MUSEU DO FUTEBOL

idbrasil Organização Social de Cultura	TERMO DE REFERÊNCIA	MUSEU DO FUTEBOL
Núcleo: TECNOLOGIA		**DATA DE EMISSÃO** 30/10/2025
Assunto: Prorrogação do Prazo para a Contratação de Empresa Especializada em PENTEST (Teste de penetração cibernética), para Detecção e Correção de Vulnerabilidades de Segurança da Infraestrutura de Tecnologia da Informação do Museu do Futebol Interna e Externa.		

1. OBJETO:

Contratação de empresa especializada em PENTEST (Teste de penetração cibernética), para detecção e correção de vulnerabilidades de segurança da infraestrutura de Tecnologia da Informação do Museu do Futebol Interna e externa.

JUSTIFICATIVA
Analisar e mitigar impactos no que se refere a segurança da informação, com o objetivo de garantir a disponibilidade e integridade do ambiente computacional da Organização Social.

CONTRATANTE:

IDBRASIL CULTURA EDUCAÇÃO E ESPORTE (MUSEU DO FUTEBOL).

CNPJ: 10.233.223/0001-52.

PRAÇA CHARLES MILLER S/Nº - PACAEMBU

CEP: 01234-010 – SÃO PAULO/SP.

2. DAS ESPECIFICAÇÕES TÉCNICAS:

AMBIENTE COMPUTACIONAL A SER ANALISADO

- 4 IPs externos;
- 2 Aplicações WEB;

- 4 Subdomínios;
- 1 VPN;
- 4 Servidores.

OBTENÇÃO DE INFORMAÇÕES E MAPEAMENTO

– Clonagem (mirroring) de sites;
– Reconhecimento através de Sites de Busca;
– Identificação de pontos de entrada;
– Identificação de versões (fingerprinting);
– Descoberta de Aplicações;
– Análise de Mensagens de Erro.

TESTE DE CONFIGURAÇÃO

– Verificação de Suporte a SSL / TLS;
– Teste de Acesso direto ao Banco de Dados (DB Listener);
– Análise das Configurações da Infraestrutura;
– Análise das Configurações da Aplicação;
– Teste de Manuseio de extensões de arquivos;
– Análise de Arquivos não referenciados, obsoletos e backups;
– Identificação de Interfaces administrativas;
– Verificação de Métodos suportados pelo servidor.

TESTES DE AUTENTICAÇÃO

– Teste sobre canais de transporte de credenciais;
– Teste de enumeração de usuários;
– Teste de descoberta de usuários comuns / padrão;
– Teste de força bruta;
– Teste visando contornar do esquema de autenticação;
– Teste sobre funções de armazenamento/redefinição de senhas;
– Teste de gerenciamento de logout e cache do navegador;
– Teste sobre o CAPTCHA;
– Teste sobre autenticação em múltiplas etapas;
– Teste sobre condições de corrida.

GERENCIAMENTO DE SESSÕES

– Análise de Esquema de Gerenciamento de Sessão;
– Análise de Atributos utilizados em Cookies;
– Teste de fixação de sessão;
– Identificação de variáveis de sessão Expostas;
– Teste de CSRF.

TESTES DE AUTORIZAÇÃO
– Teste de adulteração de caminhos de diretórios;
– Teste de contorno do esquema de autorização;
– Teste de escalada de privilégios.

TESTE DE LÓGICA DO NEGÓCIO

TESTE DE VALIDAÇÃO DE DADOS
– Cross Site Scripting Refletido / Armazenado / baseado em DOM;
– Injeção de instruções SQL / LDAP / ORM / XML / SSI / XPath;
– Injeção de código e comandos de sistema operacional e serviços;
– Estouro de buffer (buffer overflow);
– Manipulação de Validação Interna;
– HTTP Splitting/Smuggling.

TESTE DE NEGAÇÃO DE SERVIÇO
– Verificação de consultas com SQL Wildcard;
– Teste de trancamento de contas de usuários;
– Teste de estouro de buffer ou alocação de memória;
– Teste de injeção de condições de laço (loop);
– Teste de escrita de dados no disco;
– Teste de armazenamento de dados de sessão e liberação de recursos.

TESTE DE WEB SERVICES
– Teste de coleta de informações do webservice;
– Teste do WSDL;
– Teste estrutural de XML;
– Teste ao nível de conteúdo do XML;
– Teste de parâmetros HTTP/REST;
– Teste de envio de arquivos maliciosos ao web services SOAP;
– Teste de ataque de replay.

TESTE SOBRE AJAX
– Teste sobre vulnerabilidades do AJAX;
– Teste sobre AJAX.

