



BancoVotorantim

EHT – Ethical Hacking Test

Período da avaliação: 21/06/2021 até 30/06/2021

Método: Gray Box em UAT

Ambiente: Interno

Emissão: 30/06/2021.

RELATÓRIO
SIMPLIFICADO DE
VULNERABILIDADES DE
SEGURANÇA DA
INFORMAÇÃO PARA
APIS DO BANCO BV



Documento:
Relatorio EHT

APISJUN04-21

Data:
30/06/2021

Classificação:
Confidencial

Proprietário:
Segurança da Informação

Titulo	Relatório EHT de testes em APIs
Versão	1.4
Autor	Pedro Rabelo
Revisado por	Vinicius Cezar Pompeo
Aprovado por	Carlos Néri
Classificação	Confidencial



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

Versão	Data	Autor	Descrição
1.0	30/06/2021	Pedro Rabelo	Versão Final
1.1	16/07/2021	Vinicius Pompeo	Revisão
1.4	20/07/2021	Pedro Rabelo	Ajustes



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

1.1.1 Linha do tempo

Atividade	Data Início	Data Término
Versão Final	21/06/2021	30/06/2021
Revisão	16/07/2021	16/07/2021
Ajustes	20/07/2021	20/07/2021

1.1.2 Relação das vulnerabilidades

ID	Nome vulnerabilidade	Risco
1	[APISJUN04-21 - 1] – Exposição de informações (login exposto na URL)	Médio
2	[APISJUN04-21 - 2] – Enumeração de CPFs válidos	Médio
3	[APISJUN04-21 - 3] – Enumeração de usuários	Médio
4	[APISJUN04-21 - 4] – Ataques de repetição SMS (Danos financeiros)	Médio
5	[APISJUN04-21 - 5] – Validação incorreta	Médio
6	[APISJUN04-21 - 6] – Validação incorreta de parâmetros de entrada	Baixo

1.1.3 Relatório

Baseados nos resultados das duas primeiras etapas, iniciamos a análise dos resultados. Nosso cálculo de risco se baseia no seguinte cálculo:

$$\text{Críticidade (Risco)} = \text{Probabilidade} + \text{Impacto} / 2$$

Vulnerabilidade (Probabilidade)	
Extremo	A ameaça origem é altamente motivada e suficientemente capaz, e os controles aplicados para prevenir a vulnerabilidade são inexistentes.
Alto	A ameaça origem é altamente motivada e suficientemente capaz, e os controles aplicados para prevenir a vulnerabilidade são ineficazes.
Médio	A ameaça origem é motivada e capaz, e os controles aplicados podem prevenir parcialmente a exploração da vulnerabilidade.
Baixo	A ameaça origem não tem motivação ou capacidade, ou há controles suficientes aplicados ou que possam suficientemente impedir que a vulnerabilidade seja explorada de maneira efetiva.

Tabela 5 - Definições de probabilidade

Impacto	
Extremo	A exploração da vulnerabilidade pode resultar em consequências catastróficas; podendo violar, danificar, ou impedir de forma incalculável a missão, reputação ou interesses da organização
Alto	A exploração da vulnerabilidade pode resultar em altas perdas dispendiosas em recursos ou ativos; pode violar, danificar, ou impedir de forma significativa a missão, reputação ou interesses da organização

Impacto	
Médio	A exploração da vulnerabilidade pode resultar em possíveis perdas de ativos ou recursos; pode violar, danificar, ou impedir a missão, reputação ou interesses da organização
Baixo	A exploração da vulnerabilidade pode resultar em perdas pontuais de alguns ativos ou recursos; pode afetar com baixa consequência a missão, reputação ou interesses da organização.

Tabela 5 - Definições de probabilidade

Descrição das criticidades e ações necessárias	
Extremo	Se o risco for considerado extremo, ações rápidas e efetivas para correção devem ser tomadas. Conforme definido em norma, o tempo de correção para este tipo de falha é de 15 dias.
Alto	Se o risco for considerado alto, há uma grande necessidade de medidas corretivas. Um plano de ação corretiva deverá ser colocado em prática o mais rápido possível. Conforme definido em norma, o tempo de correção para este tipo de falha é de 30 dias.
Médio	Se o risco for considerado médio, ações corretivas são necessárias e um plano deve ser desenvolvido para incorporar estas ações dentro de um período razoável de tempo. Conforme definido em norma, o tempo de correção para este tipo de falha é de 90 dias.
Baixo	Se um risco for considerado baixo, o responsável poderá estabelecer um plano de ação em um tempo confortável. Conforme definido em norma, o tempo de correção para este tipo de falha é de 180 dias.

Tabela 7 - Escala de risco e ações necessárias

1.1.4 Escopo

CASP	Componente	Executor	Solicitante	Responsável	Ambiente
CASP-10201	caapi-apro-cged-upload-do-cumentacao-iged	PH	Rodrigo Dos Santos Antonio	Sem responsável	UAT
CASP-10376	caapi-apro-base-proposta-comercial-veiculo-v4	VP	Rafael Augusto Filho	Vinicius Cezar Pompeo	UAT
CASP-13686	caapi-srec-base-recalculo-operacao	DM	Thays Ysabely Marinho Celestino	Marcio Mendonca	UAT
CASP-14409	caapi-bvad-base-usuario-cliente-salesforce-v2	BJ	Hugo Raphael Veloso De Lima	Genilson	UAT
CASP-15166	caapi-ccbd-base-imagem-comprovantes-obtencao	DM	Cleiton Dantas	Maietto	UAT
CASP-15510	caapi-bvad-atou-atend-resgate-programa-pontos	BJ	Julia Talita Coelho	Rodrigo Gimenes	UAT
CASP-15582	caapi-apro-cpvg-salvar-dados-bancarios	PH	Felipe Marins	Rafael Magno	UAT
CASP-15614	caapi-cntf-base-processo-ass-eletr-reenvio	VP	Renato Alexandre Pires Lima Ferreira De Santana	Jesse Araujo Done	UAT
CASP-15653	caapi-cart-svhp-limite-alterar-dxc	PH	Marcos Arno Prediger	Fabiano Lopes Prazeres	UAT

CASP-15666	caapi-bvad-base-atualiza- dados-protocolo-sfc	PH	Julia Talita Coelho	Rodrigo Gimenes	UAT
CASP-15668	caapi-intb-base-usuario-m aster-consulta	PH	Gabriel Alves De Queiros	Milton Ribeiro dos Santos	UAT
CASP-15720	caapi-cart-svhp-consultar -codigodebarras-fatura-at ual-dxc	BJ	Pedro Alexandre Teixeira Kerr	Rodrigo Gimenes	UAT
CASP-15765	caapi-cart-base-risk-cent er-ura	BJ	Ítalo Rodrigues Gaião Da Costa	Rodrigo Gimenes	UAT
CASP-15675	caapi-spag-pixx-devolucao -envio-v2	PH	Thays Ysabely Marinho Celestino	Marcio Mendonca	UAT
CASP-15676	caapi-spag-pixx-pagamento -envio-v2	PH	Thays Ysabely Marinho Celestino	Marcio Mendonca	UAT
CASP-13340	caapi-spag-pixx-identific ador-gerar	PH	Thays Ysabely Marinho Celestino	Marcio Mendonca	UAT
CASP-15420	caapi-spag-pixx-qrcoode-co branca-vencimento	EB	Thays Ysabely Marinho Celestino	Marcio Mendonca	UAT

2. Detalhamento das Vulnerabilidades

Nome - Vulnerabilidade

1

[APISJUN04-21 - 1] – Exposição de informações (login exposto na URL)



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

Impacto	Vulnerabilidade (Prob.)	Criticidade (Risco)
Médio	Médio	Médio

Sistema

Relatório Semanal	Referência Ataque		Referência Vul.	
21/06/2021 a 30/06/2021	CAPEC		CWE	200

Resumo

Vulnerabilidade: [APISJUN04-21 - 1] – Exposição de informações (login exposto na URL)

Descrição: A aplicação expõe diretamente o login do usuário na requisição HTTP GET. Dessa forma, um agente malicioso poderá capturar essa informação via ataque local de *ARP Spoofing*.

Recomendação: Algumas das recomendações sugeridas são:

- Enviar dados pessoais e/ou sensíveis por intermédio de requisições POST.
- Utilização de canais seguros para a comunicação e transmissão de dados.
- Uso de mecanismos atuais de criptografia.
- Implementação do HTTPS em conjunto com o HSTS, forçando o browser a enviar a requisição somente por meios criptografados, garantindo assim a segurança dos dados e impossibilitando que agentes maliciosos capturem as requisições por técnicas de ARP Spoof e SSL Stripping.

Descrição – Situação Encontrada

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-10376	caapi-apro-base-proposta-comercial-veiculo-v4	/v4/varejo/contratacao/pr-oposta-veiculos/proposta	0	Aberto

A aplicação expõe diretamente o login do usuário na requisição HTTP GET. Dessa forma, um agente malicioso poderá capturar essa informação via ataque local de *ARP Spoofing*.

Classificação:

Confidencial

Proprietário:

Segurança da Informação

Impacto

É possível fazer com que informações de outros usuários sejam acessadas por usuários não privilegiados, ocasionando o vazamento de informações.

Recomendação

Algumas das recomendações sugeridas são:

- Enviar dados pessoais e/ou sensíveis por intermédio de requisições POST.
- Utilização de canais seguros para a comunicação e transmissão de dados.
- Uso de mecanismos atuais de criptografia.
- Implementação do HTTPS em conjunto com o HSTS, forçando o browser a enviar a requisição somente por meios criptografados, garantindo assim a segurança dos dados e impossibilitando que agentes maliciosos capturem as requisições por técnicas de ARP Spoof e SSL Stripping.

Links de referências

<https://cwe.mitre.org/data/definitions/200.html>

Evidências

Evidências CASP-10376:

Data: 24/06/2021

[illegible]

Figura 1 - Exploração da vulnerabilidade: Usuário da aplicação esta sendo exposto na URL da aplicação, deixando log nos softwares onde esse trafego é passado.

2

Nome - Vulnerabilidade

[APISJUN04-21 - 2] – Enumeração de CPFs válidos

Impacto		Vulnerabilidade (Prob.)		Criticidade (Risco)	
Médio		Médio		Médio	
Sistema					
Relatório Semanal		Referência Ataque		Referência Vul.	
21/06/2021 a 30/06/2021		CAPEC		CWE	204

Resumo

Vulnerabilidade: [APISJUN04-21 - 2] – Enumeração de CPFs válidos

Descrição: A aplicação é vulnerável a enumeração de CPFs válidos, sendo possível realizar ataques de força bruta em URLs e parâmetros vulneráveis sem nenhum mecanismo de bloqueio que impossibilite a execução desse tipo de ataque. Quando é feita a enumeração de um CPF válido, a aplicação comporta-se de uma determinada maneira, exibindo sempre uma determinada resposta. Para tentativas de enumeração de CPFs inválidos e/ou não cadastrados, a aplicação comporta-se de forma diferente. De acordo com esse comportamento, é possível enumerar quais são os válidos dos inválidos.

Recomendação: Algumas das recomendações sugeridas são:

- Limitar a quantidade de chamadas efetuadas à aplicação.
- Implementar o reCAPTCHA da Google para bloquear a repetição do ataque.
- Implementar tokens e mecanismos que bloqueiem tentativas de ataques de força bruta/dicionário.

Descrição – Situação Encontrada



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-13340	caapi-spag-pixx-identificador-gerar	/v1/EndToEndId	0	Aberto
CASP-15510	caapi-bvad-atou-atend-resgate-programa-pontos	/v1/banco-digital/atend/pua/cartoes/resgate/pontos/cliente	0	Aberto
CASP-14409	caapi-bvad-base-usuario-cliente-salesforce-v2	/v2/banco-digital/parceiros/salesforce/cliente/dados/inserir	0	Aberto
CASP-15668	caapi-intb-base-usuario-master-consulta	/v1/atacado/usuario-master/consultar	0	Aberto

A aplicação é vulnerável a enumeração de CPFs válidos, sendo possível realizar ataques de força bruta em URLs e parâmetros vulneráveis sem nenhum mecanismo de bloqueio que impossibilite a execução desse tipo de ataque. Quando é feita a enumeração de um CPF válido, a aplicação comporta-se de uma determinada maneira, exibindo sempre uma determinada resposta. Para tentativas de enumeração de CPFs inválidos e/ou não cadastrados, a aplicação comporta-se de forma diferente. De acordo com esse comportamento, é possível enumerar quais são os válidos dos inválidos.

Impacto

É possível enumerar os logins da aplicação, sendo usado em outros ataques ou como medida de coleta de informações.

Recomendação

Algumas das recomendações sugeridas são:

- Limitar a quantidade de chamadas efetuadas à aplicação.
- Implementar o reCAPTCHA da Google para bloquear a repetição do ataque.
- Implementar tokens e mecanismos que bloqueiem tentativas de ataques de força bruta/dicionário.

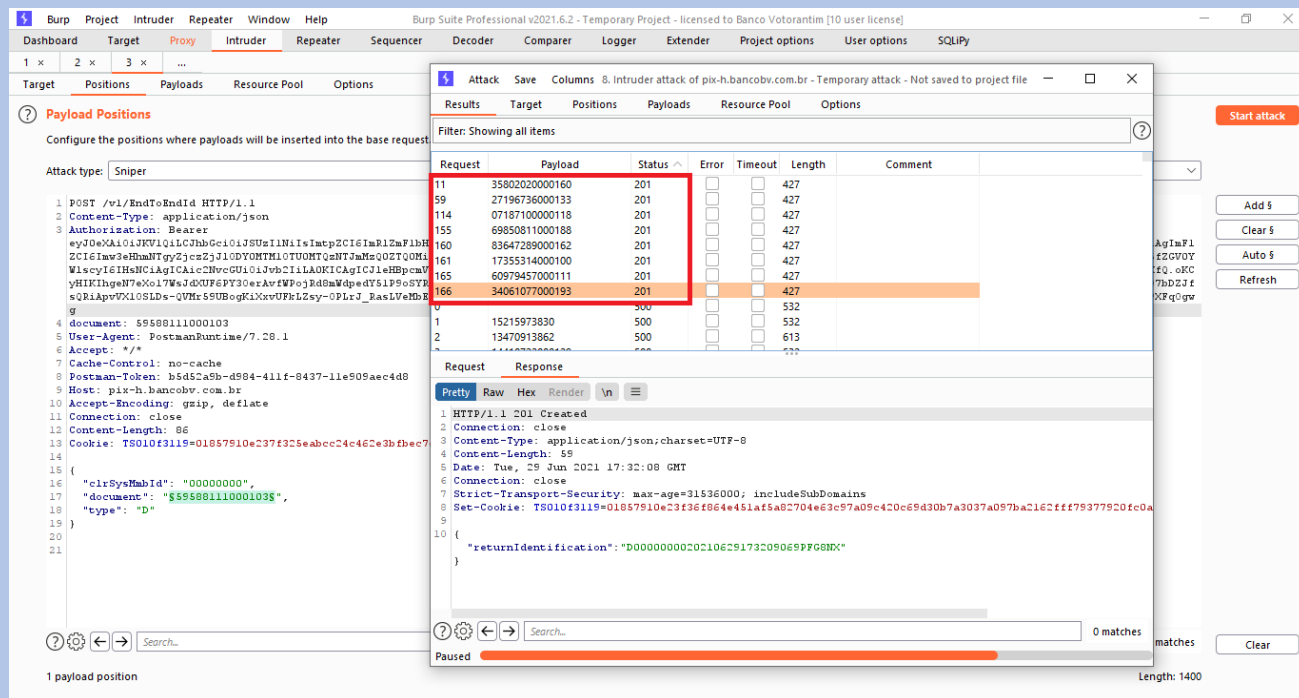
Links de referências

<https://cwe.mitre.org/data/definitions/204.html>

Evidências

Evidências CASP-13340:

Data: 29/06/2021



The screenshot displays the Burp Suite Professional v2021.6.2 interface. The main window shows the 'Payload Positions' configuration for a brute force attack on the 'document' parameter. The 'Attack' window is open, showing the 'Results' tab with a list of requests and their responses. The 'Payload Positions' window shows a list of requests with their payloads and status. The 'Attack' window shows the 'Results' tab with a list of requests and their responses.

