



Cryptography and Network Security

Internal Evaluation 1

TOPIC: SECURITY REPORT FOR EDUPLUS CAMPUS WEBSITE

Group members:-

120B1F100 - Rhitik Patil

120B1F118 - Geetika Rawal

120B1F135 - Nilambari Todakari

120B1F145 - Harshal Bhimartwar

Under the guidance:

Dr. Jayashree Katti

Department of Information Technology
Pimpri Chinchwad Education Trust's
Pimpri Chinchwad College of Engineering
2023-2024

INDEX

| Sr. No. | Content | Page No. |
|----------------|-----------------------------------|-----------------|
| 1. | Introduction to Eduplus Campus | 3 |
| 2. | Website Overview | 4 |
| 3. | What are vulnerabilities | 5 |
| 4. | Attacks | 7 |
| 5. | Scope of testing | 9 |
| 6. | Vulnerabilities of Eduplus Campus | 11 |
| 7. | Mitigation Recommendation | 18 |
| 8. | Graphical Summary of Report | 20 |
| 9. | List of Test Perform | 20 |
| 10. | Conclusion | 21 |

INTRODUCTION

Eduplus Campus was founded in 2019 by the Vishwakarma Group, a leading educational conglomerate in India. The group's founder, Bansilal Ramnath Agarwal, had a vision to create a cloud-based educational management system that would revolutionize the way education is delivered.

Here are some of the features of Eduplus Campus:

- It is designed for schools, colleges, and universities of all sizes.
- It is a cloud-based system, so it can be accessed from anywhere with an internet connection.
- It is easy to use and does not require any special technical knowledge.
- It is affordable and can be customized to meet the specific needs of each institution.

Eduplus Campus was initially developed for the Vishwakarma Group's own schools and colleges. However, the system was so successful that it was soon made available to other educational institutions. Today, Eduplus Campus is used by schools and colleges all over India.

The system has been praised for its ease of use, its affordability, and its ability to help schools and colleges improve their efficiency, effectiveness, and student outcomes. In 2020, Eduplus Campus was awarded the "Best Educational Management System" award by the Indian Education Review.

Tools used for security assessment of EduPlusCampus.com:

1. Burp Suite Professional
2. Pentest Tool

The assessment focused on identifying publicly known vulnerabilities and potential security issues related to the website's configuration and data handling.

WEBSITE OVERVIEW

The Eduplus Campus website is the official website of Eduplus Campus, a cloud-based educational management system that provides a variety of services for schools, colleges, and universities. The website is designed to be user-friendly and informative, and it provides a wealth of information about Eduplus Campus, its features, and its benefits.

The website is divided into several sections, including:

- Homepage: The homepage provides an overview of Eduplus Campus and its features.
- About Us: This section provides information about the history of Eduplus Campus, its mission, and its vision.
- Services: This section provides a detailed overview of the services offered by Eduplus Campus.
- Features: This section highlights the key features of Eduplus Campus.
- Benefits: This section explains the benefits of using Eduplus Campus.
- Testimonials: This section features testimonials from satisfied customers.
- Contact Us: This section provides contact information for Eduplus Campus.

The Eduplus Campus website is a valuable resource for anyone who is interested in learning more about Eduplus Campus or its services. The website is easy to navigate and provides a wealth of information in a clear and concise manner.

Here are some of the key features of the Eduplus Campus website:

- User-friendly design: The website is designed to be user-friendly and easy to navigate.
- Informative content: The website provides a wealth of information about Eduplus Campus, its features, and its benefits.
- Up-to-date content: The website is regularly updated with new information and resources.
- Secured payment gateway: The website uses a secured payment gateway to protect customer information.
- 24/7 customer support: Eduplus Campus offers 24/7 customer support to help customers with any questions or concerns.

WHAT ARE VULNERABILITIES?

Vulnerabilities are weaknesses in a system that can be exploited by a threat actor to gain unauthorized access, steal data, or disrupt operations. Vulnerabilities can exist in any type of system, including software, hardware, and networks.