FERRAMENTAS

AUDITORIA

– Determinar versão do serviço sendo auditado, detecção de filtros de pacotes bem como se firewalls estão manipulando o tráfego da rede;
– Análise e manipulação de tráfego da rede, utilizar proxy interceptando as requisições e mapeando parâmetros, links e aplicações;
– Verificar se no tráfego da rede do cliente é possível identificar e obter informações sensíveis/privadas que não deveriam ser trafegar desprotegidas pela rede;
– Ferramentas para a verificação manual das vulnerabilidades encontradas, permitindo testar a aplicação web de maneira abrangente. Verifica conformidade com boas práticas de segurança em aplicações web.
– Verificar se um website hospedado no servidor HTTP do ativo alvo é vulnerável a ataques do tipo injeção de SQL, cross site scripting (XSS), inclusão de arquivos locais e remotos;
– Varreduras em busca de vulnerabilidades em servidores web. Verificar se serviços ou aplicações web do ativo alvo estão desatualizados. identificar problemas em versões de software específicas e itens de configuração do servidor, tais como a possibilidade de acessar arquivos sensíveis, erros de permissões, etc;
– Realizar os ataques sobre vulnerabilidades específicas. Relacionar as vulnerabilidades descobertas com sua base de exploits a fim de efetuar as tentativas de invasão propriamente ditas. efetuar ataques de força bruta sobre os serviços identificados;
– Avaliar a possibilidade de injeções em aplicações através da submissão de dados em campos de entrada. Ele também utiliza padrão de resposta da aplicação para mapear versões de banco SQL;
– Realizar manipulação de requisições, interceptar requisições visando manipular campos e parâmetros burlando controles client-side e forjando requisições inválidas;
– Executar ataques de negação de serviço, gerar uma grande quantidade de pacotes visando avaliar o comportamento do sistema e serviço alvo mediante a ataques de stress ou negação de serviço;
– Efetuar ataques de dicionário remotamente sobre serviços providos por um dos ativos alvo tais como: CVS, FTP, HTTP (via formulários), IMAP, IRC, LDAP, MS-SQL, MYSQL, POP3, POSTGRES, RDP, SIP, SMB, SMTP, SSH, Subversion, Telnet, VNC, etc.

RETESTE

– Prazo de 3 meses para correção das falhas identificadas e reteste após entrega do relatório técnico com o objetivo de validar as correções aplicadas e assegurar que os ativos auditados não apresentam mais as vulnerabilidades reportadas.

ENTREGAS

– Relatório Técnico
– Descrição dos testes executados;
– Vulnerabilidades identificadas e nível de criticidade;
– Recomendações de mitigação;
– Evidências técnicas e provas de conceito (PoCs);
– Relatório executivo com linguagem acessível para áreas não técnicas;
– Atualização de toda a documentação do projeto ao longo de sua execução, conforme padrão do Cliente;
– Relatórios parciais para acompanhamento do andamento do projeto;
– Relatório final, vídeos e provas de conceito necessárias para o pleno entendimento das falhas exploradas.

MONITORAMENTO

– Plataforma online para monitoramento do pentest durante todo o processo e tempo de vigência do contrato, fase de testes, correções e re-teste.

3. ENVIO E FORMA DE ANÁLISE DAS PROPOSTAS:

3.1. As propostas deverão ser enviadas para os e-mails compras@idbr.org.br e felipe.macchiaverni@idbr.org.br até o dia 10/11/2025 e, o resultado da empresa vencedora se dará exclusivamente através do site do IDBrasil na aba ‘compras encerradas’.

3.2. As propostas recebidas serão analisadas conforme o critério de técnica e preço. A empresa deverá enviar currículo e/ou portfólio, juntamente com a proposta comercial.

3.3. A proposta comercial deverá contemplar todos os custos que envolverão deslocamento e alimentação da contratada.

3.4. A proposta comercial deverá ser elaborada em papel timbrado, contendo o CNPJ do proponente e assinatura.

4. A empresa vencedora deste processo deverá apresentar antes da assinatura do contrato a seguinte documentação:

- Comprovante de Inscrição Estadual;
- Comprovante de Inscrição Municipal;

- Estatuto ou contrato social consolidado, ou envio das últimas alterações;
- Cópia Cartão de CNPJ.
- Cópia do RG e CPF dos sócios e procuradores;

5.1. DAS OBRIGAÇÕES DA CONTRATADA:

5.1. A **CONTRATADA** será responsável por todas as despesas referente a seus empregados e/ou contratados, tais como, mas não limitadas a: salários, adicionais devidos, férias, décimo terceiro, seguro de acidentes de trabalho, contribuições ou encargos devidos à previdênciasocial, ao FGTS, ao PIS, bem como quaisquer outros encargos de natureza trabalhista,previdenciária ou tributária, não tendo a **CONTRATANTE** qualquer responsabilidade neste sentido;

5.2. A **CONTRATADA** será responsável pelo custeio de todos os tributos, taxas, contribuições fiscais, parafiscais, previdenciárias, trabalhistas, e de indenizações relativas a acidentes de trabalho que incidam ou venham a incidir sobre a prestação de serviços a ser realizada.

