



CWI SOFTWARE

Segurança Web OWASP 2013 - TOP 10

*O software que você procura talvez não exista,
mas a empresa que irá fabricá-lo sim.*

www.cwi.com.br

OWASP Foundation



OWASP

Open Web Application
Security Project

Por que se preocupar com isso?

Reported Russian Cyber Attack Shuts Down Pentagon Network

Hackers believed to be associated with Russia used 'new and unseen' methods.



Russia carried out a cyberattack on the Pentagon late last month, officials said.

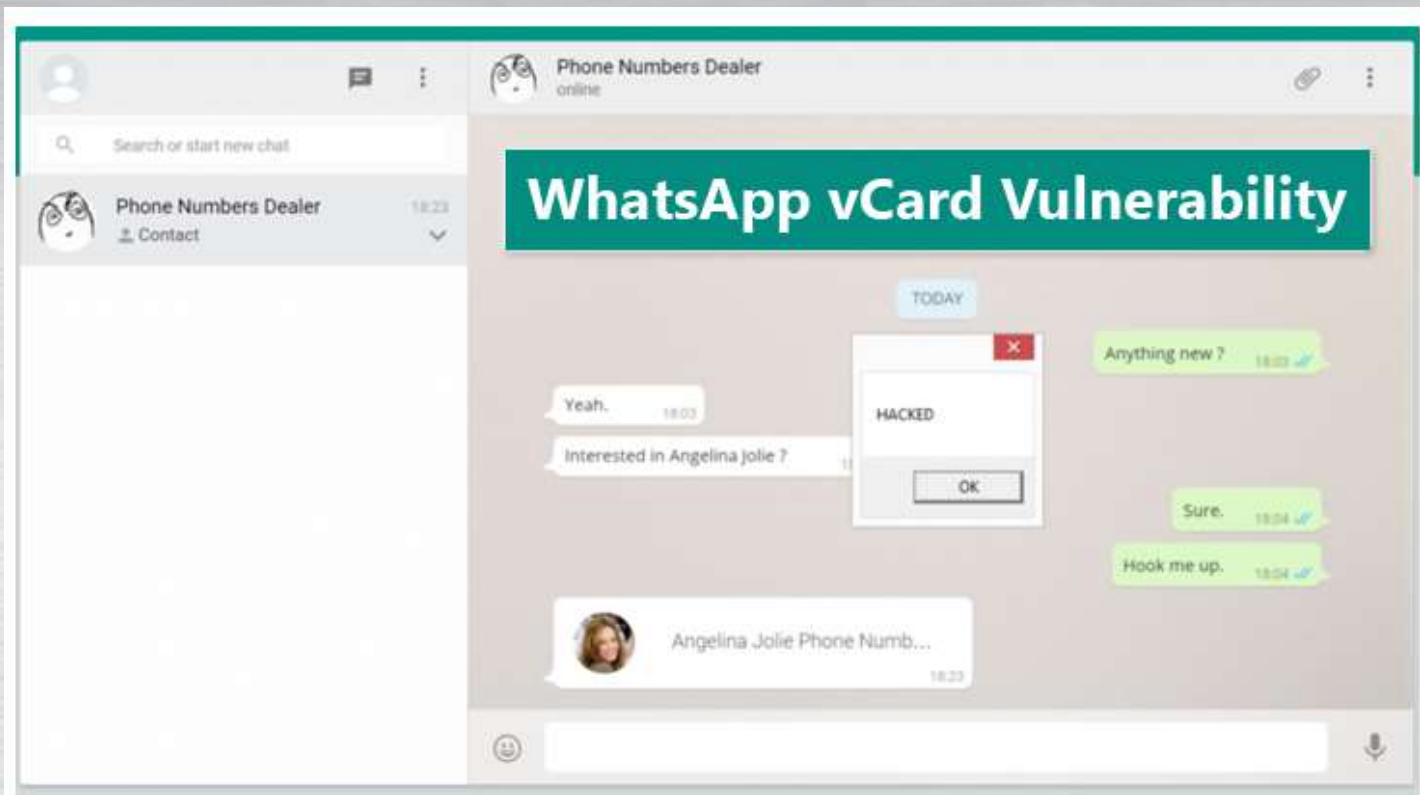
By Paul D. Shinkman

Aug. 6, 2015 | 4:51 p.m. EDT



Fonte: <http://www.usnews.com/news/articles/2015/08/06/reported-russian-cyber-attack-shuts-down-pentagon-network>

Por que se preocupar com isso?



WhatsApp recently **claimed** to have hit **900 Million monthly active users**, but a dangerous security flaw in the web version of the popular instant messaging app **puts up to 200 Million of its users at risk**.

