

REQUEST FOR PROPOSAL

Tel: 011-20863460

Ministry of Defence
Dept. of Defence (R&D)
"Aakanksha"
Development Enclave
Rao Tula Ram Marg
New Delhi-110010

1/L/IT/HERMES VA

14 Mar 24

To,

M/s Bharat Electronics Limited

Office of the GM/Software

Bel Software SBU

Bharat Electronics Limited

Jalahalli, Bengaluru -560013,

REQUEST FOR PROPOSAL FOR UNDERTAKING VA OF SECURE MOBILE COMMUNICATION NETWORK (SMCN) AT AAKANKSHA

1. Bids in sealed cover are invited for Request for proposal for undertaking VA of Secure Mobile Communication Network (SMCN) at Aakanksha on LTE basis as per scope of work given in **Appendix C of Part V** of this RFP as per two Bid System. Please super scribe the above mentioned Title, RFP reference number and Date of Opening of the Bids, as per **Para 5 of Part I** of the RFP, on the sealed cover to avoid the Bid being declared invalid.

2. The address and contact numbers for sending Bids or seeking clarifications regarding this RFP are given below:

- | | |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| (a) Bids/Queries to be addressed to | : PD ATVP [for PD (P&A)] |
| (b) Postal address for sending the Bids | : Government of India
Ministry of Defence
Dept. of Defence (R&D)
"Aakanksha"
Development Enclave
Rao Tula Ram Marg
New Delhi-110010 |
| (c) Name & designation of the contact Officer | : Captain Soubhagya Roul
PM (W&S) |
| (d) Telephone number(s) of the contact Officer | : 011- 20863460 |
| (e) Fax number(s) | : 011-20862769 |

(f) E-mail ID contact Officer

: aakitproc@gmail.com
7032901190

3. This RFP is divided into 7 parts as follows: -

(i) **Part I** contains **General Information and Instructions** for the Bidders about the RFP such as the time, place of submission and opening of tenders, Validity period of tenders, etc.

(ii) **Part II** contains **Standards Terms and Conditions of RFP**, which will form part of the Contract / Supply Order (herein after referred as the Contract) with the successful Bidder(s).

(iii) **Part III** contains **Special Terms and Conditions** applicable of this RFP and which will also form part of the Contract with the successful Bidder(s).

(iv) **Part IV** contains **Vendor Qualification Criteria**.

(v) **Part V** contains **Essential Detail of Services Required** E.g. Services details, Consignee, Delivery Period etc.

(vi) **Part VI** contains **Evaluation Criteria of Bids**.


(vii) **Part VII** contains **Format of Price Bid**. Price bid needs to be printed on one side of paper only.

4. This RFP is being issued with no financial commitment and the Buyer reserves the right to change or vary any part thereof or foreclose the procurement case at any stage. The Buyer also reserves the right to disqualify the vendor, should it be necessary, at any stage on grounds of National Security.

5. You may contact PD (P&A), HQ ATVP for any grievance related to bidding condition, bidding process and / or rejection of bid. With regard to bidding condition, this shall be done in writing at least seven days in advance of the stipulated date of submission of bid.

6. It is requested that receipt of this RFP with all enclosures be acknowledged.

Yours sincerely,


(RS Rautela)
DPM (Finance)
For PD ATVP

List of Appendices

Appendix 'A' - Undertaking for Non debarred/blacklisted Firms
Appendix 'B' - Vendor Compliance Matrix
Appendix 'C' - Detailed Scope of Work

PART I – GENERAL INFORMATION AND INSTRUCTIONS

1. **Pre-bid Conference.** A pre-bid meeting will be held in at **1430 Hrs** on **19 Mar 24** at **Aakanksha**, if required, to answer any queries or to clarify doubts regarding submission of proposals. Bidders or their authorized representatives (duly authorised in writing) are invited to attend. This event will not be postponed due to non-presence of your representative.
2. **Last Date and Time for Depositing the Bids.** On **27 Mar 24** at **1430 Hrs** The sealed Bid (both Techno-Commercial and Price Bid, in case two bids are called for) should be deposited / reach by the due date and time. The responsibility to ensure this lies with the Bidder.
3. **Location of the Tender Box.** Reception, “Aakanksha”. Bidder may drop their bids in the tender box at the designated place.
4. **Manner of Depositing the Bids.** Sealed Bids should be either dropped in the tender Box or sent by post at the address given, in the “Invitation of Bids”, so as to reach by the due date and time. Late tenders will not be considered. No responsibility will be taken for postal delay or non-delivery / non-receipt of Bid documents. Bids sent by FAX or e-mail will not be considered unless they have been specially called for by these modes.
5. **Time and Date for Opening of Bids.** On **28 Mar 24** at **1430 Hrs** If due to any exigency, the due date for opening of the bids is declared a closed holiday, the bids will be opened on the next working day at the same time or on any other day/time, as intimated by the Buyer.
6. **Place of Opening of the Bids.** The Bidders may depute their representative, duly authorized in writing, to attend the opening of Bids on the due date and time. Relevant parts and important commercial/technical clauses quoted by all Bidders will be read out in the presence of the representatives of the participating Bidders. This event will not be postponed due to non-presence of your representative.
7. **Marking of Bids.** Bids must be clearly marked with Tender Reference No., Date of opening and Type of bid (Techno-Commercial/Price Bid).
8. **Procedure for Submission of Bid.** Bid shall be submitted in two parts i.e. **Part-I: Techno-Commercial bid** and **Part-II: Price bid**. Both the parts of the Bid shall be submitted in separate sealed envelopes super scribing “Techno-Commercial bid” or “Price bid”, as applicable, along with Tender Reference No. and put both the envelopes in a third sealed envelope super scribing Title of the RFP, Tender Reference No. and Date of Opening. The EMD in a separate sealed envelope clearly depicting “EMD” and RFP number in the Envelope is to be attached along with the Techno Commercial Bid. The sealed EMD would be sighted by the Techno Commercial bid opening committee and would be kept in safe custody along with price bid. Only the Techno-Commercial bids would be opened on the time and date mentioned above. The price bid of the other bidder whose techno-commercial bid are found non-compliant, will be returned to the bidders, in sealed and unopened condition as received. Date of opening price bid will be intimated after acceptance of the Techno-Commercial bid.
9. **Forwarding of Bids.** Bids should be forwarded by Bidders, only, under their original memo / letter pad inter alia furnishing details like TIN, GST number, Bank address with NEFT Account if applicable, etc. and complete postal and e-mail addresses of their office failing which the bid would not be considered.

R

10. **Clarification Regarding Contents of the RFP.** Any clarification regarding the contents of the bidding documents should be sought from the Buyer in writing about the clarifications sought not later than 14 (Fourteen) days prior to the date of opening of the Bids. Copies of the query and clarifications by the Buyer will be sent to the bidder.

11. **Validity of Bids.** The Bids should remain valid for **180 days** from the last date of submission of the Bids.

12. **Modification and Withdrawal of Bids.** A bidder may modify or withdraw his Bid after submission provided that the written notice of modification or withdrawal is received by the Buyer prior to deadline prescribed for submission of bids. A withdrawal notice may be sent by fax, however, it should be followed by a signed confirmation copy to be sent by post and such signed confirmation should reach the purchase not later than the deadline for submission of bids. No bid shall be modified after the deadline for submission of bids. No bid may be withdrawn in the interval between the deadline for submission of bids and expiration of the specified period of bid validity.

13. **Rejection of Bids.** Canvassing by the Bidder in any form, unsolicited letter and post tender correction may invoke summary rejection with forfeiture of EMD. Conditional tenders will be rejected. Non-Compliance of applicable General Information will disqualify your Bid.

14. **Unwillingness to Quote.** Bidders unwilling to quote should ensure that intimation to this effect reaches before the due date and time of opening of the Bid, failing which the defaulting Bidder may be de-registered for the range of items in this RFP, as per the policy in vogue.

15. The Government /Aakanksha reserves the right to cancel the procurement process at any stage and accept or reject any bid, fully or partially, without assigning any reasons.

16. **Earnest Money Deposit.** Bidders are required to submit Earnest Money Deposit (EMD), in favour of the '**HQATVP (MoD)- PUBLIC FUND A/c**' Payable at **New Delhi**, for amount **2%** of Bid amount, in the form of an Account Payee Demand Draft, Bank Guarantee in acceptable form as per DRDO. BG.01, from any of the nationalized Banks, private Sector bank authorized for Govt transaction. In case of two bid system, EMD shall be enclosed in the envelope containing the Techno-Commercial bid. EMD is to remain valid for a period of forty-five days beyond the final bid validity period. EMD shall be enclosed in the envelope clearly depicting the RFP no. and written on the envelope. The EMD would be opened only with the price bid. EMD of the unsuccessful bidders will be returned to them, without any interest whatsoever, at the earliest after expiry of the final bid validity and latest on or before the thirtieth day after the award of the contract. EMD of the successful bidder would be returned without any interest whatsoever after the receipt of applicable Security Deposit/Performance and warranty bond from them as called for in the Contract. The following organization/firms are exempted from submission of EMD.

- (a) Bidders registered with DRDO, Min of Defence and NSIC.
- (b) DPSUs other Govt. Organization.
- (c) KVIC, Kendriya Bhandar/ NCCF.
- (d) Micro and Small Enterprises (MSEs) as per their registration.
- (e) Startup as recognized by Dept. of Industrial Policy and promotion (DIPP)

17. Such bidder would be required to furnish the relevant documents in their Techno-Commercial bid in support of the claim. The EMD will be forfeited if the bidder withdraws,

Q/

amends impairs or derogates from the tender in any respect within the validity period of their tender.

