




Ministério da Justiça

Projeto: Estrangeiro-WEB

Nota Técnica

MJ	e-Certidão - Nota Técnica	
-----------	----------------------------------	--

Revisão	Descrição	Autor	Data
1.0	Construção do documento	Israel Branco	13/04/2020

1 Sumário

- 2 Introdução.....4
- 3 Apresentação do cenário atual.....5
 - 3.1 Tecnologias utilizadas.....5
 - 3.2 Modelagem de dados.....6
- 4 Análise técnica.....7
 - 4.1 Padrão de codificação.....7
 - 4.2 OWASP ZAP.....10
 - 4.3 UX – User experience.....12
- 5 Conclusão.....14

2 Introdução

Este documento visa reportar o resultado da análise efetuada no sistema Estrangeiro-WEB. Para este estudo foram desconsiderados todo o contexto negocial ao qual a ferramenta está inserida juntamente com o ambiente ao qual a ferramenta opera em ambiente produtivo, sendo analisado puramente questões que tangem a qualidade de código, padrões de codificação, modelo relacional de banco de dados e concepção arquitetural.

3 Apresentação do cenário atual

Esta sessão ira descrever a arquitetura, tecnologias, frameworks e dependências que compõe a base da aplicação.

O sistema Estrangeiro-WEB foi criado para trabalhar em ambiente web sob protocolo HTTP/HTTPS com tecnologia ASP (Active Server Pages) utilizando banco de dados Microsoft SQL Server com conexão ODBC, implantada em servidor de aplicação Microsoft IIS com suporte a aplicações ASP.

3.1 Tecnologias utilizadas

Esta sessão descreve as tecnologias, frameworks e principais bibliotecas utilizadas na construção dos projetos, descrevendo versões e propósitos de utilização.

Nome	Versão	Utilização	Observação
ASP	3	Linguagem de programação.	
ODBC	x	Conexão com banco de dados	
SQL Server	x	Banco de dados	

A estrutura de banco de dados esta composta por 44 tabelas em um único schema, a tabela **NumeroProtocolo** não apresentam relacionamentos nesta estrutura.

