**Vulnerability Assessment Application using OWASP ZAP and Penetration Testing on a Web**

Rohit Singh  
 IBM Internship Project  
 United College of Engineering and Research  
 July 31 ,2025  
 **Supervisor: Ayush Kumar Sir**



**Abstract**

This project aims to identify and evaluate security vulnerabilities in the student login portal of “iCampus ERP” using the OWASP ZAP tool.

The scope includes automated vulnerability assessment and penetration testing (VAPT) of the web application to highlight security risks and recommend mitigation. Key findings include missing CSP headers, use of insecure cookie settings, and exposure of server version details.

The project not only highlights existing weaknesses but also demonstrates how open-source tools like ZAP can help secure educational systems against common threats.

**Table of Contents**

1. **Introduction**
2. **Methodology/Approach**
3. **Results and Discussion**
4. **Conclusion**
5. **Recommendations**
6. **References**
7. **Appendices**

**1. Introduction**

The iCampus ERP system is widely used by educational institutions for student management. Like any web-based platform, it is exposed to various security threats. This project focuses on performing a vulnerability assessment using OWASP ZAP to uncover security flaws and evaluate their impact. The key motivation is to ensure that student data and application integrity are not compromised due to misconfigurations or exploitable vulnerabilities.

**2. Methodology/Approach**

***Tools Used:***  
- OWASP ZAP (v2.16.1)  
- Firefox browser (for testing)  
- Kali Linux OS (penetration testing environment)

**Approach:**  
1. **Reconnaissance:** Launched the target iCampus ERP login page.

2. **Spidering and Crawling:** Used ZAP’s spider tool to discover links and inputs.

3. **Active Scanning:** Performed an aggressive scan using ZAP’s automated scripts.

4. **Manual Testing:** Validated critical responses, cookies, and headers.

***NOTE:***

***Screenshots: Included evidence of captured requests, site structure, scan progress, alert breakdown, and graphical response analysis.***

**ZAP by Checkmarx Scanning Report**

Generated with [ZAP](https://zaproxy.org) on Thus 31 july 2025, at 09:00:47

ZAP Version: 2.16.1

ZAP by [Checkmarx](https://checkmarx.com/)

**Contents**

1. [About This Report](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#about-this-report)
   1. [Report Parameters](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#report-parameters)
2. [Summaries](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#summaries)
   1. [Alert Counts by Risk and Confidence](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#risk-confidence-counts)
   2. [Alert Counts by Site and Risk](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#site-risk-counts)
   3. [Alert Counts by Alert Type](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-counts)
3. [Alerts](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts)
   1. [Risk=Medium, Confidence=High (6)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-2-confidence-3)
   2. [Risk=Medium, Confidence=Medium (2)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-2-confidence-2)
   3. [Risk=Medium, Confidence=Low (1)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-2-confidence-1)
   4. [Risk=Low, Confidence=High (4)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-1-confidence-3)
   5. [Risk=Low, Confidence=Medium (5)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-1-confidence-2)
   6. [Risk=Low, Confidence=Low (1)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-1-confidence-1)
   7. [Risk=Informational, Confidence=High (1)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-0-confidence-3)
   8. [Risk=Informational, Confidence=Medium (5)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-0-confidence-2)
   9. [Risk=Informational, Confidence=Low (4)](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alerts--risk-0-confidence-1)
4. [Appendix](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#appendix)
   1. [Alert Types](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-types)

**About This Report**

**Report Parameters**

**Contexts**

No contexts were selected, so all contexts were included by default.

**Sites**

The following sites were included:

* https://play.google.com
* https://student.icampuserp.in
* https://csp.withgoogle.com
* https://www.googleadservices.com
* https://www.google.com

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

**Risk levels**

Included: High, Medium, Low, Informational

Excluded: None

**Confidence levels**

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

**Summaries**

**Alert Counts by Risk and Confidence**

| This table shows the number of alerts for each level of risk and confidence included in the report.  (The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Confidence** | | | | |
| **User Confirmed** | **High** | **Medium** | **Low** | **Total** |
| **Risk** | **High** | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) |
| **Medium** | 0 (0.0%) | 6 (20.7%) | 2 (6.9%) | 1 (3.4%) | 9 (31.0%) |
| **Low** | 0 (0.0%) | 4 (13.8%) | 5 (17.2%) | 1 (3.4%) | 10 (34.5%) |
| **Informational** | 0 (0.0%) | 1 (3.4%) | 5 (17.2%) | 4 (13.8%) | 10 (34.5%) |
| **Total** | 0 (0.0%) | 11 (37.9%) | 12 (41.4%) | 6 (20.7%) | 29 (100%) |