6. DAS OBRIGAÇÕES DA CONTRATANTE:

6.1. Efetuar os pagamentos nas condições e preços pactuados no contrato a ser assinado;

6.2. Rejeitar, no todo ou em parte, os serviços executados em desacordo com as exigências deste Termo de Referência e do contrato.

7. DA EXECUÇÃO DOS TRABALHOS:

7.1. O desenvolvimento dos trabalhos será acompanhado por funcionários do Museu do Futebol em todas as etapas.

7.2. A **CONTRATANTE** indicará o gestor do contrato para acompanhar, fiscalizar e atestar a realização dos serviços, e terá a competência de dirimir as dúvidas que surgirem no curso de sua execução.

8. DO PAGAMENTO:

O proponente, ao apresentar a sua proposta comercial, estará ciente dos prazos de pagamentos estabelecidos pelo Núcleo Administrativo Financeiro, ciente de que não haverá pagamentos antecipados ou fora do prazo pactuado.

Os pagamentos das Notas Fiscais serão efetuados apenas nos dias 10 e 25, após execução dos trabalhos, conforme segue:

1. *Notas Fiscais emitidas e enviadas para o e-mail financeiro@museudofutebol.org.br entre os dias 01 e 15, o pagamento será efetuado no dia 25 do mesmo mês.*

2. *Notas Fiscais emitidas e enviadas para o e-mail financeiro@museudofutebol.org.br entre os dias 16 e 26, o pagamento será efetuado no dia 10 do mês seguinte.*

3. *A NF da respectiva cobrança deverá ser emitida de acordo com o CNAE do serviço realizado.*

4. *As notas fiscais devem ser emitidas e enviadas para o e-mail financeiro@museudofutebol.org.br dentro do mês de competência da prestação deserviços, sob pena de não serem aceitas fora do prazo aqui estabelecido.*

5. *O IDBRASIL recebe notas fiscais emitidas entre os dias 01 e 26 do mês da prestação dos serviços.*

6. *Notas fiscais emitidas entre os dias 27 e 30/31 não serão aceitas e, deverão ser canceladas pelo contratado.*

7. *Os pagamentos se darão exclusivamente por boleto bancário, com o CNPJ em nome da empresa CONTRATADA, o IDBrasil não realiza pagamento de factoring ou com CNPJ diferente da Razão Social da empresa CONTRATADA.*

9. DAS CONDIÇÕES GERAIS:

9.1. A contratação deste serviço não estabelece qualquer forma de associação ou relação entre a **CONTRATANTE** e a **CONTRATADA**, especialmente as de natureza previdenciária, trabalhista e societária.

9.2. O contrato determina que todas as relações entre a **CONTRATANTE** e a **CONTRATADA** são de natureza meramente civil.

9.3. Poderá participar deste processo de seleção toda e qualquer sociedade empresária do ramo, conforme CNAE (Classificação Nacional de Atividades Econômicas) que atenda às exigências mínimas contidas no presente Termo de Referência.

Eventuais dúvidas deverão ser esclarecidas por escrito através do endereço de email: compras@idbr.org.br e felipe.macchiaverni@idbr.org.br.

O proponente, ao apresentar a sua proposta comercial, declara estar ciente e manifesta sua concordância com o fato de que a CONTRATANTE, na qualidade de Organização Social qualificada perante a Secretaria da Cultura, Economia e Indústria Criativas do Estado de São Paulo, para fins de atendimento do Decreto Estadual nº 64.056/2018 e demais determinações dos órgãos públicos, disponibilizará em seu sítio eletrônico a relação dos prestadores de serviços por ela contratados, com indicação do tipo de serviço, vigência e valor do ajuste, a ser disponibilizada com a prestação de contas de cada exercício, salvo nos casos em que houver cláusula de confidencialidade previamente aprovada, ressalvando a publicação, quando as informações serão cujas informações serão apresentadas somente ao órgão contratante e aos órgãos de controle.

O IDBRASIL SE RESERVA O DIREITO DE PRORROGAR, SELECIONAR OS PARTICIPANTES, CONTRATAR PARCIALMENTE OS ITENS DESTE TR, DE ACORDO COM A DISPONIBILIDADE FINANCEIRA, CANCELAROU SUSPENDER ESTE PROCESSO SELETIVO.