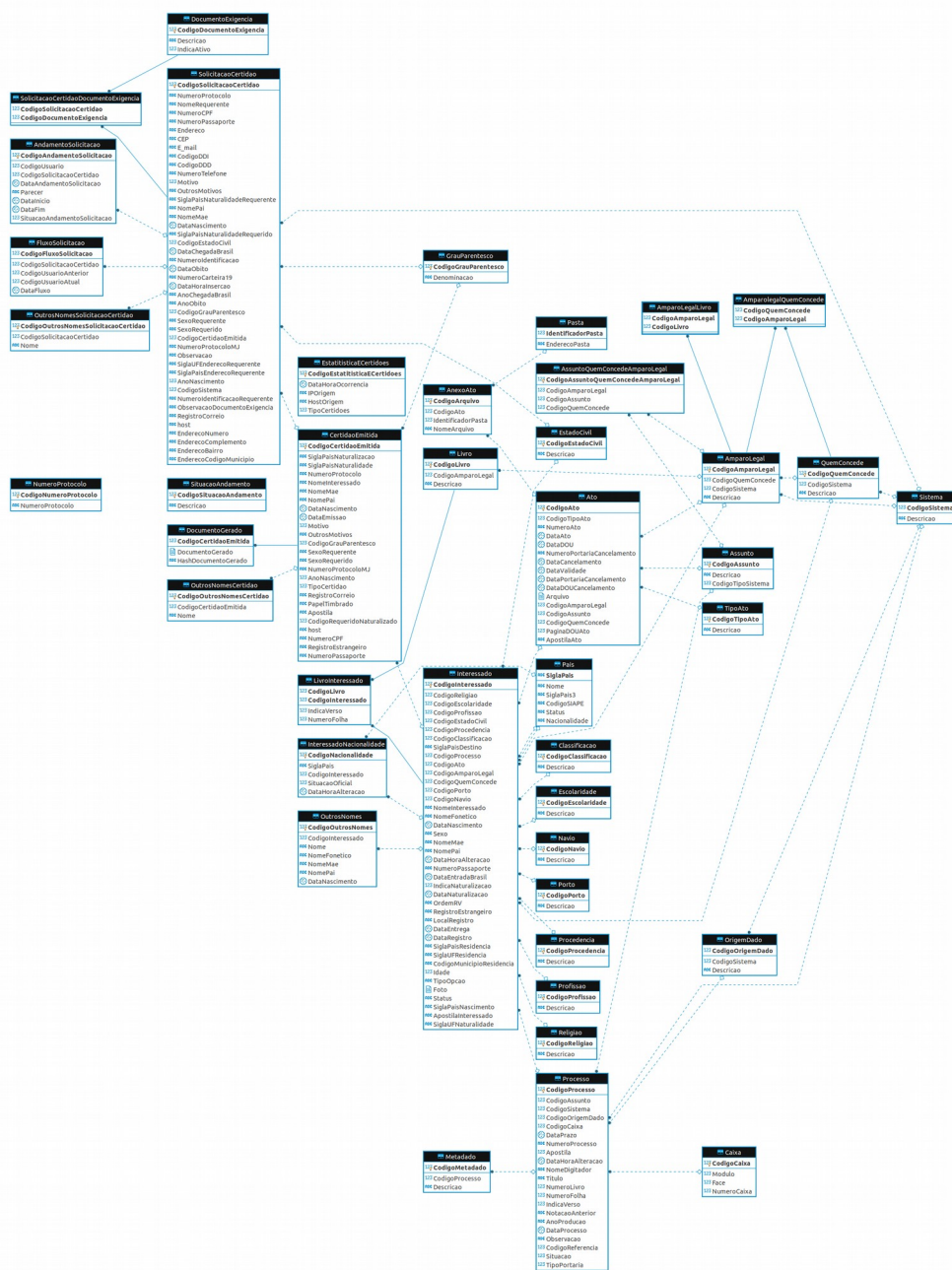


Figura 1: Mer - Banco MJCorporativo - Schema DNN

4 Análise técnica

Este tópico descreve a ferramenta do ponto de vista técnico, tanto nos aspectos de codificação, análise estática de código, análise de vulnerabilidade de dependências e particularidades de implementação.

Para esta análise, foi utilizado o repositório GIT http://git.mj.gov.br/CGTI-DIPROS-LEGADO/MJ-DEEST-MJ_ESTRANGEIROS_WEB-2015 branch stable.

4.1 Padrão de codificação

Tratando-se de tecnologia obsoleta não há ferramentas gratuitas que efetuam análise estática de código para a tecnologia ASP 3.0, as evidências demonstradas a seguir serão apresentadas com base em análise amostral de código.

O código do projeto não apresenta boa segregação e não há reaproveitamento de código com a utilização de includes de artefatos, há maioria das páginas apresentam grande quantidade de código sendo este, embaralhado entre funções ASP, JavaScript e HTML. A imagem a seguir representa o que foi relatado e encontramos este cenário em boa parte da aplicação.