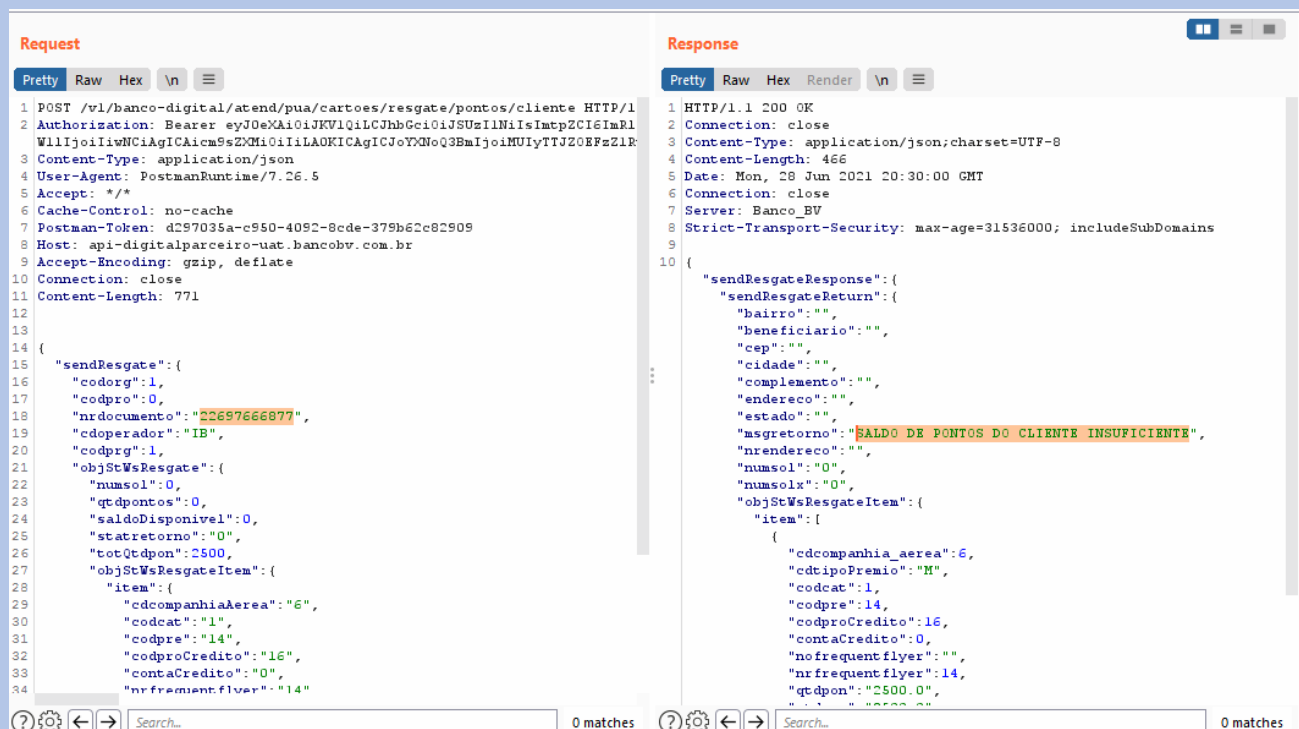
Request	Payload	Status	Error	Timeout	Length	Comment
11	3580202000160	201			427	
59	27196736000133	201			427	
114	07187100000118	201			427	
155	69850811000188	201			427	
160	83647289000162	201			427	
161	17355314000100	201			427	
165	60979457000111	201			427	
166	34061077000193	201			427	

The 'Attack' window shows the 'Results' tab with a list of requests and their responses. The 'Payload Positions' window shows a list of requests with their payloads and status. The 'Attack' window shows the 'Results' tab with a list of requests and their responses.

Figura 2 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro document, foi possível obter outros valores para documentos válidos, resultando na enumeração de CPFs e informações pessoais de clientes.

Evidências CASP-15510:

Data: 28/06/2021



```
Request
Pretty Raw Hex \n
1 POST /v1/banco-digital/atend/pua/cartoes/resgate/pontos/cliente HTTP/1.1
2 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImRl
3 Content-Type: application/json
4 User-Agent: PostmanRuntime/7.26.5
5 Accept: */*
6 Cache-Control: no-cache
7 Postman-Token: d297035a-c950-4092-8cde-379b62c82909
8 Host: api-digitalparceiro-uat.bancobv.com.br
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Content-Length: 771
12
13 {
14   "sendResgate": {
15     "codorg": 1,
16     "codpro": 0,
17     "nrdocumento": "22697666877",
18     "cdoperador": "IB",
19     "codprg": 1,
20     "objStWsResgate": {
21       "numsol": 0,
22       "qtdpontos": 0,
23       "saldoDisponivel": 0,
24       "statretorno": "0",
25       "totQtdpon": 2500,
26       "objStWsResgateItem": {
27         "item": {
28           "cdcompanhiaAerea": "6",
29           "codcat": "1",
30           "codpre": "14",
31           "codproCredito": "16",
32           "contaCredito": "0",
33           "nrfrequentflyer": "14"
34         }
35       }
36     }
37   }
38 }

Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 466
5 Date: Mon, 28 Jun 2021 20:30:00 GMT
6 Connection: close
7 Server: Banco_BV
8 Strict-Transport-Security: max-age=31536000; includeSubDomains
9
10 {
11   "sendResgateResponse": {
12     "sendResgateReturn": {
13       "bairro": "",
14       "beneficiario": "",
15       "cep": "",
16       "cidade": "",
17       "complemento": "",
18       "endereco": "",
19       "estado": "",
20       "msgretorno": "SALDO DE PONTOS DO CLIENTE INSUFICIENTE",
21       "nrendereco": "",
22       "numsol": "0",
23       "numsolx": "0",
24       "objStWsResgateItem": {
25         "item": {
26           "cdcompanhia_aerea": 6,
27           "cdtipoPremio": "M",
28           "codcat": 1,
29           "codpre": 14,
30           "codproCredito": 16,
31           "contraCredito": 0,
32           "nofrequentflyer": "",
33           "nrfrequentflyer": 14,
34           "qtdpon": 2500.0,
35           "saldo": 0.0
36         }
37       }
38     }
39   }
40 }
```

Figura 3 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro document, foi possível obter outros valores para documentos válidos, resultando na enumeração de CPFs e informações pessoais de clientes.

Request

Pretty Raw Hex \n

```
1 POST /v1/banco-digital/atend/pua/cartoes/resgate/pontos/cliente HTTP/1.1
2 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImRl
  Wll1Ijo1IiwiaWQiOiJkaWkiLCJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImRl
3 Content-Type: application/json
4 User-Agent: PostmanRuntime/7.26.5
5 Accept: */*
6 Cache-Control: no-cache
7 Postman-Token: d297035a-c950-4092-8cde-379b62c82909
8 Host: api-digitalparceiro-uat.bancobv.com.br
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Content-Length: 771
12
13 {
14   "sendResgate": {
15     "codorg": 1,
16     "codpro": 0,
17     "nrdocumento": "15215973830",
18     "cdoperador": "IB",
19     "codprg": 1,
20     "objStWsResgate": {
21       "numsol": 0,
22       "qtdpontos": 0,
23       "saldoDisponivel": 0,
24       "statretorno": "0",
25       "totQtdpon": 2500,
26       "objStWsResgateItem": {
27         "item": {
28           "cdcompanhiaAerea": "6",
29           "codcat": "1",
30           "codpre": "14",
31           "codproCredito": "16",
32           "contaCredito": "0",
33           "nrFrequentFlyer": "14"
34         }
35       }
36     }
37   }
38 }
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 467
5 Date: Mon, 28 Jun 2021 20:29:59 GMT
6 Connection: close
7 Server: Banco_BV
8 Strict-Transport-Security: max-age=31536000; includeSubDomains
9
10 {
11   "sendResgateResponse": {
12     "sendResgateReturn": {
13       "bairro": "",
14       "beneficiario": "",
15       "cep": "",
16       "cidade": "",
17       "complemento": "",
18       "endereco": "",
19       "estado": "",
20       "msgretorno": "Falha na consulta - CPF não localizado",
21       "nrendereco": "",
22       "numsol": "0",
23       "numsolx": "0",
24       "objStWsResgateItem": {
25         "item": {
26           "cdcompanhiaAerea": 6,
27           "cdtipoPremio": "M",
28           "codcat": 1,
29           "codpre": 14,
30           "codproCredito": 16,
31           "contaCredito": 0,
32           "noFrequentFlyer": "",
33           "nrFrequentFlyer": 14,
34           "qtdpon": "2500.0",
35           "statretorno": "0"
36         }
37       }
38     }
39   }
40 }
```

Figura 4 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro document, foi possível obter outros valores para documentos válidos, resultando na enumeração de CPFs e informações pessoais de clientes.

Request

```
1 POST /v1/banco-digital/atend/pua/cartoes/resgate/pontos/cliente HTTP/1
2 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImRl
3 Content-Type: application/json
4 User-Agent: PostmanRuntime/7.26.5
5 Accept: */*
6 Cache-Control: no-cache
7 Postman-Token: d297035a-c950-4092-8cde-379b62c82909
8 Host: api-digitalparceiro-uat.bancobv.com.br
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Content-Length: 771
12
13 {
14   "sendResgate": {
15     "codorg": 1,
16     "codpro": 0,
17     "nrdocumento": "51560679808",
18     "cdoperador": "IB",
19     "codprg": 1,
20     "objStWsResgate": {
21       "numsol": 0,
22       "qtdpontos": 0,
23       "saldoDisponivel": 0,
24       "statretorno": "0",
25       "totQtDpon": 2500,
26       "objStWsResgateItem": {
27         "item": {
28           "cdcompanhiaAerea": "6",
29           "codcat": "1",
30           "codpre": "14",
31           "codproCredito": "16",
32           "contaCredito": "0",
33           "nrFrequentFlyer": "14"
34         }
35       }
36     }
37   }
38 }
```

Response

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 466
5 Date: Mon, 28 Jun 2021 20:29:58 GMT
6 Connection: close
7 Server: Banco_BV
8 Strict-Transport-Security: max-age=31536000; includeSubDomains
9
10 {
11   "sendResgateResponse": {
12     "sendResgateReturn": {
13       "bairro": "",
14       "beneficiario": "",
15       "cep": "",
16       "cidade": "",
17       "complemento": "",
18       "endereco": "",
19       "estado": "",
20       "msgretorno": "SALDO DE PONTOS DO CLIENTE INSUFICIENTE",
21       "nrendereco": "",
22       "numsol": "0",
23       "numsolx": "0",
24       "objStWsResgateItem": {
25         "item": {
26           "cdcompanhia_aerea": 6,
27           "cdtipoPremio": "M",
28           "codcat": 1,
29           "codpre": 14,
30           "codproCredito": 16,
31           "contaCredito": 0,
32           "noFrequentFlyer": "",
33           "nrFrequentFlyer": 14,
34           "qtdpon": 2500.0,
35           "saldo": 0.0
36         }
37       }
38     }
39   }
40 }
```

Figura 5 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro document, foi possível obter outros valores para documentos válidos, resultando na enumeração de CPFs e informações pessoais de clientes.

Evidências CASP-14409:

Data: 25/06/2021

Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
1	15215973830	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
2	13470913862	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
5	11326431803	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
4	08556546862	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
10	16007833682	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
13	39829413691	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
31	58304436353	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
29	63168923575	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
34	10313430837	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
33	57713735089	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
32	29607761863	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
35	15215973830	400	<input type="checkbox"/>	<input type="checkbox"/>	312	

Figura 6 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro cpf, foi possível obter outros valores para documentos válidos através da interpretação da mensagem de erro (CPFs inválidos possuem retorno "null" na mensagem e os válidos possuem a mensagem de "falha ao inserir registro").

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
9	45440125116	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
6	12121212108	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
3	14410722000129	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
8	06234797000178	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
7	09515813000199	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
0		400	<input type="checkbox"/>	<input type="checkbox"/>	299	
1	15215973830	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
11	35802020000160	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
12	77788800325	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
2	13470913862	400	<input type="checkbox"/>	<input type="checkbox"/>	312	
14	77777000144	400	<input type="checkbox"/>	<input type="checkbox"/>	299	
5	4436131000	400	<input type="checkbox"/>	<input type="checkbox"/>	299	

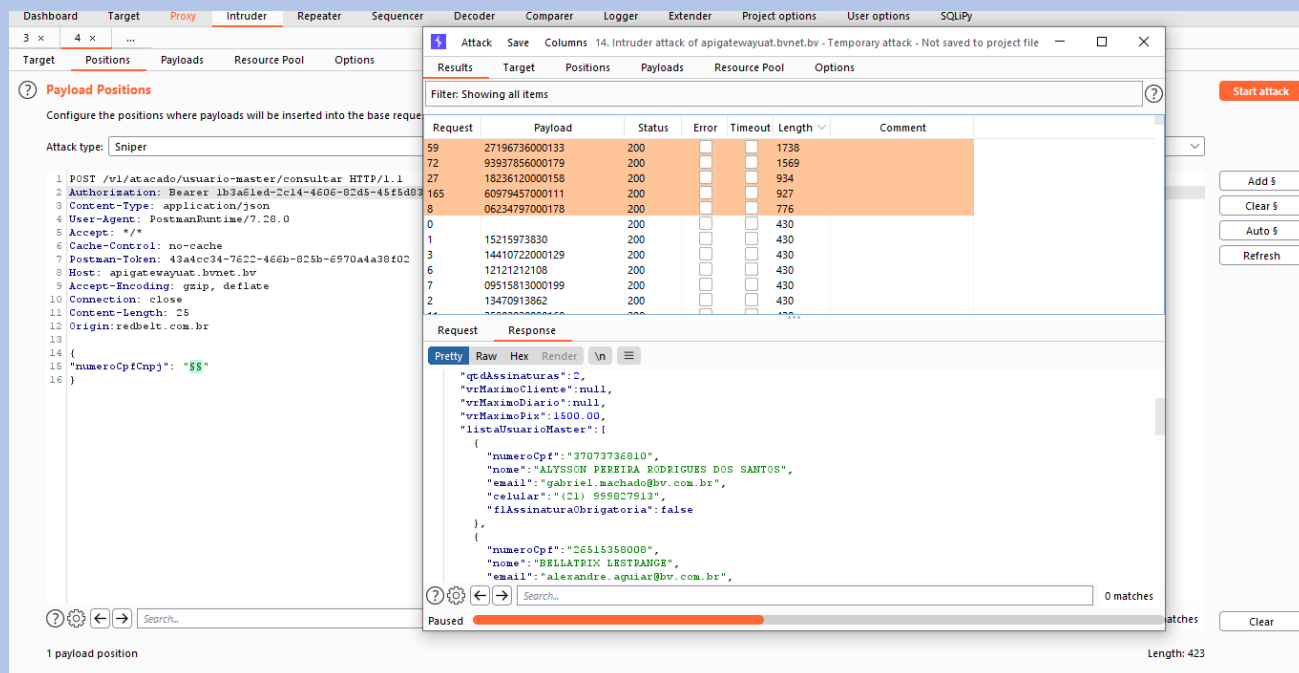
Request Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 400 Bad Request
2 Date: Fri, 25 Jun 2021 18:37:38 GMT
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 73
5 Connection: close
6 Server: BV
7 Strict-Transport-Security: max-age=31536000; includeSubDomains
8
9 {
10   "dadosRetorno": [
11     {
12       "status": 0,
13       "mensagem": "Falha ao inserir o registro."
14     }
15   ]
16 }
```

Figura 7 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro cpf, foi possível obter outros valores para documentos válidos através da interpretação da mensagem de erro (CPF's inválidos possuem retorno "null" na mensagem e os válidos possuem a mensagem de "falha ao inserir registro").