18. Clarification Regarding Contents of the Bids. During evaluation of bids, the Buyer may, at his discretion, ask the bidder for clarification on his Bid. The request for clarification will be given in writing. No clarification on the initiative of the bidder will be entertained after opening of bid.

19. Bids of debarred/blacklisted Firms will not be considered for evaluation.

R

PART II – STANDARD TERMS AND CONDITIONS

1. The Bidder is required to give confirmation of their acceptance of the Standard Terms and Conditions of the RFP mentioned below which will automatically be considered as part of the Contract concluded with the successful Bidder as selected by the Buyer. Failure to do so may result in rejection of the Bid submitted by the Bidder.

2. **Effective Date of the Contract.** In case of placement of a supply order, the date of acceptance of the Supply Order would be deemed as effective date or as agreed by both the parties. In case a contract is to be signed by both the parties, the Contract shall come into effect on the date of signatures of both the parties on the Contract (Effective Date) or as agreed by both the parties. The deliveries and supplies and performance of the services shall commence from the effective date of the Contract.

3. **Law.** The Contract shall be considered and made in accordance with the laws of the Republic of India and shall be governed by and interpreted in accordance with the laws of the Republic of India.

4. The Contractor shall comply with the statutory provisions or the regulations and / or bye-laws of any local authority and /or and public service, company or authority affected by the work, shall pay all charges there-under, and shall indemnify the Government against any fees or charges demandable by the law under such acts, regulations and or bye-laws in respect of the work.

5. **Arbitration.** All disputes or differences arising out of or in connection with the Contract shall be settled by bilateral discussions. Any dispute, disagreement or question arising out of or relating to the Contract or relating to product or performance, which cannot be settled amicably, shall be resolved by arbitration in accordance with the following applicable provision:

(a) **For Central and State PSEs:** In the event of any dispute or difference relating to the interpretation and application of the provisions of commercial contract(s), such disputes or difference shall be taken up by either party for resolution through Administrative Mechanism for Resolution of CPSEs Disputes (AMRC) as per provisions of Department of Public Enterprises OM No. 4(1)/2013-DPE(GM)/FTS-1835 dated 22-05-2018 as amended.

(b) **For Defence PSUs:** The case of arbitration shall be referred to the Secretary Defence (R&D) for the appointment of arbitrator(s) and proceedings.

(c) **For Other Firms:** Any dispute, disagreement or question arising out of or relating to the Contract or relating to product or performance, which cannot be settled amicably, shall be resolved by arbitration in accordance with either of the following provisions:

“The case of arbitration may be referred to arbitrator / arbitrators appointed as per Section 11 of Indian Arbitration and conciliation Act, 1996 as amended and the proceedings shall be conducted in accordance with procedure of Indian Arbitration and Conciliation Act, 1996, as amended.”

Q

Or

"The case of arbitration may be referred to International Centre for Alternative Dispute Resolution (ICADR) for the appointment of arbitrator and proceedings shall be conducted in accordance with procedure of Indian Arbitration and Conciliation Act, 1996, as amended."

Or

"The case of arbitration may be conducted in accordance with the rules of Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules in India. However, the arbitration proceedings shall be conducted in India under Indian Arbitration and Conciliation Act, 1996, as amended."

6. All suits arising out of this contract shall be instituted in a court of jurisdiction located within the Municipal Corporation limits of New Delhi and in no other court.

7. **Penalty for Use of Undue influence.** The Seller undertakes that he has not given, offered or promised to give, directly or indirectly, any gift, consideration, reward, commission, fees, brokerage or inducement to any person in service of the Buyer or otherwise in procuring the Contract or forbearing to do or for having done or forborne to do any act in relation to the obtaining or execution of the Contract or any other contract with the Government of India for showing or forbearing to show favour or disfavor to any person in relation to the Contract or any other contract with the Government of India. Any breach of the aforesaid undertaking by the Seller or anyone employed by him or acting on his behalf (whether with or without the knowledge of the Seller) or the commission of any offers by the Seller or anyone employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act, 1986 or any other Act enacted for the prevention of corruption shall entitle the Buyer to cancel the contract and all or any other contracts with the Seller and recover from the Seller the amount of any loss arising from such cancellation. A decision of the Buyer or his nominee to the effect that a breach of the undertaking had been committed shall be final and binding on the Seller. Giving or offering of any gift, bribe or inducement or any attempt at any such act on behalf of the Seller towards any officer/employee of the Buyer or to any other person in a position to influence any officer/employee of the Buyer for showing any favour in relation to this or any other contract, shall render the Seller to such liability/penalty as the Buyer may deem proper, including but not limited to termination of the contract, imposition of penal damages, forfeiture or the Bank Guarantee and refund of the amounts paid by the Buyer.

8. **Agents / Agency Commission.** The Seller confirms and declares to the Buyer that the Seller has not engaged any individual or firm, whether Indian or foreign whatsoever, to intercede, facilitate or in any way to recommend to the Government of India or any of its functionaries, whether officially or unofficially, to the award of the Contract to the Seller; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Seller agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in any way incorrect or if at a later stage it is discovered by the Buyer that the Seller has engaged any such individual/firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this Contract, the Seller will be liable to refund that amount to the Buyer. The Seller will also be debarred from entering into any Contract with the Government of India for a minimum period of five years. The Buyer will also have right to consider cancellation of the Contract either wholly or in part, without any entitlement or compensation to the Seller who shall in such an event be liable to refund all payments made by the Buyer in terms of the Contract along with interest at the rate of 2% above (i) MCLR (Marginal Cost of Funds based

R

Lending Rate) declared by RBI pertaining to State Bank of India for Indian bidders, and (ii), London Inter Bank Offered Rate (LIBOR) / EURIBOR for the foreign bidders. The applicable rates on the date of opening of tender shall be considered for this. The Buyer will also have the right to recover any such amount from any Contract in vogue with the Government of India.

Or

The Seller confirms and declares in the Techno-Commercial bid that they have engaged an agent, individual or firm, for performing certain services on their behalf. The Seller is required to disclose full details of any such person, party, firm or institution engaged by them for marketing of their equipment in India, either on a country specific basis or as a part of a global or regional arrangement. These details should include the scope of work and responsibilities that have been entrusted with the said party in India. If there is non-involvement of any such party, then the same also be communicated in the offers specifically. The information is to be submitted as per the format at DRDO.SA.01. Without prejudice to the obligations of the vendor as contained in various parts of this document, appointment of an Agent by vendors will be subjected to the following conditions:

- (a) Details of all Agents will be disclosed at the time of submission of offers and within two weeks of engagement of an Agent at any subsequent stage of procurement.
- (b) The Seller is required to disclose termination of the agreement with the Agent, within two weeks of the agreement having been terminated.
- (c) Buyer /MoD reserves the right to inform the Seller at any stage that the Agent so engaged is not acceptable whereupon it would be incumbent on the Seller either to interact with Buyer / MoD directly or engage another Agent. The decision of Buyer /MoD on rejection of the Agent shall be final and be effective immediately.
- (d) All payments made to the Agent 12 months prior to tender submission would be disclosed at the time of tender submission and thereafter an annual report of payments would be submitted during the procurement process or upon demand of the Buyer / MoD.
- (e) The Agent will not be engaged to manipulate or in any way to recommend to any functionaries of the Govt. of India, whether officially or unofficially, the award of the Contract to the Seller or to indulge in corrupt and unethical practices.
- (f) The Contract with the Agent will not be a conditional Contract wherein payment made or penalty levied is based, directly or indirectly, on success or failure of the award of the Contract.
- (g) On demand, the Seller shall provide necessary information/inspection of the relevant financial documents/ information, including a copy of the Contract and details of payment terms between the Seller and the Agent engaged by him.
- (h) If the equipment being offered by the Seller has been supplied with any organization, public/ private in India, the details of the same may be furnished in the technical as well as commercial offers. The Sellers are required to give a written undertaking that they have not supplied/is not supplying the similar systems or subsystems at a price lower than that offered in the present bid to any other Ministry/ Department of the Government of India and if the similar system has been supplied at

Q

a lower price, then the details regarding the cost, time of supply and quantities be included as part of the commercial offer. In case of non-disclosure, if it is found at any stage that the similar system or subsystem was supplied by the Seller to any other Ministry/Department of the Government of India at a lower price, then that very price, will be applicable to the present case and with due allowance for elapsed time, the difference in the cost would be refunded to the Buyer, if the Contract has already been concluded.

(j) Following details are also to be submitted in the Techno-Commercial bid:

- (i) Name of the Agent
- (ii) Agency Agreement between the Seller and the agent giving details of their Contract obligation
- (iii) PAN Number, name and address of bankers in India and abroad in respect of Indian agent
- (iv) The nature and scope of services to be rendered by the agent.
- (v) Percentage of agency commission payable to the agent.

9. **Handling of Classified Information by Indian Licensed Defence Industry.** Any classified document/information/ equipment being shared with Indian Licensed Defence Industries will be protected/ handled to prevent unauthorized access as per provisions of Chapter 5 of Security Manual for Indian Licensed Defence Industries issued by MoD (Department of Defence Production).

10. **Access to Books of Accounts.** In case it is found to the satisfaction of the Buyer that the Bidder / Seller has violated the provisions of use of Undue Influence and/ or Employment of Agent to obtain the Contract. The Bidder / Seller, on a specific request of the Buyer, shall provide necessary information/inspection of the relevant financial documents / information / Books of Accounts.

11. **Non-disclosure of Contract Documents.** Except with the written consent of the Buyer/Seller, other party shall not disclose the Contract or any provision, specification, plan, design, pattern, sample or information thereof to any third party.