Fonte: <http://thehackernews.com/2015/09/whatsapp-vcard-vulnerability.html>

Por que se preocupar com isso?

Ashley Madison hackers post millions of customer names



By Chris Isidore and David Goldman @CNNTech



Hackers who stole Ashley Madison customers' personal information have followed through with their threat to release it to the public.

The hackers claim to have posted 32 million names, credit card numbers, email and physical addresses along with the sexual preferences of customers entered into the cheaters' dating site.

Social Surge - What's Trending



Live: Tim Cook unveils new iPhone 6S, Apple TV and iPad Pro



U.S. oil exports: Coming soon?



Surge soda returns to store shelves

Search for Jobs

Millions of job openings!

Find Jobs

Accounting Engineering Developer
Finance Management Media
Marketing Sales See all jobs

Fonte: <http://money.cnn.com/2015/08/18/technology/ashley-madison-data-dump>

Por que se preocupar com isso?



Fonte: <http://www.conjur.com.br/2017-mai-17/ataque-cibernetico-mundial-comprova-inseguranca-internet>

OWASP Top Ten

OWASP Top 10 – 2010 (Anterior)	OWASP Top 10 – 2013 (Novo)
A1 – Injeção de código	A1 – Injeção de código
A3 – Quebra de autenticação e Gerenciamento de Sessão	A2 – Quebra de autenticação e Gerenciamento de Sessão
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos	A4 – Referência Insegura e Direta a Objetos
A6 – Configuração Incorreta de Segurança	A5 – Configuração Incorreta de Segurança
A7 – Armazenamento Criptográfico Inseguro – Agrupado com A9 →	A6 – Exposição de Dados Sensíveis
A8 – Falha na Restrição de Acesso a URL – Ampliado para →	A7 – Falta de Função para Controle do Nível de Acesso
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<Removido do A6: Configuração Incorreta de Segurança>	A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos	A10 – Redirecionamentos e Encaminhamentos Inválidos
A9 – Proteção Insuficiente no Nível de Transporte	Agrupado com 2010-A7 criando o 2013-A6

10) Redirecionamentos e Encaminhamentos Inválidos

- Aplicações web frequentemente **redirecionam** e **encaminham** usuários para outras páginas e sites, e usam dados não confiáveis para determinar as páginas de destino. Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sites de phishing ou malware, ou usar encaminhamentos para acessar páginas não autorizadas.

Exemplos:

- <http://www.example.com/redirect.jsp?url=evil.com>
- <http://www.example.com/boring.jsp?fwd=admin.jsp>

10) Redirecionamentos e Encaminhamentos Inválidos

Como evitar?

- Evitar usar “redirects” e “forwards”
- Caso sejam necessários, não utilize parâmetros para definir o destino
- Se parâmetros não podem ser evitados, valide os parâmetros de redirecionamento e verifique os valores para o usuário


9) Utilização de Componentes Vulneráveis Conhecidos

- Componentes, bibliotecas, frameworks, e outros módulos de software quase sempre são executados com privilégios elevados. Se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor.


Referências:

- Common Vulnerabilities and Exposures
<https://cve.mitre.org/>
- National Vulnerability Database
<https://nvd.nist.gov/home.cfm>

9) Utilização de Componentes Vulneráveis Conhecidos



Sponsored by
DHS/NCCIC/US-CERT



NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact Metrics	Data Feeds	Statistics	FAQs
Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments	Visualizations

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 72300 [CVE Vulnerabilities](#)
- 313 [Checklists](#)
- 249 [US-CERT Alerts](#)
- 4384 [US-CERT Vuln Notes](#)
- 10286 [OVAL Queries](#)
- 106134 [CPE Names](#)

Last updated: 9/10/2015 7:39:08 AM

CVE Publication rate: 22.6

Email List

NVD provides four mailing lists to the

National Cyber Awareness System

Vulnerability Summary for CVE-2015-2481

Original release date: 08/14/2015
Last revised: 08/18/2015
Source: US-CERT/NIST

Overview

The RyuJIT compiler in Microsoft .NET Framework 4.6 produces incorrect code during an attempt at optimization, which allows remote attackers to execute arbitrary code via a crafted .NET application, aka "RyuJIT Optimization Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2479 and CVE-2015-2480.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6


CVSS Version 2 Metrics:

Access Vector: Network exploitable; Victim must volun

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of inform service



Computer Security Resource Center

National Vulnerability Database

[GENERAL](#) [VULNERABILITIES](#) [VULNERABILITY METRICS](#) [PRODUCTS](#) [CONFIGURATIONS \(CCE\)](#)

[Vulnerabilities > Detail](#)

CVE-2017-0248 Detail

Current Description

Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to bypass Enhanced Security Usage taggings when they present a certificate that is invalid for a specific use, aka ".NET Security Feature Bypass Vulnerability."