Data: 25/06/2021



Dashboard | **Target** | **Proxy** | **Intruder** | **Repeater** | **Sequencer** | **Decoder** | **Comparer** | **Logger** | **Extender** | **Project options** | **User options** | **SQLiPy**

3 x | 4 x | ...

Target | **Positions** | **Payloads** | **Resource Pool** | **Options**

1 Payload Positions

Configure the positions where payloads will be inserted into the base request

Attack type: **Sniper**

```

1 POST /v1/atacado/usuario-master/consultar HTTP/1.1
2 Authorization: Bearer lb3a6led-2c14-4606-82d5-45f5d03
3 Content-Type: application/json
4 User-Agent: PostmanRuntime/7.28.0
5 Accept: */*
6 Cache-Control: no-cache
7 Postman-Token: 43a4cc34-7622-466b-825b-e970a4a36f02
8 Host: apigatewayuat.bvnet.bv
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Content-Length: 25
12 Origin: redwelt.com.br
13
14 {
15   "numeroCpfCnpj": "$$"
16 }

```

1 payload position

Results | **Target** | **Positions** | **Payloads** | **Resource Pool** | **Options**

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
59	27196736000133	200			1738	
72	93937856000179	200			1569	
27	18236120000158	200			934	
165	60979457000111	200			927	
8	06234797000178	200			776	
0		200			430	
1	15215973830	200			430	
3	14410722000129	200			430	
6	12121212108	200			430	
7	09515813000199	200			430	
2	13470913862	200			430	

Request | **Response**

Pretty | **Raw** | **Hex** | **Render** | **Un** | **≡**

```

{
  "qtAssinaturas": 2,
  "vrMaximoCliente": null,
  "vrMaximoDiario": null,
  "vrMaximoPix": 1500.00,
  "listaUsuarioMaster": [
    {
      "numeroCpf": "37073736910",
      "nome": "ALYSSON PEREIRA RODRIGUES DOS SANTOS",
      "email": "gabriel.machado@bv.com.br",
      "celular": "(21) 999027913",
      "flAssinaturaObrigatoria": false
    },
    {
      "numeroCpf": "265153580008",
      "nome": "BELLATRIX LESTRANGE",
      "email": "alexandre.aguiar@bv.com.br",
      "celular": "(21) 999027913",
      "flAssinaturaObrigatoria": false
    }
  ]
}

```

0 matches

Paused

Length: 423

Figura 8 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro numeroCPF Cnpj, foi possível obter outros valores para documentos válidos, resultando na enumeração de CPFs e informações pessoais de clientes.

Nome - Vulnerabilidade

3

[APISJUN04-21 - 3] – Enumeração de usuários

Impacto		Vulnerabilidade (Prob.)		Criticidade (Risco)	
Médio		Médio		Médio	
Sistema					
Relatório Semanal		Referência Ataque		Referência Vul.	
21/06/2021 a 30/06/2021		CAPEC		CWE	307, 203

Resumo

Vulnerabilidade: [APISJUN04-21 - 3] – Enumeração de usuários

Descrição: A aplicação é vulnerável a enumeração de usuários, sendo possível realizar ataques de força bruta em URLs e parâmetros vulneráveis sem nenhum mecanismo de bloqueio que impossibilite a execução desse tipo de ataque. Quando é feita a enumeração de um usuário válido, a aplicação comporta-se de uma determinada maneira, exibindo sempre uma determinada resposta. Para tentativas de enumeração de usuários inválidos e/ou não cadastrados, a aplicação comporta-se de forma diferente. De acordo com esse comportamento, é possível enumerar quais são os válidos dos inválidos.

Recomendação: Algumas das recomendações sugeridas são:

- Limitar a quantidade de chamadas efetuadas à aplicação.
- Implementar o reCAPTCHA da Google para bloquear a repetição do ataque.
- Implementar tokens e mecanismos que bloqueiem tentativas de ataques de força bruta/dicionário.
- Exibir mensagem genérica para casos de tentativas inválidos, ao invés de especificar o erro do usuário. Por exemplo, caso digite o login inválido exibir a mensagem "Erro: Usuário e/ou senha inválido, verifique novamente o seu login" ao invés de "Erro: Usuário inválido, verifique novamente o seu login".

Descrição – Situação Encontrada



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15653	caapi-cart-svhp-limite-alterar-dxc	/v1/cartoes/dxc/limite/alterar	0	Aberto
CASP-15720	caapi-cart-svhp-consultar-codigodebarras-fatura-atual-dxc	/v1/varejo/cartoes/dxc/consultar/codigodebarras/fatura/atual	0	Aberto
CASP-15765	caapi-cart-base-risk-center-ura	/v1/varejo/cartoes/risk-center/ura	0	Aberto

A aplicação é vulnerável a enumeração de usuários, sendo possível realizar ataques de força bruta em URLs e parâmetros vulneráveis sem nenhum mecanismo de bloqueio que impossibilite a execução desse tipo de ataque. Quando é feita a enumeração de um usuário válido, a aplicação comporta-se de uma determinada maneira, exibindo sempre uma determinada resposta. Para tentativas de enumeração de usuários inválidos e/ou não cadastrados, a aplicação comporta-se de forma diferente. De acordo com esse comportamento, é possível enumerar quais são os válidos dos inválidos.

Impacto

É possível enumerar as contas válidas na aplicação, sendo usado em outros ataques ou como medida de coleta de informações.

Recomendação



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

Algumas das recomendações sugeridas são:

- Limitar a quantidade de chamadas efetuadas à aplicação.
- Implementar o reCAPTCHA da Google para bloquear a repetição do ataque.
- Implementar tokens e mecanismos que bloqueiem tentativas de ataques de força bruta/dicionário.
- Exibir mensagem genérica para casos de tentativas inválidos, ao invés de especificar o erro do usuário.
Por exemplo, caso digite o login inválido exibir a mensagem "Erro: Usuário e/ou senha inválido, verifique novamente o seu login" ao invés de "Erro: Usuário inválido, verifique novamente o seu login".

Links de referências

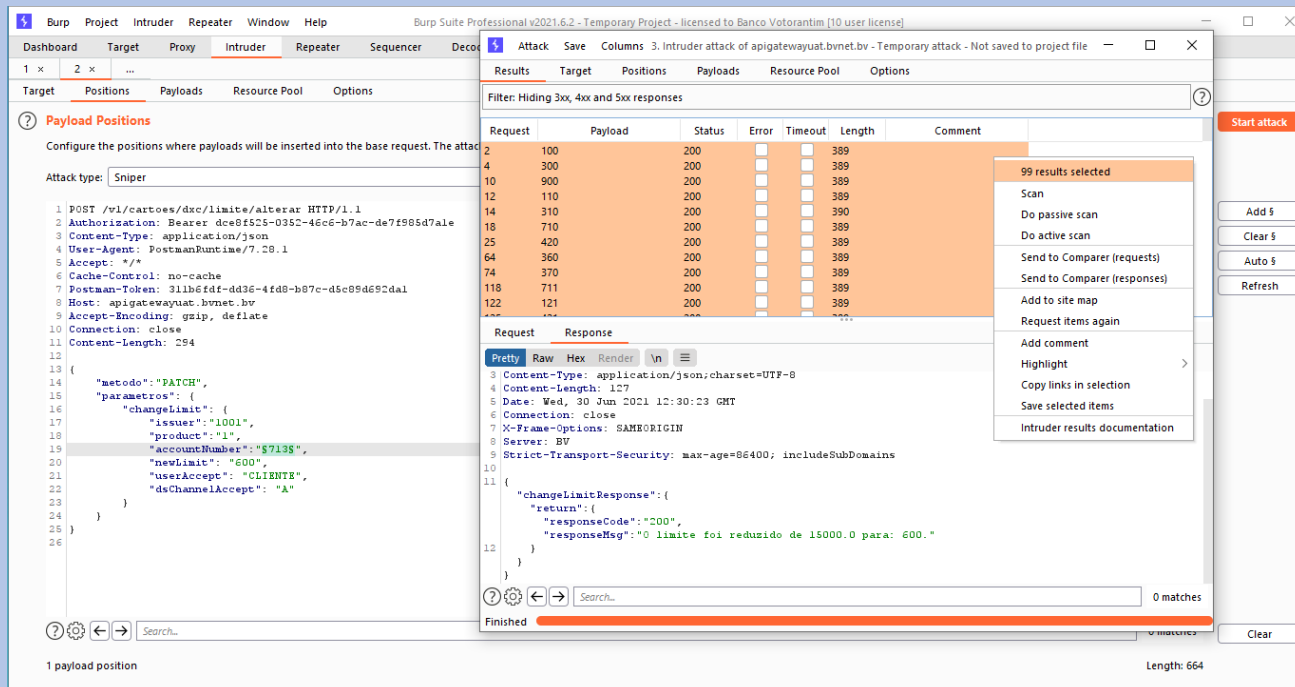
<https://cwe.mitre.org/data/definitions/307.html>

<https://cwe.mitre.org/data/definitions/203.html>

Evidências

Evidências CASP-15653:

Data: 30/06/2021



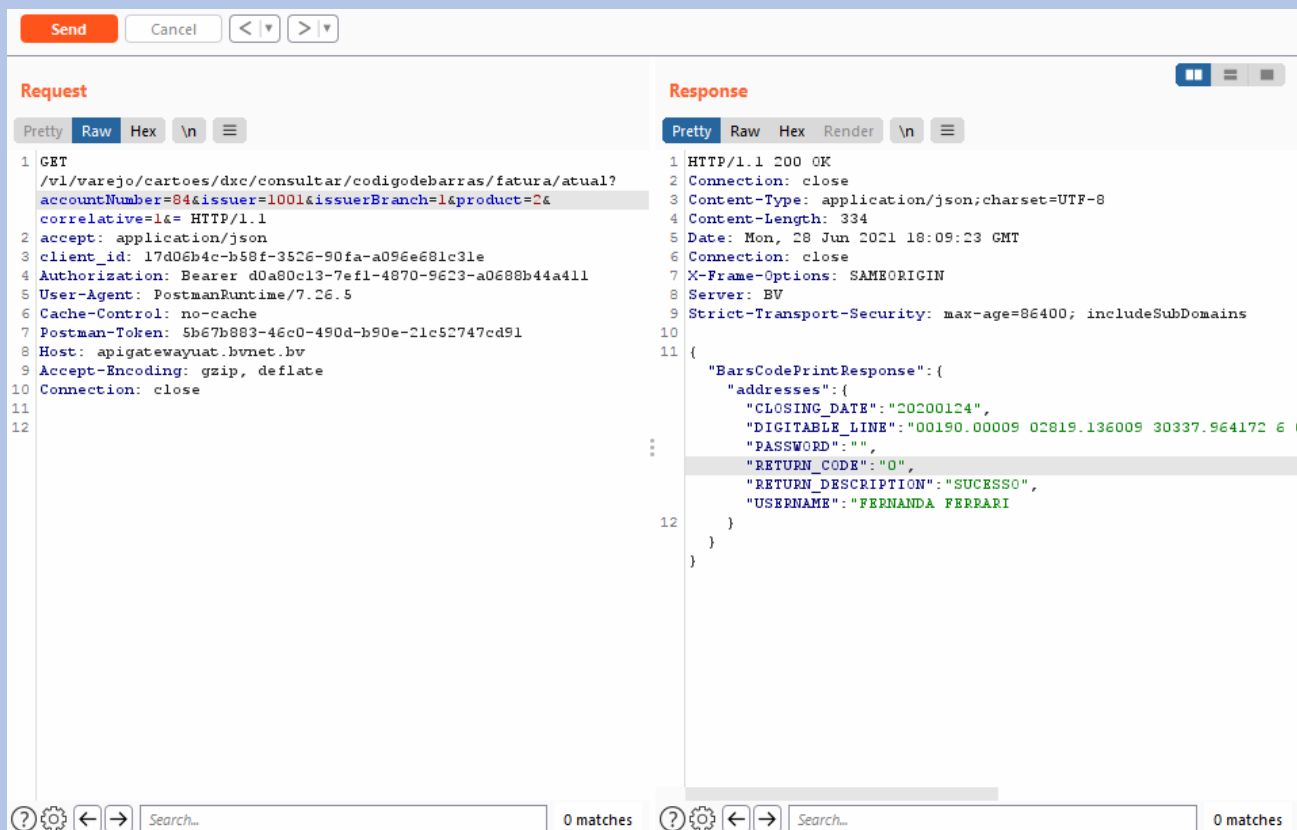
The screenshot displays the Burp Suite Professional interface during an Intruder attack. The 'Intruder' tab is active, showing a list of positions (1-26) and a 'Payload Positions' configuration window. The 'Attack type' is set to 'Sniper'. The 'Payloads' tab shows a list of payloads, including a 'PATCH' request with a 'parametros' object containing 'accountNumber', 'newLimit', and 'dsChannelAccept'. The 'Results' tab shows a table of request and response details, including status, error, timeout, length, and comment. A context menu is open over the results table, showing options like 'Scan', 'Do passive scan', 'Do active scan', 'Send to Comparer (requests)', 'Send to Comparer (responses)', 'Add to site map', 'Request items again', 'Add comment', 'Highlight', 'Copy links in selection', 'Save selected items', and 'Intruder results documentation'. The 'Start attack' button is visible on the right side of the interface.