12. **Secrecy.** Contractor agrees that all classified information related to this Contract will be treated as secret and that the contents of designs, process sheets or any other documents will not be divulged/disclose or parted with to any third party, except to the extent required for the execution of the Contract, without the written authorization by work in connection with this Contract, have noted that the Indian Official Secret Act, 1923 (XIX of 1923), applies to them, and will continue to apply even after termination or expiry of supply/design/erection or any other part of the contracted work to be published in any scientific, engineering periodicals, publications or newspaper without first obtaining the written consent of the Purchaser.

13. **Withholding of Payment.** In the event of the Seller's failure to submit the Bonds, Guarantees and Documents, supply the stores/goods and conduct trials, installation of equipment, training etc. as specified in the Contract, the Buyer may, at his discretion, withhold any payment until the completion of the Contract.

14. **Liquidated Damages(LD).** The Buyer may deduct from the Seller, as agreed, liquidated damages at the rate of 0.5% per week or part thereof, of the basic cost of the delayed services which the Seller has failed to deliver within the period agreed for delivery in the contract. LD can also be levied on the Seller on the basic cost of the stores supplied

Q

partially within the scope of the order/contract that could not be put to use due to late delivery, of the remaining stores. The maximum quantum of LD would be 10% of the total order value.”

15. For the Services portion of the contract, Liquidated Damages would be levied as follows: -

(a) The Contractor shall ensure provisioning of the required number of the personnel as required by the HQ ATVP within specified time period on receipt of written intimation from HQ ATVP. In case of inability of the Contractor to provision the required number of personnel as intimated, which would lead to interruption of work on the ground, Contractor would be liable to pay liquidated damages for a sum amounting to twice the rates decided for the respective categories of personnel, for the equivalent period that the personnel have not been provisioned.

(b) Requirement of manpower would depend on pace/quantum of progress of work at HQ ATVP. LD clause would not be applicable, if the work centre does not requisition the full strength as per contract.

(c) If person/ personnel in the work centre are absent for more than two weeks continuously, then Contractor will be liable to pay liquidated damages for a sum amounting to twice the rates decided for the respective categories of personnel, for the equivalent period.

16. **Termination of Contract.** The Buyer shall have the right to terminate the Contract in part or in full in any of the following cases: -

(a) The store/service is not received/rendered as per the Contracted schedule(s) and the same has not been extended by the Buyer.

Or

The delivery of the store/service is delayed for causes not attributable to Force Majeure for more than 03 months after the scheduled date of delivery and the delivery period has not been extended by the Buyer.

(b) The delivery of store/service is delayed due to cause of Force Majeure by more than 03 months provided Force Majeure clause is included in the Contract and the delivery period has not been extended by the Buyer.

(c) The Seller is declared bankrupt or becomes insolvent.

(d) The Buyer has noticed that the Seller has violated the provisions of use of undue influence and/ or employment of agent to obtain the Contract.

(e) As per decision of the Arbitration Tribunal.

17. **Notices.** Any notice required or permitted by the contract shall be written in English Language and may be delivered personally or may be sent by FAX or registered pre-paid mail/airmail, addressed to the last known address of the firm party to whom it is sent.

18. **Transfer and Sub-letting.** The seller has no right to give, bargain, sell, assign or sublet or otherwise dispose of the Contract or any part thereof, as well as to give or to let a

Q

third party take benefit or advantage of the Contract or any part thereof without written consent of the Buyer.”

19. **Amendments.** No provision of the Contract shall be changed or modified in any way (including this provision) either in whole or in part except when both the parties are in written agreement for amending the Contract.

20. **Taxes and Duties.**

(a) **General**

(i) Bidders must indicate separately the relevant taxes/duties as per prevalent rates for the delivery of completed goods specified in RFP. In absence of this, the total cost quoted by them in their bids will be taken into account in the ranking of bids.

(ii) If a Bidder is exempted from payment of any duty/tax upto any value of supplies from them, he should clearly state that no such duty/tax will be charged by them up to the limit of exemption which they may have. If any concession is available in regard to rate/quantum of any Duty/tax, it should be brought out clearly. In such cases, relevant certificate will be issued by the Buyer later to enable the Seller to obtain exemptions from taxation authorities.

(iii) Any changes in levies, taxes and duties/tax levied by Central/State/Local governments on final product upward as a result of any statutory variation taking place within contract period shall be allowed reimbursement by the Buyer, to the extent of actual quantum of such duty/tax paid by the Seller. Similarly, in case of downward revision in any such duty/tax, the actual quantum of reduction of such duty/tax shall be reimbursed to the Buyer by the Seller. All such adjustments shall include all reliefs, exemptions, rebates, concession etc, if any, obtained by the Seller. Section 64-A of Sales of Goods Act will be relevant in this situation.

(iv) Levies, taxes and duties levied by Central/State/Local governments on final product will be paid by the Buyer on actuals, based on relevant documentary evidence, wherever applicable. Taxes and duties on input items will not be paid by Buyer and they may not be indicated separately in the bids. Bidders are required to include the same in the pricing of their product.

(v) TDS as per Income Tax Rules will be deducted and a certificate to that effect will be issued by the Buyer.

(b) **Customs Duty**

(aa) Customs Duty Exemption Certificate (CDEC) would be issued to designated PSUs only.

(ab) In case CDEC is not issued, Customs Duty will be reimbursed at actual on submission of proof of payment of taxes by supplier.

(ac) Issue of CDEC will be governed as per prevailing orders.

R

(ad) The Supplier is to indicate the CIF value of Imports in the Price bid along with Custom Duty applicable.

(c) **Goods & Service Tax (GST)**: Bidder must indicate existing GST rate applicable while submitting the bids. GST exemption certificate will not be issued. GST paid will be reimbursed at actual on submission of documentary proof of payment.

21. **Denial Clause**. Variations in the rates of statutory levies within the original delivery schedule will be allowed if taxes are explicitly mentioned in the contract/supply order and delivery has not been made till the revision of the statutory levies. Buyer reserves the right not to reimburse the enhancement of cost due to increase in statutory levies beyond the original delivery period of the supply order/contract even if such extension is granted without imposition of LD.

22. **Risk and Expense Purchase Clause**: This clause is applicable in the event of the seller failing to honour the contractual obligation within the stipulated Delivery Period and where extension of Delivery Period is not approved. If risk purchase is restored to, the Seller is liable to pay the additional amount spent by the Buyer. If any, in procuring the said contracted goods/services through a fresh supply order/contract, i.e. the defaulting Seller has to bear the excess cost incurred as compared with the amount contracted with Seller.

23. **Undertaking from the Bidders**. An undertaking will be obtained from the Bidder that in the past they have never been banned/debarred for doing business dealings with Ministry of Defence/ Govt. of India/ any other Govt. organization and that there is no enquiry going on by /CBI/ED/ any other Govt. agency against them. (As per **Appendix A** an enclosed herewith) *Undertaking is mandatory for all Bids, without which the offer will not be considered. In case of two bids system, this undertaking is to be attached to Technical Bid.*

Q

PART III – SPECIAL TERMS AND CONDITIONS

1. The Bidder is required to give confirmation of their acceptance of Special Terms and Conditions of the RFP mentioned below which will automatically be considered as part of the Contract concluded with the successful Bidder as selected by the Buyer. Failure to do so may result in rejection of Bid submitted by the Bidder.

2. **Performance and Warranty Bond (PWB):** -

(a) **Performance Security Bond:** - The Bidder/Contractor will be required to furnish a Performance Security Bond by way of Bank Guarantee (BG) / Indemnity Bond (in case of PSUs)) in favour of the Programme Director, HQ ATPV, New Delhi, for a sum equal to 10% of the contract value (inclusive of taxes and duties) within 30 days of receipt of the Order for safeguarding the Buyer's interest in all respects during the currency of the contract. In case the execution of the contract is delayed beyond the contracted period and the Buyer grants the extension of delivery period, with or without liquidated damages, the Seller must get the Bond revalidated, The Bond submitted by way of Bank Guarantee (BG) / Indemnity Bond (in case of PSUs) should be valid upto 60 days beyond the date of completion of all contractual obligations except the one related to post acceptance.

(b) **Warranty Bond:** - The Warranty Bond is not applicable, being a service contract.

"The Performance Security will be forfeited by the Buyer, in case the condition regarding adherence to delivery schedule and/or other provisions of the Contract/SO are not fulfilled by the Seller."

3. **Permissible Time Frame for submission of Bills.** To claim payment (part or full), the Supplier shall submit the bill(s) along with the relevant documents within 30 days from the completion of the activity/supply.

4. **Payment Terms.** 100% payment within 30 days after receipt, a satisfactory work completion certificate of services and submission of bills. (30 days will be counted from submission of bills).

(a) **Reimbursement of Taxes & Duties.** Payment towards taxes & duties would be made at actuals on production of documentary proof of payment. Documents required to be submitted along with the bills are as follows: -

(i) Certified copy of Tax Challan/online receipt from the concerned tax department showing the actual amount paid against the claimed amount. Input Tax credit (ITC) availed/ used by the firm for the present contract along with necessary proof is to be submitted for processing GST invoices. In case ITC is not being availed then the price bid should clearly mention Ex ITC rates and the same is to be substantiated through suitable CA certificate during submission of bids.

(ii) Certificate from Chartered Accountant in original, linking the taxes / duties claimed by the firm with payment made by this office.

(iii) Tax invoice of the firm showing details of taxes / duties being claimed and the basic amount on which claim is being made.

R

(iv) Copy of govt. notification showing rate of taxes / duties during the original Delivery Period in case the supplies have been made during the extended Delivery Period.

(b) Invoices for all payments shall be raised by Contractor as and when due, and payments shall be made to the Supplier within 90-120 days of receipt of invoice by Purchaser.

