Segurança de Sistemas Informáticos

TP2: Vulnerabilidades e Exposições Comuns

João Araújo, A75364

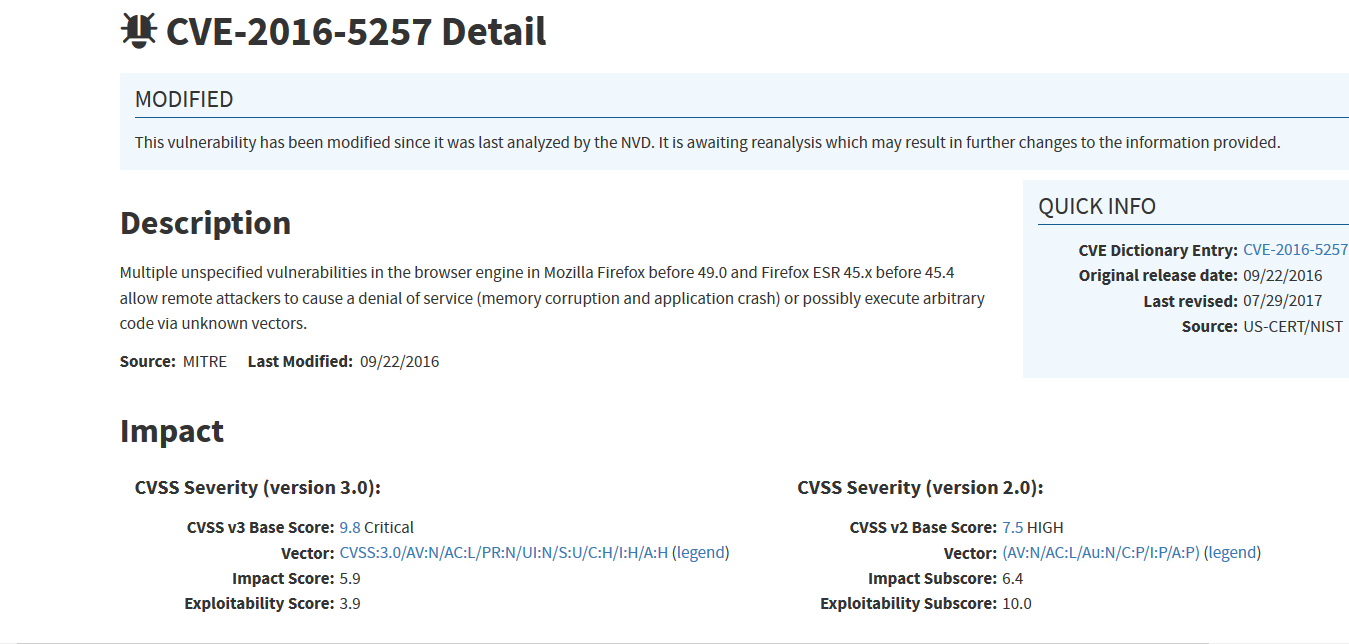
João Nuno Almeida, A75209

# Aplicações e as suas vulnerabilidades

Decidimos escolher o Firefox, Windows e Steam como as aplicações sobre as quais vamos pesquisar vulnerabilidades.

