BY SPEED POST Telex : 0135-2741987/2748041 Telephone :252 4317/4318

Indian Institute of Remote Sensing **Email: pns@iirs.gov.in**
INDIAN SPACE RESEARCH ORGANISATION
Department of Space, Govt. of India
4,Kalidas Road, Post Box No. 135
DEHRA DUN-248 001

PURCHASE DEPARTMENT

Tender Enquiry No : IIRS/PandS/MPR- 1629 M/s

Date 11-Nov-13

Due Date Tuesday, November 26, 2013 at 1500 hrs.

Kindly submit your quotations in a sealed envelope superscribed with Enquiry No. due date for the supply of the following as per terms conditions mentioned below.

Sl No	Material Description	Unit	Qty
1	Security Audit of CSSTEAP Website as per OWASP Top 10 Application Security Risks - 2013, through CERTIN empanelled IT Security Auditors (Scope of Work and Terms & Condition is attached)	No.	1

Terms and Conditions :

1. Material should be delivered & installed at IIRS.
2. Payment will be made within 30 days from date of receipt of supply and acceptance of the material for orders value upto Rs. 2.0 lakhs.
3. We cannot furnish Form C/D. Please indicate the applicable percentage of Trade tax/VAT in your quotation, if applicable. Otherwise the quoted rate will be considered as inclusive of all taxes.
4. Clearly mention the Make/Brand of the item in your quotation. Please enclosed the Authorization Certificate from the principal of the quoted Make/Model along with the quotation.
5. Also clearly mention the exact delivery period and validity of your offer shall be min. 60 days.

Purchase and Stores Officer
Indian Institute of Remote Sensing

Please See Our Web Site :- "www.iirs.gov.in" for all tenders

Scope of Work

The scope of work is to conduct offsite black-box approach website security audit of CSSTEAP website according to OWASP (Open Web Application Security Project) Top 10 Application Security Risks – 2013 (given in annexure 1) through CERT-IN empanelled IT Security Auditors.

CSSTEAP Website Details:

- Content Management System- Drupal 7.22
- Front-end: PHP 5.4.x
- Back-end: MySql 5.x
- Total No of pages: 150 (approx.) including static and dynamic pages
- Total No of dynamic modules: Two modules i.e. Discussion Forum and Alumni modules where students can register and post queries.
- No. of Users Role: 2 ; a) Students/Alumni, b) CMS Admin (super user)
- Upload/download feature

To ensure that the website is free from the above vulnerabilities, the audit exercise will need to undertake the following activities:

1. Conducting the first round of security audit of the website.
2. Submission of website security audit report after first round of security audit along with recommendations. The website development team will fix the vulnerabilities as per the detailed recommendations in the report and inform the auditor within 1-2 weeks time to conduct second round (re-audit) of website.
3. Auditor needs to re-audit the website again for compliance check followed by submission of the re-audit report.
4. Submission of the final audit report along with the website 'Safe to Host' security clearance certificate only if there are no vulnerabilities found in the re-audit report. Cost for subsequent or extra rounds of audit, if required, needs to be provided by the auditor.

Terms and Condition

- Organizations/firms should be CERT-in-empanelled. Proof needs to be attached.
- For conducting the website security audit of CSSTEAP website, access to the website on the staging server along with the login details for accessing dynamic modules including CMS admin Panel will be provided.
- The Organizations/firms needs to inform the timeline for conducting the website security audit well in advance.
- The website security audit needs to be conducted offsite.
- The Organizations/firms needs to support the website development team, over telephone and e-mail, in resolving the identified vulnerabilities
- The first round of security audit report should be submitted within 10 days after the order issued and second and subsequent round reports if any should be submitted within 5 working days.
- The payment will be made only after submitting the final security audit certificate on completion of audit of website

Deliverables:

- Website Security Audit Report and
- 'Safe to Host' website security clearance certificate.

ANNEXURE -1

OWASP Top 10 Application Security Risks – 2013

A1 – Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 – Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5 – Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6 – Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7 – Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8 - Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9 - Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10 – Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.