Source: MITRE **Last Modified:** 05/12/2017 [View Analysis Description](#)

9) Utilização de Componentes Vulneráveis Conhecidos

Como evitar?

- É difícil.
- Não usar nenhuma biblioteca?
- Verificar com o fornecedor as bibliotecas que estão sendo utilizadas, incluindo as suas dependências;
- Manter as bibliotecas atualizadas

8) *Cross-Site Request Forgery (CSRF)*

- Usuário se autentica normalmente no site exemplo.com.br
- Sem efetuar logout, o usuário visita o site virus.com.br, que faz uma requisição maliciosa para o site exemplo.com.br
- Como o usuário ainda está autenticado, caso o site exemplo.com.br não esteja protegido, a requisição funcionará normalmente

8) Cross-Site Request Forgery (CSRF)

FILE

HOME

SEND / RECEIVE

FOLDER

VIEW

New Email

Favorites

Caixa de entrada 1

Email Não Lido 59

Mensagens enviadas

giovani@cw.com.br

Caixa de entrada 1

Antigo

Azure

Walmart :: CE Melhorias

Walmart :: SGP Readiness

Rascunhos 2

Mensagens enviadas

Itens Excluídos 1841

Caixa de Saída

Conversation History

Junk E-Mail 87

RSS Feeds

Search Folders

Caixa de entrada - giovani@cw.com.br - Outlook

All Unread

Search Current Mailbox (Ctrl+E)

Current Mailbox

FROM

SUBJECT

RECEIVED

SIZE

CATEGORIES

Date: Today

Giovani Decusati Sistema de Pedidos OnLine qua 09/09/2015 10:13 95 KB

A nova versão do sistema de gestão de pedidos está disponível no site. Para acessar clique aqui <http://localhost:6065/pages/Blocks/Security/loginWrong.aspx?ReturnUrl=http://localhost:8082/fakesrc.html> ! <end>

Date: Yesterday

Date: Last Week

Date: Two Weeks Ago

Date: Three Weeks Ago

Date: Last Month


Date: Older

Reply

Reply All

Forward

IM

 Giovani Decusati

Giovani Decusati

Sistema de Pedidos OnLine

10:13

A nova versão do sistema de gestão de pedidos está disponível no site. Para acessar clique aqui!

CWIFORGE

Microsoft - NorthWind

Olá root - > Sal

Início

Panel de Controle

Cadastros

Controle de pedidos

Relatórios

Rotinas

Comandos

Novo

Editar

Excluir

Limpar

Last Name

First Name

Title

Title Of Courtesy

Birth Date

Hire Date

Extension

Reports To

Address

City

Region

Postal Code

Country

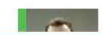
Phone

Fax

Notes

ID	Last Name	First Name	Title	Birth	Hire	Address	City	Region	Postal Code	Country	Phone
1	Todd	Lynn	Sales Representative	1804/1961	01/07/2003	34 Waterloo Road	Melbourne	AU	3000	Victoria	1 (11) 500 555-0190
2	Yvonne	Rachel	Sales Representative	29/08/1965	01/07/2003	Passado 951	Berlin	DE	14111	Hamburg	1 (11) 500 555-0140
3	Abbas	Syed	Pacific Sales Manager	11/02/1965	15/04/2003	7484 Roundtree Drive	Bethel	US	98011	Washington	808-555-0182
4	Maria Annun	Tate	Sales Representative	06/02/1966	01/11/2002	3987 Via De Luna	Cambridge	US	82139	Massachusetts	615-555-0153
5	Vincent	Choudhury	Sales Representative	30/10/1965	01/07/2002	84, rue Descartes	Bordeaux	FR	33000	Grande	1 (11) 500 555-0117
6	Wei	Yee	Sales Representative	02/12/1968	01/07/2003	Po Box 77991	Pasadena	US	91109	California	714 555-0166

Click a photo to see recent emails and social updates.



setembro 2015

D S T Q F S S

30 31 1 2 3 4 5

6 7 8 9 10 11 12

13 14 15 16 17 18 19

20 21 22 23 24 25 26

27 28 29 30 1 2 3

4 5 6 7 8 9 10

Today

You have nothing else scheduled today.

