAL AREAS 115

PROPOSED MODEL FOR BETTER ENGLISH LANGUAGE ACQUISITION, BASED ON WEARABLE DEVICES 123

OPEN SOURCE LEARNING PLATFORM – MOODLE 132

СПОРЕДБЕНА ТЕХНО-ЕКОНОМСКА АНАЛИЗА ПОМЕЃУ ТЕРМИЧКИ ИЗОЛИРАН И ТЕРМИЧКИ НЕИЗОЛИРАН СТАНБЕН ОБЈЕКТ 139

COMPARISON OF PERT AND MONTE CARLO SIMULATION 149

E-LEARNING – CYBER SECURITY CHALLENGES AND PROTECTION MECHANISMS 156

SECURITY AND PRIVACY WITH E-LEARNING SOFTWARE 164

ROOTKITS – CYBER SECURITY CHALLENGES AND MECHANISMS FOR PROTECTION 174

TOOLS AND TECHNIQUES FOR MITIGATION AND PROTECTION AGAINST SQL INJECTION ATACKS 182

INFLUENCE OF ROTATION ANGLE OF LUMINAIRES WITH ASYMMETRICAL LUMINOUS INTENSITY DISTRIBUTION CURVE ON CALCULATED PHOTOMETRIC PARAMETERS 189

PHOTOMETRIC PARAMETERS OF LED LUMINAIRES WITH SWITCHABLE CORRELATED COLOUR TEMPERATURE 197

ENERGY-EFFICIENT STREET LIGHTING SYSTEM OF THE CITY OF SHTIP USING SOLAR ENERGY AND LED TECHNOLOGY 204

NANOTECHNOLOGY–BASED BIOSENSORS IN DRUG DELIVERY SYSTEMS: A REVIEW 212

IOT SYSTEM FOR SHORT-CIRCUIT DETECTION OF DC MOTOR AT EKG-15 EXCAVATOR 222

DESIGN OF A PHOTOVOLTAIC POWER PLANT 231

DEVELOPMENT OF COMPUTER SOFTWARE FOR CREATING CHOREOGRAPHY 241

AUTOMATED SYSTEM FOR SMART METER TESTING 249

INFLUENCE DIMING OF LED LAMPS TO ELECTRICAL PARAMETERS 255

INRUSH CURRENT OF LAMP 261

COMPLEX EVALUATION MODEL OF A SMALL-SCALE PHOTOVOLTAIC INSTALLATION PROFITABILITY 269

IMPACT OF FAULTS IN TRANSMISSION AND DISTRIBUTION NETWORK ON VOLTAGE SAGS 278

ON APPLICABILITY OF BLACK-SCHOLES MODEL TO MSE 290

ACOUSTIC SIGNAL DENOISING BASED ON ROBUST PRINCIPAL COMPONENT ANALYSIS 300

INVESTIGATION OF EFFICIENCY ASPECTS IN 3×3 PHOTOVOLTAIC PLANT USING MODEL OF SHADING 309

PROGRESS OF NO-INSULATION HTS MAGNET DEVELOPMENT TOWARDS ULTRA-HIGH MAGNETIC FIELD GENERATION 319

GRID-CONNECTED HYBRID PV SYSTEM WITH BATTERY STORAGE 326

INVESTIGATION ON STABILITY OF PANCAKE COILS WOUND WITH BUNDLED MULTIPLE REBCO CONDUCTORS 336

ON-LINE МУЛТИМЕДИСКИ ОБРАЗОВНИ КАРТИЧКИ 343

АЛГОРИТАМОТ „ВЕШТАЧКА КОЛОНИЈА НА ПЧЕЛИ“ 352

UDC: 004.491:004.65.056.5

TOOLS AND TECHNIQUES FOR MITIGATION AND PROTECTION AGAINST SQL INJECTION ATACKS

Dimitar Bogatinov,[1] Goce Stevanoski,[2] Monika Kachurova[3]

[1]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, monikakacurova@hotmail.com
[2]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, goce.stevanoski@ugd.edu.mk
[3]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, dimitar.bogatinov@ugd.edu.mk

Abstract

Most of the services we enjoy on the Web are provided by database applications. Web-based email, online shopping, forums, corporate web sites, and portals are all database-driven. To build a modern web site, you need to develop a database application, usually a SQL database, which is responsible for managing data in a structured way. Recent attacks can lead ad to the conclusion that web applications are insufficiently protected and are the biggest threat to database security. The most popular form of attacks is the SQL injection attacks that use the data entry, search and username or password fields to inject code into the SQL database.
These attacks can detect sensitive data, alter database data, or destroy an entire database. An attacker could even damage the operating system. Usually, the SQL injection attacks are just an introduction to some other attacks, so preventing these attacks can also mean protection from other potentially more dangerous attacks. The purpose of this paper is to review the most common SQL Injection attacks, as well as to propose technical solutions and measures that can contribute to the mitigation of this kind of attacks.
Key words*: SQL injection, vulnerabilities, security, privacy*