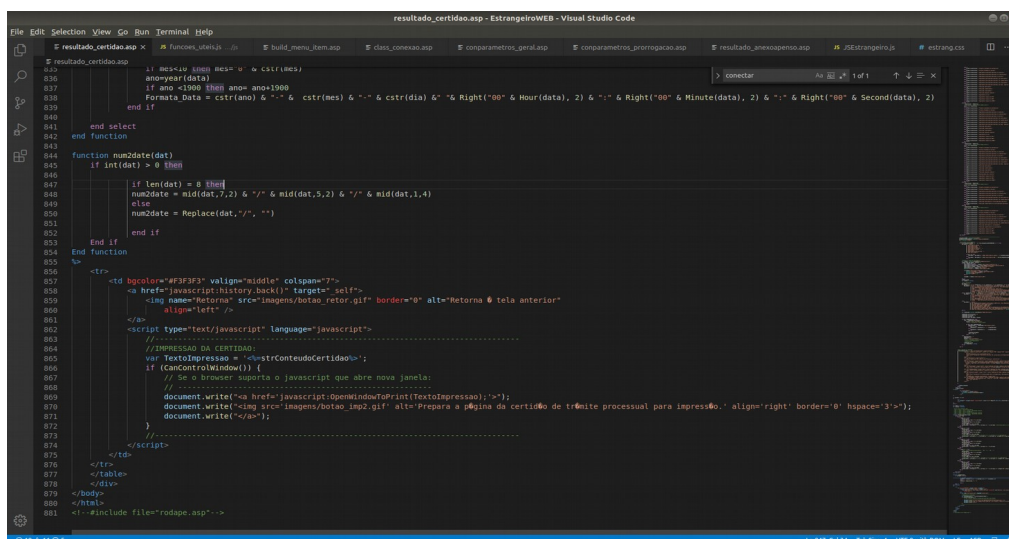


Figura 2: resultado-certificado.asp

Código macarrônico ou código espagete é o termo utilizado para descrever o *AntiPattern* que não segue regras de programação estruturada, mal organizada, com desvios e códigos difíceis de analisar. Este AntiPattern descreve o código produzido para o sistema EstrangeiroWeb, a mistura de tecnologias ao longo das páginas e a altíssima complexidade ciclomática dificultam a testabilidade funcional do sistema e as manutenções corretivas.

