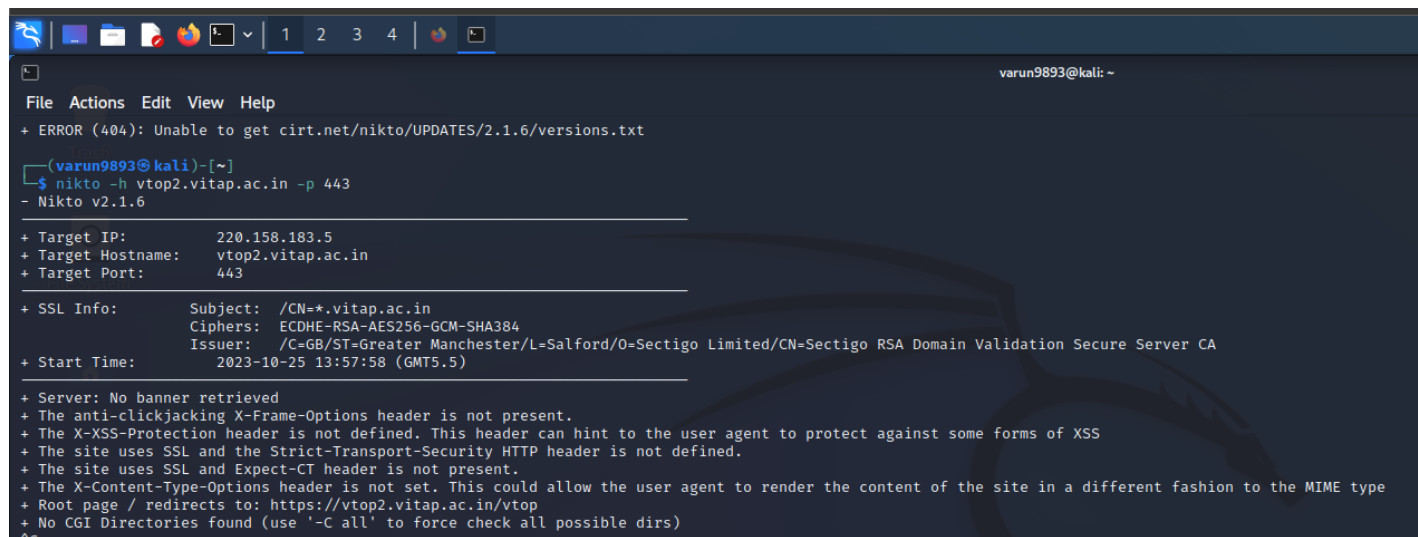


# Main Website

## Vulnerability Scan Report

Test URL: <https://vtop2.vitap.ac.in>



```
File Actions Edit View Help
+ ERROR (404): Unable to get cirt.net/nikto/UPDATES/2.1.6/versions.txt

(varun9893@kali)-[~]
$ nikto -h vtop2.vitap.ac.in -p 443
- Nikto v2.1.6

+ Target IP: 220.158.183.5
+ Target Hostname: vtop2.vitap.ac.in
+ Target Port: 443

+ SSL Info: Subject: /CN=*.vitap.ac.in
            Ciphers: ECDHE-RSA-AES256-GCM-SHA384
            Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time: 2023-10-25 13:57:58 (GMT5.5)

+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://vtop2.vitap.ac.in/vtop
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

### 1. Vulnerability Name: Clickjacking

**CWE:** CWE-451 (User Interface (UI) Misrepresentation of Critical Information)

**OWASP Category:** OWASP Top Ten - A6: Security Misconfiguration

**Description:** Clickjacking is a type of attack where a malicious website can trick a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or taking control of their actions without their knowledge or consent. The absence of the anti-clickjacking X-Frame-Options header means that the website does not specify that it should not be embedded within an iframe, leaving it vulnerable to clickjacking attacks.

**Business Impact:** Clickjacking attacks can lead to various malicious activities, such as unauthorized access to sensitive information, performing actions on behalf of the user without their consent, or stealing user credentials. This can result in reputation damage, loss of customer trust, legal consequences, and financial losses due to data breaches or unauthorized transactions.

### 2. Vulnerability Name: Cross-Site Scripting (XSS)

**CWE:** CWE-79 (Improper Neutralization of Input During Web Page Generation)

**OWASP Category:** OWASP Top Ten - A7: Cross-Site Scripting (XSS)

**Description:** Cross-Site Scripting (XSS) is a security vulnerability that allows attackers to inject malicious scripts into web pages viewed by users. When the X-XSS-Protection header is not defined, the user agent (such as a web browser) may not have specific instructions to protect against certain forms of XSS attacks. Without this header, malicious scripts can be injected into the web application, potentially leading to the execution of arbitrary code in the context of the user's browser session.

**Business Impact:** XSS attacks can lead to unauthorized access, theft of sensitive data, session hijacking, defacement of websites, and potentially spreading malware to site visitors. This can result in reputational damage, loss of customer trust, legal liabilities, and financial losses due to legal consequences or theft of sensitive information.

### 3. Vulnerability Name: Missing Strict-Transport-Security Header

**CWE:** CWE-523 (Unprotected Transport of Credentials)

**OWASP Category:** OWASP Top Ten - A3: Cross-Site Scripting (XSS)

**Description:** Strict-Transport-Security (HSTS) is a security feature that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. When the Strict-Transport-Security HTTP header is not defined, the website is vulnerable to attacks where an attacker could potentially intercept communication between the client and server, leading to unauthorized access or data theft.

**Business Impact:** Without HSTS, sensitive data such as login credentials and session tokens transmitted between the client and server could be intercepted by attackers. This can lead to unauthorized access, data breaches, identity theft, financial loss, and damage to the organization's reputation. Additionally, failure to implement HSTS could result in regulatory non-compliance and legal consequences if customer data is compromised.

### 4. Vulnerability Name: Missing Expect-CT Header

**CWE:** CWE-319 (Cleartext Transmission of Sensitive Information)

**OWASP Category:** OWASP Top Ten - A3: Cross-Site Scripting (XSS)

**Description:** The Expect-CT header is a security feature that allows a website to determine if they are ready for the upcoming Chrome Certificate Transparency enforcement. When the

Expect-CT header is not present, the website is not enforcing Certificate Transparency (CT) for its SSL certificates. CT is a mechanism designed to enhance the security of SSL certificates, making it more difficult for attackers to issue fraudulent certificates for a domain.