Tomorrow

13:00 Apresentação Segurança

sexta-feira

12:00 CNova :: Cartão Presente

São Leopoldo - Sala 5.1

segunda-feira

08:00 ENC: Reunião

São Leopoldo - Sala 5.1

Arrange by: Importance

High

Type a new task

Normal

Maturidade de Projetos

Dojo

Trazer ideias para inovação, evidenciar ...

Haggstron Segurança

ITEMS: 26 UNREAD: 1

ALL FOLDERS ARE UP TO DATE. CONNECTED TO: MICROSOFT EXCHANGE

100%

VS2012 x64 Cross T...

TRN.Hibernate (Ru...

TRN.Hibernate - Mi...

fakesrc.html - Ata...

LoginWrong - Inter...

09/09/2015

8) *Cross-Site Request Forgery (CSRF)*

Como evitar?

- Evitar CSRF geralmente implica em criar uma token em cada requisição HTTP(s). Essa token deve ser única e mudar, no mínimo, a cada nova sessão.
- O token também pode ser incluído na URL (através da query string, mas isso é menos seguro)
- CAPTCHAs também ajudam a proteger contra CSRF.

7) Falta de Função para Controle do Nível de Acesso

Como funciona?

- Um usuário malicioso simplesmente muda a URL ou muda um parâmetro e acessa uma funcionalidade do sistema que deveria estar bloqueada.

7) Falta de Função para Controle do Nível de Acesso

Como evitar?

- O mecanismo de autorização deve, por padrão, negar acesso a uma funcionalidade e só permitir acesso caso o usuário possua a permissão explicitamente definida
- A maior parte das aplicações não exibem links e botões para telas/rotinas bloqueadas, mas essa validação também deve ser efetuada no Controller ou na lógica de negócio

6) Exposição de Dados Sensíveis

- Como são armazenados os dados confidenciais (ex.: senhas, número de cartões de crédito)?
- Os dados são trafegados por HTTPS ao invés de HTTP?

6) Exposição de Dados Sensíveis

SQLQuery1.sql - ...vo (audit (65))*

```
select top 100 * from TB_PEDIDOS order by datacad desc
```

Results Messages

	IpConexao	Cartao_Nome	Cartao_Numero	Cartao_Codi...	Cartao_Valida...	P
1	189.31.109.75	[REDACTED]	5214001700004740	601	03/2010	:
2	177.76.12.110	[REDACTED]	4984420000040070	026	00/2010	:
3	189.106.144.129					:
4	177.97.115.112					:
5	186.231.6.24				01/2010	:
6	187.41.236.186	[REDACTED]	5305101401070100	007	10/2010	:
7	189.62.88.223	[REDACTED]	4500200047000000	040	04/2010	:
8	201.75.158.141	[REDACTED]	4010747272470004	504	08/2010	:
9	187.67.217.163	M [REDACTED]	4004700040000077	000	05/2010	:

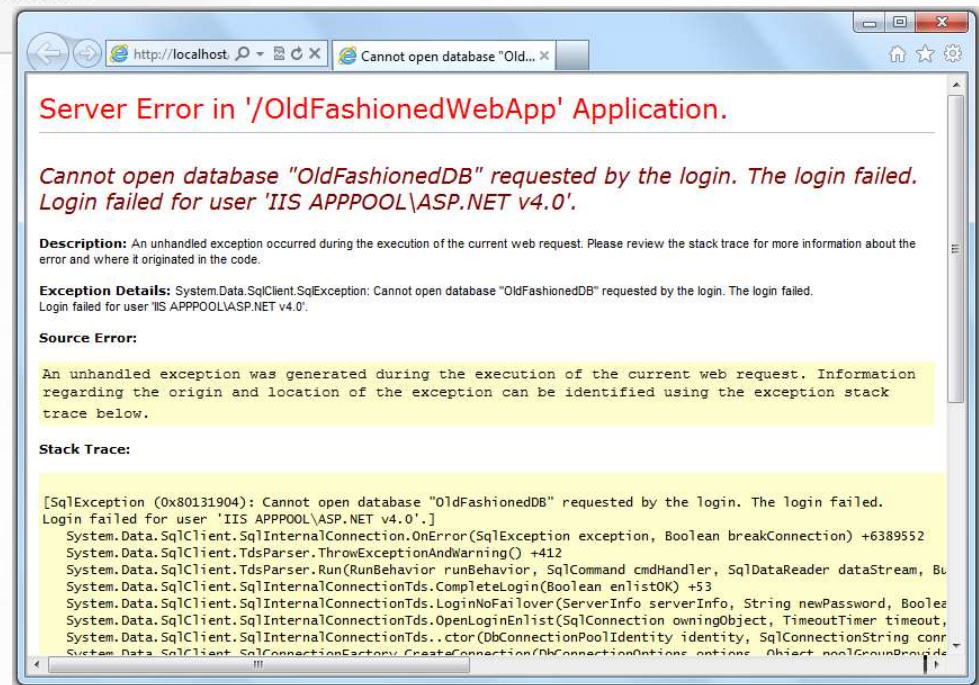
Fonte: Auditoria de arquitetura realizada em cliente.