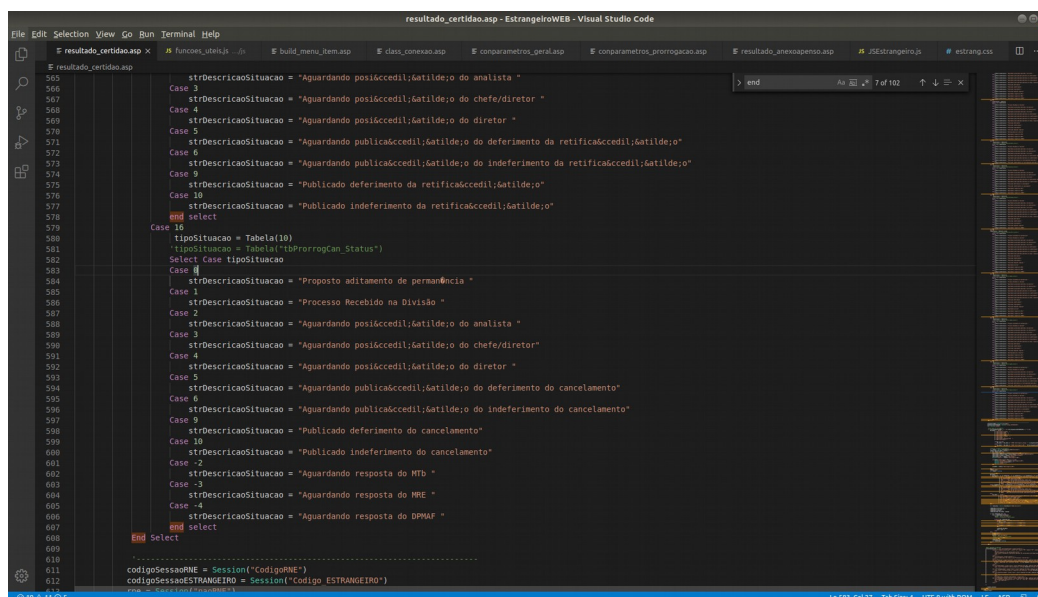


Figura 3: Complexidade ciclomática



```
resultado_certidao.asp - EstrangeiroWEB - Visual Studio Code
File Edit Selection View Go Run Terminal Help
resultado_certidao.asp x # funcoes_utilis.js -js # build_menu_item.asp # class_conexao.asp # conparametros_geral.asp # conparametros_prorrogacao.asp # resultado_anexoopenso.asp # JSestrangeiro.js # estrangeiro.css
654 rsDados.close
655 set rsDados = nothing
656
657 'Busca Dependente
658 SQL_Dados = ""
659 if (auxAnalise = "5" or auxAnalise = "6" or auxAnalise = "7" or auxAnalise = "8" or auxAnalise = "9" or auxAnalise = "10") then
660     SQL_Dados = "SELECT dbo.tbProcessoPermInteressado.tbDocumento_NumeroDoc, dbo.tbProcessoPermInteressado.tbTipoDependencia_Codigo, "
661     &"& dbo.tbTipoDependencia.tbTipoDependencia_Descricao, dbo.tbEstrangeiro.tbEstrangeiro_Codigo, dbo.tbEstrangeiro.tbEstrangeiro_RNE, "
662     &"& dbo.tbEstrangeiro.tbEstrangeiro_Nome "
663     &"& FROM dbo.tbProcessoPermInteressado INNER JOIN "
664     &"& dbo.tbEstrangeiro ON dbo.tbProcessoPermInteressado.tbEstrangeiro_Codigo = dbo.tbEstrangeiro.tbEstrangeiro_Codigo LEFT OUTER JOIN "
665     &"& dbo.tbTipoDependencia ON dbo.tbProcessoPermInteressado.tbTipoDependencia_Codigo = dbo.tbTipoDependencia.tbTipoDependencia_Codigo "
666     &"& WHERE (dbo.tbProcessoPermInteressado.tbDocumento_NumeroDoc = '% Request("CampoPesquisado") &"& ')"
667 else if (auxAnalise = "11" or auxAnalise = "12" or auxAnalise = "13" or auxAnalise = "14" or auxAnalise = "15" or auxAnalise = "16") then
668     SQL_Dados = "SELECT dbo.tbProcessoProrInteressado.tbDocumento_NumeroDoc, dbo.tbProcessoProrInteressado.tbTipoDependencia_Codigo, "
669     &"& dbo.tbTipoDependencia.tbTipoDependencia_Descricao, dbo.tbEstrangeiro.tbEstrangeiro_Codigo, dbo.tbEstrangeiro.tbEstrangeiro_RNE, "
670     &"& dbo.tbEstrangeiro.tbEstrangeiro_Nome "
671     &"& FROM dbo.tbProcessoProrInteressado INNER JOIN "
672     &"& dbo.tbEstrangeiro ON dbo.tbProcessoProrInteressado.tbEstrangeiro_Codigo = dbo.tbEstrangeiro.tbEstrangeiro_Codigo LEFT OUTER JOIN "
673     &"& dbo.tbTipoDependencia ON dbo.tbProcessoProrInteressado.tbTipoDependencia_Codigo = dbo.tbTipoDependencia.tbTipoDependencia_Codigo "
674     &"& WHERE (dbo.tbProcessoProrInteressado.tbDocumento_NumeroDoc = '% Request("CampoPesquisado") &"& ')"
675 else
676     SQL_Dados = " SELECT "
677     &"& dbo.tbDependenteEstrangeiro.tbEstrangeiro_RNETitular, dbo.tbDependenteEstrangeiro.tbEstrangeiro_RNEDependente, "
678     &"& dbo.tbEstrangeiro.tbEstrangeiro_Nome "
679     &"& FROM dbo.tbEstrangeiro INNER JOIN "
680     &"& dbo.tbTipoDependencia INNER JOIN "
681     &"& dbo.tbDependenteEstrangeiro ON dbo.tbTipoDependencia.tbTipoDependencia_Codigo = dbo.tbDependenteEstrangeiro.tbTipoDependencia_Codigo ON "
682     &"& dbo.tbEstrangeiro.tbEstrangeiro_RNE = dbo.tbDependenteEstrangeiro.tbEstrangeiro_RNEDependente "
683     &"& WHERE dbo.tbDependenteEstrangeiro.tbEstrangeiro_RNETitular = '% Session("Codigo") &"& ' "
684 end if
685
686 Set rsDadosDep = Server.CreateObject("ADODB.Recordset")
687
688 rsDadosDep.CursorLocation = #
689 rsDadosDep.CursorType = #
690 rsDadosDep.LockType = #
691 rsDadosDep.Open SQL_Dados, Conexao
692
693 if (not rsDadosDep.eof) then
694     cont = rsDadosDep.RecordCount
695     Texto0 = "pelos estrangeiros"
696     'Texto1 = "residentes e domiciliados"
697
698 Do While Not rsDadosDep.EOF
699     DependenteAux = rsDadosDep("tbEstrangeiro_Nome")
700     if cont = 1 then
701         Dependente = Dependente &"& " e " &"& DependenteAux
702     else
703         Dependente = Dependente &"& " e " &"& DependenteAux
704     end if
705     rsDadosDep.MoveNext
706 end while
707
708 rsDadosDep.Close
709 set rsDadosDep = nothing
```

