

# Information Gathering

GETTING INFORMATION OF A WEBSITE

MUHAMMAD ADNAN

MUHAMMAD TAYAB

# Information Gathering Report on “old.uktech.ac.in”

## WEBSITE PAGE:



**वीर माधो सिंह भंडारी उत्तराखण्ड प्रौद्योगिकी विश्वविद्यालय**  
**VEER MADHO SINGH BHANDARI UTTARAKHAND TECHNICAL UNIVERSITY**  
[ FORMERLY UTTARAKHAND TECHNICAL UNIVERSITY ]  
A State Government University Established by Uttarakhand State Government vide Act No. 4/2005

**Announcement**  
[Examination Papers for QDD Sem Law, QDD Sem BHMT & QDD Sem Pharmacy I.I](#) | [NEW CURRICULUM FOR 2022-23](#)





**Dr. Nand Lal Singh**  
Vice-Chancellor



**Prof. Anil Kumar Singh**  
Deputy Vice-Chancellor



**Prof. Anil Kumar Singh**  
Deputy Vice-Chancellor



**Prof. Gagan Singh**  
Vice-Chancellor

**UNIVERSITY MANAGEMENT SYSTEM**

**AFFILIATION PORTAL**

**NEW CURRICULUM FOR 2022-2023**

**HOME**

Veer Madho Singh Bhandari Uttarakhand Technical University, Dehradun was established on 27th January 2005 by Govt. of Uttarakhand through the Uttarakhand Technical University Act 2005. The Veer Madho Singh Bhandari Uttarakhand Technical University campus is situated at NH-72 Suddhowala, Dehradun. Dehradun is the capital of Uttarakhand State and is well connected through Rail, Road and Air transport. The University has been established in an area of 8.272 hectare and it is the only affiliating University of the state for technical institutions. There are 81 Affiliated Private Institutions and 12 Government Institutions in the University. University is running 68 UG, 6 PG and 18 Ph.D. Programmes with approximately twenty thousand students in various courses detailed below. [Read More](#)

**CIRCUIT**

**ADMS**

**EXAMS**

**RESULT**

**PHD NEWS**

- 15/4/2022 – Regarding filling of examination form on the portal under Special Back Examination 2022-23 for pass out students in session 2021-22
- 18/12/2022 – Regarding Academic Registration & Enrolment Form Date extension
- 12/12/2022 – Regarding Book Writing Competition 2021-22 on Economics/Banking/Finance in Hindi
- 09/12/2022 – EXAMINATION FORM FOR REGULAR STUDENT FOR QDD SEM EXAM
- 07/12/2022 – Regarding Qdd Sem Exam 2022-23 and attendance
- 06/12/2022 – Academic Registration & Enrolment Schedule & Instructions for Session 2022-23
- 04/12/2022 – Ph.D. Entrance Examination 2022-23
- 04/12/2022 – Tender Notice for Theory and Practical Answer Booklet
- 04/12/2022 – Special Back Paper Exam Form Date
- 26/11/2022-Collaboration Opportunities with Switzerland
- 25/11/2022-Proposed Syllabus for Bio Technology & Chemical Engineering open for suggestions on email mentioned in document
- 24/11/2022-Meeting of University Officials with European Union Delegation was held in University Campus
- 21/11/2022-Notification for Viva Voce Examination of Ms. Savita Patel on 26.11.2022
- 19/11/2022-Announcement of Hakeem Scholarship for the year 2022-23
- 14/11/2022-Prime Minister's Scholarship Scheme(PMSS) for the wards of State/UTs police personnel of various State/Union Territories who martyred during terror/naxal attacks for academic year 2022-23

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

**Quick Links**

[Online e-Payment](#)  
[Download Android App](#)  
[App](#)  
[Spoken Tutorial](#)  
[SWAYAM](#)  
[NAAC](#)  
[Press Release](#)  
[Photo Gallery](#)  
[Annual Report](#)  
[Newsletter](#)  
[Affiliated Colleges](#)  
[University Kulgeet](#)  
[Bookings](#)  
[GATE PREPARATION](#)  
[SATWAYDE](#)  
[TECHNOLOGY](#)