5) Configuração Incorreta de Segurança

Exemplos:

- 1) Existem recursos desnecessários habilitados ou instalados (ex. portas, serviços, páginas, contas, privilégios)?
- 2) Os usuários e senhas padrão foram alterados?
- 3) No caso de erros no sistema, o stack trace é exibido para os usuários (ou qualquer outra informação excessiva)?
- 4) As configurações padrão de segurança nos frameworks de desenvolvimento (ASP.NET, Spring, Struts) foram alteradas?

5) Configuração Incorreta de Segurança



4) Referência Insegura e Direta a Objetos

Exemplo:

- <http://www.meusite.com/compras/detalhe?idCompra=1234>

4) Referência Insegura e Direta a Objetos

URL: https://admin.341-7.com.br/EcommerceNew/faturar_pedidos_boleto.asp?id=1937682

Boleto Bancário - Windows Internet Explorer

https://a... Boleto Bancário

Itaú Banco Itaú |341-7| 34191.75017 93768.332939 81404.860009 1 56250000007665

Local de Pagamento					Vencimento
Até o vencimento, preferencialmente no Itaú.					02/03/2013
Cedente					Agência / Código Cedente
					2938/14048-6
Data Documento	Número Documento	Tipo Docu.	Aceite	Data Processamento	Nosso Numero
27/02/2013	01937683			27/02/2013	175/01937683-3
Uso Banco	Carteira	Espécie	Quantidade	Valor	Valor do Documento
	175	R\$	1	R\$ 76,65	R\$ 76,65
Sacado Giovanni Decusati					
[REDACTED]					

Autenticação Mecânica / FICHA DE COMPENSAÇÃO

Boleto Bancário

https://a... Boleto Bancário

Itaú Banco Itaú |341-7| 34191.75017 93768.092939 81404.860009 1 56250000007082

Local de Pagamento					Vencimento
Até o vencimento, preferencialmente no Itaú.					02/03/2013
Cedente					Agência / Código Cedente
					2938/14048-6
Data Documento	Número Documento	Tipo Docu.	Aceite	Data Processamento	Nosso Numero
27/02/2013	01937680			27/02/2013	175/01937680-9
Uso Banco	Carteira	Espécie	Quantidade	Valor	Valor do Documento
	175	R\$	1	R\$ 70,82	R\$ 70,82
Sacado CRISTANE CAROLINA REINERT DE SOUZA VIEIRA					
[REDACTED]					

Autenticação Mecânica / FICHA DE COMPENSAÇÃO

Fonte: Auditoria de arquitetura realizada em cliente.

3) Cross-Site Scripting (XSS)

- Um usuário malicioso envia texto contendo scripts que serão interpretados pelo browser
- Praticamente qualquer fonte de dados pode ser a origem da injeção de scripts: campos de texto, URL, banco de dados
- O impacto da injeção de script inclui: roubar sessão, modificar sites (phishing), redirecionar usuários, forçar download de arquivos, etc.

3) Cross-Site Scripting (XSS)

Como evitar?

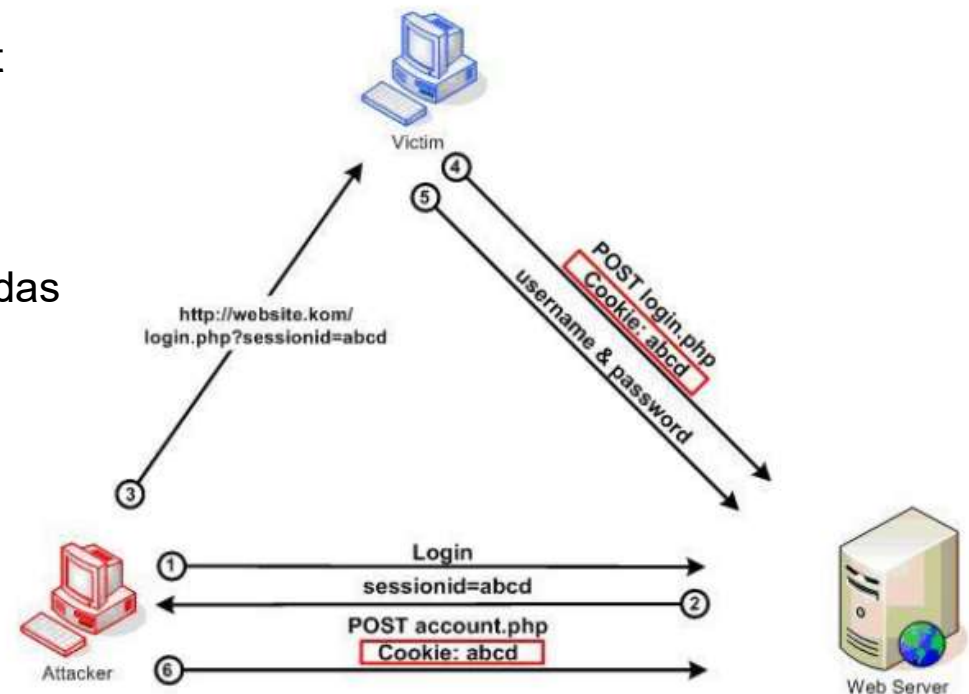
- Nunca confiar em dados fornecidos pelo usuário
- Fazer escape dos caracteres que serão exibidos na página/script/url
- Content-Security-Policy header
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