Figura 4: Complexidade ciclomática

4.2 OWASP ZAP

Ferramenta funciona como scanner de segurança, utilizada para realização de testes de vulnerabilidade de aplicações WEB. Atualmente trata-se de um dos projetos mais ativos na comunidade de software livre.

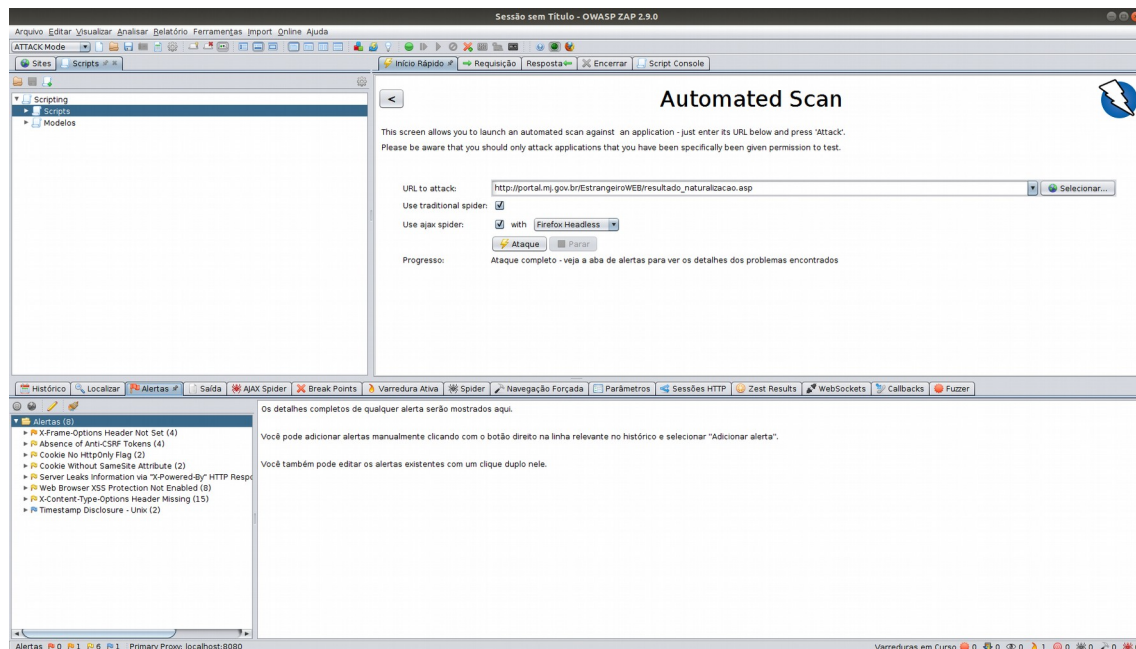


Figura 5: OWASP-ZAP - relatório de intrusão

O relatório completo deste teste está disponível no anexo I deste documento, o detalhamento desta análise está classificada em:

- 0 vulnerabilidades de severidade alta;
- 1 vulnerabilidades de severidade média;
- 6 vulnerabilidades de baixa média;
- 1 vulnerabilidades a nível informativo;