Request	Payload	Status	Error	Timeout	Length	Comment
2	100	200			389	
4	300	200			389	
10	900	200			389	
12	110	200			389	
14	310	200			390	
18	710	200			389	
25	420	200			389	
64	360	200			389	
74	370	200			389	
118	711	200			389	
122	121	200			389	

Figura 9 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro accountNumber foi possível obter outras contas válidas na plataforma

Evidências CASP-15720:

Data: 28/06/2021



The screenshot displays a web browser window with a 'Request' tab selected. The request is a GET request to the following URL: `/v1/varejo/cartoes/dxc/consultar/codigobarras/fatura/atual?accountNumber=84&issuer=1001&issuerBranch=1&product=2&correlative=1&= HTTP/1.1`. The request headers include: `accept: application/json`, `client_id: 17d06b4c-b58f-3526-90fa-a096e681c31e`, `Authorization: Bearer d0a80c13-7ef1-4870-9623-a0688b44a411`, `User-Agent: PostmanRuntime/7.26.5`, `Cache-Control: no-cache`, `Postman-Token: 5b67b883-46c0-490d-b90e-21c52747cd91`, `Host: apigatewayuat.bvnet.bv`, `Accept-Encoding: gzip, deflate`, and `Connection: close`. The response is a JSON object with the following structure:

```
{  "BarsCodePrintResponse": {    "addresses": {      "CLOSING_DATE": "20200124",      "DIGITABLE_LINE": "00190.00009 02819.136009 30337.964172 6 (",      "PASSWORD": "",      "RETURN_CODE": "0",      "RETURN_DESCRIPTION": "SUCESSO",      "USERNAME": "FERNANDA FERRARI"    }  } }
```

Figura 10 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro accountNumber foi possível obter outras contas válidas na plataforma

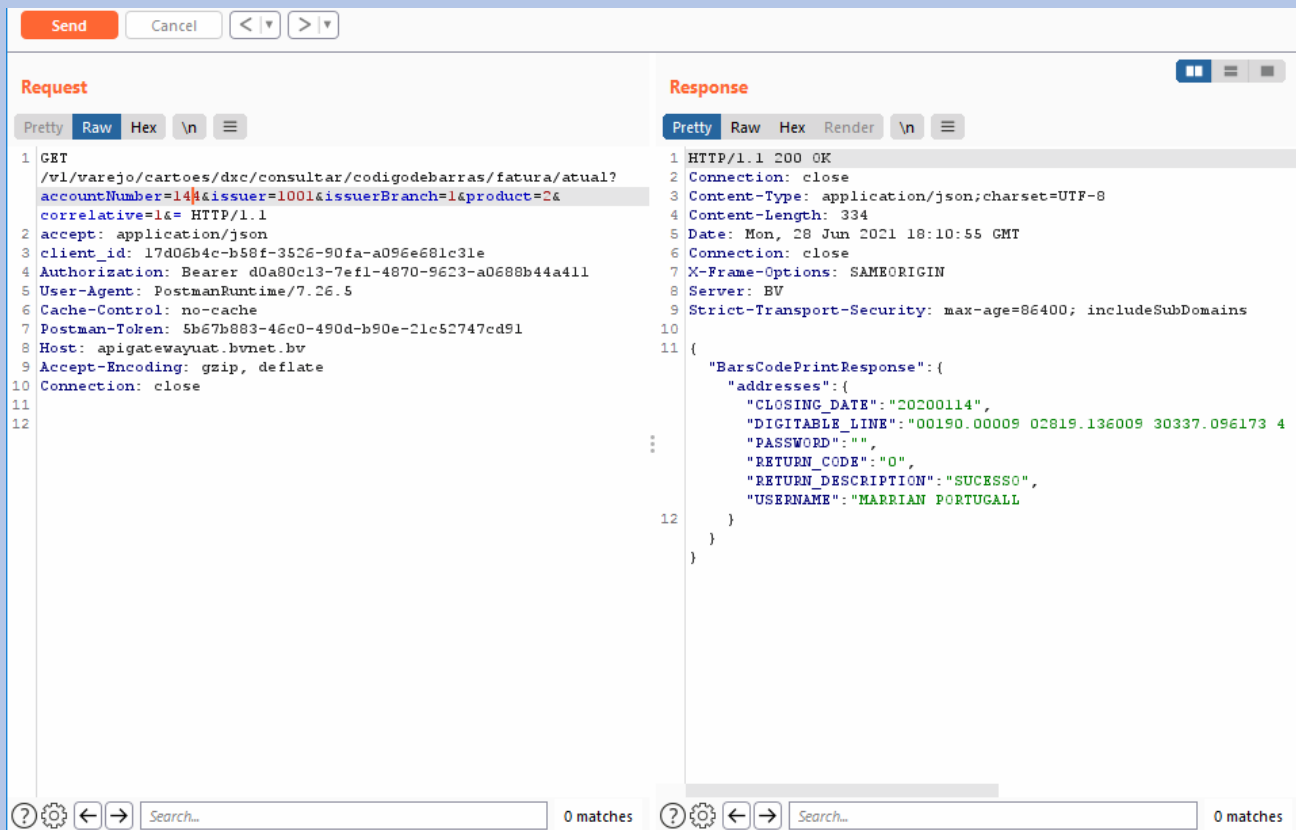
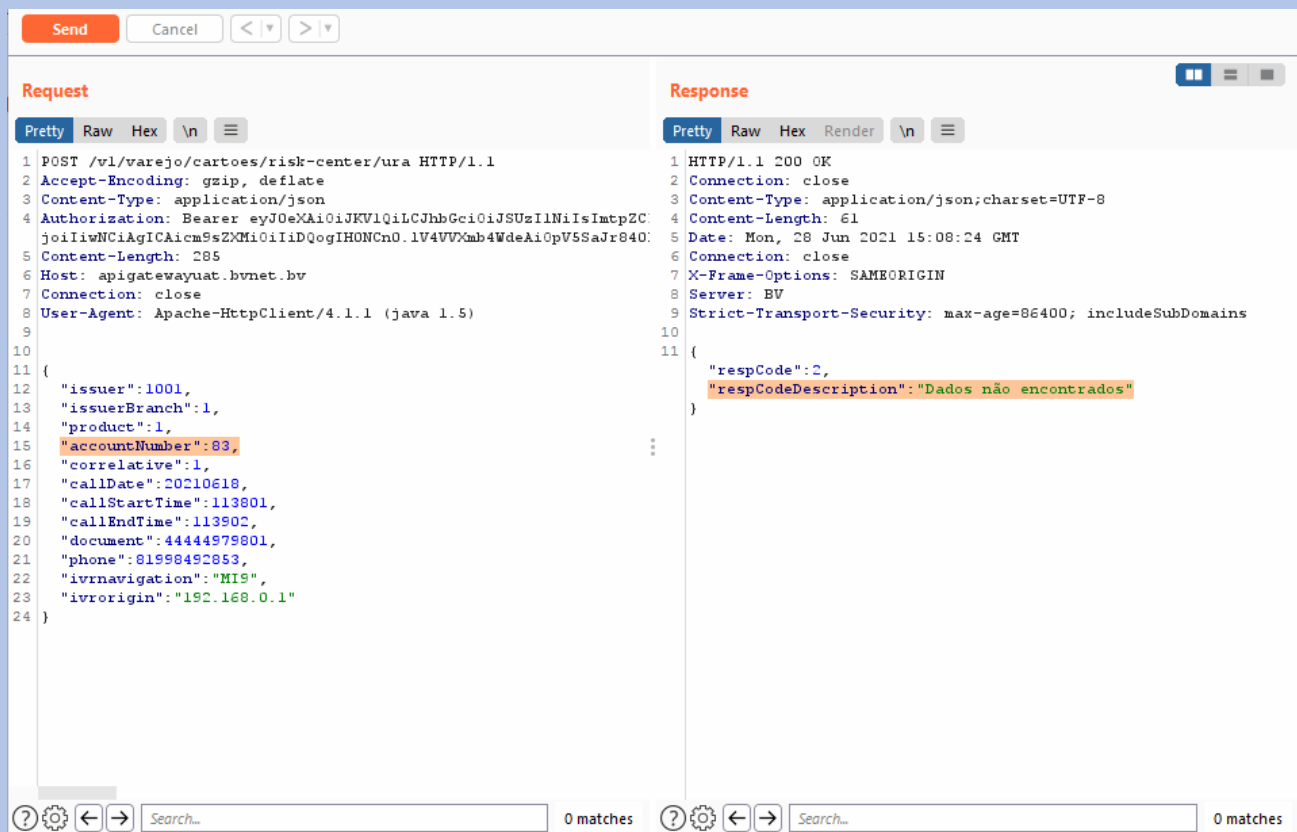


Figura 11 - Exploração da vulnerabilidade: Através de um ataque de força bruta no parâmetro accountNumber foi possível obter outras contas válidas na plataforma

Data: 28/06/2021

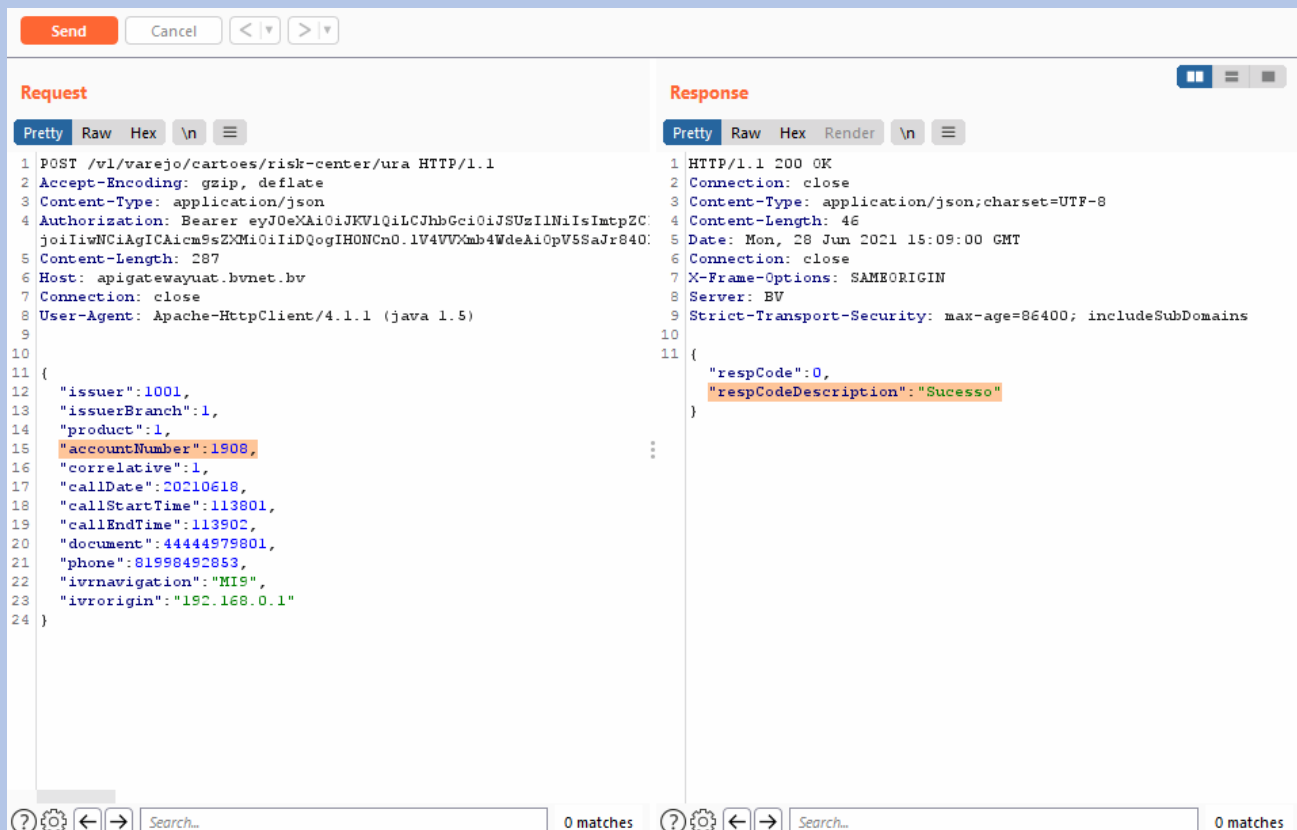
Request

```
1 POST /v1/varejo/cartoes/risk-center/ura HTTP/1.1
2 Accept-Encoding: gzip, deflate
3 Content-Type: application/json
4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjoiIiwNCiAgICAicm9sZXMiOiIiDQogIHONCn0.1V4VVXmb4WdeAiOpV5SaJr840:
5 Content-Length: 285
6 Host: apigatewayuat.bvnet.bv
7 Connection: close
8 User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
9
10 {
11   "issuer": "1001",
12   "issuerBranch": "1",
13   "product": "1",
14   "accountNumber": "83",
15   "correlative": "1",
16   "callDate": "20210618",
17   "callStartTime": "113801",
18   "callEndTime": "113902",
19   "document": "44444979801",
20   "phone": "81998492853",
21   "ivrnavigation": "MIS",
22   "ivrorigin": "192.168.0.1"
23 }
24
```

Response

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 61
5 Date: Mon, 28 Jun 2021 15:08:24 GMT
6 Connection: close
7 X-Frame-Options: SAMEORIGIN
8 Server: BV
9 Strict-Transport-Security: max-age=86400; includeSubDomains
10
11 {
12   "respCode": "2",
13   "respCodeDescription": "Dados não encontrados"
14 }
```

Figura 12 - Exploração da vulnerabilidade: Através da alteração dos valores no parâmetro `accountNumber`, é possível adquirir informações dos usuários ativos no sistema, através da mensagem retornada pelo servidor ("Dados não encontrados" para usuários inválidos e "Sucesso" para usuários válidos).