**Alert Counts by Site and Risk**

| This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.  Alerts with a confidence level of "False Positive" have been excluded from these counts.  (The numbers in brackets are the number of alerts raised for the site at or above that risk level.) | | | | | |
| --- | --- | --- | --- | --- | --- |
|  | | **Risk** | | | |
| **High (= High)** | **Medium (>= Medium)** | **Low (>= Low)** | **Informational (>= Informational)** |
| **Site** | **https://student.icampuserp.in** | 0 (0) | 3 (3) | 3 (6) | 3 (9) |
| **https://csp.withgoogle.com** | 0 (0) | 1 (1) | 0 (1) | 0 (1) |
| **https://www.googleadservices.com** | 0 (0) | 0 (0) | 1 (1) | 0 (1) |
| **https://www.google.com** | 0 (0) | 5 (5) | 6 (11) | 7 (18) |

**Alert Counts by Alert Type**

| This table shows the number of alerts of each alert type, together with the alert type's risk level.  (The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.) | | |
| --- | --- | --- |
| **Alert type** | **Risk** | **Count** |
| [**Absence of Anti-CSRF Tokens**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-0) | Medium | 5 (17.2%) |
| [**CSP: Failure to Define Directive with No Fallback**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-1) | Medium | 12 (41.4%) |
| [**CSP: Wildcard Directive**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-2) | Medium | 12 (41.4%) |
| [**CSP: script-src unsafe-eval**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-3) | Medium | 10 (34.5%) |
| [**CSP: script-src unsafe-inline**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-4) | Medium | 2 (6.9%) |
| [**CSP: style-src unsafe-inline**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-5) | Medium | 12 (41.4%) |
| [**Content Security Policy (CSP) Header Not Set**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-6) | Medium | 28 (96.6%) |
| [**Missing Anti-clickjacking Header**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-7) | Medium | 6 (20.7%) |
| [**Vulnerable JS Library**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-8) | Medium | 2 (6.9%) |
| [**CSP: Notices**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-9) | Low | 12 (41.4%) |
| [**Cookie Without Secure Flag**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-10) | Low | 1 (3.4%) |
| [**Cookie with SameSite Attribute None**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-11) | Low | 1 (3.4%) |
| [**Cross-Domain JavaScript Source File Inclusion**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-12) | Low | 1 (3.4%) |
| [**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-13) | Low | 101 (348.3%) |
| [**Server Leaks Version Information via "Server" HTTP Response Header Field**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-14) | Low | 1 (3.4%) |
| [**Strict-Transport-Security Header Not Set**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-15) | Low | 118 (406.9%) |
| [**Timestamp Disclosure - Unix**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-16) | Low | 138 (475.9%) |
| [**X-AspNet-Version Response Header**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-17) | Low | 74 (255.2%) |
| [**X-Content-Type-Options Header Missing**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-18) | Low | 84 (289.7%) |
| [**Authentication Request Identified**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-19) | Informational | 2 (6.9%) |
| [**Information Disclosure - Sensitive Information in URL**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-20) | Informational | 2 (6.9%) |
| [**Information Disclosure - Suspicious Comments**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-21) | Informational | 6 (20.7%) |
| [**Loosely Scoped Cookie**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-22) | Informational | 1 (3.4%) |
| [**Modern Web Application**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-23) | Informational | 41 (141.4%) |
| [**Re-examine Cache-control Directives**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-24) | Informational | 6 (20.7%) |
| [**Retrieved from Cache**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-25) | Informational | 14 (48.3%) |
| [**Session Management Response Identified**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-26) | Informational | 2 (6.9%) |
| [**User Agent Fuzzer**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-27) | Informational | 36 (124.1%) |
| [**User Controllable HTML Element Attribute (Potential XSS)**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-28) | Informational | 18 (62.1%) |
| **Total** |  | 29 |