(c) **Recovery of dues.** Whenever, under the Contract, any sum of money is payable by the Supplier to the Customer, the same shall be deducted from any sum then due, or which at any time, thereafter may become due, to the Supplier under this Contract. Should this sum not be sufficient to cover the full amount due, the Supplier shall pay to the Customer on demand the balance dues with interest, to be decided in consultation with Controller Defence Accounts / Audit authorities, for the period of retention of excess sum. However, a notice of 30 days will be given to the Supplier before any recovery is made

5. **Mode of Payment.** It will be mandatory for the Bidders to indicate their bank account numbers and other relevant e-payment details to facilitate payments through ECS/NEFT mechanism instead of payment through cheque, wherever feasible.

6. **Documents to be Furnished for Claiming Payment.**

(a) The payment of bills will be made on submission of the following documents, if applicable, by the Supplier to the Buyer:

(i) Ink- signed copy of Commercial Invoice / Supplier's Bill.

(ii) Bank Guarantee for Advance, if applicable.

(iii) Guarantee/Warranty Certificate, if applicable.

(iv) Performance Bank Guarantee/ Indemnity Bond, if applicable.

(v) Details for electronic payment viz. Bank name, Branch name and address, Account Number, IFS Code, MICR Number (if these details are not already incorporated in the Contract).

(vi) Original copy of the Contract and amendments thereon, if any.

(vii) Ink signed copy of contingent Bill.

(viii) Any other documents / certificates that may be provided for in the contract.

7. **Force Majeure Clause.**

(a) Neither party shall bear responsibility for the complete or partial non-performance of any of its obligations, if the non-performance results from such Force Majeure circumstances as Flood, Fire, Earth Quake and other acts of God as well as War, Military operations, blockade, Acts or Actions of State Authorities or any other circumstances beyond the parties control that have arisen after the conclusion of the present contract.

Q

(b) In such circumstances the time stipulated for the performance of an obligation under the Contract is extended correspondingly for the period of time commensurate with actions or circumstances and their consequences.

(c) The party for which it becomes impossible to meet obligations under the Contract due to Force Majeure conditions, is to notify in written form to the other party of the beginning and cessation of the above circumstances immediately, but in any case not later than 10 (Ten) days from their commencement.

(d) Certificate of a Chamber of Commerce (Commerce and Industry) or other competent authority or organization of the respective country shall be considered as sufficient proof of commencement and cessation of the above circumstances.

(e) If the impossibility of complete or partial performance of an obligation lasts for more than 6(Six) months, either party hereto reserves the right to terminate the Contract totally or partially upon giving prior written notice of 30(Thirty) days to the other party of the intention to terminate without any liability other than reimbursement on the terms provided in the agreement for the goods received.

Q

PART IV- VENDOR QUALIFICATION CRITERIA

1. **Submission of Bids.** The Tenderer shall clearly specify the following at the time of submission of Bids: -
- (a) **Tenderer's Site Organisation.** The Tenderer shall furnish details of its organisation along with his Tender, for execution of the present Contract/ Purchase Order/Supply Order/Work Order.
 - (b) **Validity of Tender.** The Bidder shall keep his offer valid **for 180 days** from the date submission of the Bids.
 - (c) **Financial Capabilities.** The Bidder should have minimum financial resources to execute the order.
 - (d) **Compliance Statement.** The vendor compliance matrix, placed at **Appendix B**, needs to be furnished by Seller a part of the Techno-Commercial Bid.



PART V – ESSENTIAL DETAILS OF SERVICE REQUIRED

1. The Broad details of services are as follows: -

S. No.	Details of Services
(a)	Firewall Audit
(b)	Configuration Review (CIS/MBS) (i) Firewall (ii) Switch (iii) Base Server (iv) Servers (DNS, XMPP, MDM, Auth, DB, Base)
(c)	Android Application PT (Kiosk Escape, Sandbox, System integration and Management)
(d)	Web Application PT (Dashboard)
(e)	Infrastructure- VPN and network Coverage (Internal and External)
(f)	One-time Revalidation Testing

2. **Detailed Scope of Work** – The detailed broad scope of work is placed at **Appendix-C**.

- (a) **Enclosure 1** – Web Application Pentesting Checklist
- (b) **Enclosure 2** – Desktop Application Checklist
- (c) **Enclosure 3** – API Security Checklist
- (d) **Enclosure 4** – Mobile Application Pentesting Checklist

3. **Delivery Period** Expected Delivery Period for rendering services would be **90 days** from the Effective Date of the Contract.

4. **Consignee details**

The Programme Director
[For PD (WL&IT)]
'Aakanksha', Min of Defence
Development Enclave
Rao Tula Ram Marg
New Delhi-110010

5. **Deviations**. Deviations from approved specifications specified in Technical requirements, if any, will render the order liable to rejection. The Seller shall not be entitled to make any additions or alterations in specifications of the upgradation cum maintenance without written instructions of the Buyer.

PART VI – EVALUATION CRITERIA FOR BIDS

1. **Evaluation Criteria**. The bid being considered on LTE basis shall be evaluated once found to be fulfilling all the eligibility and qualifying requirements of the tender, both technically and commercially.
2. **Compliance Statement**. The Vendor compliance matrix, needs to be furnished by Seller in Techno-Commercial Bid indicating acceptance or otherwise of all the technical specifications, terms & conditions and the technical and quality criteria indicated in the RFP (Compliance statement with a matrix showing compliance to each Para of Part I to Part-VII of this RFP). It is to be noted that detail of documents being attached are to be mentioned in the Vendor Compliance matrix. Generic **Yes / No** is not acceptable and may lead to disqualification of the Bid.
3. **Opening of Technical Bid**. The date of opening of technical bid will be as per Part I of this RFP. The Seller or his authorized representative is welcome to be present at the opening of the bids. The technical bid shall be opened by a 'Technical Evaluation Committee' (TEC) constituted by the Buyer. After scrutiny of the bid by the TEC, your reps shall be invited for discussions, clarifications and detailed understanding, if required. There may be a necessity of resubmitting the Technical Bid based on the discussions held with the TEC and your reps.
4. **Opening of Commercial Bid**. The date of opening of the commercial bid will be communicated separately. Once all queries raised by the TEC have been clarified, the commercial bid will be opened by the Price Negotiation Committee (PNC) in presence of the firm's representatives.
5. **Placement of Order**. The Purchase Order will be placed post clearance by the PNC and approval of the PNC Report.
6. **Award of Contract/ Purchase Order/Supply Order**. The Buyer also reserves the right to accept the whole or a portion of any bid as they may think fit, without assigning any reason.



PART VII – PRICE BID FORMAT

1. **Price Bid Format:** The Price Bid Format as given below is required to be filled by Bidders: -

S. No.	Details of Service	Basic Cost
(a)	Firewall Audit	
(b)	Configuration Review (CIS/MBS) (i) Firewall (ii) Switch (iii) Base Server (iv) Servers (DNS, XMPP, MDM, Auth, DB, Base)	
(c)	Android Application PT (Kiosk Escape, Sandbox, System integration and Management)	
(d)	Web Application PT (Dashboard)	
(e)	Infrastructure- VPN and network Coverage (Internal and External)	
(f)	One-time Revalidation Testing	
Total		
GST@ 18%		
Grand Total		

Note:

- (a) Basic cost of the Services.
- (b) Is GST extra? If yes, then mention following: -
- (i) Total value on which GST is leviable.
 - (ii) Rate of GST.
 - (iii) Total value of GST leviable.
- (c) Any other Taxes / Duties / Overheads / Other costs.
- (d) Grand Total



This Undertaking on Company letterhead is mandatory without which the offer will not be considered

Company Letter Head

Sub: Undertaking w.r.t Enquiry by CBI/ED/ any other Govt. Agency- Reg.

Ref: RFP No. _____ Dated _____

We, _____ (Name & Address of the firm) hereby confirm that we have never been banned/ debarred for doing business dealing with Ministry of Defence / Govt. of India/ any other Govt. organization and there is no enquiry going on by CBI / ED/ any other Govt. agency against us.

Date:

(Authorized Signatory)

Company Seal:

✓

VENDOR COMPLIANCE MATRIX

Sl. No.	Documents	Remarks	Compliance (Yes/No)
(a)	Copy of Firm's PAN No.	Copy of PAN Card	
(b)	Copy of Company GST No. & Copy of Registration	Copy of GST Registration Certificate last years GST Challan	
(c)	Income tax clearance certificate	Income tax clearance certificate for latest assessment year countersigned by the Income Tax Officer of his area under Seal of his office	
(d)	The bidder must have successfully completed/executed at least three contracts of Services of VA/PT of similar type any Govt. organization. At least two contracts for a minimum value of ₹ 10 Lakh.	Copy of Work orders/Contract agreement to be provided as proof. Satisfactory work completion certificate from Govt. organizations for execution of these orders/contracts is to be provided.	
(e)	Proof of average Turnover of the bidder during last three years	Balance sheets of Three financial years are to be submitted.	
(f)	Declaration of dedicated telephone numbers / email IDs for Supplier and Service Support.	Bidder must submit details of Buyer care/contract person number along with escalation matrix on its letter head.	
(g)	Acceptance of all terms and conditions of the Bid	Undertaking to be submitted.	
(h)	Technical Evaluation Matrix (point by point compliance of all technical specifications of VA/PT services as per RFP)	Bidder must submit point by point compliance of all Technical specifications of product as per RFP	
(i)	The firm should not be Debarred/blacklisted	Undertaking to be submitted. (As per Appendix A)	
(k)	Bid Security Declaration	Undertaking to be submitted.	
(l)	Police Verification Certificate of Employees being deputed for Audit and during VA/PT.	Undertaking to be submitted that PVC will be furnished prior to placement of SO.	
(p)	Earnest Money Deposit (EMD)	Copy of Certificate, If bidder registered with DRDO/ Min. of Defence/ NSIC/DPSUs, other Govt. organizations, KVIC, Kendriya Bhandar / NCCF, Micro and Small Enterprises (MSEs)	