Вовед и преглед на литература

Со напредувањето на технологијата, современото општество постигна многу незамисливи цели. Сепак, како што се развива технологијата, така се зголемува и ризикот вклучен во нејзиното користење. Ист е случајот со веб – апликациите. Од 2003 година, SQL Injection останува на списокот на OWASP безбедносни ризици со кои се борат компаниите. Нови случаи на ранливост на веб апликациите стануваат се потешки за да се пронајдат и да се искористат. Секоја веб апликација има база на податоци во позадина, и најмногу поради тоа нападите врз бази на податоци се случува преку слабостите во веб апликациите. Може слободно да заклучиме дека веб апликациите се недоволно добро заштитени, и се најголемата закана за безбедноста на базите на податоци кои се во нивната позадина на серверот.

Најсериозните напади на веб апликациите се оние во кои се доаѓа до чувствителни податоци или се добива пристап до системите што работат во позадината на апликацијата. За многу компании, било каков напад на системот што предизвикува прекин во работењето е критичен.

Според многу написи и споделени искуства, токму во областа на безбедносните веб апликациите се одвива голема битка помеѓу напаѓачите и оние кои се бранат со податоци и ресурси.

Карактеристики на "SQL"

"SQL" е кратенка за "Structured Query language" и широко се користи како јазик за бази со податоци, обезбедувајки средства за манипулација со податоците (чување, превземање, измена, бришење) и креирање на бази со податоци. Скоро сите модерни системи за управување со релационите бази со податоци како што се MS SQL Server, Microsoft Access, MSDE, Oracle, DB2, SyBase, MySQL, Postgre,

Informix, користат "SQL" како стандарден јазик за работа со базите на податоци. Прашалниците (Query) се примарни механизми за превземање на информации од базите со податоци и се состојат од прашања кои ја презентираат базата со податоци во соодветен формат. Во "SQL"-от постојат два вида на прашања:

- Data Definition Language (DDL)
- Data Manipulation Language (DML)

DDL прашалниците ја менуваат структурата на базата со податоци, додека DML прашалниците манипулираат со содржината на базата со податоци. "SQL Injection" се напади со вметнување на код во кој се вклучени влезните податоци во динамички конструиран "SQL" прашалник и се третира како "SQL" код. На Веб страните кај кои се користат бази со податоци, "SQL Injection" ранливоста е посебно изразена, затоа што напаѓачите лесно ги наогаат и продираат во базата со податоци. Едно истражување направено од "Gartner Group" дошло до сознание дека од преку 300 тестирани веб страни, дури 97% од нив биле ранливи на "SQL Injection". Со откривањето на "SQL Injection" ранливоста, напагачите обично ги извлекуваат и ги менуваат податоците со правење на DDL и DML прашалници.

Со мала измена во програмскиот код т.е. со воведување на додатни проверки е можно да се одбрани страната од поголем број напади со вметнување на SQL код. Секако, упорниот напаѓач и покрај тоа може да изведе SQL напад. Сепак ако некоја страна (и нејзината база на податоци) е добро заштитена, повеќето напаѓачи, ќе се откажат брзо и ќе пристапат кон напад на друга страница која не е толку добро заштитена.

Извори на напад на SQLI

Ранливоста на SQL инјектирањето може да се најде во кој било параметар на апликациите што можат да се користат во базата на податоци. Во понатамошниот текст наведени се четири извори, преку кои може да се започне SQL [1]:

Инјектирање со корисничка улога: Веб апликациите, генерално, користат форми за собирање на податоци од корисници (како што се регистрирање, најава итн.) или да дозволат на корисниците да ги специфицираат податоците што треба да се превземат (како што се пребарување, адаптиран приказ итн.). Овие форми што содржат „поле за текст" може да ги искористат напаѓачите за да инјектираат малициозен код што резултира со добивање тајни податоци.

Инјектирање преку колачиња: Неодамнешните веб-апликации користат колачиња за складирање на преференциите на корисниците. Колачињата се датотеки зачувани на клинтската машина кои содржат информации генерирани од веб апликациите. Напаѓачот може да вметне злонамерен код во содржината на колачињата зачувани во

неговиот компјутер, користејќи ја содржината на колачињата за да изгради SQL пребарувања кои се ранливи на напади.