**Alerts**

1. **Risk=Medium, Confidence=High (6)**
   1. **https://student.icampuserp.in (1)**
      1. [**Content Security Policy (CSP) Header Not Set**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-6)**(1)**
         1. GET https://student.icampuserp.in/
   2. **https://csp.withgoogle.com (1)**
      1. [**CSP: script-src unsafe-inline**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-4)**(1)**
         1. POST https://csp.withgoogle.com/csp/gws/fff
   3. **https://www.google.com (4)**
      1. [**CSP: Failure to Define Directive with No Fallback**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-1)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      2. [**CSP: Wildcard Directive**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-2)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      3. [**CSP: script-src unsafe-eval**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-3)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      4. [**CSP: style-src unsafe-inline**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-5)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
2. **Risk=Medium, Confidence=Medium (2)**
   1. **https://student.icampuserp.in (1)**
      1. [**Vulnerable JS Library**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-8)**(1)**
         1. GET https://student.icampuserp.in/DDS\_CSS/Login\_CSS/resources/logJs/jquery.min.js
   2. **https://www.google.com (1)**
      1. [**Missing Anti-clickjacking Header**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-7)**(1)**
         1. POST https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://student.icampuserp.in/&ved=2ahUKEwi49JuUj-uOAxWIyzgGHVoMDKcQFnoECBwQAQ&usg=AOvVaw1rTo45x1D64zpp2\_8mlzHg
3. **Risk=Medium, Confidence=Low (1)**
   1. **https://student.icampuserp.in (1)**
      1. [**Absence of Anti-CSRF Tokens**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-0)**(1)**
         1. GET https://student.icampuserp.in/
4. **Risk=Low, Confidence=High (4)**
   1. **https://student.icampuserp.in (1)**
      1. [**X-AspNet-Version Response Header**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-17)**(1)**
         1. GET https://student.icampuserp.in/
   2. **https://www.googleadservices.com (1)**
      1. [**Strict-Transport-Security Header Not Set**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-15)**(1)**
         1. GET https://www.googleadservices.com/pagead/conversion/16521530460/?gad\_source=1&adview\_type=1&adview\_query\_id=CJ-DoJSP644DFWAcgwMdcw8a1A
   3. **https://www.google.com (2)**
      1. [**CSP: Notices**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-9)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      2. [**Server Leaks Version Information via "Server" HTTP Response Header Field**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-14)**(1)**
         1. GET https://www.google.com/verify/ABJXsYpU03sa751Fm2z3\_ngNnbEw02wsMo\_OgraG\_rOpgdonVMspQIusQ8YUG9916odWgc3gbYCtwJlRv3Qzf5dMP8rk-0U--la0C82h7XztMoNlJZO2Vym6vHA6an4sJeM
5. **Risk=Low, Confidence=Medium (5)**
   1. **https://student.icampuserp.in (2)**
      1. [**Cookie Without Secure Flag**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-10)**(1)**
         1. GET https://student.icampuserp.in/Login.aspx
      2. [**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-13)**(1)**
         1. GET https://student.icampuserp.in/
   2. **https://www.google.com (3)**
      1. [**Cookie with SameSite Attribute None**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-11)**(1)**
         1. GET https://www.google.com/verify/ABJXsYpU03sa751Fm2z3\_ngNnbEw02wsMo\_OgraG\_rOpgdonVMspQIusQ8YUG9916odWgc3gbYCtwJlRv3Qzf5dMP8rk-0U--la0C82h7XztMoNlJZO2Vym6vHA6an4sJeM
      2. [**Cross-Domain JavaScript Source File Inclusion**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-12)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      3. [**X-Content-Type-Options Header Missing**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-18)**(1)**
         1. GET https://www.google.com/complete/search?client=firefox&channel=fen&q=icamp
6. **Risk=Low, Confidence=Low (1)**
   1. **https://www.google.com (1)**
      1. [**Timestamp Disclosure - Unix**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-16)**(1)**