a

DETAILED SCOPE OF WORK

1. The detailed of SoW is as under: -

WEB APPLICATION PENTESTING CHECKLIST

<u>S.No.</u>	<u>Controls</u>	<u>Test Conducted</u>	<u>Vulnerability Detected</u>	<u>Remarks</u>
INFORMATION GATHERING				
1.	Open Source Reconnaissance			
	(a) Perform Google Dorks search			
	(b) Perform OSINT			
2.	Fingerprinting Web Server			
	(a) Find the Type of Web Server			
	(b) Find the version detail of the Web Server			
3.	Looking For Metafiles			
	(a) View the Robots. txt file			
	(b) View the Sitemap.xml file			
	(c) View the Humans. txt file			
	(d) View the Security. txt file			
4.	Enumerating Web Server's Application			
	(a) Enumerating with Nmap			
	(b) Enumerating with Netcat			
	(c) Perform a DNS lookup			
	(d) Perform a Reverse DNS lookup			
5.	Review The Web Contents			
	(a) Inspect the page source for sensitive info			
	(b) Try to find Sensitive Java script codes			
	(c) Try to find any keys			
	(d) Make sure the autocomplete is disabled			
6.	Identifying Application's Entry Points			
	(a) Identify what the methods used are?			
	(b) Identify where the methods used are?			
	(c) Identify the Injection point			
7.	Mapping Execution Paths			
	(a) Use Burp Suite			
	(b) Use Dirsearch			
	(c) Use Gobuster			
8.	Fingerprint Web Application Framework			
	(a) Use the Wappalyzer browser extension			
	(b) Use Whatweb			
	(c) View URL extensions			
	(d) View HTML source code			
	(e) View the cookie parameter			
	(f) View the HTTP headers			
9.	Map Application Architecture			
	(a) Map the overall site structure			
CONFIGURATION & DEPLOYMENT MANAGEMENT TESTING				
10.	Test Network Configuration			
	(a) Check the network configuration			

	(b)	Check for default settings			
	(c)	Check for default credentials			
11.	Test Application Configuration				
	(a)	Ensure only required modules are used			
	(b)	Ensure unwanted modules are disabled			
	(c)	Ensure the server can handle DOS			
	(d)	Check how the application is handling 4xx & 5xx errors			
	(e)	Check for the privilege required to run			
	(f)	Check log for sensitive info			
12.	Test File Extension Handling				
	(a)	Ensure the server won't return sensitive extensions			
	(b)	Ensure the server won't accept malicious extensions			
	(c)	Test for file upload vulnerabilities			
13.	Review Backup & Unreferenced Files				
	(a)	Ensure unreferenced files don't contain any sensitive info			
	(b)	Ensure the namings of old and new backup files			
	(c)	Check the functionality of unreferenced pages			
14.	Enumerate Infrastructure & Admin Interfaces				
	(a)	Try to find the Infrastructure Interface			
	(b)	Try to find the Admin Interface			
	(c)	Identify the hidden admin functionalities			
15.	Testing HTTP Methods				
	(a)	Discover the supported methods			
	(b)	Ensure the PUT method is disabled			
	(c)	Ensure the OPTIONS method is disabled			
	(d)	Test access control bypass			
	(e)	Test for XST attacks			
	(f)	Test for HTTP method overriding			
16.	Test HSTS				
	(a)	Ensure HSTS is enabled			
17.	Test RIA Cross Domain Policy				
	(a)	Check for Adobe's Cross Domain Policy			
	(b)	Ensure it has the least privilege			
18.	Test File Permission				
	(a)	Ensure the permissions for sensitive files			
	(b)	Test for directory enumeration			
19.	Test For Subdomain Takeover				
	(a)	Test DNS, A, and CNAME records for subdomain takeover			
	(b)	Test NS records for subdomain takeover			
	(c)	Test 404 response for subdomain takeover			
20.	Test Cloud Storage				
	(a)	Check the sensitive paths of AWS			
	(b)	Check the sensitive paths of Google Cloud			
	(c)	Check the sensitive paths of Azure			
IDENTITY MANAGEMENT TESTING					
21.	Test Role Definitions				
	(a)	Test for forced browsing			
	(b)	Test for IDOR (Insecure Direct Object Reference)			

A✓

	(c)	Test for parameter tampering			
	(d)	Ensure low privilege users can't able to access high privilege resources			
22.	Test User Registration Process				
	(a)	Ensure the same user or identity can't register again and again			
	(b)	Ensure the registrations are verified			
	(c)	Ensure disposable email addresses are rejected			
	(d)	Check what proof is required for successful registration			
23.	Test Account Provisioning Process				
	(a)	Check the verification for the provisioning process			
	(b)	Check the verification for the de- provisioning process			
	(c)	Check the provisioning rights for an admin user to other users			
	(d)	Check whether a user is able to de- provision themselves or not?			
	(e)	Check for the resources of a de- provisioned user			
24.	Testing For Account Enumeration				
	(a)	Check the response when a valid username and password entered			
	(b)	Check the response when a valid username and an invalid password entered			
	(c)	Check the response when an invalid username and password entered			
	(d)	Ensure the rate-limiting functionality is enabled in username and password fields			
25.	Test For Weak Username Policy				
	(a)	Check the response for both valid and invalid usernames			
	(b)	Check for username enumeration			
AUTHENTICATION TESTING					
26.	Test For Un-Encrypted Channel				
	(a)	Check for the HTTP login page			
	(b)	Check for the HTTP register or sign-in page			
	(c)	Check for HTTP forgot password page			
	(d)	Check for HTTP change password			
	(e)	Check for resources on HTTP after logout			
	(f)	Test for forced browsing to HTTP pages			
27.	Test For Default Credentials				
	(a)	Test with default credentials			
	(b)	Test organization name as credentials			
	(c)	Test for response manipulation			
	(d)	Test for the default username and a blank password			
	(e)	Review the page source for credentials			
28.	Test For Weak Lockout Mechanism				
	(a)	Ensure the account has been locked after 3-5 incorrect attempts			
	(b)	Ensure the system accepts only the valid CAPTCHA			
	(c)	Ensure the system rejects the invalid CAPTCHA			

	(d)	Ensure CAPTCHA code regenerated after reloaded			
	(e)	Ensure CAPTCHA reloads after entering the wrong code			
	(f)	Ensure the user has a recovery option for a lockout account			
29.	Test For Bypassing Authentication Schema				
	(a)	Test forced browsing directly to the internal dashboard without login			
	(b)	Test for session ID prediction			
	(c)	Test for authentication parameter tampering			
	(d)	Test for SQL injection on the login page			
	(e)	Test to gain access with the help of session ID			
	(f)	Test multiple logins allowed or not?			
30.	Test For Vulnerable Remember Password				
	(a)	Ensure that the stored password is encrypted			
	(b)	Ensure that the stored password is on the server-side			
31.	Test For Browser Cache Weakness				
	(a)	Ensure proper cache-control is set on sensitive pages			
	(b)	Ensure no sensitive data is stored in the browser cache storage			
32.	Test For Weak Password Policy				
	(a)	Ensure the password policy is set to strong			
	(b)	Check for password reusability			
	(c)	Check the user is prevented to use his username as a password			
	(d)	Check for the usage of common weak passwords			
	(e)	Check the minimum password length to be set			
	(f)	Check the maximum password length to be set			
33.	Testing For Weak Security Questions				
	(a)	Check for the complexity of the questions			
	(b)	Check for brute-forcing			
34.	Test For Weak Password Reset Function				
	(a)	Check what information is required to reset the password			
	(b)	Check for password reset function with HTTP			
	(c)	Test the randomness of the password reset tokens			
	(d)	Test the uniqueness of the password reset tokens			
	(e)	Test for rate limiting on password reset tokens			
	(f)	Ensure the token must expire after being used			
	(g)	Ensure the token must expire after not being used for a long time			
35.	Test For Weak Password Change Function				

	(a)	Check if the old password asked to make a change			
	(b)	Check for the uniqueness of the forgotten password			
	(c)	Check for blank password change			
	(d)	Check for password change function with HTTP			
	(e)	Ensure the old password is not displayed after changed			
	(f)	Ensure the other sessions got destroyed after the password change			
36.	Test For Weak Authentication In Alternative channel				
	(a)	Test authentication on the desktop browsers			
	(b)	Test authentication on the mobile browsers			
	(c)	Test authentication in a different country			
	(d)	Test authentication in a different language			
	(e)	Test authentication on desktop applications			
	(f)	Test authentication on mobile applications			
AUTHORIZATION TESTING					
37.	Testing Directory Traversal File include				
	(a)	Identify the injection point on the URL			
	(b)	Test for Local File Inclusion			
	(c)	Test for Remote File Inclusion			
	(d)	Test Traversal on the URL parameter			
	(e)	Test Traversal on the cookie parameter			
38.	Testing Traversal With Encoding				
	(a)	Test Traversal with Base64 encoding			
	(b)	Test Traversal with URL encoding			
	(c)	Test Traversal with ASCII encoding			
	(d)	Test Traversal with HTML encoding			
	(e)	Test Traversal with Hex encoding			
	(f)	Test Traversal with Binary encoding			
	(g)	Test Traversal with Octal encoding			
	(h)	Test Traversal with Gzip encoding			
39.	Testing Traversal With Different OS Schemes				
	(a)	Test Traversal with Unix schemes			
	(b)	Test Traversal with Windows schemes			
	(c)	Test Traversal with Mac schemes			
40.	Test Other Encoding Techniques				
	(a)	Test Traversal with Double encoding			
	(b)	Test Traversal with all characters encode			
	(c)	Test Traversal with only special characters encode			
41.	Test Authorization Schema Bypass				
	(a)	Test for Horizontal authorization schema bypass			
	(b)	Test for Vertical authorization schema bypass			
	(c)	Test override the target with custom headers			
42.	Test For Privilege Escalation				
	(a)	Identify the injection point			
	(b)	Test for bypassing the security measures			
	(c)	Test for forced browsing			
	(d)	Test for IDOR			
	(e)	Test for parameter tampering to high			