## Firefox

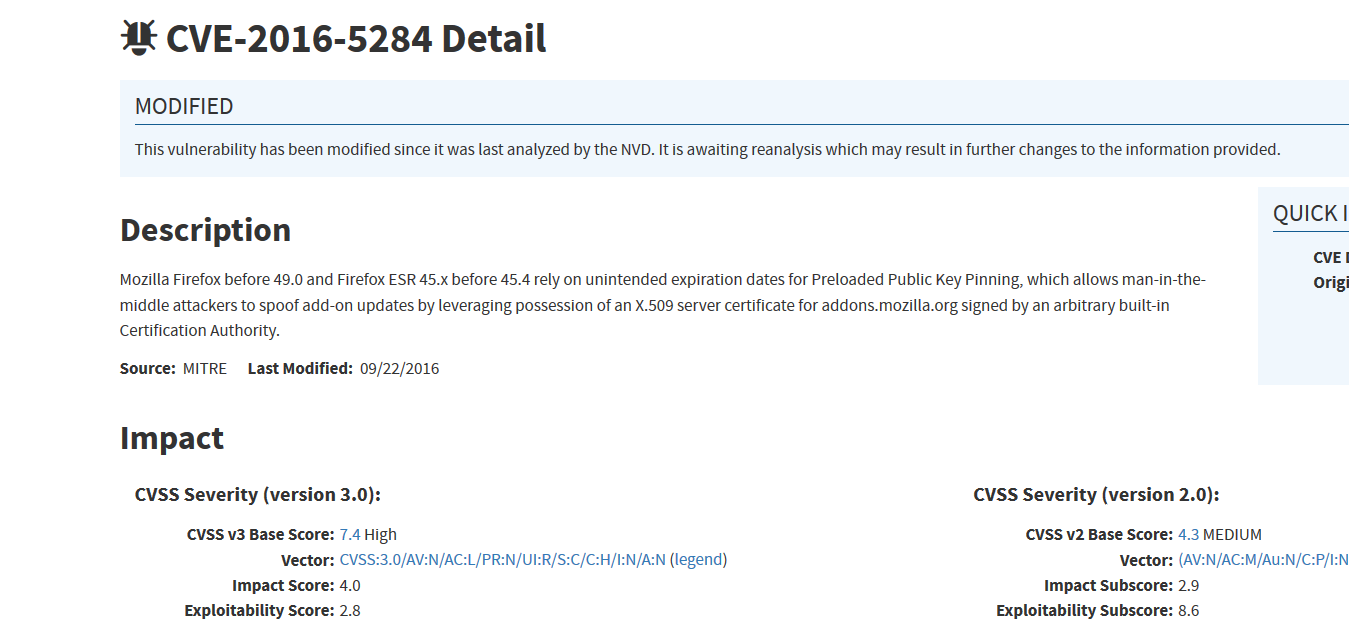
* CVE-2016-5257



Esta vulnerabilidade no *browser* toma partido de várias vulnerabilidades não especificadas que permitem aos atacantes lançar ataques de DOS (*Denial Of Service*) por corrupções de memória que permitem execução de código arbitrário.

A partir das versões 49 e ESR 45.4 (*Extended Support Release*) do *browser* a CVE foi corrigida.