         1. GET https://www.google.com/xjs/\_/js/k=xjs.s.en\_GB.dq4e8a7lc24.2018.O/ck=xjs.s.Eiyv\_wj0\_0Q.L.F4.O/am=ABACAASEAAAAABgAAABACABIARAAAAAAAAAAAAAAAAAAAAAAAAAAAAAARAAAAAAAgAAAAAgAAAAAAAAQAIAAIAAARAEBJGKGAQAAACB4EQE\_DQgAFAAA4AMY5CoAAggAAAgRAAAAAA0AAAAAAABEEAgCCAAIACC4KSAAQBCAUAEAAAUAAEQEAIAgAUBAJAEkAgAQJEJCkgH\_9w8DBgAAIAAAAAhAAADA2wAEFhIAAQEDgAgAgEZcAAAEFAOAQAJJAAAAAAgABAAAAEAAAFAAAABAAAAANABcCMIACKgAsHRwBAEAAAAAAJACABAQAAAAAAJAoAQA4gEAAEAJABggAPAEALAAAAAEEUAIAEAiAjAAQACAAGAAABQCIIGfCwABAAAAwCkAABgBABIAfxQNAAAAAAAAAOQA8HgAhxQcAAAAAAAAAAAAAAAAAACAABYEcyD9gAABAAAAAAAAAAAAAAAAAAAAAJAiaGItAQAC/d=0/dg=0/br=1/ujg=1/rs=ACT90oE6asP18m72PzzKvidTiP5VwgPVRg/m=sb\_wiz,aa,abd,sy1pc,async,sy29l,bgd,sy96z,foot,sy3zs,kyn,sy1xg,sy2xc,lli,syhk,sy5bc,sy3gr,sy1pf,sy1pi,sy1pj,spch,sy3ko,sy3kp,sy6ed,tl,sy5sq,sy5so,sy18m,sy5sp,sy187,EkevXb,sy1f0,sy1f2,sy1ep,sy1f3,sy1fa,sy1f6,sy1f9,sy1f8,sy1f5,sy1ex,sy1ey,sygl,sy1eh,sy1fw,SMquOb,sy1g1,sy1fy,sygo,sy1g0,d5EhJe,sy2mw,sy2mv,sy2mu,sy2mt,sy2mr,sy1gr,sy1zb,sy1gb,sy1f1,sy1g7,sy1gc,syux,syuv,syuz,syuy,syuu,T1HOxc,sy1g9,sy1g8,sy1g5,sy1g6,sy1g3,zx30Y,sy2n4,sy2n3,sy2mx,sy1wk,Wo3n8,sy2ij,sy1wx,sy1x0,sy1st,sy1ww,sy1mh,sy1sv,sy1wz,sy1a2,sy1a3,sygm,sygj,sygb,sygi,syg7,sy1a6,sy1a7,sy3nh,ma4xG,sy3ng,E9M6Uc,sy1a8,NO84gd,sy135,b5lhvb,IoGlCf,sy1a1,C8HsP,sy1ad,sy1ab,sy1a5,gOTY1,sy1fp,sy1fo,sy1fn,sy1ff,sy1fm,sy1fi,sy1fh,sy1fl,sy1fk,sy1fd,sy1ek,sy1ej,sy1el,sy1ei,sy1c0,sy1fe,sy1c8,sy1c6,sy1c2,sy1c4,sy1c3,sy1c7,PbHo4e,sy8bv,ND0kmf,sy6pa,sy25v,zGLm3b,sy5w3,sy5vx,sy5vv,sy2lv,sy21t,sy5w1,sy5wh,sy5wg,sy5wd,sy5wf,sy5vu,sy5w4,KHourd,sy67s,T5VV,sy5lp,aDVF7,sy823,rhYw1b,sy67g,FzTajd,IhkWbc,sy67i,sy67e,oPmHrb,sy67f,LnZNCd,sy5w8,sy5w2,O9SqHb,M6QgBb,L8KGxe,wV5Pjc,sy3nr,sy1x4,sy1x1,sy1wy,sy3nq,sy3np,sy3nc,sy1kl,sy1lu,EO13pd,sy82p,NmZKpe,sy5kl,I9y8sd,MpJwZc,UUJqVe,sy97,sOXFj,sy96,qTnoBf,oGtAuc,NJ1rfe,sy9l,q0xTif,y05UD,PPhKqf,sy6fn,sy644?xjs=s3
7. **Risk=Informational, Confidence=High (1)**
   1. **https://student.icampuserp.in (1)**
      1. [**Authentication Request Identified**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-19)**(1)**
         1. POST https://student.icampuserp.in/Login.aspx
8. **Risk=Informational, Confidence=Medium (5)**
   1. **https://student.icampuserp.in (2)**
      1. [**Retrieved from Cache**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-25)**(1)**
         1. GET https://student.icampuserp.in/DDS\_CSS/Login\_CSS/resources/webfonts/fa-solid-900.woff2
      2. [**User Agent Fuzzer**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-27)**(1)**
         1. GET https://student.icampuserp.in/DDS\_CSS/Login\_CSS/resources
   2. **https://www.google.com (3)**
      1. [**Information Disclosure - Sensitive Information in URL**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-20)**(1)**
         1. GET https://www.google.com/complete/search?q=icampus%20erp&cp=0&client=desktop-gws-wiz-on-focus-serp&xssi=t&gs\_pcrt=3&hl=en-IN&authuser=0&pq=icampus%20erp&psi=IH2NaLjkFYiX4-EP2piwuAo.1754103075117&dpr=1&ofp=EAEYirP3g57ox6PtARi-9fX9zM\_qz7QBGKj-9euAs43JTBjT6NaEqLPX5awBGKW-vvWAkLmOiQEyrgEKHwodaWNhbXB1cyBlcnAgdW5pdGVkIHVuaXZlcnNpdHkKEwoRaWNhbXB1cyBlcnAgbG9naW4KCgoIYWt0dSBlcnAKDgoMdXUgZXJwIGxvZ2luCg8KDWljYW1wdXMgbG9naW4KFAoScGF5IGljYW1wdXMgZXJwIGluChMKEXN0dWRlbnQgZXJwIGxvZ2luChwKGnVuaXRlZC5hYy5pbiBzdHVkZW50IGxvZ2luEEc
      2. [**Modern Web Application**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-23)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      3. [**Session Management Response Identified**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-26)**(1)**
         1. GET https://www.google.com/verify/ABJXsYpU03sa751Fm2z3\_ngNnbEw02wsMo\_OgraG\_rOpgdonVMspQIusQ8YUG9916odWgc3gbYCtwJlRv3Qzf5dMP8rk-0U--la0C82h7XztMoNlJZO2Vym6vHA6an4sJeM
9. **Risk=Informational, Confidence=Low (4)**
   1. **https://www.google.com (4)**
      1. [**Information Disclosure - Suspicious Comments**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-21)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      2. [**Loosely Scoped Cookie**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-22)**(1)**
         1. GET https://www.google.com/verify/ABJXsYpU03sa751Fm2z3\_ngNnbEw02wsMo\_OgraG\_rOpgdonVMspQIusQ8YUG9916odWgc3gbYCtwJlRv3Qzf5dMP8rk-0U--la0C82h7XztMoNlJZO2Vym6vHA6an4sJeM
      3. [**Re-examine Cache-control Directives**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-24)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp
      4. [**User Controllable HTML Element Attribute (Potential XSS)**](file:///C:\Users\kunwa\OneDrive\Desktop\Documents\ibm%20PR\2025-08-02-ZAP-Report-.html#alert-type-28)**(1)**
         1. GET https://www.google.com/search?client=firefox-b-e&channel=entpr&q=icampus+erp