R

		privileged user			
43.	Test For Insecure Direct Object Reference				
	(a)	Test to change the ID parameter			
	(b)	Test to add parameters at the endpoints			
	(c)	Test for HTTP parameter pollution			
	(d)	Test by adding an extension at the end			
	(e)	Test with outdated API versions			
	(f)	Test by wrapping the ID with an array			
	(g)	Test by wrapping the ID with a JSON object			
	(h)	Test for JSON parameter pollution			
	(j)	Test by changing the case			
	(k)	Test for path traversal			
	(l)	Test by changing words			
	(m)	Test by changing methods			
SESSION MANAGEMENT TESTING					
44.	Test For Session Management Schema				
	(a)	Ensure all Set-Cookie directives are secure			
	(b)	Ensure no cookie operation takes place over an unencrypted channel			
	(c)	Ensure the cookie can't be forced over an unencrypted channel			
	(d)	Ensure the HTTP Only flag is enabled			
	(e)	Check if any cookies are persistent			
	(f)	Check for session cookies and cookie expiration date/time			
	(g)	Check for session fixation			
	(h)	Check for concurrent login			
	(j)	Check for session after logout			
	(k)	Check for session after closing the browser			
	(l)	Try decoding cookies (Base64, Hex, URL, etc.)			
45.	Test For Cookie Attributes				
	(a)	Ensure the cookie must be set with the secure attribute			
	(b)	Ensure the cookie must be set with the path attribute			
	(c)	Ensure the cookie must have the HTTP Only flag			
46.	Test For Session Fixation				
	(a)	Ensure new cookies have been issued upon a successful authentication			
	(b)	Test manipulating the cookies			
47.	Test For Exposed Session Variables				
	(a)	Test for encryption			
	(b)	Test for GET and POST vulnerabilities			
	(c)	Test if GET request incorporating the session ID used			
	(d)	Test by interchanging POST with GET method			
48.	Test For Back Refresh Attack				
	(a)	Test after password change			
	(b)	Test after logout			
49.	Test For Cross Site Request Forgery				
	(a)	Check if the token is validated on the server-side or not			
	(b)	Check if the token is validated for full or			

R

		partial length			
	(c)	Check by comparing the CSRF tokens for multiple dummy accounts			
	(d)	Check CSRF by interchanging POST with GET method			
	(e)	Check CSRF by removing the CSRF token parameter			
	(f)	Check CSRF by removing the CSRF token and using a blank parameter			
	(g)	Check CSRF by using unused tokens			
	(h)	Check CSRF by replacing the CSRF token with its own values			
	(j)	Check CSRF by changing the content type to form-multipart			
	(k)	Check CSRF by changing or deleting some characters of the CSRF token			
	(l)	Check CSRF by changing the referrer to Referrer			
	(m)	Check CSRF by changing the host values			
	(n)	Check CSRF alongside clickjacking			
50.	Test For Logout Functionality				
	(a)	Check the logout function on different pages			
	(b)	Check for the visibility of the logout button			
	(c)	Ensure after logout the session was ended			
	(d)	Ensure after logout we can't able to access the dashboard by pressing the back button			
	(e)	Ensure proper session timeout has been set			
51.	Test For Session Timeout				
	(a)	Ensure there is a session timeout exists			
	(b)	Ensure after the timeout, all of the tokens are destroyed			
52.	Test For Session Puzzling				
	(a)	Identify all the session variables			
	(b)	Try to break the logical flow of the session generation			
53.	Test For Session Hijacking				
	(a)	Test session hijacking on target that doesn't has HSTS enabled			
	(b)	Test by login with the help of captured cookies			
INPUT VALIDATION TESTING					
54.	Test For Reflected Cross Site Scripting				
	(a)	Ensure these characters are filtered<>"&'"			
	(b)	Test with a character escape sequence			
	(c)	Test by replacing < and > with HTML entities & lt; and & gt;			
	(d)	Test payload with both lower and upper case			
	(e)	Test to break firewall regex by new line /r/n			
	(f)	Test with double encoding			
	(g)	Test with recursive filters			
	(h)	Test injecting anchor tags without whitespace			
	(j)	Test by replacing whitespace with bullets			
	(k)	Test by changing HTTP methods			
55.	Test For Stored Cross Site Scripting				
	(a)	Identify stored input parameters that will			

Q

		reflect on the client side			
	(b)	Look for input parameters on the profile page			
	(c)	Look for input parameters on the shopping cart page			
	(d)	Look for input parameters on the file upload page			
	(e)	Look for input parameters on the settings page			
	(f)	Look for input parameters on the forum,			
	(g)	Test uploading a file with XSS payload as its file name			
	(h)	Test with HTML tags			
56.	Test For HTTP Parameter Pollution				
	(a)	Identify the backend server and parsing method used			
	(b)	Try to access the injection point			
	(c)	Try to bypass the input filters using HTTP Parameter Pollution			
57.	Test For SQL Injection				
	(a)	Test SQL Injection on authentication forms			
	(b)	Test SQL Injection on the search bar			
	(c)	Test SQL Injection on editable characteristics			
	(d)	Try to find SQL keywords or entry point detections			
	(e)	Try to inject SQL queries			
	(f)	Use tools like SQL map or Hackbar			
	(g)	Use Google dorks to find the SQL keywords			
	(h)	Try GET based SQL Injection			
	(i)	Try POST based SQL Injection			
	(k)	Try COOKIE based SQL Injection			
	(l)	Try HEADER based SQL Injection			
	(m)	Try SQL Injection with null bytes before the SQL query			
	(n)	Try SQL Injection with URL encoding			
	(p)	Try SQL Injection with both lower and upper cases			
	(q)	Try SQL Injection with SQL Tamper scripts			
	(r)	Try SQL Injection with SQL Time delay payloads			
	(s)	Try SQL Injection with SQL Conditional delays			
	(t)	Try SQL Injection with Boolean based SQL			
	(u)	Try SQL Injection with Time based SQL			
58.	Test For LDAP Injection				
	(a)	Use LDAP search filters			
	(b)	Try LDAP Injection for access control bypass			
59.	Testing For XML Injection				
	(a)	Check if the application is using XML for processing			
	(b)	identify the XML Injection point by XML metacharacter			
	(c)	Construct XSS payload on top of XML			
60.	Test For Server Side Includes				
	(a)	Use Google dorks to find the SSI			
	(b)	Construct RCE on top of SSI			

R

	(c)	Construct other injections on top of SSI			
	(d)	Test Injecting SSI on login pages, header fields, referrer, etc.			
61.	Test For XPATH Injection				
	(a)	Identify XPATH Injection point			
	(b)	Test for XPATH Injection			
62.	Test For IMAP SMTP Injection				
	(a)	Identify IMAP SMTP Injection point			
	(b)	Understand the data flow			
	(c)	Understand the deployment structure of the system			
	(d)	Assess the injection impact			
63.	Test For Local File Inclusion				
	(a)	Look for LFI keywords			
	(b)	Try to change the local path			
	(c)	Use LFI payload list			
	(d)	Test LFI by adding a null byte at the end			
64.	Test For Remote File Inclusion				
	(a)	Look for RFI keywords			
	(b)	Try to change the remote path			
	(c)	Use RFI payload list			
65.	Test For Command Injection				
	(a)	Identify the Injection points			
	(b)	Look for Command Injection keywords			
	(c)	Test Command injection using different delimiters			
	(d)	Test Command Injection with payload list			
	(e)	Test Command Injection with different OS commands			
66.	Test For Format String Injection				
	(a)	Identify the Injection points			
	(b)	Use different format parameters as payloads			
	(c)	Assess the injection impact			
67.	Test For Host Header Injection				
	(a)	Test for HHI by changing the real Host parameter			
	(b)	Test for HHI by adding X-Forwarded Host parameter			
	(c)	Test for HHI by swapping the real Host and X-Forwarded Host parameter			
	(d)	Test for HHI by adding two Host parameters			
	(e)	Test for HHI by adding the target values in front of the original values			
	(f)	Test for HHI by adding the target with a slash after the original values			
	(g)	Test for HHI with other injections on the Host parameter			
	(h)	Test for HHI by password reset poisoning			
68.	Test For Server Side Request Forgery				
	(a)	Look for SSRF keywords			
	(b)	Search for SSRF keywords only under the request header and body			
	(c)	Identify the Injection points			
	(d)	Test if the Injection points are exploitable			
	(e)	Assess the injection impact			
69.	Test For Server Side Template Injection				