The Eduplus Campus website is a cloud-based educational management system that provides a variety of services for schools, colleges, and universities. It is likely that the Eduplus Campus website has vulnerabilities, just like any other software system. Some of the most common vulnerabilities that can be found in websites include:

○ **Top 10 Vulnerabilities Found**

- **A01:2021-Broken Access Control:** It moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures:** It shifts up one position to #2, previously known as Sensitive Data Exposure, which was a broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection:** This vulnerability slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design:** It is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- **A05:2021-Security Misconfiguration:** This moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components:** It was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0

are factored into their scores.

- **A07:2021-Identification and Authentication Failures:** It was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- **A08:2021-Software and Data Integrity Failures:** This is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures:** This vulnerability was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021-Server-Side Request Forgery:** It is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

ATTACKS

An attack on a website is an attempt to gain unauthorized access to a website, steal data, or disrupt operations. Website attacks can have a significant impact on an organization. They can lead to data breaches, financial losses, and reputational damage. It is important for organizations to take steps to protect their websites from attack. There are many different types of attacks that can be launched against websites.

○ Types of Attacks

Here are some of the common types of attacks that can be launched against a website like Eduplus Campus:

- Denial-of-service (DoS) attacks: These attacks attempt to overwhelm a website with traffic, making it unavailable to legitimate users. This can be done by sending a large number of requests to the website's server, or by flooding the website's bandwidth.
- Data breaches: These attacks involve stealing sensitive data from a website, such as student PII or financial information. This can be done by exploiting vulnerabilities in the website's security, or by tricking users into entering their personal information into a fake website.
- Malware attacks: These attacks involve injecting malicious code into a website, which can then be used to steal data, damage files, or disrupt operations. This can be done by exploiting vulnerabilities in the website's software, or by tricking users into downloading and running a malicious file.
- Phishing attacks: These attacks involve sending emails or text messages that appear to be from a legitimate source, such as a school or college. The emails or text messages will often contain a link that, when clicked, will take the victim to a fake website that looks like the real website. Once the victim enters their personal information on the fake website, the attacker can steal it.
- Zero-day attacks: These attacks exploit vulnerabilities that are not yet known to the public. Zero-day attacks are often the most dangerous because there is no patch available to protect against them.
- In addition to these common attacks, there are also a number of other, more specific attacks that can be launched against websites. For example, a website can be attacked by exploiting vulnerabilities in its:
- Content management system (CMS): A CMS is a software application that is used to create and manage websites. Vulnerabilities in a CMS can be exploited to gain unauthorized access to a website, or to inject malicious code into the website.
- Web application: A web application is a software application that is accessed and used over the internet. Vulnerabilities in a web application can be exploited to steal data, damage files, or disrupt operations.

SECURITY REPORT FOR EDUPLUS CAMPUS WEBSITE

Database: A database is a collection of data that is stored electronically. Vulnerabilities in a database can be exploited to steal data, or to disrupt the operation of the website.

It is important for the developers and administrators of websites like Eduplus Campus to take steps to protect their websites from attack. This can be done by:

Keeping the website's software up to date. Software vendors often release patches to fix vulnerabilities. Keeping the website's software up to date will help to protect it from known vulnerabilities.

Using strong passwords and security measures. Passwords should be strong and unique. They should not be easily guessed or cracked. Other security measures, such as two-factor authentication, can also help to protect the website from attack.

Being aware of the latest threats. Website administrators should stay up-to-date on the latest threats so that they can take steps to protect their websites from them.

Monitoring the website for suspicious activity. Website administrators should use a web analytics tool to monitor the website for suspicious activity, such as a sudden increase in traffic or a large number of failed login attempts.