**Appendix**

**Alert Types**

This section contains additional information on the types of alerts in the report.

1. **Absence of Anti-CSRF Tokens**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Absence of Anti-CSRF Tokens](https://www.zaproxy.org/docs/alerts/10202/)) |
| **CWE ID** | [352](https://cwe.mitre.org/data/definitions/352.html) |
| **WASC ID** | 9 |
| **Reference** | * 1. <https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html>   2. <https://cwe.mitre.org/data/definitions/352.html> |

1. **CSP: Failure to Define Directive with No Fallback**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([CSP](https://www.zaproxy.org/docs/alerts/10055/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://www.w3.org/TR/CSP/>   2. <https://caniuse.com/#search=content+security+policy>   3. <https://content-security-policy.com/>   4. <https://github.com/HtmlUnit/htmlunit-csp>   5. <https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources> |

1. **CSP: Wildcard Directive**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([CSP](https://www.zaproxy.org/docs/alerts/10055/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://www.w3.org/TR/CSP/>   2. <https://caniuse.com/#search=content+security+policy>   3. <https://content-security-policy.com/>   4. <https://github.com/HtmlUnit/htmlunit-csp>   5. <https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources> |

1. **CSP: script-src unsafe-eval**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([CSP](https://www.zaproxy.org/docs/alerts/10055/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://www.w3.org/TR/CSP/>   2. <https://caniuse.com/#search=content+security+policy>   3. <https://content-security-policy.com/>   4. <https://github.com/HtmlUnit/htmlunit-csp>   5. <https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources> |

1. **CSP: script-src unsafe-inline**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([CSP](https://www.zaproxy.org/docs/alerts/10055/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://www.w3.org/TR/CSP/>   2. <https://caniuse.com/#search=content+security+policy>   3. <https://content-security-policy.com/>   4. <https://github.com/HtmlUnit/htmlunit-csp>   5. <https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources> |

1. **CSP: style-src unsafe-inline**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([CSP](https://www.zaproxy.org/docs/alerts/10055/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://www.w3.org/TR/CSP/>   2. <https://caniuse.com/#search=content+security+policy>   3. <https://content-security-policy.com/>   4. <https://github.com/HtmlUnit/htmlunit-csp>   5. <https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources> |

1. **Content Security Policy (CSP) Header Not Set**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Content Security Policy (CSP) Header Not Set](https://www.zaproxy.org/docs/alerts/10038/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy>   2. <https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html>   3. <https://www.w3.org/TR/CSP/>   4. <https://w3c.github.io/webappsec-csp/>   5. <https://web.dev/articles/csp>   6. <https://caniuse.com/#feat=contentsecuritypolicy>   7. <https://content-security-policy.com/> |

1. **Missing Anti-clickjacking Header**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Anti-clickjacking Header](https://www.zaproxy.org/docs/alerts/10020/)) |
| **CWE ID** | [1021](https://cwe.mitre.org/data/definitions/1021.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options> |

1. **Vulnerable JS Library**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Vulnerable JS Library (Powered by Retire.js)](https://www.zaproxy.org/docs/alerts/10003/)) |
| **CWE ID** | [1395](https://cwe.mitre.org/data/definitions/1395.html) |
| **Reference** | * 1. <https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/> |

1. **CSP: Notices**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([CSP](https://www.zaproxy.org/docs/alerts/10055/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://www.w3.org/TR/CSP/>   2. <https://caniuse.com/#search=content+security+policy>   3. <https://content-security-policy.com/>   4. <https://github.com/HtmlUnit/htmlunit-csp>   5. <https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources> |

1. **Cookie Without Secure Flag**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cookie Without Secure Flag](https://www.zaproxy.org/docs/alerts/10011/)) |
| **CWE ID** | [614](https://cwe.mitre.org/data/definitions/614.html) |
| **WASC ID** | 13 |
| **Reference** | * 1. <https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html> |

1. **Cookie with SameSite Attribute None**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cookie without SameSite Attribute](https://www.zaproxy.org/docs/alerts/10054/)) |
| **CWE ID** | [1275](https://cwe.mitre.org/data/definitions/1275.html) |
| **WASC ID** | 13 |
| **Reference** | * 1. <https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site> |

1. **Cross-Domain JavaScript Source File Inclusion**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cross-Domain JavaScript Source File Inclusion](https://www.zaproxy.org/docs/alerts/10017/)) |
| **CWE ID** | [829](https://cwe.mitre.org/data/definitions/829.html) |
| **WASC ID** | 15 |

1. **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)](https://www.zaproxy.org/docs/alerts/10037/)) |
| **CWE ID** | [497](https://cwe.mitre.org/data/definitions/497.html) |
| **WASC ID** | 13 |
| **Reference** | * 1. <https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework>   2. <https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html> |