**Business Impact:** Without the Expect-CT header, the website is susceptible to various SSL-related attacks, including man-in-the-middle attacks and phishing attacks. Attackers could potentially present fraudulent SSL certificates, leading to unauthorized access, data interception, and impersonation of the website. This could result in financial loss, damage to reputation, loss of customer trust, and legal consequences if sensitive data is compromised. Additionally, failure to implement CT could lead to non-compliance with industry standards and regulations.

## 5. Vulnerability Name: MIME Sniffing / Content Type Mismatch

**CWE:** CWE-116 (Improper Encoding or Escaping of Output)

**OWASP Category:** OWASP Top Ten - A6: Security Misconfiguration

**Description:** MIME Sniffing, also known as Content Type Mismatch, occurs when the Content-Type header sent by the server doesn't match the actual content of the file. In this case, the absence of the X-Content-Type-Options header allows browsers to interpret files in a different way than intended. Browsers might attempt to determine the content type of a response based on the content itself, leading to potential security risks, especially when dealing with certain file types like scripts or executables.

**Business Impact:** MIME Sniffing vulnerabilities can lead to various attacks, such as script injection, data theft, or content spoofing. If a browser interprets a file as a different content type (e.g., treating an executable file as a script), it can result in unexpected behaviors, potentially allowing attackers to execute malicious code in the context of the user's session. This can lead to unauthorized access, data breaches, loss of customer trust, and reputational damage.

## 6. Vulnerability Name: Directory Listing

**CWE:** CWE-548 (Exposure of Information Through Directory Listing)

**OWASP Category:** OWASP Top Ten - A5: Security Misconfiguration

**Description:** Directory Listing vulnerability occurs when a web server does not have an index file (like index.html or index.php) in a directory, and directory listing is not disabled. As a result, when a user accesses a directory without specifying a particular file, the server may list the contents of the directory, revealing sensitive information about the server's file structure and potentially exposing files or directories that were not meant to be public.

**Business Impact:** Directory Listing can provide attackers with valuable information, such as the names of files, directories, or technologies in use. This information can be leveraged in various attacks, including directory traversal attacks, information gathering for social engineering attacks, or targeted attacks against specific files. It can also lead to disclosure of sensitive data, loss of intellectual property, and reputational damage if sensitive information is exposed to unauthorized parties.

## 7. Vulnerability Name: Information Disclosure

**CWE:** CWE-200 (Information Exposure)

**OWASP Category:** OWASP Top Ten - A6: Security Misconfiguration or A3: Sensitive Data Exposure

**Description:** The "snoop.jsp" file is displaying information about page retrievals, including those of other users. This indicates a misconfiguration or a lack of access control, allowing unauthorized users to view sensitive information about the activities and retrievals made by other users of the web application.

**Business Impact:** Information disclosure vulnerabilities can lead to the exposure of sensitive data, user activities, or system configurations. In this case, if unauthorized users can view other users' activities, it could lead to privacy breaches, leakage of sensitive information, and potential misuse of user data. This can result in loss of customer trust, reputational damage, legal consequences, and financial losses if regulatory fines are imposed or if the exposed information is misused. It's crucial to address this vulnerability promptly to prevent unauthorized access and information disclosure.