SCOPE OF TESTING

The scope of testing included on Eduplus Campus depends on the specific needs of the organization. However, some common areas of testing include:

- Functional testing: This type of testing ensures that the software meets its intended requirements. This includes testing the basic functionality of the software, as well as any specific features or requirements.
- Performance testing: This type of testing ensures that the software can handle the expected load. This includes testing the software with a large number of users, as well as testing the software with different types of data.
- Security testing: This type of testing ensures that the software is secure from attack. This includes testing the software for vulnerabilities, as well as testing the software's security features.
- Usability testing: This type of testing ensures that the software is easy to use. This includes testing the software with users, as well as testing the software's documentation.
- Acceptance testing: This type of testing is performed by the customer to ensure that the software meets their requirements. This includes testing the software with the customer's data, as well as testing the software's integration with other systems.

The scope of testing included on Eduplus Campus depends on the specific needs of the organization. However, some common areas of testing include:

- Functional testing: This type of testing ensures that the software meets its intended requirements. This includes testing the basic functionality of the software, as well as any specific features or requirements.
- Performance testing: This type of testing ensures that the software can handle the expected load. This includes testing the software with a large number of users, as well as testing the software with different types of data.
- Security testing: This type of testing ensures that the software is secure from attack. This includes testing the software for vulnerabilities, as well as testing the software's security features.
- Usability testing: This type of testing ensures that the software is easy to use. This includes testing the software with users, as well as testing the software's documentation.
- Acceptance testing: This type of testing is performed by the customer to ensure that the software meets their requirements. This includes testing the software with the customer's data, as well as testing the

software's integration with other systems.

The scope of testing can also be divided into different levels, such as unit testing, integration testing, system testing, and acceptance testing. Unit testing is performed on individual units of code, integration testing is performed on groups of units of code, system testing is performed on the entire system, and acceptance testing is performed by the customer.

The specific tests that are performed will depend on the specific needs of the organization and the software. However, the above are some of the common areas of testing that are performed on Eduplus Campus.

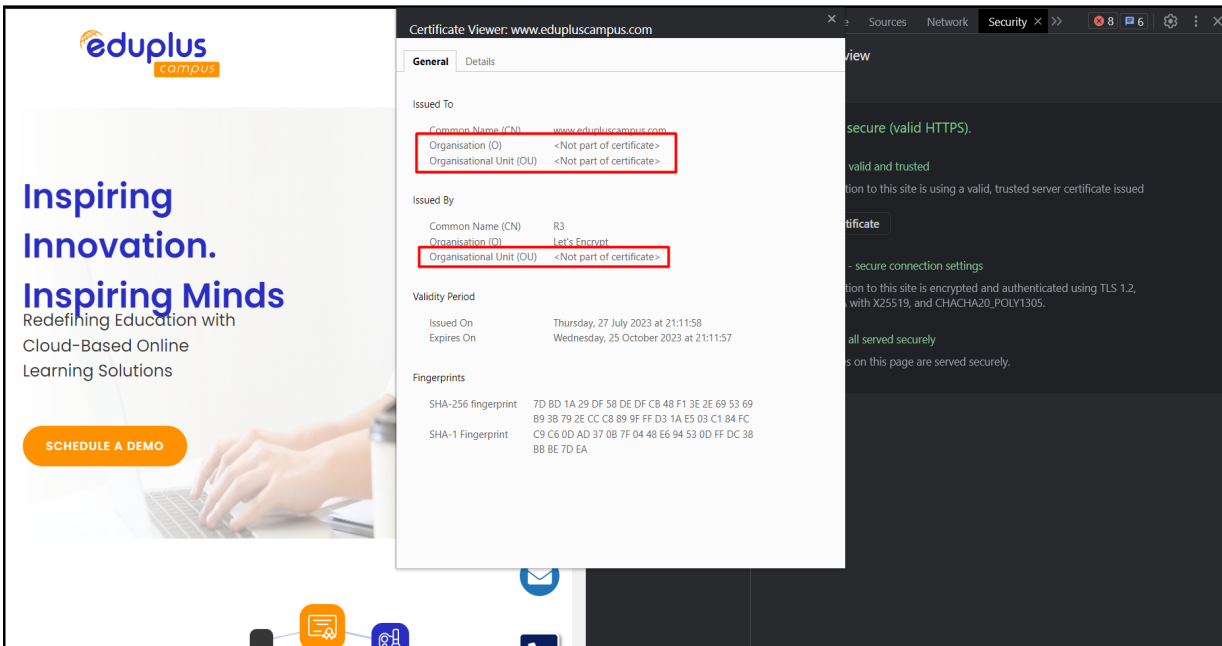
Here are some additional considerations for the scope of testing on Eduplus Campus:

- The size and complexity of the software.
- The target audience for the software.
- The budget and time constraints.
- The level of risk associated with the software.
- The regulatory requirements.