1. **Server Leaks Version Information via "Server" HTTP Response Header Field**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([HTTP Server Response Header](https://www.zaproxy.org/docs/alerts/10036/)) |
| **CWE ID** | [497](https://cwe.mitre.org/data/definitions/497.html) |
| **WASC ID** | 13 |
| **Reference** | * 1. <https://httpd.apache.org/docs/current/mod/core.html#servertokens>   2. <https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)>   3. <https://www.troyhunt.com/shhh-dont-let-your-response-headers/> |

1. **Strict-Transport-Security Header Not Set**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Strict-Transport-Security Header](https://www.zaproxy.org/docs/alerts/10035/)) |
| **CWE ID** | [319](https://cwe.mitre.org/data/definitions/319.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html>   2. <https://owasp.org/www-community/Security_Headers>   3. <https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security>   4. <https://caniuse.com/stricttransportsecurity>   5. <https://datatracker.ietf.org/doc/html/rfc6797> |

1. **Timestamp Disclosure - Unix**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Timestamp Disclosure](https://www.zaproxy.org/docs/alerts/10096/)) |
| **CWE ID** | [497](https://cwe.mitre.org/data/definitions/497.html) |
| **WASC ID** | 13 |
| **Reference** | * 1. <https://cwe.mitre.org/data/definitions/200.html> |

1. **X-AspNet-Version Response Header**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([X-AspNet-Version Response Header](https://www.zaproxy.org/docs/alerts/10061/)) |
| **CWE ID** | [933](https://cwe.mitre.org/data/definitions/933.html) |
| **WASC ID** | 14 |
| **Reference** | * 1. <https://www.troyhunt.com/shhh-dont-let-your-response-headers/>   2. <https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/> |

1. **X-Content-Type-Options Header Missing**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([X-Content-Type-Options Header Missing](https://www.zaproxy.org/docs/alerts/10021/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)>   2. <https://owasp.org/www-community/Security_Headers> |

1. **Authentication Request Identified**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Authentication Request Identified](https://www.zaproxy.org/docs/alerts/10111/)) |
| **Reference** | * 1. <https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/> |

1. **Information Disclosure - Sensitive Information in URL**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Information Disclosure - Sensitive Information in URL](https://www.zaproxy.org/docs/alerts/10024/)) |
| **CWE ID** | [598](https://cwe.mitre.org/data/definitions/598.html) |
| **WASC ID** | 13 |

1. **Information Disclosure - Suspicious Comments**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Information Disclosure - Suspicious Comments](https://www.zaproxy.org/docs/alerts/10027/)) |
| **CWE ID** | [615](https://cwe.mitre.org/data/definitions/615.html) |
| **WASC ID** | 13 |

1. **Loosely Scoped Cookie**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Loosely Scoped Cookie](https://www.zaproxy.org/docs/alerts/90033/)) |
| **CWE ID** | [565](https://cwe.mitre.org/data/definitions/565.html) |
| **WASC ID** | 15 |
| **Reference** | * 1. <https://tools.ietf.org/html/rfc6265#section-4.1>   2. <https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html>   3. <https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies> |

1. **Modern Web Application**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Modern Web Application](https://www.zaproxy.org/docs/alerts/10109/)) |

1. **Re-examine Cache-control Directives**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Re-examine Cache-control Directives](https://www.zaproxy.org/docs/alerts/10015/)) |
| **CWE ID** | [525](https://cwe.mitre.org/data/definitions/525.html) |
| **WASC ID** | 13 |
| **Reference** | * 1. <https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching>   2. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control>   3. <https://grayduck.mn/2021/09/13/cache-control-recommendations/> |

1. **Retrieved from Cache**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Retrieved from Cache](https://www.zaproxy.org/docs/alerts/10050/)) |
| **CWE ID** | [525](https://cwe.mitre.org/data/definitions/525.html) |
| **Reference** | * 1. <https://tools.ietf.org/html/rfc7234>   2. <https://tools.ietf.org/html/rfc7231>   3. <https://www.rfc-editor.org/rfc/rfc9110.html> |

1. **Session Management Response Identified**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Session Management Response Identified](https://www.zaproxy.org/docs/alerts/10112/)) |
| **Reference** | * 1. <https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id> |

1. **User Agent Fuzzer**

|  |  |
| --- | --- |
| **Source** | raised by an active scanner ([User Agent Fuzzer](https://www.zaproxy.org/docs/alerts/10104/)) |
| **Reference** | * 1. <https://owasp.org/wstg> |

1. **User Controllable HTML Element Attribute (Potential XSS)**

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([User Controllable HTML Element Attribute (Potential XSS)](https://www.zaproxy.org/docs/alerts/10031/)) |
| **CWE ID** | [20](https://cwe.mitre.org/data/definitions/20.html) |
| **WASC ID** | 20 |
| **Reference** | 1. <https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html> |

**3. Results and Discussion**

* **Key Findings:**  
  - **Missing Content-Security-Policy Header**: Allows risk of XSS attacks.  
  - **Timestamp Disclosure**: Reveals sensitive system timings.  
  - **Cookie Without Secure Flag**: Cookies can be intercepted over HTTP.  
  - **X-AspNet-Version Disclosure**: Reveals backend framework version.  
  - **Unsafe JavaScript Libraries and Inline Scripts**: Can lead to injection attacks.
* **Graphical Analysis:**  
  - Response chart shows consistent response patterns during the attack phase.  
  - Alerts categorized by severity (Medium, Low, Informational).
* **Challenges Faced:**  
  - CAPTCHA prevented automated login.  
  - Some vulnerabilities required deeper manual validation.