[<](#) [||](#) [>](#)

# Information Gathering Report on "old.uktech.ac.in"

## INFORMATION ABOUT THE DOMAIN:

Server: <b>192.168.233.2</b>
Address: <b>192.168.233.2#53</b>
<b>Non-authoritative answer:</b>
Name: <b>old.uktech.ac.in</b>
Address: <b>119.18.54.69</b>
(COLLECTED USING nslookup)

## Port numbers active:

**21,22,26,53,80,110,443,465,993,995,2082,2083,2086,2087,2222,3306**

## Other Information about the domain:

City: "Mumbai"

Region: "Maharashtra"

Country: "IN"

Location: "19.0728,72.8826"

Org:"AS394695 PDR"

Postal:"400017"

Timezone: "Asia/Kolkata"

ASN:"AS394695"

Name: "PDR"

Domain:"publicdomainregistry.com"

Route:"119.18.54.0/24"

Type: "hosting"

Name: "Hostgator Asian Operations Division"

Domain:"hostgator.in"

**Address: "1st Floor, Near Mahatma Nagar Cricket Ground, Mahatma Nagar, Nashik, Maharashtra, India",**

email:"abuse@publicdomainregistry.com",

# Information Gathering Report on “old.uktech.ac.in”

Name: "ABUSE HGINDIAAP",

network:"119.18.48.0/20",

## MAIN EMAIL TEMPLATE

[registrar@uktech.ac.in](mailto:registrar@uktech.ac.in)

## LOCATION

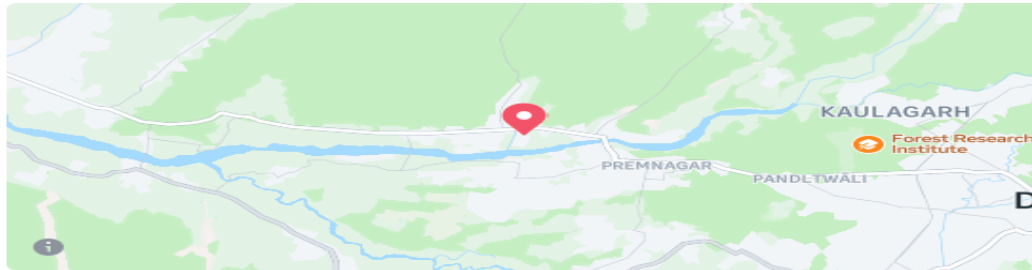
Phone


**0135 277 0059**


**Uttarakhand Technical University**

**GOVT. GIRLS POLYTECHNIC CAMPUS, PREMNAGAR SUDHOWALA, Dehradun, Uttarakhand 248007, IN**

### Contact info



 **Veer Madho Singh Bhandari Uttarakhand Technical University, Chandanwadi, Prem Nagar, Sudhowala, Dehradun (Uttarakhand), Dehra Dun, India, 248007**  
Address

 **Dehra Dun, Uttarakhand, India**  
Service area

## Company Information

**Number of Employees: 251-1K**

**Type: Education**

**Annual Revenue: \$100M-\$250M**

**Name: Uttarakhand Technical University**

# Information Gathering Report on “old.uktech.ac.in”

## Subdomains:

www.uktech.ac.in

affiliation.uktech.ac.in

www.affiliation.uktech.ac.in

fot.uktech.ac.in

www.fot.uktech.ac.in

ihub.uktech.ac.in

old.uktech.ac.in

payadmin.uktech.ac.in

payment.uktech.ac.in

result.uktech.ac.in

teqip.uktech.ac.in

www.teqip.uktech.ac.in

uksee.uktech.ac.in

utu.uktech.ac.in

## Vulnerabilities

### 2023

#### CVE-2023-51767

OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm\_answer\_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

#### CVE-2023-51385

In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

#### CVE-2023-48795

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from

# Information Gathering Report on “old.uktech.ac.in”

the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in `chacha20-poly1305@openssh.com` and (if CBC is used) the `-etm@openssh.com` MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, `golang.org/x/crypto` before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGO before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the `net-ssh` gem 7.2.0 for Ruby, the `mscdex ssh2` module before 1.15.0 for Node.js, the `thrussh` library before 0.35.1 for Rust, and the `Russh` crate before 0.40.2 for Rust.