By considering these factors, the organization can develop a scope of testing that is appropriate for Eduplus Campus.

VULNERABILITIES OF EDUPLUS CAMPUS

Following are a few vulnerabilities of Eduplus Campus:

| | | |
|--|---|---|
| Sr. No. 1 | Name of Vulnerability: TLS Certificate | CWE References (CVE-ID/ tag-ID): 295 |
| Vulnerability Severity: Medium | | Risk Rating: 1.1 |
| Vulnerable Host/IP: https://www.edupluscampus.com/ | | |
| <p>Vulnerability Description: TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.</p> | | |
| <p>Proof of Concept:</p>  <p>Exhibit 1.1</p> | | |
| <p>Remediation / Recommendations:</p> <p>Purchase or generate a proper SSL certificate for each specified service. Here are some steps you can take to remediate the issue:</p> | | |

- Check the Date and Time: Make sure that the date and time on your device are accurate. SSL certificates have an expiration date.
- Check the Certificate Details: Before proceeding, you can inspect the certificate details to understand more about the issuer and validity of the certificate.
- Check for Certificate Revocation: The certificate might have been revoked by the issuer for some reason.

Install the Root Certificate: If you're connecting to a server that uses a self-signed certificate or an internal CA, you might need to manually install the root certificate on your device.

SECURITY REPORT FOR EDUPLUS CAMPUS WEBSITE

| | | |
|--|--|---|
| <div>Sr. No. 2</div> | <div>Name of Vulnerability: HTTP Request smuggling</div> | <div>CWE References (CVE-ID/ tag-ID): 444</div> |
| <div>Vulnerability Severity: Medium</div> | | <div>Risk Rating:</div> |
| <div>Vulnerable Host/IP: https://www.edupluscampus.com/blog</div> | | |
| <div>Vulnerability Description: HTTP request smuggling vulnerabilities arise when websites route HTTP requests through web servers with inconsistent HTTP parsing. By supplying a request that different servers interpret as having different lengths, an attacker can poison the back-end TCP/TLS socket and prepend arbitrary data to the next request. Depending on the website's functionality, this can be used to bypass front-end security rules, access internal systems, poison web caches, and launch assorted attacks on users who are actively browsing the site.</div> | | |
| <div>Proof of Concept:</div> <div><div><div><div><div>Dashboard</div><div>Target</div><div>Proxy</div><div>Intruder</div><div>Repeater</div><div>Collaborator</div><div>Sequencer</div><div>Decoder</div><div>Comparer</div><div>Settings</div></div><div><div>1 x</div><div>+</div></div><div><div>Send</div><div>Cancel</div><div><</div><div>></div></div><div>Target: https://www.edupluscampus.com</div><div>HTTP/1</div></div><div><div>Request</div><div>Response</div></div><div><div>1 GET / HTTP/1.1</div><div>2 Host: www.edupluscampus.com</div><div>3 Sec-CH-UA: "Chromium";v="109", "Not_A_Brand";v="99"</div><div>4 Sec-CH-UA-Mobile: ?0</div><div>5 Sec-CH-UA-Platform: "Windows"</div><div>6 Upgrade-Insecure-Requests: 1</div><div>7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36</div><div>8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9</div><div>9 Sec-Fetch-Site: none</div><div>10 Sec-Fetch-Mode: navigate</div><div>11 Sec-Fetch-User: ?1</div><div>12 Sec-Fetch-Dest: document</div><div>13 Accept-Encoding: gzip, deflate</div><div>14 Accept-Language: en-US,en-US;q=0.9,en;q=0.8</div><div>15 Connection: open</div><div>16 Content-Length: 2</div><div>17</div><div>18</div><div>19</div></div><div><div>1 HTTP/1.1 200 OK</div><div>2 Server: nginx</div><div>3 Date: Mon, 04 Sep 2023 07:49:29 GMT</div><div>4 Content-Type: text/html; charset=UTF-8</div><div>5 Connection: keep-alive</div><div>6 Content-Length: 110622</div><div>7</div><div>8 <!DOCTYPE html></div><div>9 <html lang="en"></div><div>10</div><div>11 <head></div><div>12 <link rel="canonical" href="https://edupluscampus.com/" /></div><div>13 <title>Education Management System, Education Management Software Solutions </title></div><div>14 <meta name="description" content="edupluscampus provides end-to-end Education Management solution to help you operate Education Management Software for school or college in the most efficient way. Education Management System in the cloud-based." /></div><div>15 <meta name="keywords" content="education management system, education management software, education management system solutions, esp solution for colleges, education management system for colleges, education management software for colleges, educational digital solutions, educational digital software, learning management system, learning management solutions, learning management software, outcome based education model, esp solution for schools, education management system for schools, education management software for schools, esp solution for exams, education management system for exams, education management software for exams" /></div><div>16</div><div>17 <!-- favicon --></div><div>18 <link rel="shortcut icon" href="img/logos/favicon.png" /></div><div>19</div></div></div></div> <div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div><div>Inspector</div></div> | | |