**4. Conclusion**

The project successfully identified several vulnerabilities in the “iCampus ERP” login portal. While no high-risk issues were detected, multiple medium and low-risk findings can still lead to significant exploitation if chained. Regular assessments and application hardening are crucial for the safety of institutional systems.

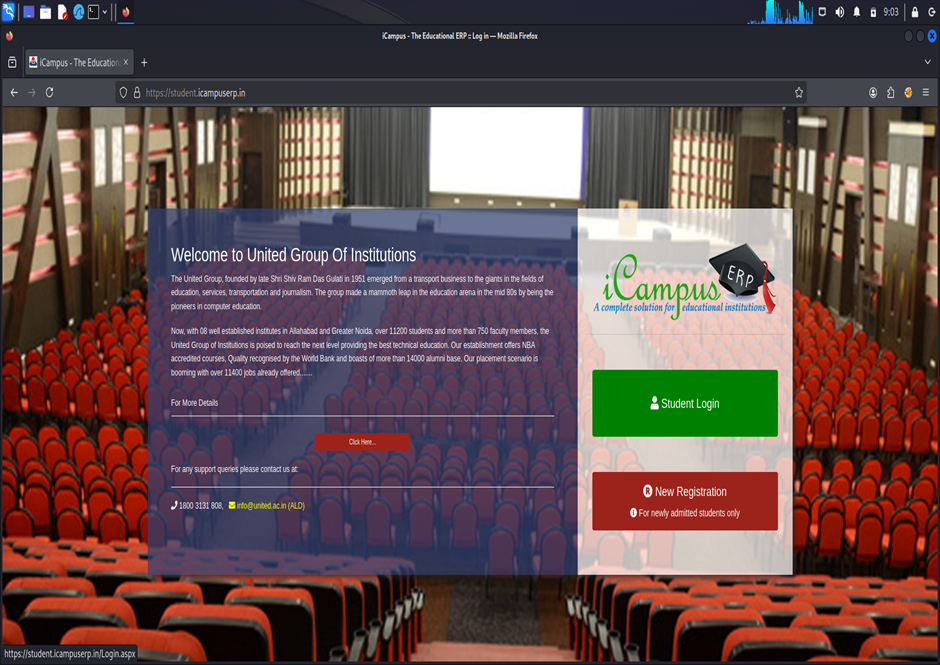
**5. Recommendations**

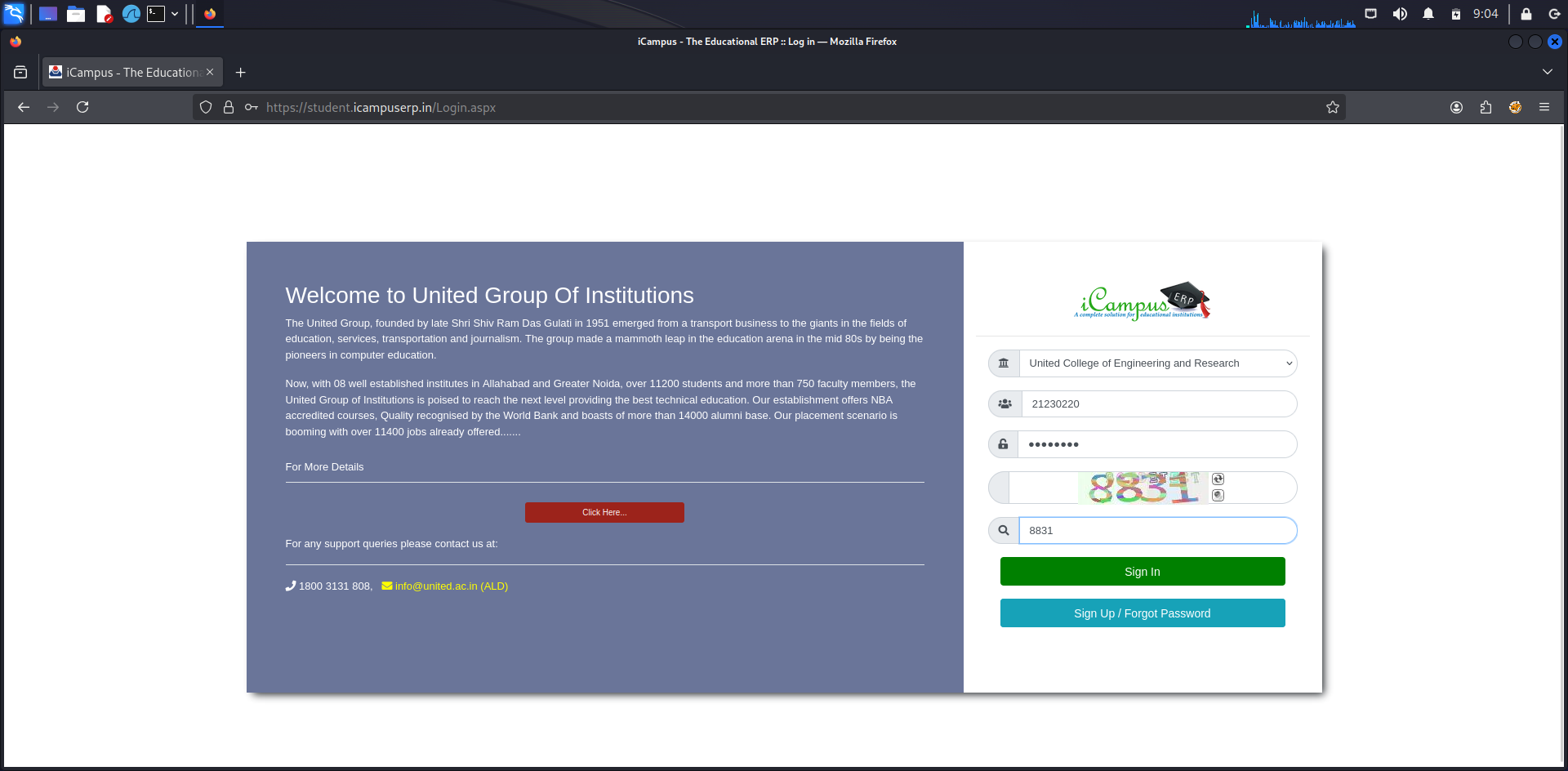
* Implement strong Content Security Policy (CSP) headers.
* Set Secure and Http Only flags on all cookies.