Инјектирање преку сервер варијабили: Сервер варијабилите се збир на параметри кои содржат мрежни заглавија, HTTP податоци и варијабили на околината. Веб апликациите ги користат овие варијабили на серверот за ревизија на статичките податоци за употреба и идентификување на трендовите на прелистување. Ако овие променливи се зачувани во базата на податоци без валидација, напаѓачите можат да ја искористат оваа ранливост со поставување на SQLIA директно во варијабилите на серверот.

Зачувано инјектирање: Во зачуваното инјектирање напаѓачите вметнуваат малициозни влезови во базата на податоци за индиректно да вметнат SQLIA секој пат кога ќе се користи влезот [2].

Видови на напади на SQL

SQL нападот може да биде во неколку форми и во следниот дел се класифицираат главните типови на напади на SQLI[3].

Tautology: Општата цел на нападот базиран на tautology, е да внесе код во една или повеќе условени изјави, така што тие секогаш се проценуваат како вистинити. Најчестите начини на употреба се заобиколување на страниците за автентикација и извлекување на податоци.

Bling SQL инјекција: вид на напад на SQLI што ја прашува базата на податоци точни или погрешни прашања и го одредува одговорот врз основа на одговорот на апликацијата. Овој напад често се користи кога вел – апликацијата е конфигурирана да прикажува генерички пораки за грешки, но не го ублажила кодот што е ранлив на SQL инјекција

Union query: Во овој вид на напад, напаѓачот го користи операторот на UNION за да се приклучи на злонамерно барање до оригиналното барање, дозволувајќи му на напаѓачот да ги добие вредностие на колоните на другите табели.

Piggy-backed query: Во овој вид на напад, напаѓачот има намера да инјектира дополнителни пребарувања за да извлече податоци или да измени/додаде податоци. Напаѓачите инјектираат дополнителни пребарувања на оригиналното пребарување и како резултат, DBMS добива повеќе SQL пребарувања.

Зачувани процедури: Напаѓачот има за цел да преработува зачуваните процедури кои се веќе зачувани во базата на податоци. Притоа, повеќето постојни бази на податоци се проширени со стандарден сет на имплеметирани функции наречени складирани процедури кои овозможуваат дури и интеракција со оперативниот систем. Овие зачувани процедури генрално го избегнуваат повторното пишување на стандардни функции.

Алтернативно кодирање: Во алтернативното кодирање, напаѓачот се обидува да го скрие вметнатиот текст со цел да избегне откривање со дефанзивни практики за кодирање и техники на автоматска превенција. Поточно, алтернативните кодирања овозможуваат техники со кои напаѓачите ги избегнуваат контрамерките за откривање. Овие техники на затајување се широко користени од натрапникот, затоа што тие знаат дека повеќето IDS го скенираат барањето за одредени познати „лоши карактери“, како што се единечните понуди.

Нелегални/логичко неточни пребарувања: Во нелегално неточни пребарувања, напаѓачите имаат намера да внесат манипулиран пребарувач во базата на податоци за да генерираат порака за грешка која содржи некои информации за причината за грешката.

Валидирање на податоците

Најважен совет за заштита од напади со вметнување на SQL код е да се валидираат сите податоци коишто корисникот ќе ги внесе. Всушност, проследување на внесените податоци кон базата со податоци, без нивна претходна валидација, овозможува напади со вметнување на SQL код дури и на напагачите аматери. Во продолжение се наведени некои совети во врска со проверките на податоците пред да се проследат на базата со податоци:

Проверка на податоците би требало да се прави на серверската страна. Имено, доколку проверката се извршува на клиентската страна, напагачот може едноставно да ја добие веб страната како ".html" датотека и да го преработи делот со кодот каде што се прави проверката. После тоа напагачот може да ја стави веб страната локално и да праќа прашалници без притоа тие прашалници да се проверуваат.

Да се прилагоди типот на податоци кој се очекува. На пример, проверката на корисничкото име е различна од проверката на бројот на кредитната картица коишто корисникот ги внесува при интернет купувањето. Кај проверувањето на бројот на кредитната картица, треба да се провери дали навистина сите внесени карактери се броеви. Додека кај проверката на корисничкото име таква проверка нема смисла, затоа што корисничкото име може да се состои од букви, од броеви, од специјални знаци. Доколку добиените карактери не одговараат на очекуваниот тип на податоци, тогаш прашалникот не смее да се проследи кон базата со податоци.