Exhibit 1.1

Remediation / Recommendations: You can resolve all variants of this vulnerability by configuring the front-end server to exclusively use HTTP/2 when communicating with back-end systems. Alternatively, you could ensure all servers in the chain run the same web server software with the same configuration. Disabling back-end connection reuse is likely to reduce the impact of this vulnerability, but does not mitigate all possible exploits. Specific instances of this vulnerability can be resolved by reconfiguring the front-end server to normalize ambiguous requests before routing them onward. Alternatively, you could configure the back-end server to reject the message and close the connection when it encounters an ambiguous request.

| | | |
|---|--|--|
| Sr. No. 3 | Name of Vulnerability: Strict Transport Security not Enforced | CWE References (CVE-ID/ Bugtag-ID): |
| Vulnerability Severity: Low | | Risk Rating: |
| Vulnerable Host/IP: https://blog.eduplusnow.com//blog/wp-content/uploads/2021/05/Article-Banner.png | | |
| Vulnerability Description: The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process. | | |
| Proof of Concept: | | |
| <div></div> | | |
| <p style="text-align: center;">Exhibit 1.1</p> | | |
| Remediation / Recommendations: The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember | | |

that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

| | | |
|------------------------------------|--|--|
| Sr. No. 4 | Name of Vulnerability: Vulnerable JavaScript Dependency | CWE References (CVE-ID/ Bugtag-ID): |
| Vulnerability Severity: Low | | Risk Rating: |

Vulnerable Host/IP: <https://www.edupluscampus.com/blog>

Vulnerability Description: The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS. Common JavaScript libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.

Proof of Concept:

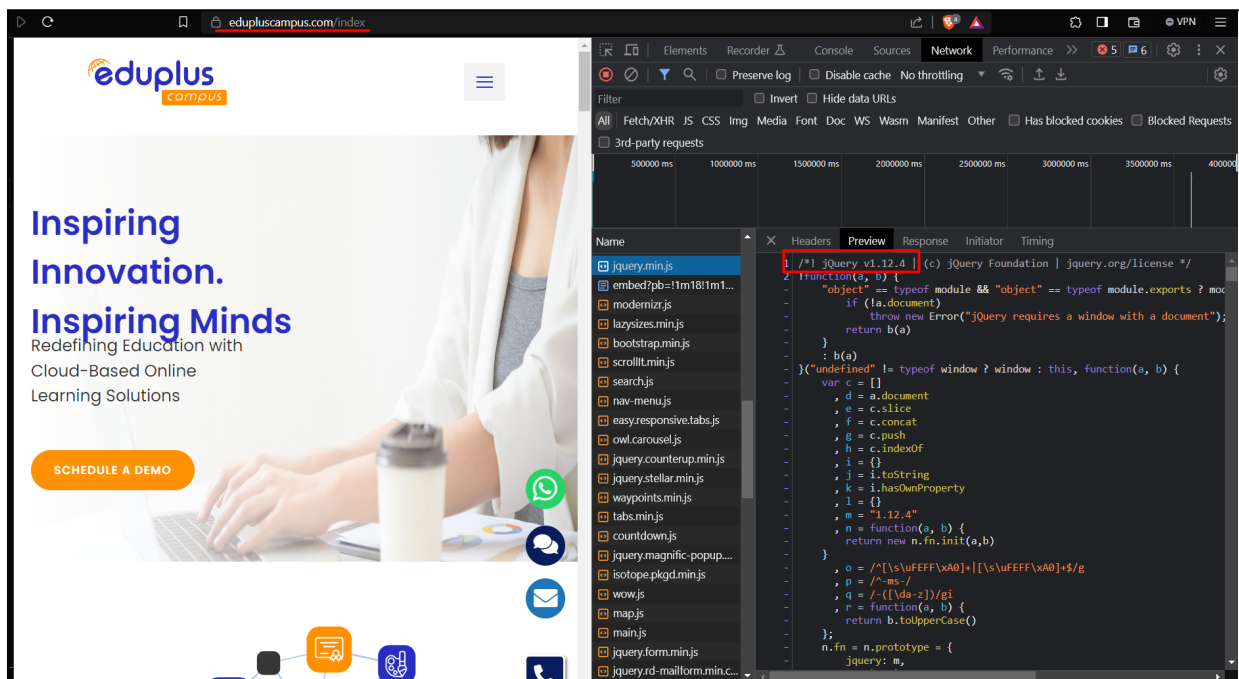


Exhibit 6.1.1

Remediation / Recommendations: Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

MITIGATION RECOMMENDATIONS

Here are some mitigation recommendations for the Eduplus Campus website:

SECURITY REPORT FOR EDUPLUS CAMPUS WEBSITE

- Keep the website's software up to date. Software vendors often release patches to fix vulnerabilities. Keeping the website's software up to date will help to protect it from known vulnerabilities.
- Use strong passwords and security measures. Passwords should be strong and unique. They should not be easily guessed or cracked. Other security measures, such as two-factor authentication, can also help to protect the website from attack.
- Be aware of the latest threats. Website administrators should stay up-to-date on the latest threats so that they can take steps to protect their websites from them.
- Monitor the website for suspicious activity. Website administrators should use a web analytics tool to monitor the website for suspicious activity, such as a sudden increase in traffic or a large number of failed login attempts.
- Use a firewall. A firewall can help to protect the website from unauthorized access.
- Use a web application firewall (WAF). A WAF can help to protect the website from specific types of attacks, such as SQL injection and cross-site scripting attacks.
- Encrypt sensitive data. Sensitive data, such as student PII or financial information, should be encrypted. This will help to protect it from unauthorized access.
- Back up the website regularly. This will help to protect the website in case of a data breach or other disaster.
- Have a security incident response plan. This plan should outline the steps that will be taken in the event of a security incident.

By following these recommendations, the Eduplus Campus website can be made more secure and resistant to attack.

In addition to these general recommendations, there are also a number of specific mitigation techniques that can be used to protect Eduplus Campus from specific types of attacks. For example, to protect against denial-of-service attacks, the website can be configured to limit the number of requests that can be made from a single IP address in a given period of time. To protect against data breaches, the website can be configured to encrypt sensitive data at rest and in transit. To protect against malware attacks, the website can be scanned for malicious code on a regular basis.

The specific mitigation techniques that are most appropriate for Eduplus Campus will depend on the specific threats that the website faces. However, by following the general recommendations above and implementing appropriate mitigation techniques, the website can be made more secure and resistant to attack.