Q

	(a)	Identify the Template injection vulnerability points			
	(b)	Identify the Templating engine			
	(c)	Use the tplmap to exploit			
ERROR HANDLING TESTING					
70.	Test For Improper Error Handling				
	(a)	Identify the error output			
	(b)	Analyze the different outputs returned			
	(c)	Look for common error handling flaws			
	(d)	Test error handling by modifying the URL parameter			
	(e)	Test error handling by uploading unrecognized file formats			
	(f)	Test error handling by entering unrecognized inputs			
	(g)	Test error handling by making all possible errors			
WEAK CRYPTOGRAPHY TESTING					
71.	Test For Weak Transport Layer Security				
	(a)	Test for DROWN weakness on SSLv2 protocol			
	(b)	Test for POODLE weakness on SSLv3 protocol			
	(c)	Test for BEAST weakness on TLSv1.0 protocol			
	(d)	Test for FREAK weakness on export cipher suites			
	(e)	Test for Null ciphers			
	(f)	Test for NOMORE weakness on RC4			
	(g)	Test for LUCKY 13 weakness on CBC mode ciphers			
	(h)	Test for CRIME weakness on TLS compression			
	(i)	Test for LOGJAM on DHE keys			
	(k)	Ensure the digital certificates should have at least 2048 bits of key length			
	(l)	Ensure the digital certificates should have at least SHA - 256 signature algorithm			
	(m)	Ensure the digital certificates should not use MD5 and SHA -1			
	(n)	Ensure the validity of the digital certificate			
	(p)	Ensure the minimum key length requirements			
	(q)	Look for weak cipher suites			
BUSINESS LOGIC TESTING					
72.	Test for Business Logic				
	(a)	Identify the logic of how the application works			
	(b)	Identify the functionality of all the buttons			
	(c)	Test by changing the numerical values into high or negative values			
	(d)	Test by changing the quantity			
	(e)	Test by modifying the payments			
	(f)	Test for parameter tampering			
73.	Test For Malicious File Upload				
	(a)	Test malicious file upload by uploading malicious files			

Q

	(b)	Test malicious file upload by putting your IP address on the file name			
	(c)	Test malicious file upload by right to left override			
	(d)	Test malicious file upload by encoded file name			
	(e)	Test malicious file upload by XSS payload on the file name			
	(f)	Test malicious file upload by RCE payload on the file name			
	(g)	Test malicious file upload by LFI payload			
	(h)	Test malicious file upload by RFI payload on the file name			
	(j)	Test malicious file upload by SQL payload on the file name			
	(k)	Test malicious file upload by other injections on the file name			
	(l)	Test malicious file upload by Inserting the payload inside of an image by the bmp.pl tool			
	(m)	Test malicious file upload by uploading large files (leads to DOS)			
CLIENT SIDE TESTING					
74.	Test For DOM Based Cross Site Scripting				
	(a)	Try to identify DOM sinks			
	(b)	Build payloads to that DOM sink type			
75.	Test For URL Redirect				
	(a)	Look for URL redirect parameters			
	(b)	Test for URL redirection on domain parameters			
	(c)	Test for URL redirection by using a payload list			
	(d)	Test for URL redirection by using a whitelisted word at the end			
	(e)	Test for URL redirection by creating a new subdomain with the same as the target			
	(f)	Test for URL redirection by XSS			
	(g)	Test for URL redirection by profile URL flaw			
76.	Test For Cross Origin Resource Sharing				
	(a)	Look for "Access-Control-Allow-Origin" on the response			
	(b)	Use the CORS HTML exploit code for further exploitation			
77.	Test For Clickjacking				
	(a)	Ensure "X-Frame-Options" headers are enabled			
	(b)	Exploit with iframe HTML code for POC			
OTHER COMMON ISSUES					
78.	Test For No-Rate Limiting				
	(a)	Ensure rate limiting is enabled			
	(b)	Try to bypass rate limiting by changing the case of the endpoints			
	(c)	Try to bypass rate limiting by adding / at the end of the URL			
	(d)	Try to bypass rate limiting by adding HTTP headers			
	(e)	Try to bypass rate limiting by adding HTTP headers twice			

2

	(f)	Try to bypass rate limiting by adding Origin headers			
	(g)	Try to bypass rate limiting by IP rotation			
	(h)	Try to bypass rate limiting by using null bytes at the end			
	(j)	Try to bypass rate limiting by using race conditions			
79.	Test For EXIF Geo data				
	(a)	Ensure the website is stripping the geodata			
	(b)	Test with EXIF checker			
80.	Test For Broken Link Hijack				
	(a)	Ensure there is no broken links are there			
	(b)	Test broken links by using the blc tool			
81.	Test For SPF				
	(a)	Ensure the website is having SPF record			
	(b)	Test SPF by ns lookup command			
82.	Test For Weak 2FA				
	(a)	Try to bypass 2FA by using poor session management			
	(b)	Try to bypass 2FA via the OAuth mechanism			
	(c)	Try to bypass 2FA via brute-forcing			
	(d)	Try to bypass 2FA via response manipulation			
	(e)	Try to bypass 2FA by using activation links to login			
	(f)	Try to bypass 2FA by using status code manipulation			
	(g)	Try to bypass 2FA by changing the email or password			
	(h)	Try to bypass 2FA by using a null or empty entry			
	(j)	Try to bypass 2FA by changing the boolean into false			
	(k)	Try to bypass 2FA by removing the 2FA parameter on the request			
83.	Test For Weak OTP Implementation				
	(a)	Try to bypass OTP by entering the old OTP			
	(b)	Try to bypass OTP by brute-forcing			
	(c)	Try to bypass OTP by using a null or empty entry			
	(d)	Try to bypass OTP by response manipulation			
	(e)	Try to bypass OTP by status code manipulation			

✓

DESKTOP APPLICATION CHECKLIST

<u>S. No.</u>	<u>Controls</u>	<u>Test Conducted</u>	<u>Vulnerability Detected</u>	<u>Remarks</u>
<u>INFORMATION GATHERING</u>				
1.	Information Gathering			
	(a) Find Out the application architecture (two-tier or three-tier)			
	(b) Find out the technologies used (languages and frameworks)			
	(c) Identify network communication			
	(d) Observe the application process			
	(e) Observe each functionality and behavior of the application			
	(f) Identify all the entry points			
	(g) Analyze the security mechanism (authorization and authentication)			
	(h) Tools Used : CFF Explorer, Sysinternals Suite, Wireshark, PEid, Detect It Easy (DIE), Strings			
<u>GUI TESTING</u>				
2.	Test For GUI Object Permission			
	(a) Display hidden form object			
	(b) Try to activate disabled functionalities			
	(c) Try to uncover the masked password			
3.	Test GUI Content			
	(a) Look for sensitive information			
4.	Test For GUI Logic			
	(a) Try for access control and injection-based vulnerabilities			
	(b) Try for access control and injection-based vulnerabilities			
	(c) Check improper error handling			
	(d) Check weak input sanitization			
	(e) Try privilege escalation (unlocking admin features to normal users)			
	(f) Try payment manipulation			
	(g) Tools Used : UISpy, Winspy++, Window Detective, Snoop WPF			
<u>File Testing</u>				
5.	Test For Files Permission			
	(a) Check permission for each and every file and folder			
6.	Test For File Continuity			
	(a) Check strong naming			
	(b) Authenticate code signing			
7.	Test For File Content Debugging			
	(a) Look for sensitive information on the file system (symbols, sensitive data, passwords, configurations)			

✓

	(b)	Look for sensitive information on the config file			
	(c)	Look for Hardcoded encryption data			
	(d)	Look for Clear text storage of sensitive data			
	(e)	Look for side-channel data leakage			
	(f)	Look for unreliable log			
8.	Test For File And Content Manipulation				
	(a)	Try framework back dooring			
	(b)	Try DLL preloading			
	(c)	Perform Race condition check			
	(d)	Test for Files and content replacement			
	(e)	Test for Client-side protection bypass using reverse engineering			
9.	Test For Function Exported				
	(a)	Try to find the exported functions			
	(b)	Try to use the exported functions without authentication			
10.	Test For Public Methods				
	(a)	Make a wrapper to gain access to public methods without authentication			
11.	Test For Decompile And Application Rebuild				
	(a)	Try to recover the original source code, passwords, keys			
	(b)	Try to decompile the application			
	(c)	Try to rebuild the application			
	(d)	Try to patch the application			
12.	Test For Decryption And DE obfuscation				
	(a)	Try to recover original source code			
	(b)	Try to retrieve passwords and keys			
	(c)	Test for lack of obfuscation			
13.	Test For Disassemble and Reassemble				
	(a)	Try to build a patched assembly			
	(b)	Tools Used : Strings, dnSpy, Procmon, Process Explorer, Process Hacker			
	(c)	Try to build a patched assembly			
REGISTRY TESTING					
14.	Test For Registry Permissions				
	(a)	Check read access to the registry keys			
	(b)	Check to write access to the registry keys			
15.	Test For Registry Contents				
	(a)	Inspect the registry contents			
	(b)	Check for sensitive info stored on the registry			
	(c)	Compare the registry before and after executing the application			
16.	Test For Registry Manipulation				
	(a)	Try for registry manipulation			
	(b)	Try to bypass authentication by registry manipulation			
	(c)	Try to bypass authorization by registry manipulation			
	(d)	Tools Used : Reshot, Procmon, Accessenum			
NETWORK TESTING					
17.	Test For Network				