Проверка на бројот на карактерите. Доколку бројот на карактери во полињата за внес на податоци не е ограничен, тогаш е потребно да се провери колку карактери има внесено корисникот. Преголем број на внесени карактери може да укажува на потенцијален напад. На пример, познато е колку карактери содржи бројот на кредитната картица. Доколку бројот на карактери што ќе ги внесе корисникот го преминуваат тој број, прашалникот во базата со податоци не би смеел да се изврши. Дополнително, 100 карактери во корисничкото име исто така треба да предизвикаат сомнеж дека е тоа регуларен внес на податоци.

Проверка на наводници. Во повеќето случаи корисниците немаат потреба од внесување на наводници (единечни или дупли). За разлика од нив, напагачите користат наводници во своите напади, како што е покажано претходно во претходниот дел. Заради тоа е добра пракса да се направи проверка дали постојат наводници пред да се обработат влезните податоци од корисниците.

Проверка на постоење на процедури. Процедурите може да им бидат на напагачите многу корисни алатки. Доколку се користи база со податоци Microsoft SQL Server, се препорачува да се провери постоење на низата „xp_" во корисничките податоци. Нивното постоење може да укаже на обид за напад со вметнување на SQL код кој ги користи претходно направените процедури како xp_cmdshell.

Техники за детекција и превенција

Проверувач на tautology: Статичката анализа се користи за да се спречи нападот на tautology. Аритметичките и логичките јамки се користат за да се провери можната SQL инјекција. Особено, сетот на SQL пребарувања кои програмата може да ги генерира како автомат со конечна состојба се приближни. Овој метод не е погоден за откривање на други напади на SQL инјекции.

AMNESIA: Техника која детектира и спречува напади со инјектирање на SQL. Комбинира статичка аначиза и мониторинг на runtime. Овој метод е многу ефикасен и ефективен против SQL инјектирањето. Како прв чекор е идентификација на критичните точки во апликацискиот код и потоа се гради моделот за SQL пребарувања. После секоја идентификувана критична точка се испраќа повик за мониторинг.

SQL проверка: Пристапот е потврден со SQLCHECK кој што претставува имплементација за поставување на команди занапади за инјектирање. SQLCHECK се оценува на реални веб-апликации со реални податоци за напади како инпут кои се системски составени. Времетраењето е кратко и може да се примени директно на веб-апликации напишани со употреба на различни програмски јазици.

Спречување на напади со зачувани процедури: Овој метод ја елиминира појавата на SQL напади со комбинирање на статичка анализа, а кодот за апликација со валидација на времето на траење. Главната цел на овој метод е да се спореди оригиналната структура на SQL изјава со изјавата која што вклучува кориснички инпут. Користењето на оваа техника може да бие автоматизирано и може да биде само кога е потребно.

Машинско учење: Машинското учење се користи за да се откријат малициозни веб побарувања добиени преку логови, кои успешно откриваат малициозни логови. Покрај тоа, совпаѓањето на низата се користи за да одговара на карактеристиките во фазата на класификација. „Машинското учење се заснова на алгоритми кои можат да учат од податоците без да се потпираат на програмирање засновано на правила“. Оваа дефиниција значи дека машинското учење е техника за давање дозвола на машината да донесе своја одлука со имплементација на алгоритми за машинско учење без употреба на програмибилни кодови. Ова истражување ќе се насочи кон еден од видовите на машинското учење, а тоа е надгледувано учење чија што цел е да обезбеди предвидувања за откривање на SQL напади. Надгледуваното учење може да се категорисира како:

Регресија: Анализа на регресија е предвидување на следната вредност врз основа на статистиката на претходните податоци за тестот со набљудување на примерокот. Идејата е податоците да бидат распределени на линеарен график, за да се извлече праг од активностите за да се разликува резултатот што ќе се категоризира.

Класификација: Техниката на класификација е вид на надгледуван метод за класифицирање на атрибутот на податоците за време на фазата на обука, така што може да се класифицира атрибутот за следната одлука.Овој метод е добро позната техника и најшироко се користи кај истражувачите. Се користи овој пристап како класификатор за детекторот да ги класифицира логовите на URL – адресите, без разлика дали истите се малициозни[4].