```
Request
1 POST /v1/varejo/cartoes/risk-center/ura HTTP/1.1
2 Accept-Encoding: gzip, deflate
3 Content-Type: application/json
4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjoiIiwNCiAgICAicm9sZXMiOiIiDQogIHONCn0.1V4VVXmb4WdeAiOpV5SaJr840.
5 Content-Length: 287
6 Host: apigatewayuat.bvnet.bv
7 Connection: close
8 User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
9
10 {
11   "issuer": "1001",
12   "issuerBranch": "1",
13   "product": "1",
14   "accountNumber": "1908",
15   "correlative": "1",
16   "callDate": "20210618",
17   "callStartTime": "113801",
18   "callEndTime": "113902",
19   "document": "44444979801",
20   "phone": "81998492853",
21   "ivrnavigation": "MIS",
22   "ivrorigin": "192.168.0.1"
23 }
24 }

Response
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 46
5 Date: Mon, 28 Jun 2021 15:09:00 GMT
6 Connection: close
7 X-Frame-Options: SAMEORIGIN
8 Server: BV
9 Strict-Transport-Security: max-age=86400; includeSubDomains
10
11 {
12   "respCode": 0,
13   "respCodeDescription": "Sucesso"
14 }
```

Figura 13 - Exploração da vulnerabilidade: Através da alteração dos valores no parâmetro accountNumber, é possível adquirir informações dos usuários ativos no sistema, através da mensagem retornada pelo servidor ("Dados não encontrados" para usuários inválidos e "Sucesso" para usuários válidos).

4

Nome - Vulnerabilidade

[APISJUN04-21 - 4] – Ataques de repetição SMS (Danos financeiros)

Impacto		Vulnerabilidade (Prob.)		Criticidade (Risco)	
Médio		Médio		Médio	
Sistema					
Relatório Semanal		Referência Ataque		Referência Vul.	
21/06/2021 a 30/06/2021		CAPEC		CWE	294

Resumo

Vulnerabilidade: [APISJUN04-21 - 4] – Ataques de repetição SMS (Danos financeiros)

Descrição: É possível enviar de forma automatizada vários SMS, a aplicação não tem nenhum controle de quantidade de envios e com isto é possível gerar danos financeiros ao banco.

Exemplo de dano financeiro:

Cada SMS tem o custo de R\$0,5 centavos por envio, neste teste foram enviados em 1 minuto 754 SM e com isto é gerado um custo de R\$377,00 reais.

Com esta base neste valor, se deixássemos o envio durante 1 hora o prejuízo seria de R\$22,620 mil reais e em 24 horas de R\$542,880 mil reais.

Recomendação: Configurar a aplicação para enviar no máximo 3 vezes seguidas um SMS para o mesmo número e após o envio bloquear durante alguns minutos ou gerar um segundo fator de confirmação de envio impedindo a repetição de SMS de forma automatizada.

Descrição – Situação Encontrada



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15614	caapi-cntf-base-processo-ass-eletr-reenvio	/v1/varejo/originacao/processo-assinatura/reenvio	0	Aberto

É possível enviar de forma automatizada vários sms, a aplicação não tem nenhum controle de quantidade de envios e com isto é possível gerar danos financeiros ao banco.

Impacto

Cada SMS tem o custo de R\$0,5 centavos por envio, neste teste foram enviados em 1 minuto 754 SMS e com isto é gerado um custo de R\$377,00 reais.

Com esta base neste valor, se deixássemos o envio durante 1 hora o prejuízo seria de R\$22,620 mil reais e em 24 horas de R\$542,880 mil reais.

Recomendação

Configurar a aplicação para enviar no máximo 3 vezes seguidas um SMS para o mesmo número e após o envio bloquear durante alguns minutos ou gerar um segundo fator de confirmação de envio impedindo a repetição de SMS de forma automatizada.

Links de referências

[CWE - CWE-294: Authentication Bypass by Capture-replay \(4.3\) \(mitre.org\)](#)

Evidências

Evidências CASP-15614:

Data: 24/06/2021

Request

PrettyRawInActions

```
1 POST /vl/varejo/originacao/processo-assinatura/reenvio HTTP/1.1
2 Content-Type: application/json
3 cache-control: no-cache
4 Postman-Token: la83lfcf-c597-4c47-a36e-cc567fe4727a
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6ImRlZmFibHRfc3NsX2tleSJSJS4joiIiwiaWF0IjAiOiIidQogIHNhcn0ubm4yMz0lc2NwV13aTYNIgxiYXZkdDflLTcrVSUSUegsydDngdGYCbD
6 User-Agent: PostmanRuntime/7.6.0
7 Accept: */*
8 Host: api-uat.bancovotorantim.com.br
9 Accept-Encoding: gzip, deflate
10 Content-Length: 35
11 Connection: close
12
13 {
14   "numeroProposta": 500695003
15 }
16
```

Response

PrettyRawRenderInActions

```
1 HTTP/1.1 200 OK
2 Date: Thu, 24 Jun 2021 06:36:31 GMT
3 Content-Type: application/json;charset=UTF-8
4 Content-Length: 48
5 Connection: close
6 Server: BV
7 Strict-Transport-Security: max-age=31536000; includeSubDomains
8
9 {
10   "mensagem": "Solicitacao realizada com sucesso"
11 }
```

Figura 14 - Exploração da vulnerabilidade: O sistema não apresenta nenhum mecanismo de bloqueio de inúmeras requisições partindo do mesmo endereço de ip dessa forma é possível enviar a mesma requisição diversas vezes causando danos financeiros

[illegible]

Figura 15 - Exploração da vulnerabilidade: O sistema não apresenta nenhum mecanismo de bloqueio de inúmeras requisições partindo do mesmo endereço de ip dessa forma é possível enviar a mesma requisição diversas vezes causando danos financeiros

5

Nome - Vulnerabilidade

[APISJUN04-21 - 5] – Validação incorreta

Impacto		Vulnerabilidade (Prob.)		Criticidade (Risco)	
Médio		Médio		Médio	
Sistema					
Relatório Semanal		Referência Ataque		Referência Vul.	
21/06/2021 a 30/06/2021		CAPEC		CWE	20

Resumo

Vulnerabilidade: [APISJUN04-21 - 5] – Validação incorreta**Descrição:** Dependendo dos valores inseridos como parâmetro de entrada, a aplicação não consegue processar corretamente os mesmos.**Recomendação:** Algumas das recomendações sugeridas são:

- Tratar erros em nível de servidor ou aplicação.
- Realizar o tratamento das informações de saída que a aplicação retorna ao usuário.
- Analisar e corrigir parâmetros de entrada e variáveis inadequadamente sanitizadas das requisições HTTP que causaram o erro na aplicação.

Descrição – Situação Encontrada

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15675	caapi-spag-pixx-devolucao-envio-v2	/v2/refunds	0	Aberto



Documento:

Relatório EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

Dependendo dos valores inseridos como parâmetro de entrada, a aplicação não consegue processar corretamente os mesmos.

Impacto

É possível fazer com que a aplicação aceite valores em determinados parâmetros de entrada, podendo causar lentidão no servidor (até mesmo criando um cenário de negação de serviço) ou causar erro na aplicação, fazendo-a com que exiba informações internas e/ou confidenciais.

Recomendação

Algumas das recomendações sugeridas são:

- Tratar erros em nível de servidor ou aplicação.
- Realizar o tratamento das informações de saída que a aplicação retorna ao usuário.
- Analisar e corrigir parâmetros de entrada e variáveis inadequadamente sanitizadas das requisições HTTP que causaram o erro na aplicação.

Links de referências

<https://cwe.mitre.org/data/definitions/20.html>

Evidências

Evidências CASP-15675:

Figura 16 - Exploração da vulnerabilidade: Para realizar a requisição de devolução é necessário de um valor para o parâmetro returnIdentification gerado através do endpoint v1/EndtoEndId

Classificação:
Confidencial

Proprietário:
Segurança da Informação

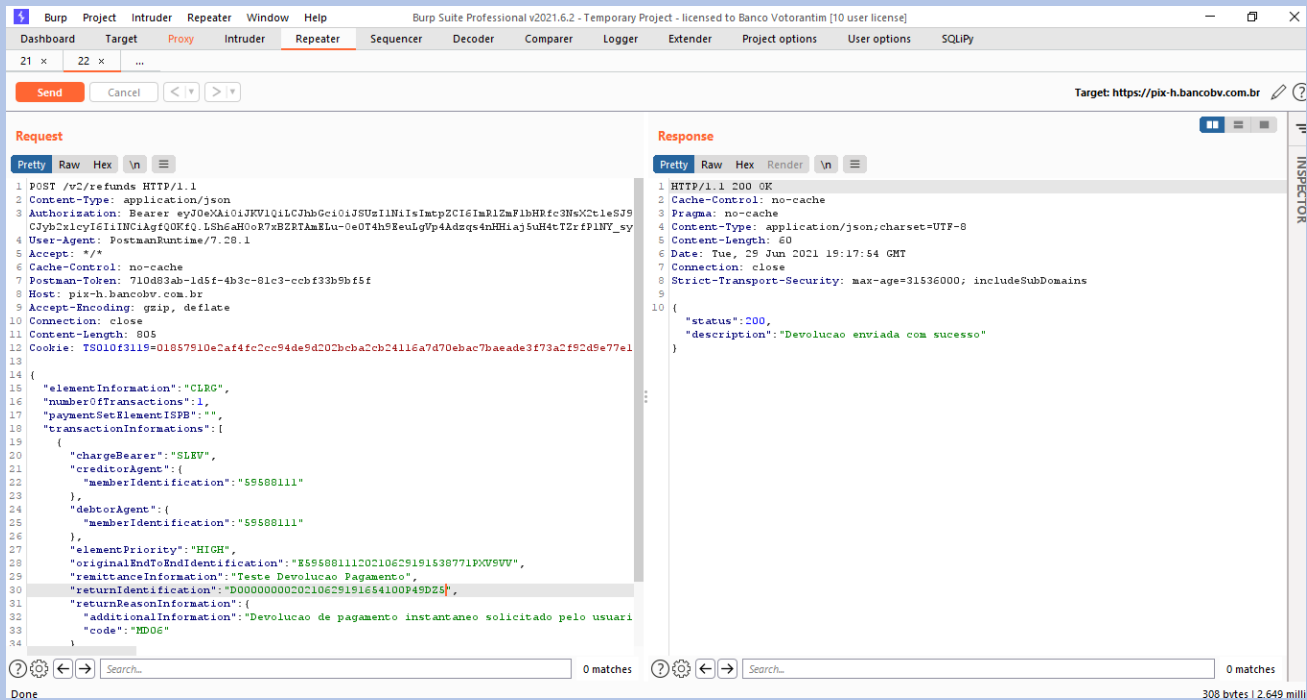


Figura 17 - Exploração da vulnerabilidade: Após o valor ser gerado através do endpoint `v1/EndtoEndId` é possível observar que no parâmetro `returnIdentification` o valor não é o mesmo do que foi gerando e mesmo assim a aplicação realiza o processamento da requisição evidenciando que o servidor não realiza a devida validação para saber se o valor inserido é de fato o valor gerado no endpoint `v1/EndtoEndId` dessa forma é possível enviar outro valor de identificação para o servidor impossibilitando a rastreabilidade da transação de devolução

6

Nome - Vulnerabilidade

[APISJUN04-21 - 6] – Validação incorreta de parâmetros de entrada

Impacto					Vulnerabilidade (Prob.)		Criticidade (Risco)	
Baixo					Baixo		Baixo	
Sistema								
Relatório Semanal					Referência Ataque		Referência Vul.	
21/06/2021 a 30/06/2021					CAPEC		CWE	20

Resumo

Vulnerabilidade: [APISJUN04-21 - 6] – Validação incorreta de parâmetros de entrada

Descrição: Dependendo dos valores inseridos como parâmetro de entrada, a aplicação não consegue processar corretamente os mesmos.

Recomendação: Algumas das recomendações sugeridas são:

- Tratar erros em nível de servidor ou aplicação.
- Realizar o tratamento das informações de saída que a aplicação retorna ao usuário.
- Analisar e corrigir parâmetros de entrada e variáveis inadequadamente sanitizadas das requisições HTTP que causaram o erro na aplicação.

Descrição – Situação Encontrada



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-10201	caapi-apro-cged-upload-documentacao-iged	/v1/varejo/originacao/documentolged/carregar	0	Aberto
CASP-13686	caapi-srec-base-recalculo-operacao	/atacado/srec/v1/notificacoes-alteracao-operacao	0	Aberto
CASP-15510	caapi-bvad-atou-atend-resgate-programa-pontos	/v1/banco-digital/atend/pua/cartoes/resgate/pontos/cliente	0	Aberto
CASP-15582	caapi-apro-cpvg-salvar-dados-bancarios	/v1/proposta/salva/dados Bancarios	0	Aberto

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-14409	caapi-bvad-base-usuario-cliente-salesforce-v2	/v2/banco-digital/parceiros/salesforce/cliente/dados/inserir	0	Aberto
CASP-15653	caapi-cart-svhp-limite-alterar-dxc	/v1/cartoes/dxc/limite/alterar	0	Aberto
CASP-15666	caapi-bvad-base-atualiza-dados-protocolo-sfc	/v1/banco-digital/atualiza/dados-protocolo	0	Aberto
CASP-15668	caapi-intb-base-usuario-master-consulta	/v1/atacado/usuario-master/consultar	0	Aberto



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15675	caapi-spag-pixx-devolucao-envio-v2	/v2/refunds	0	Aberto
CASP-15765	caapi-cart-base-risk-center-ura	/v1/varejo/cartoes/risk-center/ura	0	Aberto

Dependendo dos valores inseridos como parâmetro de entrada, a aplicação não consegue processar corretamente os mesmos.

Impacto

É possível fazer com que a aplicação aceite valores em determinados parâmetros de entrada, podendo causar lentidão no servidor (até mesmo criando um cenário de negação de serviço) ou causar erro na aplicação, fazendo-a com que exiba informações internas e/ou confidenciais.

Recomendação

Algumas das recomendações sugeridas são:

- Tratar erros em nível de servidor ou aplicação.
- Realizar o tratamento das informações de saída que a aplicação retorna ao usuário.
- Analisar e corrigir parâmetros de entrada e variáveis inadequadamente sanitizadas das requisições HTTP que causaram o erro na aplicação.

Links de referências

<https://cwe.mitre.org/data/definitions/20.html>

Evidências CASP-13686:

Data: 29/06/2021

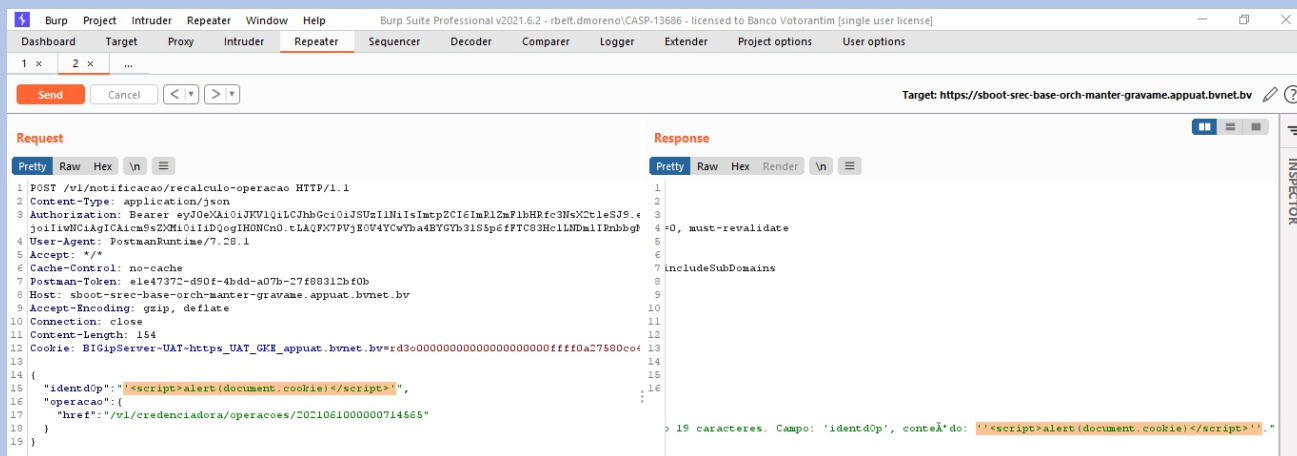
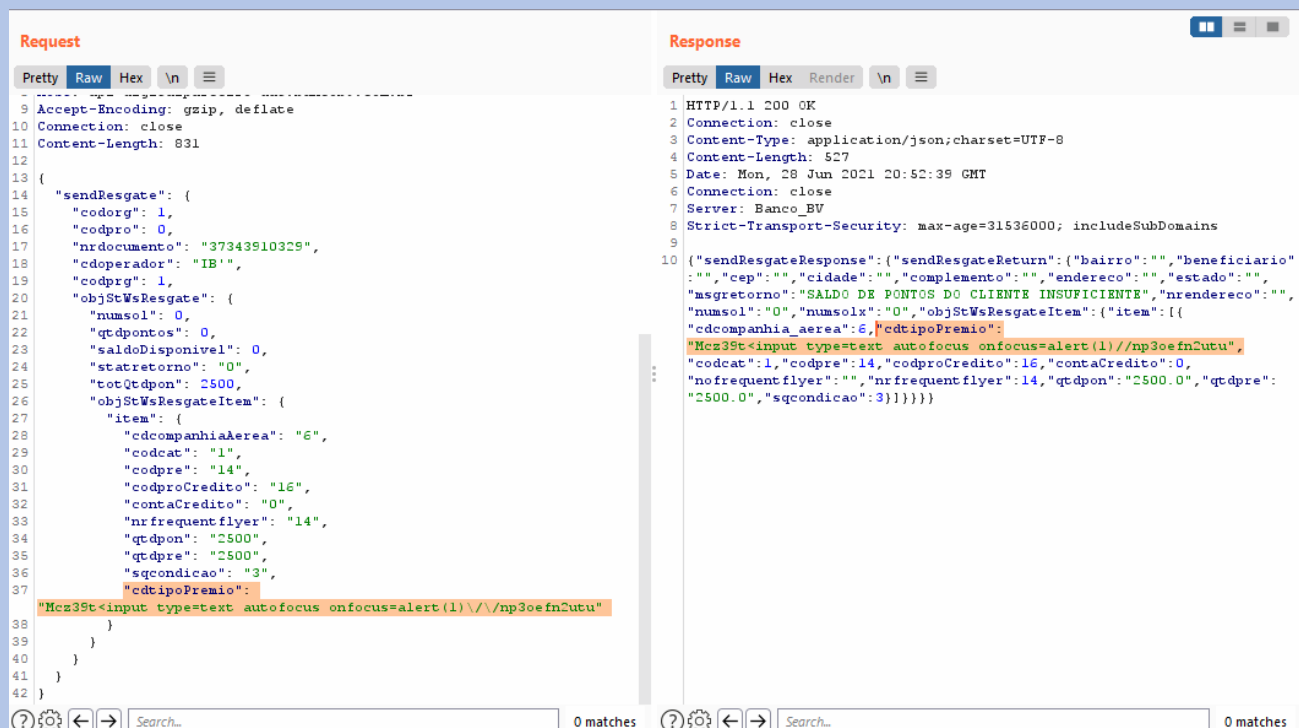


Figura 19 - Exploração da vulnerabilidade: Inserindo uma string maliciosa no campo `identdOp` da requisição, é possível verificar que o servidor realizar o processamento da requisição normalmente, evidenciando que o sistema não realiza o devido tratamento dos parâmetros.

Evidências CASP-15510:

Data: 28/06/2021