## CVE-2023-38408

The PKCS#11 feature in `ssh-agent` in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in `/usr/lib` is not necessarily safe for loading into `ssh-agent`.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

## 2021

## CVE-2021-41617

**4.4** `sshd` in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for `AuthorizedKeysCommand` and `AuthorizedPrincipalsCommand` may run with privileges associated with group memberships of the `sshd` process, if the configuration specifies running the command as a different user.

## CVE-2021-36368

**2.6** An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without `-oLogLevel=verbose`, and an attacker has silently modified the server to support the `None` authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."

# Information Gathering Report on “old.uktech.ac.in”

## 2020

### CVE-2020-15778

**6.8** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

### CVE-2020-14145

**4.3** The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

### CVE-2020-11023

**4.3** In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

### CVE-2020-11022

**4.3** In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

## 2019

### CVE-2019-11358

**4.3** jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable \_\_proto\_\_ property, it could extend the native Object.prototype.

### CVE-2019-6111

**5.8** An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized\_keys file).

### CVE-2019-6110

# Information Gathering Report on “old.uktech.ac.in”

**4.0** In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

## CVE-2019-6109

**4.0** An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects `refresh_progress_meter()` in `progressmeter.c`.

## 2018

### CVE-2018-20685

**2.6** In OpenSSH 7.9, `scp.c` in the `scp` client allows remote SSH servers to bypass intended access restrictions via the filename of `.` or an empty filename. The impact is modifying the permissions of the target directory on the client side.

### CVE-2018-15919

**5.0** Remotely observable behaviour in `auth-gss2.c` in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

### CVE-2018-15473

**5.0** OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to `auth2-gss.c`, `auth2-hostbased.c`, and `auth2-pubkey.c`.