2) Quebra de Autenticação e Gerenciamento de sessão

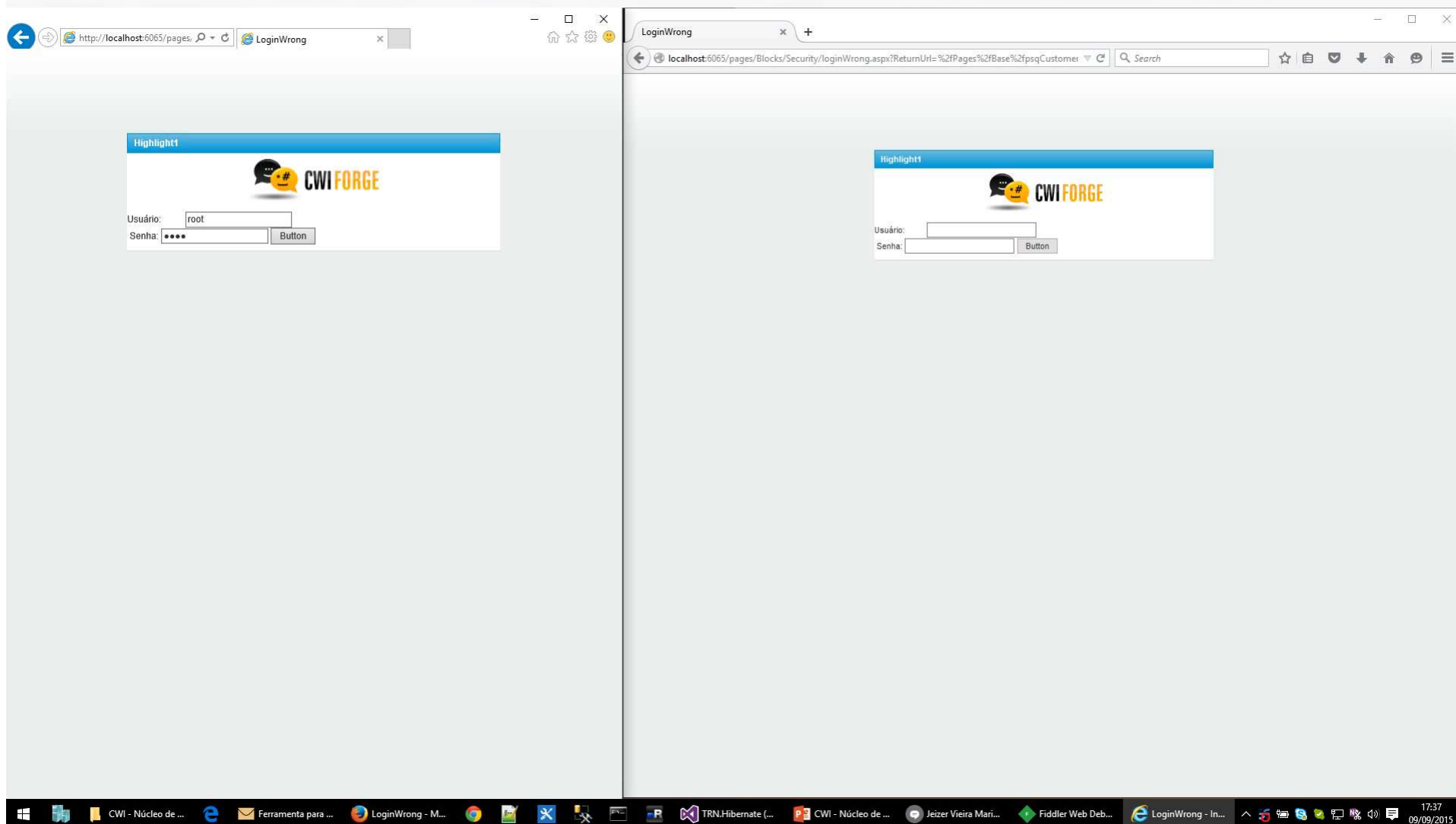
- Autenticação e gerenciamento de sessão é difícil de implementar corretamente;
- As aplicações normalmente possuem falhas que permitem usuários maliciosos obter senhas, logins, tokens de sessão ou explorar outras falhas para utilizar a identidade de outro usuário