Medium (Medium)		X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.	
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).	
Low (Medium)		Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.	
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.	
Low (Medium)		X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.	
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.	
Low (Medium)		Absence of Anti-CSRF Tokens
Description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRLF, one-click attack, session riding, confused deputy, and sea surf.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"> * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. <p>CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.</p>	
Solution	<p>Phase: Architecture and Design</p> <p>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.</p> <p>For example, use anti-CSRF packages such as the OWASP CSRFGuard.</p> <p>Phase: Implementation</p> <p>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.</p> <p>Phase: Architecture and Design</p> <p>Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).</p> <p>Note that this can be bypassed using XSS.</p> <p>Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.</p> <p>Note that this can be bypassed using XSS.</p> <p>Use the ESAPI Session Management control.</p> <p>This control includes a component for CSRF.</p> <p>Do not use the GET method for any request that triggers a state change.</p> <p>Phase: Implementation</p> <p>Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.</p>	
Low (Medium)		Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server	
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.	
Low (Medium)		Cookie Without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.	
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.	
Low (Medium)		Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.	
Solution	Ensure that the HttpOnly flag is set for all cookies.	
Informational (Low)		Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix	
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.	

A aplicação não apresenta navegação facilitada por navegação em menu e assim a ferramenta não consegue navegar na aplicação como um todo, o resultado apresentado está restrito a página **resultado_naturalizacao.asp**. Por amostragem em ataques as demais páginas ASP que compõe a ferramenta, os resultados obtidos apontam as mesmas vulnerabilidades do relatório acima.

4.3 UX – User experience

A ferramenta não apresenta padronização de interfaceamento gráfico compatível com as especificações do Governo Federal (<http://epwg.governoeletronico.gov.br/guia-administracao>), também não há menu de navegação e a funcionalidade voltar sempre remete a última página visitada pelo usuário e isso pode ocasionar o redirecionamento do usuário para fora do escopo da aplicação.

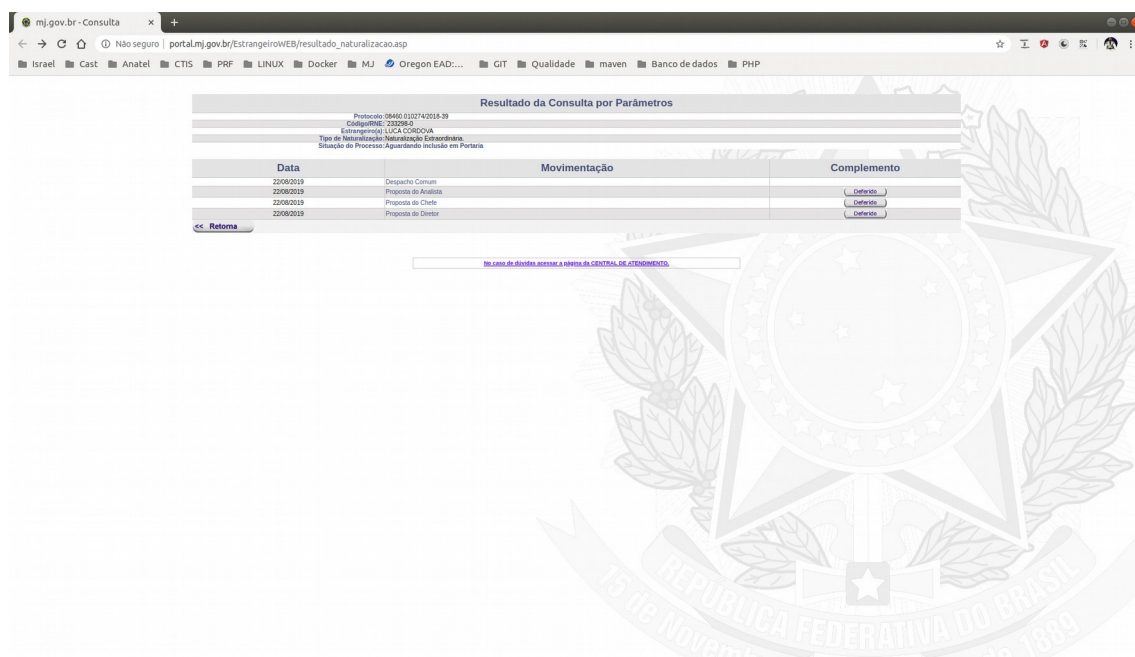


Figura 6: Padrão visual

Também foram encontrados problemas de encode de caracteres durante a navegação.