Заклучок

Нападите со вметнување на SQL код претставуваат голема закана за секоја веб страна која користи база со податоци. Бројни веб страни се нападнати на ваков начин, а од нападите не биле поштедени ни "големите" страни како страните на Microsoft или страната на MySQL. Со нападите може да се откријат осетливи податоци, да се менуваат податоците во базите или пак да се уништи цела база со податоци. Напаѓачот дури може да му наштети и на оперативниот систем. Некои од нападите со вметнување на SQL код се само вовед во некои други напади, па затоа спречувањето на овие напади може да значи и заштита и од други потенцијално поопасни напади. Доколку не е воведена никаква заштита од вметнување на SQL код и напаѓачите без големо искуство можат да изведат успешен напад со несогледливи последици. На Интернет постојат бројни примери на злонамерно обликуван SQL код со кој може да се креираат напади. Доколку страницата не е осигурана со основните проверки на корисничките внесови на податоци, напаѓачот може едноставно да ископира некој од SQL кодовите и да проба дали може да изведе напад. Со воведување на основните проверки на корисничкиот внес на податоци, како што е проверката на постоење на наводници, знакот точка-запирка или SQL клучните зборови, на повеќето злонамерни корисници доволно им се отежнува нападот за да се откажат од него. За дополнителна сигурност потребно е да се воведат измени во самата база со податоци или на серверот. Такви измени секако се препорачуваат, затоа што штетата предизвикана со нападот може во потполност да ја уништи веб страната или базата со податоци. Како и кај другите сигурносни ранливости, потребно е постојано да се надгледува сигурноста на системот. Не е доволно еднаш да се воведат измени и да се заклучи дека страната е доволно заштитена. Напаѓачите се сè повеќе спремни и покреативни, па затоа и администраторите на базите со податоци мора постојано да го надоградуваат својот систем како би бил отпорен на напади како што се вметнување на SQL код.

Со оглед дека одржувањето и подигнувањето на нивото на сигурноста на апликациите и базите со податоци е обемна работа, затоа треба да се ангажираат сите структури од развојниот тим, како што е претставено, потребна е тимска работа, за да програмерите превентивно делуваат на сигурноста, тестерите да ги воочат пропустите во развојот и да ги поправат истите, и на крајот адинистраторот кој ја одржува апликацијата да се бори со нападите во реално време, а сè со цел заради зголемување на сигурноста на податоците.

Користена литература

1. Kuldeep Rana, "Classification of SQL Injection Attacks And Using Encryption As A Countermeasure", Bhagwan Parshuram Instt. of Technology (GGSIPU) 2008
2. M. Howard and D. LeBlanc "Writing Secure Code" , Redmond, Washington : Microsoft Press second edition 2003
3. E. M. Fayo, "Advanced SQL Injection in Oracle Databases". Black Hat USA : Technical report, Argeniss Information Security, Black Hat Briefings, 2005
4. Y. Huang, F. Yu, C. Hang, C. H. Tsai, D. T. Lee, and S. Y. Kuo, "Securing Web Application Code by Static Analysis and Runtime Protection", In Proceedings of the 12th International World Wide Web Conference (WWW 04) 2004
5. SQL Injection, http://php.net/manual/en/security.database.sql-injection.php, 2011
6. AltexSoft. (2019). Web Application Architecture: How the Web Works. AltexSoft. https://www.altexsoft.com/blog/engineering/webapplication-architecture-how-the-web-works/
7. Chaturvedi, V. A., Bagdi, S., & Choudhary, V. (2016). Analysis of SQL Injections Attacks and Vulnerabilities. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3), 106-110.
8. Choi, J., Kim, H., Choi, C., & Kim, P. (2011, September). Efficient malicious code detection using n-gram analysis and SVM. In 2011 14th International Conference on Network-Based Information Systems (pp. 618-621). IEEE. https://doi.org/10.1109/NBiS.2011.104
9. GeeksforGeeks. (2019). Supervised and Unsupervised learning. GeeksforGeeks. https://www.geeksforgeeks.org/supervised unsupervised-learning/
10. GeeksforGeeks. https://www.geeksforgeeks.org/clustering-inmachine-learning/
11. Greene, D., Cunningham, P., & Mayer, R. (2008). Unsupervised learning and clustering. In Machine learning techniques for multimedia (pp. 51-90). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-75171-7_3
12. Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE international symposium on secure software engineering (Vol. 1, pp. 13-15). IEEE. https://www.cc.gatech.edu/~orso/papers/halfond.vie gas.orso.ISSSE06.pdf
13. Jansen, B. J. (2006). Search log analysis: What it is, what's been done, how to do it. Library & Information Science Research, 28(3), 407-432. https://doi.org/10.1016/j.lisr.2006.06.005
14. Joshi, A., & Geetha, V. (2014, July). SQL Injection detection using machine learning. In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 1111-1115). IEEE. https://doi.org/10.1109/ICCICCT.2014.6993127