✓

	(a)	Check for sensitive data in transit			
	(b)	Try to bypass firewall rules			
	(c)	Try to manipulate network traffic			
	(d)	Tools Used : Wire shark, TCP view			
ASSEMBLY TESTING					
18.	Test For Assembly				
	(a)	Verify Address Space Layout Randomization (ASLR)			
	(b)	Verify Safe SEH			
	(c)	Verify Data Execution Prevention (DEP)			
	(d)	Verify strong naming			
	(e)	Verify Control Flow Guard			
	(f)	Verify Highentropy VA			
	(g)	Tools Used : PE Security			
MEMORY TESTING					
19.	Test For Memory Content				
	(a)	Check for sensitive data stored in memory			
20.	Test For Memory Manipulation				
	(a)	Test For Memory Manipulation			
	(b)	Try to bypass authentication by memory manipulation			
	(c)	Try to bypass authorization by memory manipulation			
21.	Test For Run Time Manipulation				
	(a)	Try to analyse the dump file			
	(b)	Check for process replacement			
	(c)	Check for modifying assembly in the memory			
	(d)	Try to debug the application			
	(e)	Try to identify dangerous functions			
	(f)	Use breakpoints to test each and every functionality			
	(g)	Tools Used : Process Hacker, HxD, Strings			
TRAFFIC TESTING					
22.	Test For Traffic				
	(a)	Analyse the flow of network traffic			
	(b)	Try to find sensitive data in transit			
	(c)	Tools Used : Echo Mirage, MITM Relay, Burp Suite			
COMMON VULNERABILITIES TESTING					
23.	Test For Common Vulnerabilities				
	(a)	Try to decompile the application			
	(b)	Try for reverse engineering			
	(c)	Try to test with OWASP WEB Top 10			
	(d)	Try to test with OWASP API Top 10			
	(e)	Test for DLL Hijacking			
	(f)	Test for signature checks (Use Sig check)			
	(g)	Test for binary analysis (Use Bin scope)			
	(h)	Test for business logic errors			
	(i)	Test for TCP/UDP attacks			
	(j)	Test with automated scanning tools (Use Visual Code Grepper - VCG)			

API SECURITY CHECKLIST

<u>S No.</u>	<u>Controls</u>	<u>Test Conducted</u>	<u>Vulnerability Detected</u>	<u>Remarks</u>
<u>Authentication</u>				
1.	Don't use Basic Auth. Use standard authentication instead (e.g., JWT).			
2.	Don't reinvent the wheel in Authentication token generation, password storage. Use the standards.			
3.	Use Max Retry and jail features in Login.			
4.	Use encryption on all sensitive data.			
<u>JWT (JSON Web Token)</u>				
5.	Use a random complicated key (JWT Secret) to make brute forcing the token very hard.			
6.	Don't extract the algorithm from the header. Force the algorithm in the backend (HS256 or RS256).			
7.	Make token expiration (TTL, RTTL) as short as possible.			
8.	Don't store sensitive data in the JWT payload, it can be decoded easily.			
9.	Avoid storing too much data. JWT is usually shared in headers and they have a size limit.			
<u>Access</u>				
10.	Limit requests (Throttling) to avoid DDoS / brute- force attacks.			
11.	Use HTTPS on server side with TLS 1.2+ and secure ciphers to avoid MITM (Man in the Middle Attack).			
12.	Use HSTS header with SSL to avoid SSL Strip attacks.			
13.	Turn off directory listings.			
14.	For private APIs, allow access only from safe listed IPs/hosts			
<u>Authorization</u>				
<u>O Auth</u>				
15.	Always validate redirect URL server side to allow only safe listed URLs.			
16.	Always try to exchange for code and not tokens (don't allow response type token).			
17.	Use state parameter with a random hash to prevent CSRF on the OAuth authorization process.			
18.	Define the default scope, and validate scope parameters for each application.			
<u>Input</u>				
19.	Use the proper HTTP method according to the operation: GET (read), POST (create), PUT/PATCH (replace/update), and DELETE (to delete a record), and respond with 405 Method Not Allowed if the requested method isn't appropriate for the requested resource.			

2

20.	Validate content-type on request Accept header (Content Negotiation) to allow only your supported format (e.g., application/xml, application/json, etc.) and respond with 406 Not Acceptable response if not matched.			
21.	Validate content-type of posted data as you accept (e.g., application/x-www-form-urlencoded, multipart/form-data, application/json, etc.)			
22.	Validate user input to avoid common vulnerabilities (e.g., XSS, SQL Injection, Remote Code Execution, etc.)			
23.	Don't use any sensitive data (credentials, Passwords, security tokens, or API keys) in the URL, but use standard Authorization header.			
24.	Use only server-side encryption.			
25.	Use an API Gateway service to enable caching, Rate Limit policies (e.g., Quota, Spike Arrest, or Concurrent Rate Limit) and deploy APIs resources dynamically.			
Processing				
26.	Check if all the endpoints are protected behind authentication to avoid broken authentication process.			
27.	User own resource ID should be avoided. Use /me/orders instead of /user/654321/orders.			
28.	Don't auto-increment IDs. Use UUID instead.			
29.	if you are parsing XML data, make sure entity parsing is not enabled to avoid XXE (XML external entity attack).			
30.	If you are parsing XML, YAML or any other language with anchors and refs, make sure entity expansion is not enabled to avoid Billion Laughs/XML bomb via exponential entity expansion attack.			
31.	Use a CDN for file uploads			
32.	If you are dealing with huge amount of data, use Workers and Queues to process as much as possible in background and return response fast to avoid HTTP Blocking.			
33.	Do not forget to turn the DEBUG mode OFF.			
34.	Use non-executable stacks when available.			
Output				
35.	Send X-Content-Type-Options: nosniff header.			
36.	Send X-Frame-Options: deny header.			
37.	Send Content-Security-Policy: default-src 'none' header.			
38.	Remove fingerprinting headers - X-Powered-By, Server, X-Asp Net Version, etc.			
39.	Force content-type for your response. If you return application/json, then your content-type response is application/json.			
40.	Don't return sensitive data like credentials, passwords, or security tokens.			

Q

41.	Return the proper status code according to the operation completed, (e.g., 200 OK, 400 Bad Request, 401 Unauthorized , 405 Method Not Allowed, etc.)			
CI & CD				
42.	Audit your design and implementation with unit/integration tests coverage.			
43.	Use a code review process and disregard self- approval.			
44.	Ensure that all components of your services are statically scanned by AV software before pushing to production, including vendor libraries and other dependencies.			
45.	Continuously run security tests (static/dynamic analysis) on your code.			
46.	Check your dependencies (both software and OS) for known vulnerabilities.			
47.	Design a rollback solution for deployments.			
Monitoring				
48.	Use centralized logins for all services and components			
49.	Use agents to monitor all traffic, errors, requests, and responses			
50.	Use alerts for SMS, Slack, Email, Telegram, Kibana, Cloud watch, etc.			
51.	Ensure that you aren't logging any sensitive data like credit cards, passwords, PINs, etc.			
52.	Use an IDS and/or IPS system to monitor your API requests and instances.			
See also:				
53.	yosriady/api – development – tools - A collection of useful resources for building RESTful HTTP+JSON APIs			
Contribution				
54.	Feel free to contribute by forking this repository, making some changes, and submitting pull requests. For any questions drop us an email at team@shieldfy.io.			

MOBILE APPLICATION PENTESTING CHECKLIST

<u>S No.</u>	<u>Controls</u>	<u>Test Conducted</u>	<u>Vulnerability Detected</u>	<u>Remarks</u>
STATIC ANALYSIS				
1.	Reverse Engineering the Application Code (Code Obfuscating Checking)			
2.	Information leakage/Hardcoded credential in the binaries			
3.	Unauthorized Code Modification			
4.	Misuse of App permissions			
5.	Insecure version of OS Installation Allowed			
6.	Abusing Android Components through IPC intents ("exported" and "intent-filter")			
7.	Unrestricted Backup file			
8.	Cryptographic Based Storage Strength			
9.	Poor key management process			
10.	Use of custom encryption protocols			
11.	Debuggable Application			
DYNAMIC AND RUNTIME ANALYSIS				
12.	Misuse of Keychain , Touch ID and other			
13.	Minimum Device Security Requirements absent			
14.	Unencrypted Database files			
15.	Insecure Shared Storage			
16.	Insecure Application Data Storage			
17.	Information Disclosure through Logcat/Apple System Log (ASL)			
18.	Application Backgrounding (Screenshot)			
19.	Copy/Paste Buffer Caching			
20.	Keyboard Press Caching			
21.	Unrestricted Backup file			
22.	Remember Credentials Functionality (Persistent authentication)			
23.	Client Side Based Authentication Flaws			
24.	Client Side Authorization Breaches			
25.	Content Providers: SQL Injection and Local File inclusion			
26.	Broadcast Receiver			
27.	Service component			
28.	Insufficient Web View hardening			
29.	Injection (SQLite Injection, XML Injection)			
30.	Local File Inclusion through Web views			
31.	Abusing URL schemes or Deep links			
32.	Sensitive Information Masking			
33.	Runtime Manipulation			
34.	Rooted or Jail-broken device checking			
35.	Passwords/ Connection String disclosure			
36.	Hidden and Unscrutinised functionalities			
COMMUNICATION CHANNEL				
37.	Insecure Transport Layer Protocols			

38.	Use of Insecure and Deprecated algorithms			
39.	Use of Disabling certificate validation			
40.	SSL pinning Implementation			
41.	End-to-end encryption			
SERVER SIDE - WEBSERVICES AND API				
42.	Excessive port opened at Firewall			
43.	Default credentials on Application Server			
44.	Weak password policy Implementation			
45.	Exposure of Web services through WSDL document			
46.	Security Misconfiguration on Server API			
47.	Security Patching on Server API			
48.	input validation on API			
49.	Information Exposure through API response message			
50.	Control of interaction frequency on API (Replay Attack)			
51.	Session invalidation on Backend			
52.	Session Timeout Protection			
53.	Cookie Rotation			
54.	Multiple concurrent logins			
55.	Exposing Device Specific Identifiers in Attacker Visible Elements			
56.	Token/Session Creation and handling			
57.	Insecure Direct Object references			
58.	Missing function level access control			
59.	Bypassing business logic flaws			