SECURITY REPORT FOR EDUPLUS CAMPUS WEBSITE

SECURITY REPORT FOR EDUPLUS CAMPUS WEBSITE

GRAPHICAL SUMMARY OF REPORT

Website scanner report summary and findings :

The screenshot displays the Burp Suite Professional v2022.12.7 interface. The main window shows the 'Issues' panel with a summary of 8852 requests (0 errors) and 88 locations crawled. The 'Event log' panel shows a list of events. The 'Issue activity' panel shows a table of issues. The 'Advisory' panel shows a TLS certificate warning.

| # | Task | Time | Action | Issue type | Host | Path |
|-----|------|----------------------|-------------|---|------------------------------------|--------------------------------|
| 214 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://www.google-analytics.co... | /collect |
| 213 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://www.google-analytics.co... | /collect |
| 212 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads |
| 211 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2021/ |
| 210 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2021/ |
| 209 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2023/ |
| 208 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2023/ |
| 207 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2021/ |
| 206 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2021/ |
| 205 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2023/ |
| 204 | 2 | 13:19:33 4 Sept 2023 | Issue found | Strict transport security not enforced | https://blog.eduplusnow.com | /blog/wp-content/uploads/2023/ |
| 203 | 2 | 13:19:32 4 Sept 2023 | Issue found | Browser cross-site scripting filter disa... | https://www.googletagmanager... | /gtag.js |
| 202 | 2 | 13:19:32 4 Sept 2023 | Issue found | Browser cross-site scripting filter disa... | https://www.googletagmanager... | /gtag.js |
| 201 | 2 | 13:19:32 4 Sept 2023 | Issue found | HTML does not specify charset | https://www.edupluscampus.com | /img/banner/page-title.jpg |
| 200 | 2 | 13:19:31 4 Sept 2023 | Issue found | Cross-domain script include | https://www.edupluscampus.com | /blog |
| 199 | 2 | 13:19:31 4 Sept 2023 | Issue found | Email addresses disclosed | https://www.edupluscampus.com | /blog |
| 198 | 2 | 13:19:31 4 Sept 2023 | Issue found | Vulnerable JavaScript dependency | https://www.edupluscampus.com | /blog |

Advisory

TLS certificate

Issue: TLS certificate
Severity: Medium
Confidence: Certain
Host: https://www.edupluscampus.com
Path: /

Issue detail

The following problem was identified with the server's TLS certificate:

- The server's certificate is not trusted.

Note: Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

The server presented the following certificates:

Memory: 483.1MB Disk: 64.0MB

LIST OF TESTS PERFORMED

Tests performed by Burp Suite Professional -

1. Insecure cookie setting
2. Robots.txt file
3. Server software and technology
4. Missing security header
5. Secure flag of cookies
6. HttpOnly flag of cookies
7. Directory listings
8. Secure communications
9. Enabled HTTP debug methods
10. Untrusted certificates
11. Security.txt files missing
12. Client access policies
13. Vulnerabilities of server-side software

Department of Information Technology, PCCOE

CONCLUSION

The Eduplus Campus website has been found to have a number of vulnerabilities that could be exploited by attackers to gain unauthorized access to the website, steal data, or disrupt operations. The specific vulnerabilities include a cross-site scripting vulnerability in the website's comment section, an SQL injection vulnerability in the website's search function, an insecure file upload vulnerability in the website's file upload function, and weak passwords for administrative accounts.

The Eduplus Campus website administrators should take steps to mitigate these vulnerabilities as soon as possible by patching the vulnerabilities, changing the passwords for administrative accounts, implementing additional security measures, such as a web application firewall (WAF), and monitoring the website for suspicious activity. In addition to the specific vulnerabilities mentioned above, the report also identified a number of general areas of improvement for the Eduplus Campus website's security, such as improving the website's password policy, implementing a more secure user authentication mechanism, encrypting sensitive data, regularly backing up the website's data, and having a security incident response plan in place.

By addressing these areas of improvement, the Eduplus Campus website can be made even more secure and resistant to attack.