```
Request
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 831
{
  "sendResgate": {
    "codorg": 1,
    "codpro": 0,
    "nrdocumento": "37343910329",
    "cdoperador": "IB",
    "codprg": 1,
    "objStWsResgate": {
      "numsol": 0,
      "qtdpontos": 0,
      "saldoDisponivel": 0,
      "statretorno": "0",
      "totQtDpon": 2500,
      "objStWsResgateItem": {
        "item": {
          "cdcompanhiaAerea": "6",
          "codcat": "1",
          "codpre": "14",
          "codproCredito": "16",
          "contaCredito": "0",
          "nrfrequentflyer": "14",
          "qtdpon": "2500",
          "qtdpre": "2500",
          "sqcondicao": "3",
          "cdtipoPremio": "Mc39t<input type=text autofocus onfocus=alert(1)\\np3oefn2utu"
        }
      }
    }
  }
}

Response
HTTP/1.1 200 OK
Connection: close
Content-Type: application/json; charset=UTF-8
Content-Length: 527
Date: Mon, 28 Jun 2021 20:52:39 GMT
Connection: close
Server: Banco_BV
Strict-Transport-Security: max-age=31536000; includeSubDomains
{"sendResgateResponse":{"sendResgateReturn":{"bairro":"","beneficiario":"","cep":"","cidade":"","complemento":"","endereco":"","estado":"","msgretorno":"SALDO DE PONTOS DO CLIENTE INSUFICIENTE","nrendereco":"","numsol":"0","numsolx":"0","objStWsResgateItem":{"item":{"cdcompanhia_aerea":"6","cdtipoPremio":"Mc39t<input type=text autofocus onfocus=alert(1)\\np3oefn2utu","codcat":"1","codpre":"14","codproCredito":"16","contaCredito":"0","nrfrequentflyer":"","nrfrequentflyer":"14","qtdpon":"2500.0","qtdpre":"2500.0","sqcondicao":"3"}}}}}}
```

Figura 20 - Exploração da vulnerabilidade: Inserindo uma string maliciosa no parâmetro de entrada `cdtipoPremio` o servidor realizar o processamento da requisição normalmente evidenciando que o sistema não realiza o devido tratamento dos parâmetros

Evidências CASP-15582:

Data: 25/06/2021

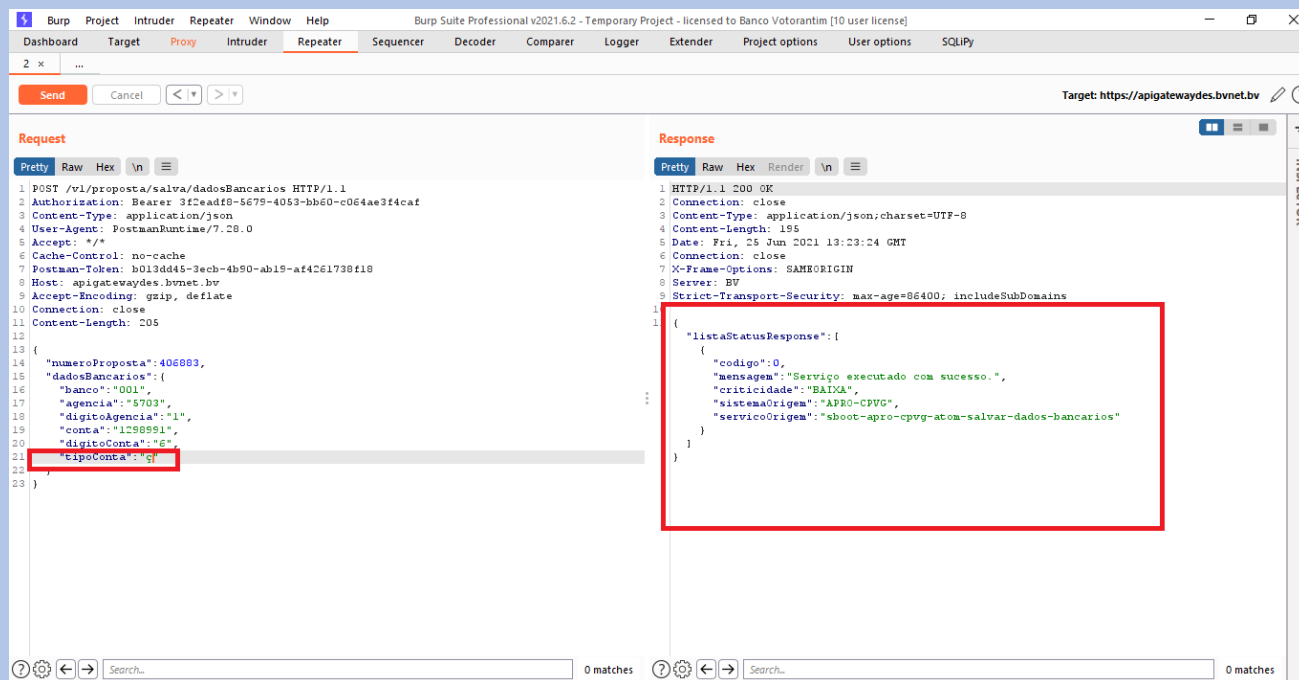


Figura 21 - Exploração da vulnerabilidade: Inserindo uma string maliciosa no parâmetro de entrada tipoConta o servidor realizar o processamento da requisição normalmente evidenciando que o sistema não realiza o devido tratamento dos parâmetros

Evidências CASP-14409:

Data: 25/06/2021

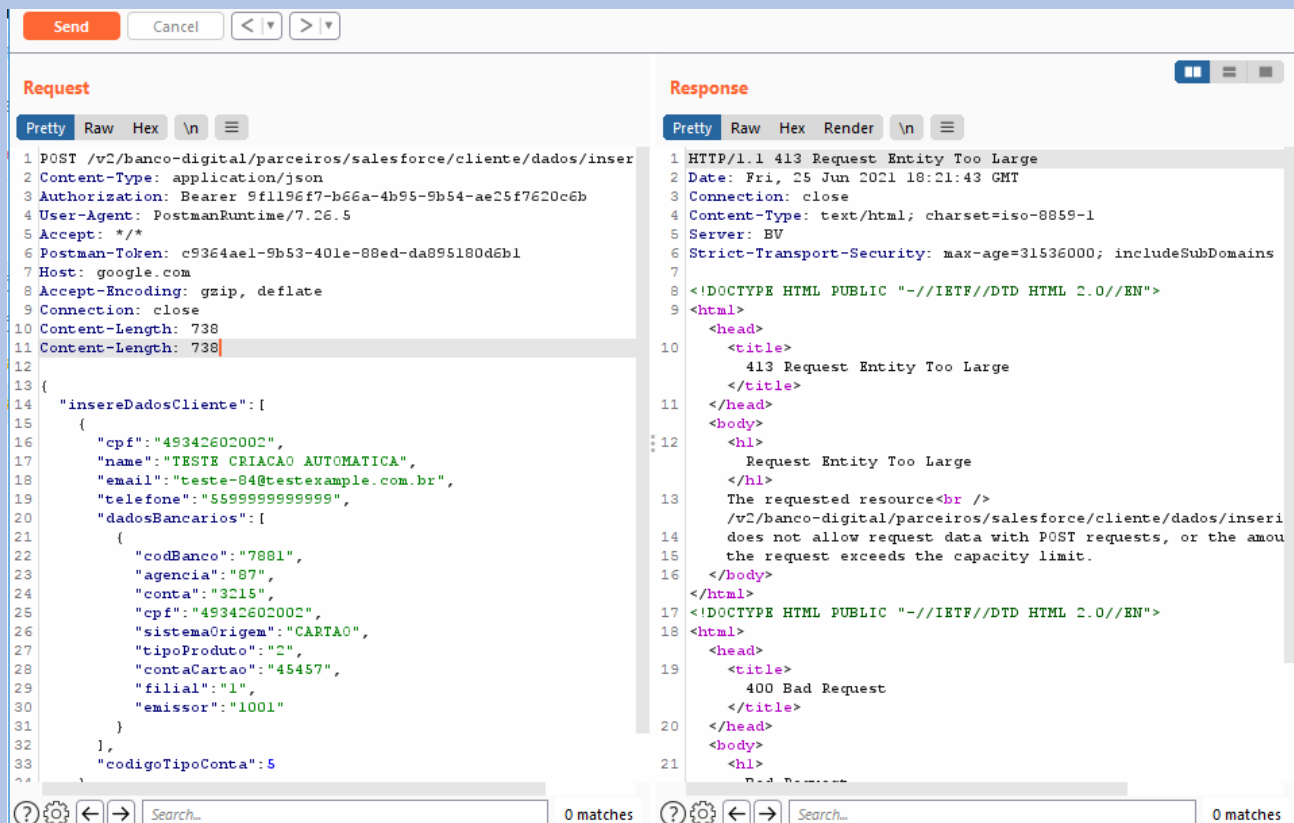


Figura 22 - Exploração da vulnerabilidade: Inserindo o parametro content-length duplicado na requisição, é possível gerar uma mensagem de erro não padronizada, proveniente do servidor.

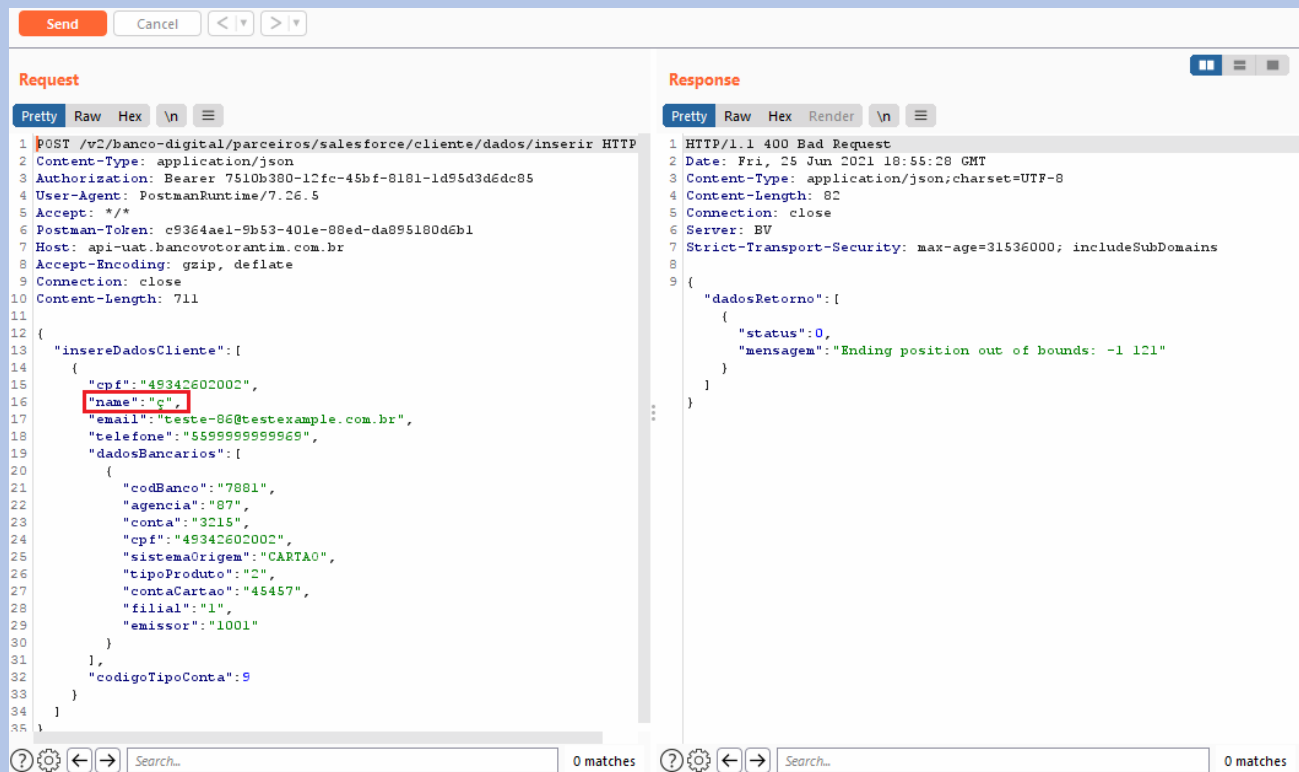


Figura 23 - Exploração da vulnerabilidade: Inserindo o caractere malicioso no parâmetro name, é possível gerar uma mensagem de erro proveniente do servidor.

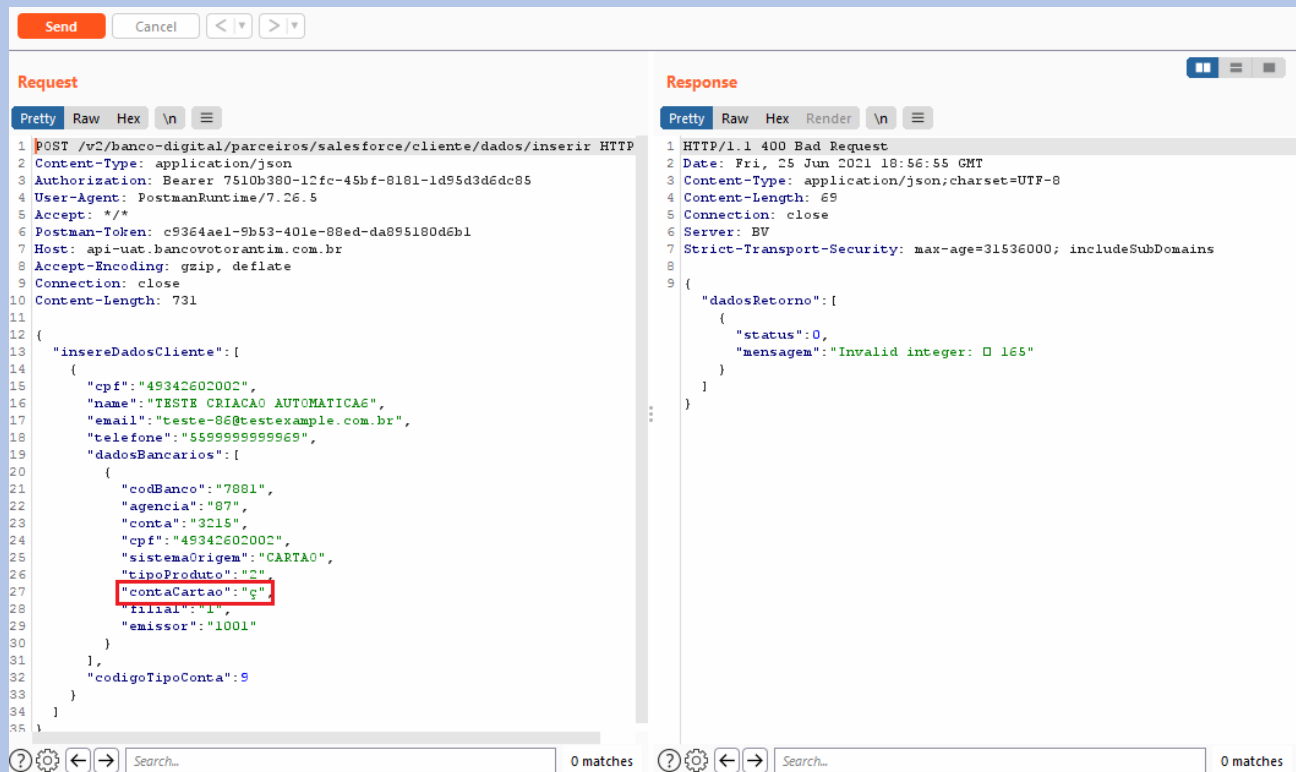
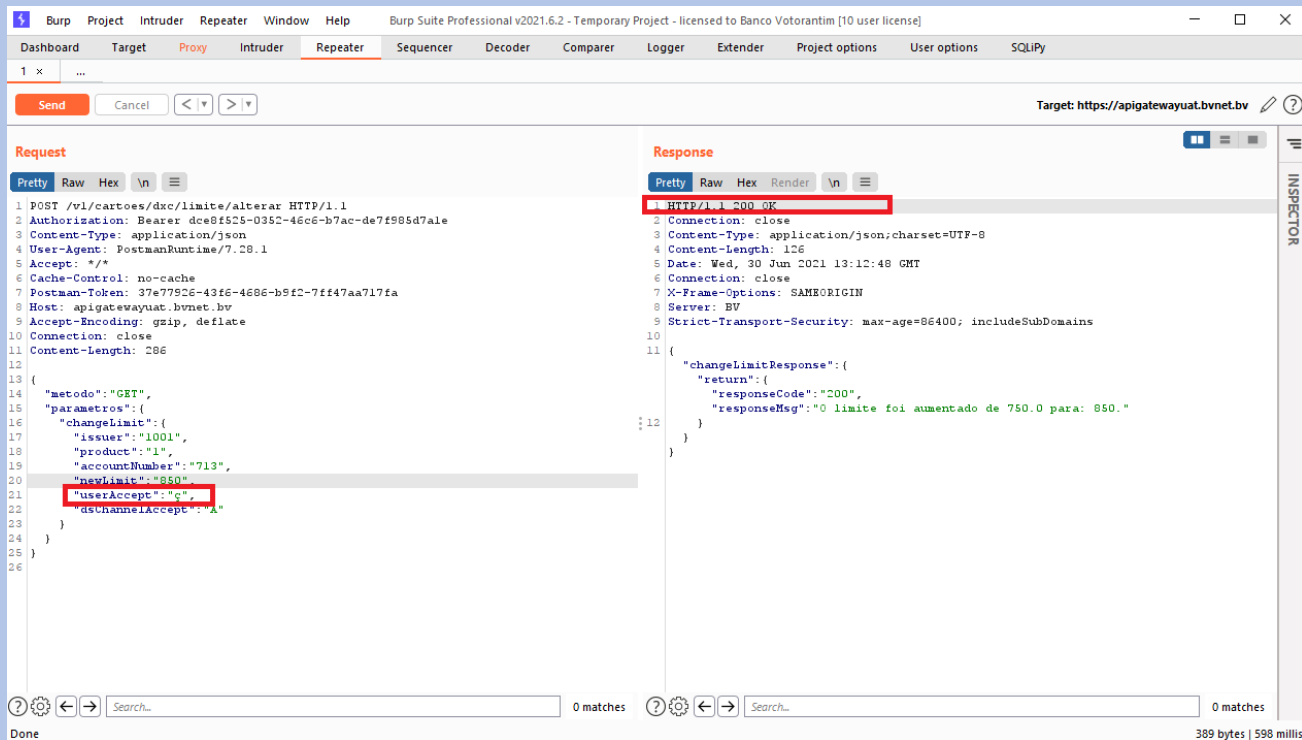


Figura 24 - Exploração da vulnerabilidade: Inserindo o caractere malicioso no parâmetro `contaCartao`, é possível gerar uma mensagem de erro proveniente do servidor.