2) Quebra de Autenticação e Gerenciamento de sessão

1. Senhas não são criptografadas durante o armazenamento
2. Credenciais podem ser adivinhadas, recuperadas ou alteradas através de funções como “esqueci minha senha”, “mudar senha”, etc;
3. Sessions Ids são expostos na URL (URL rewriting)
4. Sessão não é invalidada durante o logout ou nunca expira
5. Senhas/session ids são enviados sem criptografia em conexões não criptografadas (ex.: HTTP)



2) Quebra de Autenticação e Gerenciamento de sessão



1) Injeção

- As falhas de Injeção, tais como injeção de SQL, de SO (Sistema Operacional) e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados.

1) Injeção

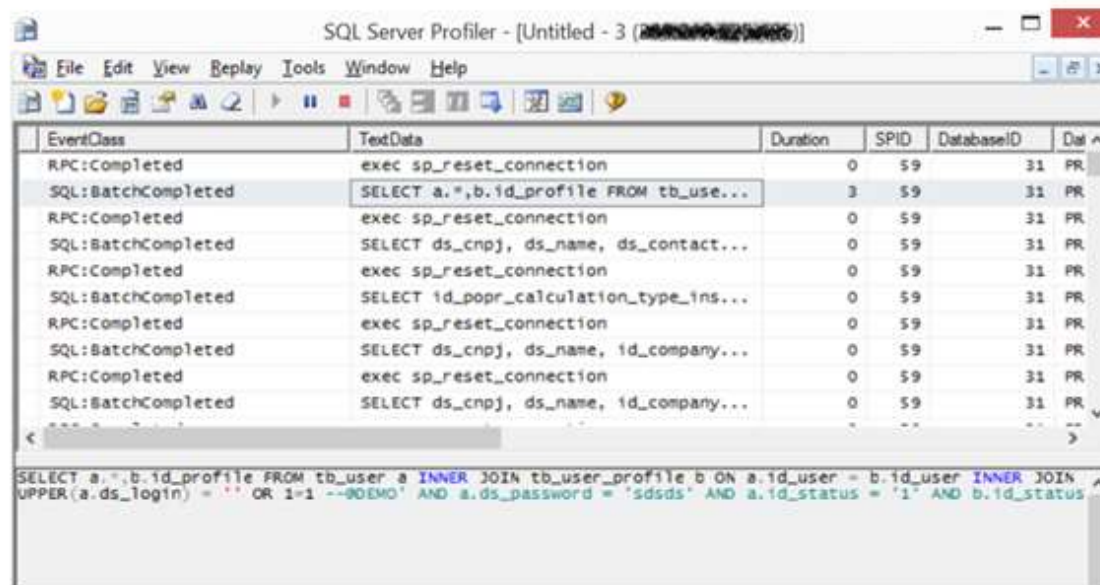


1) Injeção



A screenshot of a web application login interface. At the top, there is a blurred header area. Below it, there are two input fields: 'Usuário:' and 'Senha:'. The 'Usuário:' field contains the text ' ' or 1=1 --@demo'. The 'Senha:' field contains a series of dots representing a password. Below the input fields is a blue button labeled 'Acessar'.

Figura 10 - Inputs aceitam injeção de SQL



A screenshot of the SQL Server Profiler window. The window title is 'SQL Server Profiler - [Untitled - 3 (200809022006)]'. The menu bar includes File, Edit, View, Replay, Tools, Window, and Help. Below the menu bar is a toolbar with various icons. The main area displays a table of events with columns: EventClass, TextData, Duration, SPID, DatabaseID, and Data. The table contains several rows of events, including RPC:Completed and SQL:BatchCompleted. The last row of the table is highlighted, showing a SQL injection query. Below the table, there is a detailed view of the selected event, showing the full SQL query text.