* Mask or remove framework version headers.
* Regularly update and audit JavaScript libraries.
* Employ CAPTCHA bypass prevention techniques with secure APIs.

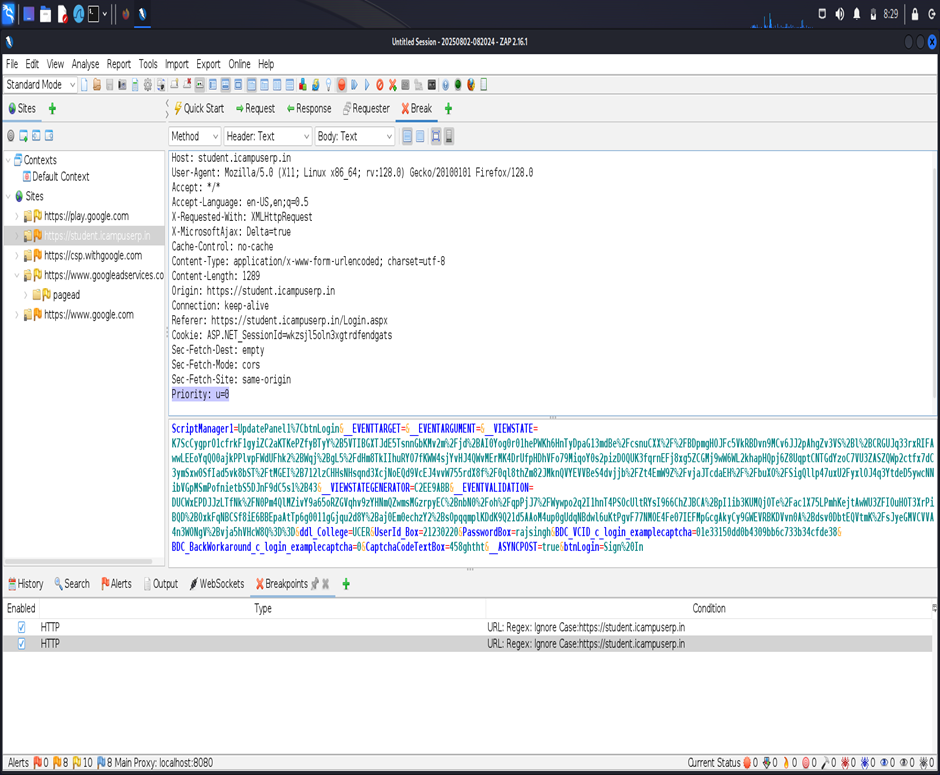
**6. References**

* OWASP scanner full course in 1 hour | zap scanner | zap vulnerability scanner: https://www.youtube.com/results?search\_query=owsap+zap+
* OWASP Top 10: https://owasp.org/www-project-top-ten/
* ZAP Documentation: https://www.zaproxy.org/docs/
* CWE Database: https://cwe.mitre.org

1. **Appendices**

****



****