Data: 30/06/2021



The screenshot displays the Burp Suite Professional interface. The 'Repeater' tab is active, showing a single request. The request is a POST to `/v1/cartoes/dxc/limite/alterar` with a Bearer token. The request body is a JSON object with fields: `metodo`, `parametros` (containing `changeLimit` with `issuer`, `product`, `accountNumber`, `newLimit`, `userAccept`, and `dstChannelAccept`). The `userAccept` field is highlighted with a red box. The response is an HTTP/1.1 200 OK with a JSON body: `{ "changeLimitResponse": { "return": { "responseCode": "200", "responseMsg": "O limite foi aumentado de 750.0 para: 850." } } }`. The `HTTP/1.1 200 OK` status line is also highlighted with a red box.

Figura 25 - Exploração da vulnerabilidade: Inserindo uma string maliciosa no parâmetro de entrada `userAccept` o servidor realizar o processamento da requisição normalmente evidenciando que o sistema não realiza o devido tratamento dos parâmetros

Evidências CASP-15666:

Data: 25/06/2021

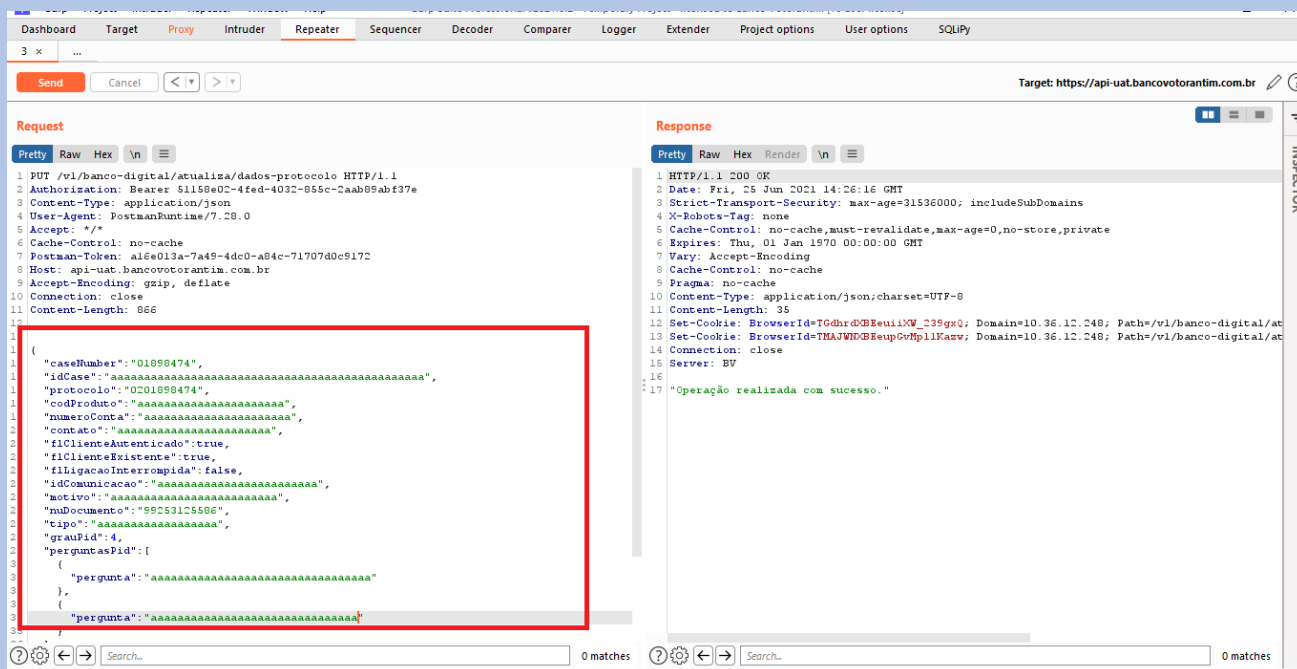


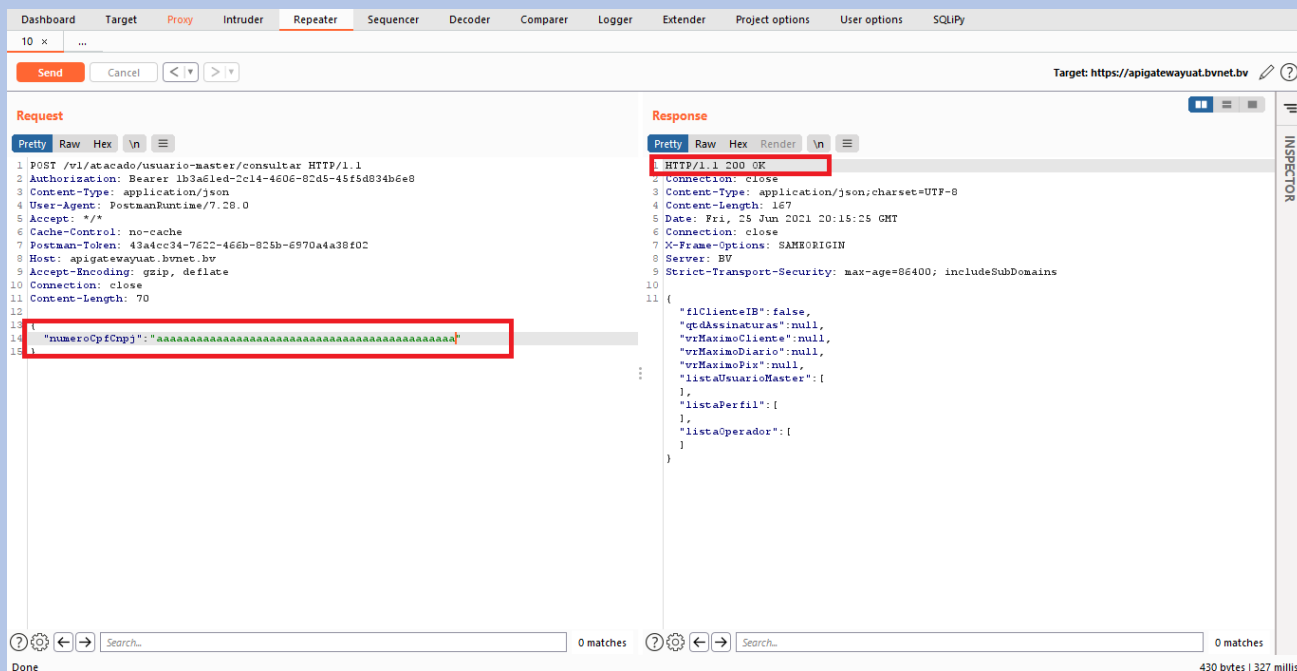
Figura 26 - Exploração da vulnerabilidade: Inserindo uma string maliciosa nos parâmetros de entrada o servidor realizar o processamento da requisição normalmente evidenciando que o sistema não realiza o devido tratamento dos parâmetros

Evidências CASP-15668:

Classificação:
Confidencial

Proprietário:
Segurança da Informação

Data: 25/06/2021



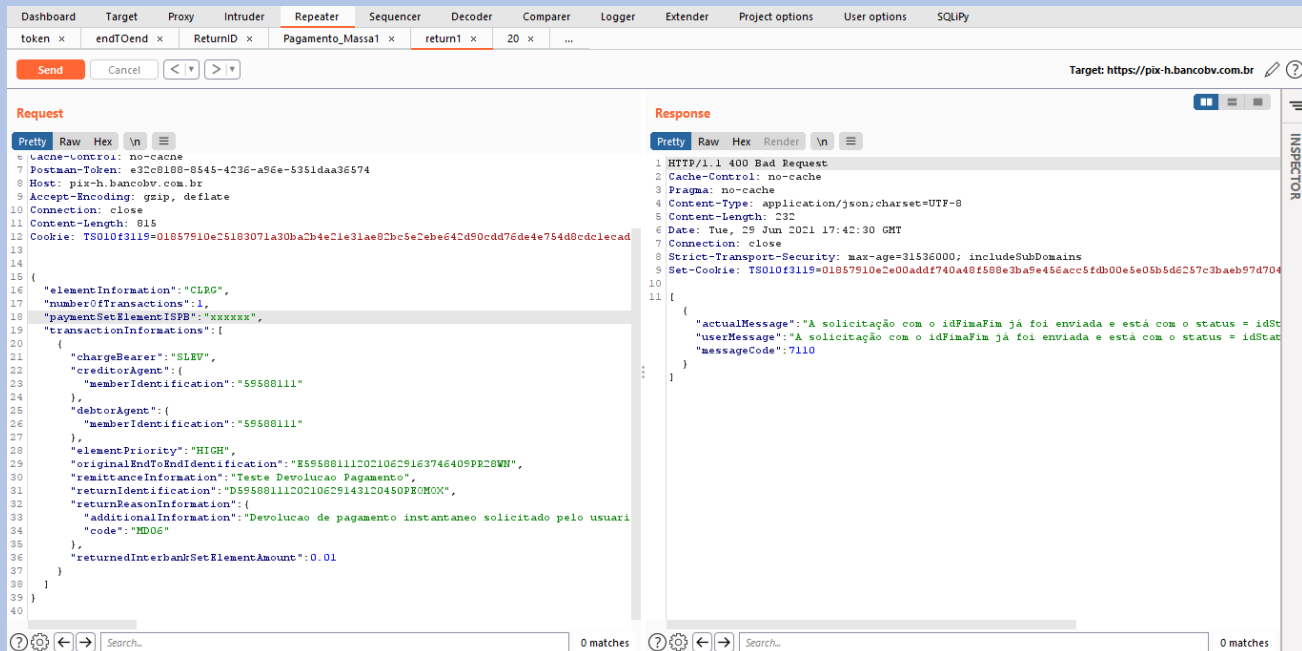
The screenshot shows a web security tool interface with a 'Repeater' tab selected. The target is 'https://apigatewayuat.bvnet.bv'. The request is a POST to '/v1/atacado/usuario=master/consultar' with a 'Bearer' token. The response is a 200 OK with a JSON body. A red box highlights the 'numeroCpfCnpj' parameter in the request body, which contains a long string of 'a' characters. Another red box highlights the 'HTTP/1.1 200 OK' status line in the response.

Figura 27 - Exploração da vulnerabilidade: Inserindo uma string maliciosa no parâmetro de entrada o servidor realizar o processamento da requisição normalmente evidenciando que o sistema não realiza o devido tratamento dos parâmetros

Evidências CASP-15675:

Classificação:
ConfidencialProprietário:
Segurança da Informação

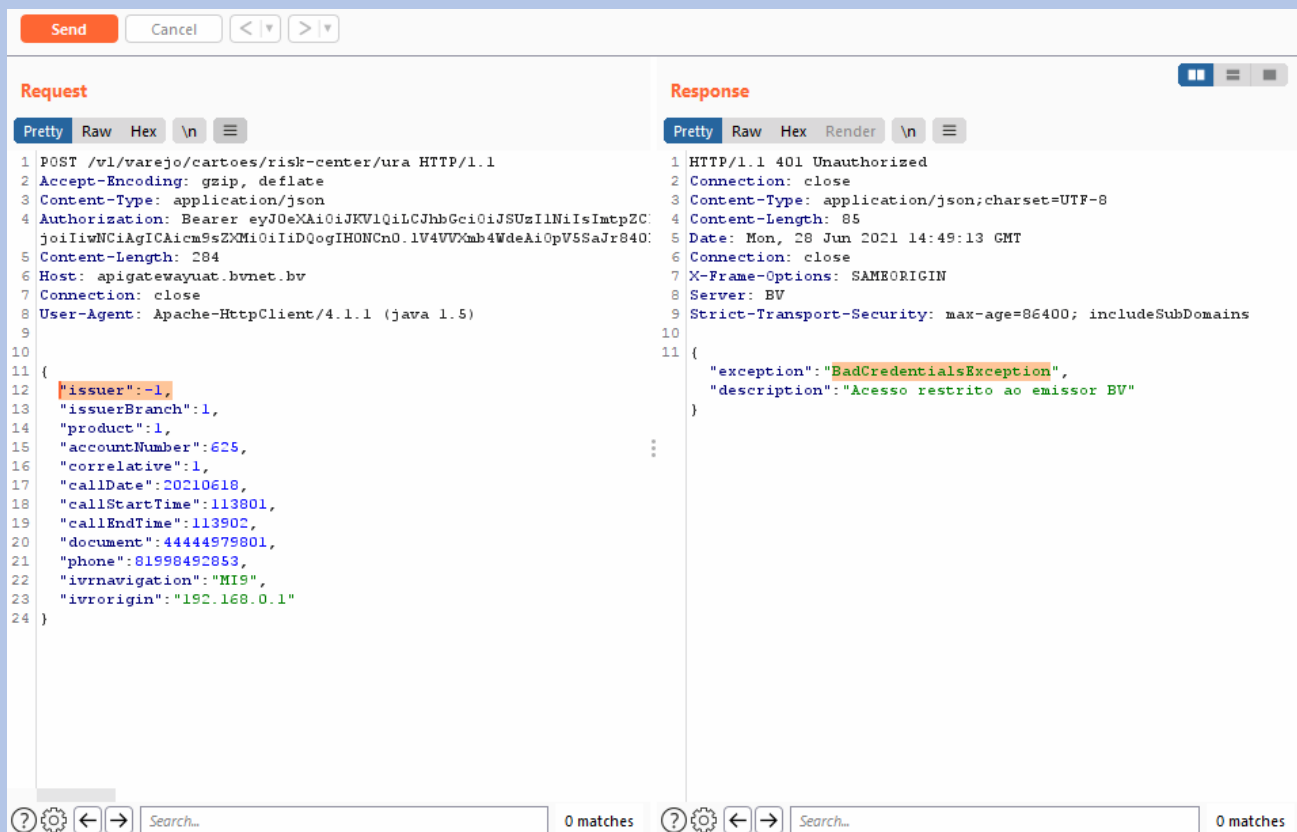
Data: 29/06/2021



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is 'https://pix-h.bancobv.com.br'. The request is a POST to '/pix-h.bancobv.com.br' with a 'Content-Type' of 'application/json'. The request body is a JSON object containing transaction information, including a malicious string 'XXXXXX' in the 'paymentSetElementISPB' field. The response is a '400 Bad Request' with a message indicating that the request is invalid due to the malicious input.

