1. Apresentamos abaixo as argumentações para as alegações apresentadas pela I9 SOLUTIONS – SOLUÇÕES COMERCIAIS E GESTÃO DE TRANSPORTES LTDA-ME, em seu recurso interposto.

1.1. No item “Do Direito” do recurso interposto:

1.1.1 A empresa recorrente alega no início da sua peça recursal que “não foram demostrados quais os tipos de falhas que determinaram as inconsistências, sem nenhuma prova existente neste sentido”.
Neste sentido, seguem os trechos do relatório que identificaram a não aprovação nos itens:

6.4.2 Segurança Injection e Cross-site

Arquivo: 2 ciclo - 12-08\Segurança\Relatorio de Segurança - Web.pdf

Página 2:

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
11285	Insecure Transport: Weak SSL Cipher	Critical	Yes	Fail	1
5665	Insecure Deployment: Unpatched Application	Critical	Yes	Pass	-
5663	phpBB2 Local File Include Vulnerability	Critical	Yes	Pass	-

Página 9:

2217	Cross-Site Scripting: Reflected	Critical	Yes	Pass	-
775	Insecure Deployment: Unpatched Application	Critical	Yes	Pass	-
742	Poor Error Handling: Unhandled Exception	Critical	Yes	Pass	-
11395	Insecure Transport: Weak SSL Protocol	High	Yes	Fail	1
11201	Session Fixation	High	Yes	Fail	1
5579	Insecure Deployment: Unpatched Application	High	Yes	Pass	-
5519	PHP Info Memory Content Disclosure	High	Yes	Pass	-
5504	Insecure Deployment: Unpatched Application	High	Yes	Pass	-
5385	Blog Torrent Password File Disclosure	High	Yes	Pass	-

Página 17:

3051	Poor Error Handling: Unhandled Exception	High	Yes	Pass	-
2229	Web Server Misconfiguration: Unprotected File	High	Yes	Pass	-
10963	Cross-Site Request Forgery	Medium	Yes	**Fail**	4
5606	Insecure Deployment: Unpatched Application	Medium	Yes	Pass	-
5600	Insecure Deployment: Unpatched Application	Medium	Yes	Pass	-

Página 89:

Scan Type: Site **Client:** FF

Server: https://portal.huby.com.br:443

Critical

Insecure Transport: Weak SSL Cipher

Page: https://portal.huby.com.br:443/Login.aspx?ReturnUrl=%2f

Medium

Cross-Site Request Forgery

Page: https://portal.huby.com.br:443/Login.aspx

Page: https://portal.huby.com.br:443/CancelarAtendimento.aspx?id=fLOFzn0o2tswdKa2%2f9MshQ%3d%3d

Page: https://portal.huby.com.br:443/Master/Main.aspx

Page: https://portal.huby.com.br:443/relatorio_usuarios.aspx

Abaixo os detalhamentos destas vulnerabilidades apontadas:

Descrição das vulnerabilidades (Summary), forma de exploração(execution), implicações(implication), sugestões de correções (Fix):

página 93 e 94:

Critical **Insecure Transport: Weak SSL Cipher**

Summary:

WebInspect has detected support for weak TLS/SSL ciphers on the server **https://portal.huby.com.br:443/**.

The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols provide a mechanism to help protect authenticity, confidentiality and integrity of the data transmitted between a client and web server. The strength of this protection mechanism is determined by the authentication, encryption and hashing algorithms. These are collectively known as a cipher suite - chosen for the transmission of sensitive information over the TLS/SSL channel. Most web servers support a range of such cipher suites of varying strengths. Using a weak cipher or an encryption key of insufficient length, for example, could enable an attacker to defeat the protection mechanism and steal or modify sensitive information.

If misconfigured, a web server could be manipulated into choosing weak cipher suites. Also, new versions of the TLS protocols are backward compatible and provide support for older ciphersuites defined in previous versions of the SSL/TLS protocols. For example, it is possible to configure TLS 1.2 to use older and weak ciphers that use RC4, MD5, SHA-1 and so on.

We recommend updating the web server configuration to remove weak ciphers and to always choose the strongest ciphers for encryption.

Execution:

Each weak cipher was enumerated by establishing an SSL connection with the target host and specifying the cipher to test in the Client Hello message of the SSL handshake.

Implication:

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current methods and resources. An attacker could possibly execute a man-in-the-middle attack which would allow them to intercept, monitor and tamper with sensitive data.