EventClass	TextData	Duration	SPID	DatabaseID	Data
RPC:Completed	exec sp_reset_connection	0	59	31	PR
SQL:BatchCompleted	SELECT a.~,b.id_profile FROM tb_user...	3	59	31	PR
RPC:Completed	exec sp_reset_connection	0	59	31	PR
SQL:BatchCompleted	SELECT ds_cnpj, ds_name, ds_contact...	0	59	31	PR
RPC:Completed	exec sp_reset_connection	0	59	31	PR
SQL:BatchCompleted	SELECT id_popr_calculation_type_ins...	0	59	31	PR
RPC:Completed	exec sp_reset_connection	0	59	31	PR
SQL:BatchCompleted	SELECT ds_cnpj, ds_name, id_company...	0	59	31	PR
RPC:Completed	exec sp_reset_connection	0	59	31	PR
SQL:BatchCompleted	SELECT ds_cnpj, ds_name, id_company...	0	59	31	PR

SELECT a.~,b.id_profile FROM tb_user a INNER JOIN tb_user_profile b ON a.id_user = b.id_user INNER JOIN UPPER(a.ds_login) = ' ' OR 1=1 --@demo' AND a.ds_password = 'sdsds' AND a.id_status = '1' AND b.id_status

Fonte: Auditoria de arquitetura realizada em cliente.

Não pare por aí

- **Não pare nos Top Ten! Mais de 500.000 vulnerabilidades**
- **Organizações devem se concentrar para reduzir o número de vulnerabilidades**
- **ASVS: Application Security Verification Standard**

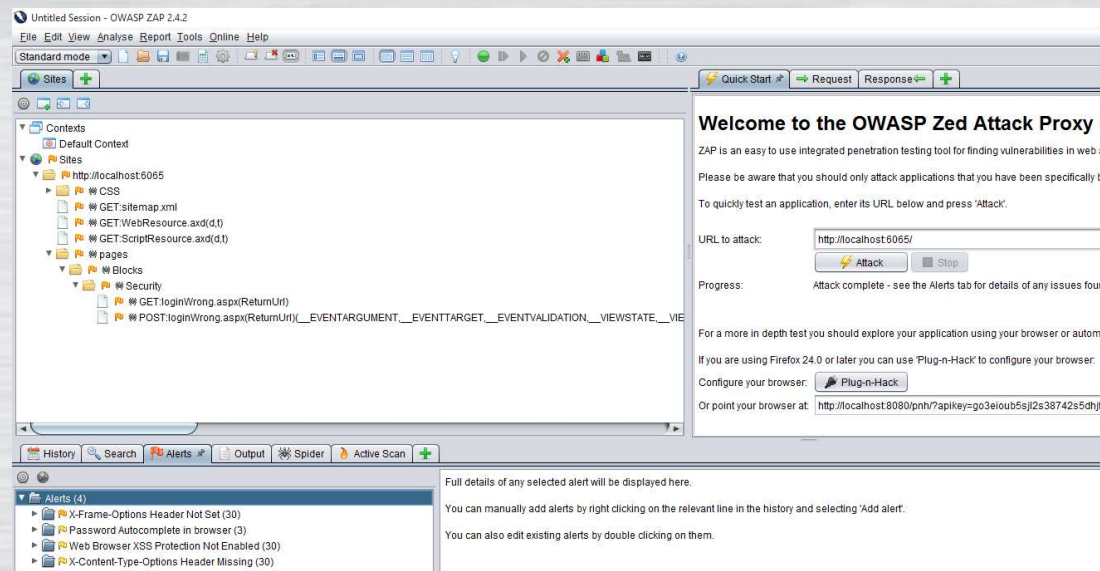
- OWASP ZAP

- **HP Tools**

- Fortify
- WebInspect

- **Free**

- <http://sqlmap.org/>
- <http://www.metasploit.com/>
- <https://portswigger.net/burp/>
- <http://www.backtrack-linux.org/>
- <https://www.kali.org/>



Referências

- <https://www.owasp.org>
- [https://www.owasp.org/index.php/Category:OWASP Application Security Verification Standard Project](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)
- <https://freedom-to-tinker.com/blog/wzeller/popularwebsites-vulnerable-cross-site-request-forgery-attacks>
- [https://www.owasp.org/index.php/XSS Filter Evasion Cheat Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)



CWI SOFTWARE

Giovani Decusati

giovani@cw.com.br

www.cw.com.br

PORTO ALEGRE | RS +55 51 3092.7500

SÃO LEOPOLDO | RS +55 51 3081.3600

CAXIAS DO SUL | RS +55 54 3535.3635

SÃO PAULO | SP +55 11 3614.7800

RIO DE JANEIRO | RJ +55 21 2586.6377