## 2017

### CVE-2017-15906

**5.0** The `process_open` function in `sftp-server.c` in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

## 2016

### CVE-2016-20012

**4.3** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product



# Information Gathering Report on “old.uktech.ac.in”

## 2008

### CVE-2008-3844

**9.3** Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

## 2007

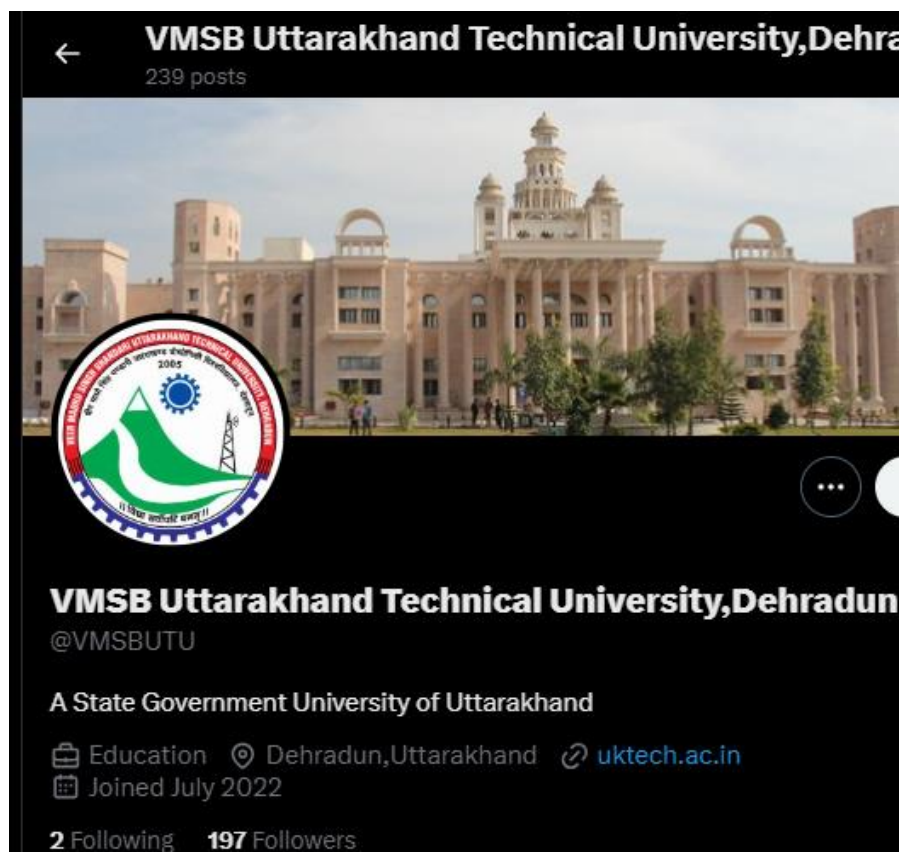
### CVE-2007-2768

**4.3** OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

---

## Social Links:

Twitter Handle: [VMSBUTU](#)



# Information Gathering Report on “old.uktech.ac.in”

Facebook Handle: [uttrakhandtechnicaluniversity](#)

facebook



## Uttarakhand Technical University

5.6K likes • 5.8K followers

Posts

About


Reels

Photos


Videos

### Intro

Veer Madho Singh Bhandari Uttarakhand Technical University(Formerly Uttarakhand Technical University)

 Page · University

 Veer Madho Singh Bhandari Uttarakhand Technical University, Chandanwadi, Prem Nagar, Sudhowala, Dehradun (Uttarakhand), Dehra Dun, India, Uttarakhand

 registrar@uktech.ac.in

 [uktech.ac.in](#)

★ 76% recommend (38 reviews) 


# Information Gathering Report on “old.uktech.ac.in”

LinkedIn Handle: [school/uttarakhandtechnicaluniversity](https://www.linkedin.com/school/uttarakhandtechnicaluniversity)

 Articles People Learning Jobs Games Get th Join now Sign in

**UTTARAKHAND TECHNICAL UNIVERSITY**  
उत्तराखण्ड तकनीकी विश्वविद्यालय  
A State Government University

**Uttarakhand Technical University, Dehradun**  
Higher Education  
Dehradun, Uttarakhand · 8,018 followers  
Public university in Sudhowala, Uttarakhand

 View all open jobs  
 View all 70 employees

[See alumni](#) [Follow](#)

Overview

Alumni

## About us





Uttarakhand Technical University is a public university in the Indian state of Uttarakhand set up by the Government of Uttarakhand on 27 January 2005, through the Uttarakhand Technical University Act 2005. It has 8 constituent institutes and approximately 132 affiliated colleges spread all over the state. This is an unofficial LinkedIn page, Manage by Individual.

Website	<a href="http://www.uktech.ac.in">http://www.uktech.ac.in</a>
Industry	Higher Education
Company size	1,001-5,000 employees
Headquarters	Dehradun, Uttarakhand
Type	Educational
Founded	2005

## Locations

**Primary**  
GOVT. GIRLS POLYTECHNIC CAMPUS  
PREMNAGAR SUDHOWALA  
Dehradun, Uttarakhand 248007, IN  
[Get directions](#)

## Employees at Uttarakhand Technical University, Dehradun

- **Anubhooti Papola**  
Graphic Era University
- **Naveen Badola**  
LV Motors Sales and Marketing | Channel Development | Business Development
- **Manjit Rauthan**  
Legal Services Professional
- **Arvind Tyagi**  
Director Systems & Rolling Stock

# Information Gathering Report on “old.uktech.ac.in”

## Important Persons of this Organization

1. Prof. Onkar Singh Dr. Onkar Singh-Vice Chancellor VMSB Uttarakhand Technical University, Dehradun/Ex-VC-Madan Mohan Malaviya Univ of Tech,Gorakhpur;UPTU,Lucknow VCSGUUHF,Bharsar