Fix:

Disable support for weak ciphers on the server. Weak ciphers are generally defined as:

- Any cipher with key length less than 128 bits
- Export-class cipher suites
- NULL ciphers
- Ciphers that support unauthenticated modes
- Ciphers assessed at security strengths below 112 bits
- All RC4 ciphers
- All 64-bit block ciphers
- All ciphers using MD5 and SHA1 for cryptographic hash functions

The following ciphers supported by the server are weak and should be disabled:

- **TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)**

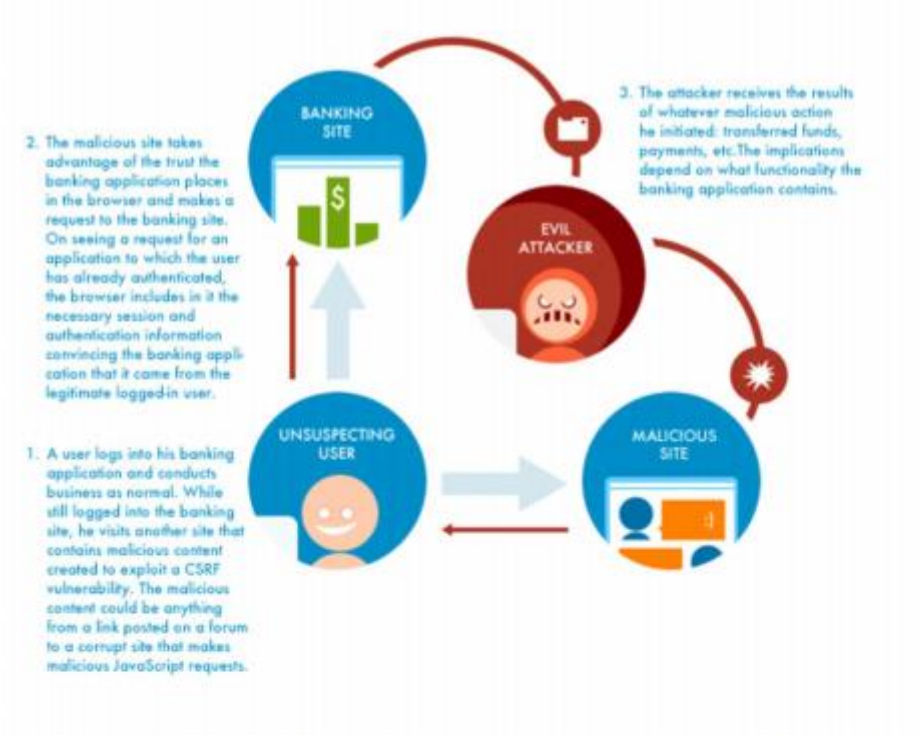
Páginas 97, 98 e 99:

File Names: • https://portal.huby.com.br:443/Login.aspx?ReturnUrl=%2f

Medium **Cross-Site Request Forgery**

Summary:

–



Cross-Site Request Forgery (XSRF or CSRF) has been detected. Because browsers can run code sent by multiple sites, an XSRF attack can occur if one site sends a request (never seen by the user) to another site on which the user has authenticated that will mistakenly be received as if the user authorized the request. If a user visits a vulnerable site, the attacker can make the user's browser send a request to a different target site that performs an action on behalf of the user. The target site only sees a normal authenticated request coming from the user and performs whatever sensitive action was requested. Whatever functionality exists on the target site can be manipulated in this fashion. Recommendations include utilizing CAPTCHA's or anti-Cross-Site Request Forgery tokens to prevent Cross-Site Request Forgery attacks.

Execution:

Criteria for identifying CSRF:

1. This check is only run against POST requests.
2. The page must be either a login page, or a page in restricted session (i.e. an authenticated session) .
* Note: In order to avoid testing every POST request made during authenticated sessions, we will only run the check against a URL one time. This means that forms with multiple parameters will only be tested one time and not multiple times like a XSS or parameter injection check.
3. The page is not a re-authentication page. This is to avoid cases where a user is asked to either change a password or provide their password when they are already in an authenticated session. A re-authentication page is not CSRF vulnerable.
4. The page does not contain CAPTCHA. A CAPTCHA page is not CSRF vulnerable
5. The page is not an error page or an invalid page from the server.

More information on Login CSRF can be found here: http://seclab.stanford.edu/websec/csrf/csrf.pdf.

Implication:

Any functionality contained within the application can be exploited if it is vulnerable to XSRF. For instance, a banking application could be made to transfer funds, etc.