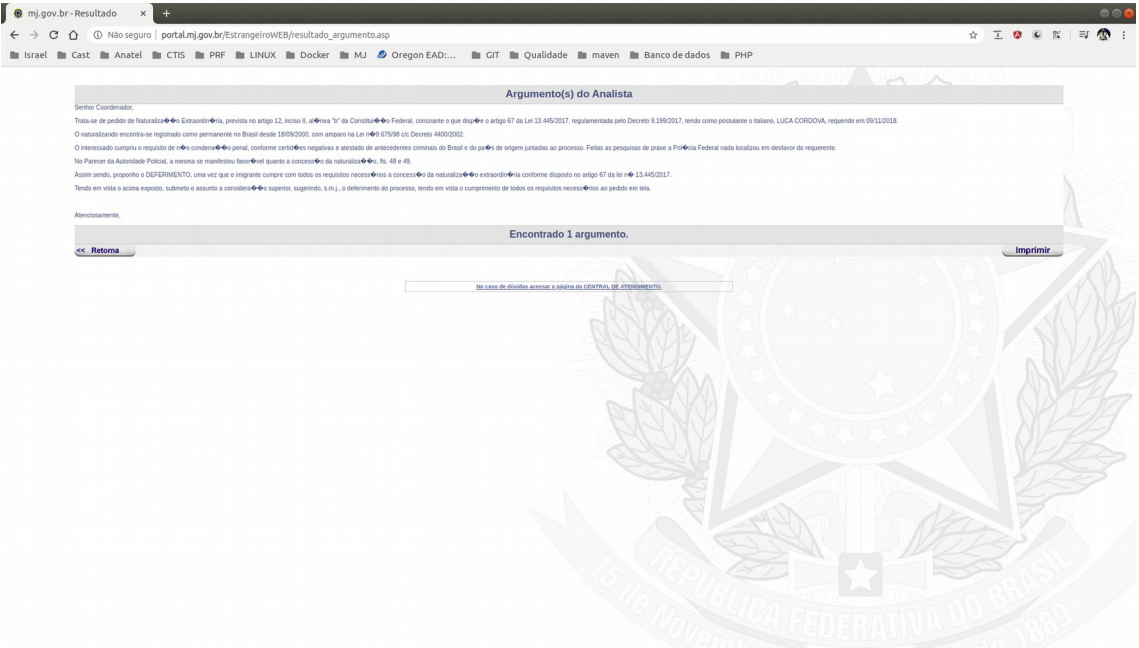


Figura 7: Problemas de encode

5 Conclusão

A aplicação não apresenta boas práticas em sua construção, também não apresenta boa apresentação visual e boa usabilidade.

Por estar concebida com tecnologia defasada, há dificuldades na manutenção do ambiente produtivo para hospedagem e escalabilidade da mesma. Em se tratando de ambiente, a aplicação não está utilizando protocolo seguro para tráfego de dados HTTPS.

Há extrema complexidade ciclomática nas páginas que compõe o contexto da solução, esta complexidade certamente dificulta os testes funcionais e as manutenções corretivas e evolutivas.

Uma vez que não atende aos padrões de codificação, usabilidade, manutenção e segurança da informação, não recomenda-se a manutenção da aplicação em ambiente produtivo, sugere-se que a mesma seja reescrita utilizando a arquitetura de referência adotada para as aplicações WEB do Ministério da Justiça respeitando as características negociais hoje aplicados e as necessidades de evolução do contexto negocial da solução.