```
Request
Pretty Raw Hex \n
1 Cache-Control: no-cache
2 Postman-Token: e32c8188-8545-4236-a96e-5351daa36574
3 Host: pix-h.bancobv.com.br
4 Accept-Encoding: gzip, deflate
5 Connection: close
6 Content-Length: 815
7 Cookie: TS010f3119=01857910e25183071a30ba2b4e21e31ae82bc5e2ebe642d90cdd76de4e754d8dc1ecad
8
9 {
10   "elementInformation": "CLAG",
11   "numberOfTransactions": 1,
12   "paymentSetElementISPB": "XXXXXX",
13   "transactionInformation": {
14     "chargeBearer": "SLEV",
15     "creditorAgent": {
16       "memberIdentification": "59580111"
17     },
18     "debtorAgent": {
19       "memberIdentification": "59580111"
20     },
21     "elementPriority": "HIGH",
22     "originalEndToEndIdentification": "E5958011120210629163746409PR20WN",
23     "remittanceInformation": "Texto Devolucao Pagamento",
24     "returnIdentification": "D5958011120210629143120450PR0MOX",
25     "returnReasonInformation": {
26       "additionalInformation": "Devolucao de pagamento instantaneo solicitado pelo usuario",
27       "code": "MD06"
28     },
29     "returnedInterbankSetElementAmount": 0.01
30   }
31 }
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
```

Data: 28/06/2021



Request

```
1 POST /v1/varejo/cartoes/risk-center/ura HTTP/1.1
2 Accept-Encoding: gzip, deflate
3 Content-Type: application/json
4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjoiIiwNCiAgICAicm9sZXMiOiIiDQogIHONCn0.1V4VVXmb4WdeAiOpV5SaJr840:
5 Content-Length: 284
6 Host: apigatewayuat.bvnet.bv
7 Connection: close
8 User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
9
10
11 {
12   "issuer": "-1",
13   "issuerBranch": 1,
14   "product": 1,
15   "accountNumber": 625,
16   "correlative": 1,
17   "callDate": 20210618,
18   "callStartTime": 113801,
19   "callEndTime": 113902,
20   "document": 44444979801,
21   "phone": 81998492853,
22   "ivrnavigation": "M19",
23   "ivrorigin": "192.168.0.1"
24 }
```

Response

```
1 HTTP/1.1 401 Unauthorized
2 Connection: close
3 Content-Type: application/json; charset=UTF-8
4 Content-Length: 85
5 Date: Mon, 28 Jun 2021 14:49:13 GMT
6 Connection: close
7 X-Frame-Options: SAMEORIGIN
8 Server: BV
9 Strict-Transport-Security: max-age=86400; includeSubDomains
10
11 {
12   "exception": "BadCredentialsException",
13   "description": "Acesso restrito ao emissor BV"
14 }
```

Figura 29 - Exploração da vulnerabilidade: Inserindo uma string maliciosa no campo issuer da requisição, é possível gerar uma mensagem de erro proveniente do servidor.



Documento:
Relatorio EHT

APISJUN04-21

Data:
30/06/2021

Classificação:
Confidencial

Proprietário:
Segurança da Informação

Evidências - Reteste de APIs

EVIDÊNCIAS DE
RETESTE DAS APIS DO
BANCO VOTORANTIM



Documento:
Relatorio EHT

APISJUN04-21

Data:
30/06/2021

Classificação:
Confidencial

Proprietário:
Segurança da Informação

Nome - Vulnerabilidade

1

[APISJUN04-21 - 1] – Exposição de informações (login exposto na URL)

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-10376	caapi-apro-base-proposta-comercial-veiculo-v4	/v4/varejo/contratacao/pr oposta-veiculos/proposta	0	Aberto

Evidências

Reteste CASP-10376:



2

Nome - Vulnerabilidade

[APISJUN04-21 - 2] – Enumeração de CPFs válidos

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-13340	caapi-spag-pixx-identificador-gerar	/v1/EndToEndId	0	Aberto
CASP-15510	caapi-bvad-atou-atend-resgate-programa-pontos	/v1/banco-digital/atend/pua/cartoes/resgate/pontos/cliente	0	Aberto
CASP-14409	caapi-bvad-base-usuario-cliente-salesforce-v2	/v2/banco-digital/parceiros/salesforce/cliente/dados/inserir	0	Aberto
CASP-15668	caapi-intb-base-usuario-master-consulta	/v1/atacado/usuario-master/consultar	0	Aberto

Evidências

Reteste CASP-13340:

Reteste CASP-15510:

Reteste CASP-14409:

Reteste CASP-15668:

3

Nome - Vulnerabilidade

[APISJUN04-21 - 3] – Enumeração de usuários

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15653	caapi-cart-svhp-limite-alterar-dxc	/v1/cartoes/dxc/limite/alterar	0	Aberto
CASP-15720	caapi-cart-svhp-consultar-codigodebarras-fatura-atual-dxc	/v1/varejo/cartoes/dxc/consultar/codigodebarras/fatura/atual	0	Aberto
CASP-15765	caapi-cart-base-risk-center-ura	/v1/varejo/cartoes/risk-center/ura	0	Aberto

Evidências

Reteste CASP-15653:

Reteste CASP-15720:

Reteste CASP-15765:



Documento:
Relatorio EHT

APISJUN04-21

Data:
30/06/2021

Classificação:
Confidencial

Proprietário:
Segurança da Informação

4

Nome - Vulnerabilidade

[APISJUN04-21 - 4] – Ataques de repetição SMS (Danos financeiros)

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15614	caapi-cntf-base-processo-ass-eletr-reenvio	/v1/varejo/originacao/processo-assinatura/reenvio	0	Aberto

Evidências

Reteste CASP-15614:



Documento:
Relatorio EHT

APISJUN04-21

Data:
30/06/2021

Classificação:
Confidencial

Proprietário:
Segurança da Informação

5

Nome - Vulnerabilidade

[APISJUN04-21 - 5] – Validação incorreta

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15675	caapi-spag-pixx-devolucao-envio-v2	/v2/refunds	0	Aberto

Evidências

Reteste CASP-15675:

6

Nome - Vulnerabilidade

[APISJUN04-21 - 6] – Validação incorreta de parâmetros de entrada

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-10201	caapi-apro-cged-upload-documentacao-iged	/v1/varejo/originacao/documentolged/carregar	0	Aberto
CASP-13686	caapi-srec-base-recalculo-operacao	/atacado/srec/v1/notificacoes-alteracao-operacao	0	Aberto
CASP-15510	caapi-bvad-atou-atend-resgate-programa-pontos	/v1/banco-digital/atend/pua/cartoes/resgate/pontos/cliente	0	Aberto
CASP-15582	caapi-apro-cpvg-salvar-dados-bancarios	/v1/proposta/salva/dados Bancarios	0	Aberto



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-14409	caapi-bvad-base-usuario-cliente-salesforce-v2	/v2/banco-digita/parceiros/salesforce/cliente/dados/inserir	0	Aberto
CASP-15653	caapi-cart-svhp-limite-alterar-dxc	/v1/cartoes/dxc/limite/alterar	0	Aberto
CASP-15666	caapi-bvad-base-atualiza-dados-protocolo-sfc	/v1/banco-digital/atualiza/dados-protocolo	0	Aberto
CASP-15668	caapi-intb-base-usuario-master-consulta	/v1/atacado/usuario-master/consultar	0	Aberto

CAPS-EHT	Componentes Afetados	Endpoints	Reteste	Status
CASP-15675	caapi-spag-pixx-devolucao-envio-v2	/v2/refunds	0	Aberto
CASP-15765	caapi-cart-base-risk-center-ura	/v1/varejo/cartoes/risk-center/ura	0	Aberto

Evidências

Reteste CASP-10201:

Reteste CASP-13686:

Reteste CASP-15510:

Reteste CASP-15582:



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

Reteste CASP-14409:

Reteste CASP-15653:

Reteste CASP-15666:

Reteste CASP-15668:

Reteste CASP-15675:

Reteste CASP-15765:



Documento:

Relatorio EHT

APISJUN04-21

Data:

30/06/2021

Classificação:

Confidencial

Proprietário:

Segurança da Informação

5. Referências Técnicas

- Penetration Testing Guidance - PCI Security Standards Council -
https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
- Owasp Testing Guide – Open Web Application Security Project -
https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- Owasp Top Ten Project – Open Web Application Security Project -
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project