Fix:

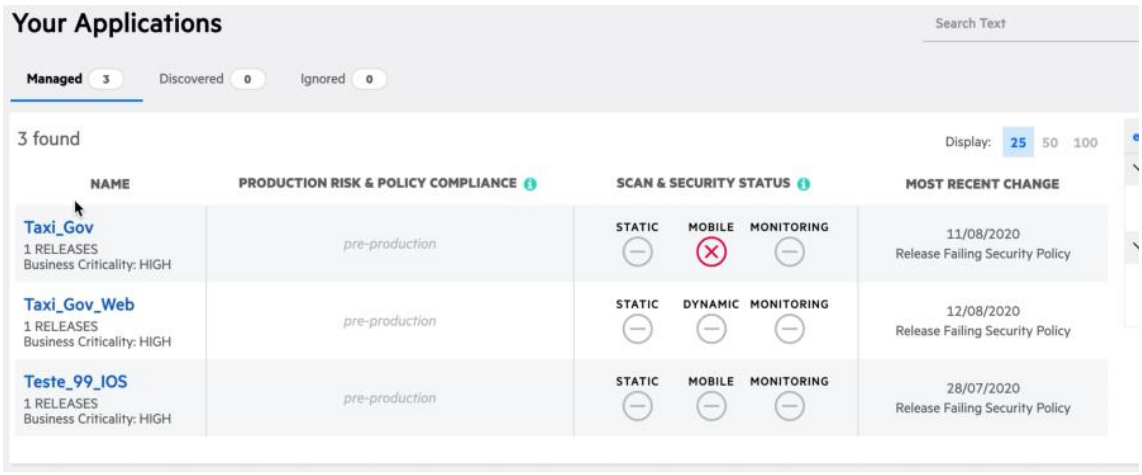
Resolving Cross-Site Request Forgery may require recoding every form and feature of a web application. You can use anti-Cross-Site Request Forgery tokens or CAPTCHAs to prevent Cross-Site Request Forgery attacks. Other methods are easier but not as effective.

While no method of preventing Cross-Site Request Forgery is perfect, using Cross-Site Request Forgery nonce tokens eliminates most of the risk. Although an attacker may guess a valid token, nonce tokens are effective in preventing Cross-Site Request Forgery attacks. You can verify that a user is legitimate by generating a "secret," such as a secret hash or token, after the user logs in. You should store "the secret" in a server-side session and then include it in every link and sensitive form. Each subsequent HTTP request should include this token; otherwise, the request is denied and the session invalidated. Do not make the token the same as the session ID in case a Cross-Site Scripting vulnerability exists. Initialize the token as other session variables. You can validate it with a simple conditional statement, and you can limit it to a small timeframe to enhance its effectiveness. Attackers need to include a valid token with a Cross-Site Request Forgery attack in order to match

6.4.2.2.2 IOS

Arquivo: 2 ciclo - 12-08\Segurança\Fortify_corrupt binary.mov

No vídeo é possível visualizar a falha do arquivo binário ao ser submetido na ferramenta, conforme os print's abaixo:



Quanto a alegação *"As vulnerabilidades encontradas, no total de 4, apontavam para as páginas que seguem, que ao acessá-las, nada de incomum pode ser observado, vejamos:"*

4 vulnerabilidades encontradas

Páginas:

https://portal.huby.com.br:443/Login.aspx
https://portal.huby.com.br:443/CancelarAtendimento.aspx?id=fLOFzn0o2tswdKa2%2f9MshQ%3d%3d
https://portal.huby.com.br:443/Master/Main.aspx
https://portal.huby.com.br:443/relatorio_usuarios.aspx

Não há de se confundir o funcionamento do sistema e de seus fluxos, com a existência de vulnerabilidades de segurança, uma página que apresenta pleno funcionamento, pode estar suscetível a exploração de vulnerabilidades de segurança, o relatório com os apontamentos indicam justamente isso, de posse de vulnerabilidades, pessoas mal intencionadas e com conhecimento técnico avançado podem fazer uso destas brechas para provocar mal funcionamento do sistema, interceptar informações, dentre outras possibilidades de gerar dano aos usuários e ao Ministério.

1.1.1.1 Porém, a alegação da empresa não merece prosperar, tendo em vista que, ao final de cada rodada da Prova de Conceito é emitido um Relatório de Teste, contendo análise da ferramenta quanto à adequação aos critérios do Edital. Nota-se que o relatório mostra de forma concisa em quais itens o sistema da I9 Solutions não foi aprovado.

1.1.1.2 Do supracitado relatório, pode ser verificado nos itens 6.3.2, 6.4.2 e 6.4.2.2.2 os motivos pelos quais a solução havia sido reprovada, tendo o resumo sido apresentado no item 8 do mesmo documento.

1.1.1.3 Além disso, para os itens em que o sistema não foi aprovado, a Administração oportunizou à empresa realização de outra rodada de Prova de Conceito (PoC). Conforme previsão editalícia, a empresa foi convocada com 5 dias úteis de antecedência e, durante esse período, poderia ter dirimido dúvidas que porventura existiam. Porém, a empresa não o fez de modo oficial, podendo depreender que a empresa entendeu os motivos pelos quais alguns requisitos do sistema não foram aprovados.

1.1.1.4 Cabe enfatizar a clareza da Prova de Conceito aplicada, seguindo de forma precisa o item 7 do Termo de Referência, onde é estabelecido de forma direta quais itens do sistema do fornecedor são objeto de análise pela área técnica do Ministério da Economia. Todos os testes foram realizados em sessão pública realizada de forma online prevista inicialmente entre os dias 20/07 a 24/07, das 9h às 12h e das 14h às 17h30 e dia 12/08 das 9h às 12h e das 14h às 18h. As sessões foram iniciadas e finalizadas por servidor do Ministério da Economia responsável pela PoC, com o conhecimento de todos os presentes na sala virtual. Com a concordância de todos os presentes, algumas sessões iniciaram ou encerraram em horários diverso do previsto inicialmente.

1.1.1.5 Toda a metodologia de testes aplicados foi apresentada durante a PoC na realização dos testes previstos, com esclarecimentos prestados a todas as situações levantadas pelos presentes na sala virtual. Foi alertado aos presentes que o único canal para peticionar eventuais dúvidas, esclarecimentos ou quaisquer outras situações posteriormente ou fora dos horários da PoC seria por meio do pregoeiro.

1.1.2 Quanto à alegação de que houve impedimento de acesso aos dados que subsidiam a reprovação do sistema na Prova de Conceito, informamos o que se segue:

1.1.2.1 Conforme se verifica nos relatórios emitidos, mais especificamente no item "7 - Referências", consta um link para o repositório do Ministério da Economia no qual estão disponibilizadas as evidências e relatórios com o detalhamento dos erros de segurança que foram identificados no teste pela ferramenta utilizada. Referidos documentos também podiam ter sido solicitados pela empresa durante a execução da POC, o que não foi feito.

1.1.2.2 Compactou-se, também, em arquivo único o mesmo conteúdo com os artefatos gerados e disponibilizados em repositório, por meio do link https://drive.economia.gov.br/owncloud/index.php/s/hxbiHlozwalWS35.

1.1.3 A empresa recorrente informa ainda que a empresa RSI Informática se negou a realizar mais uma rodada de testes, porém este pedido foi solicitado após ser declarado o encerramento da sessão pública da Prova de Conceito.

1.1.3.1 Durante a sessão, não houve manifestação da empresa quanto a isso. A sessão estava sendo acompanhada por outros licitantes, de modo a conferir transparência à ação. Desta forma, de modo a não prejudicar a legitimidade, lisura e transparência do processo licitatório, não se realizou novos testes.

1.1.3.2 Importante mencionar que a comunicação estabelecida por meio de WhatsApp entre a I9 e a RSI, empresa que atua nas aplicações de PoCs do Ministério da Economia, mostrou-se inócua, uma vez que se tratou de um ambiente inadequado para solicitações ou esclarecimento como foi disposto por servidor do Ministério da Economia ao início da sessão da PoC. Consequentemente o pleito por realizar novos testes no sistema, solicitado por meio de WhatsApp, possuiu vício e não foi considerado.

1.1.4 Quanto à realização de Prova de Conceito para a I9 Solutions e a não realização da mesma etapa para o fornecedor Vip Service, é preciso observar que o item 7.6 do Termo de Referência possibilita a dispensa de Prova de Conceito em caso de aprovação em outra Prova de Conceito realizada anteriormente pela Central de Compras ou outro órgão da Administração Pública.

1.1.4.1 Importante destacar que, segundo o mesmo item do Termo de Referência, cabe discricionariedade à Central de Compras quanto a realização da prova de conceito.

1.1.4.2 A Vip Service, como relatado pelo pregoeiro e transcrito no recurso da I9, foi aprovada nas Provas de Conceito do TáxiGov para a cidade de Brasília. Por se tratar do mesmo sistema aprovado anteriormente e a metodologia da Prova de Conceito ser igual à realizada em Brasília, jugou-se dispensável a Prova para Florianópolis e, no mesmo sentido, entende-se que para Cuiabá é dispensável.

1.1.4.3 Em relação a não dispensa da I9, que foi aprovada nas Provas de Conceito do TRE-PA, MPT, AGU Nordeste, IFPR e TRE-CE, não se considerou razoável a dispensa de Prova de Conceito para o pregão eletrônico em questão, devido ao desconhecimento por parte da Central de Compras da metodologia e da acurácia das medições, bem como dos itens objeto de avaliação das Provas de Conceitos realizadas.

2. Visto que as alegações não apresentam fundamento, conclui-se que o recurso apresentado não deve ser acatado pelo Pregoeiro, podendo prosseguir as demais