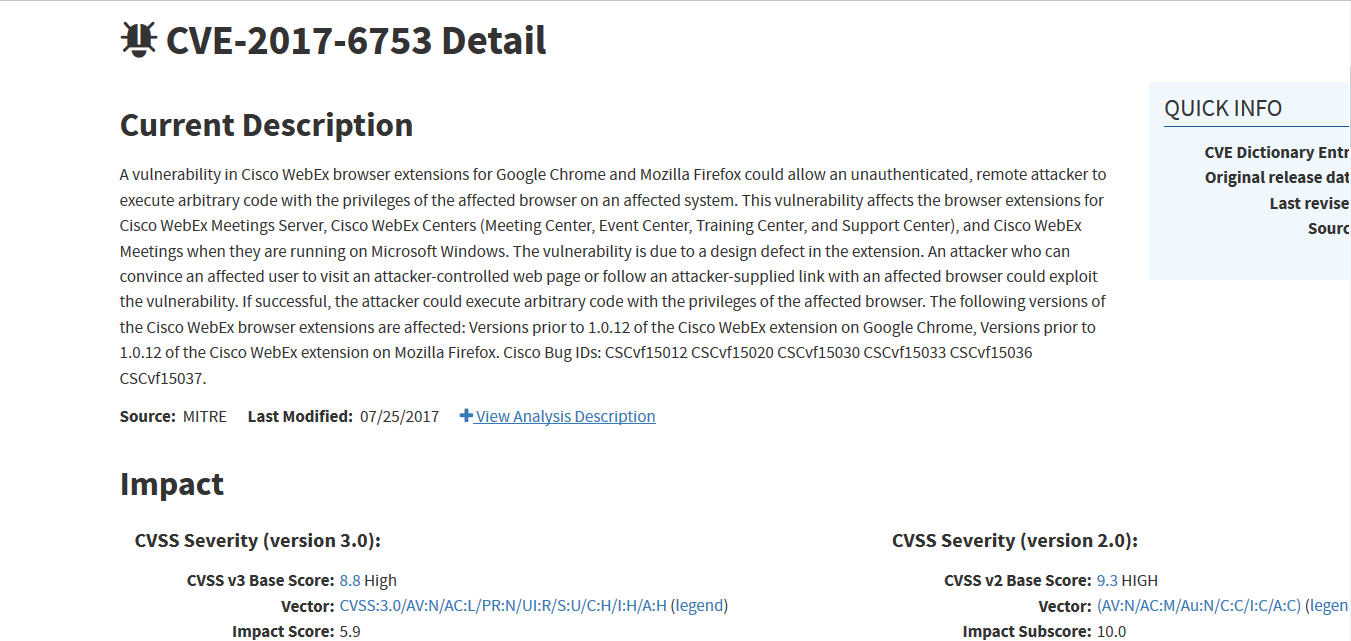
* CVE-2016-5284



Esta vulnerabilidade permite a um prevaricador simular o servidor responsável pelas atualizações de *add-ons* do Firefox, dependendo de datas de expiração em chaves públicas não planeadas, permitindo portanto aliciar o utilizador com falsas atualizações com potenciais intenções maliciosas.

Tal como na CVE anterior, versões superiores à 49 ou ESR 45.4 têm esta vulnerabilidade corrigida.

* CVE-2017-6753



Esta vulnerabilidade afeta uma extensão em particular, a Cisco WebEx, tanto no Firefox como no Chrome devido a utilizarem a mesma *framework* de extensões (*WebExtensions*). Também só quando os *browsers* estão a correr no SO Microsoft Windows é que a vulnerabilidade se manifesta. Caso um utilizador aceda a um *link* fornecido por um atacante, este último pode explorar a extensão para correr código não intencionado com os privilégios de próprio *browser*.

Versões desta extensão posteriores à 1.0.12 já corrigiram esta CVE.

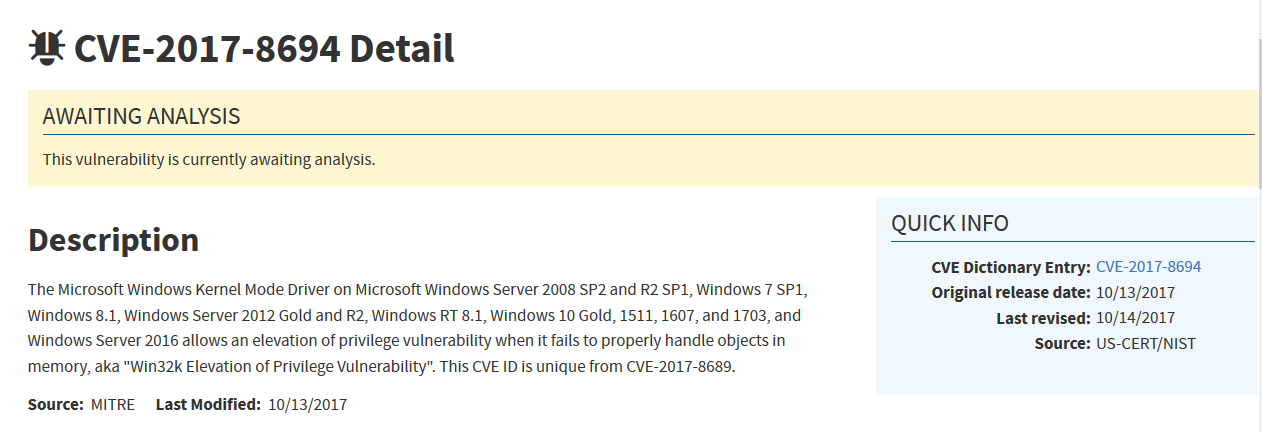
## Windows

* CVE-2017-8727



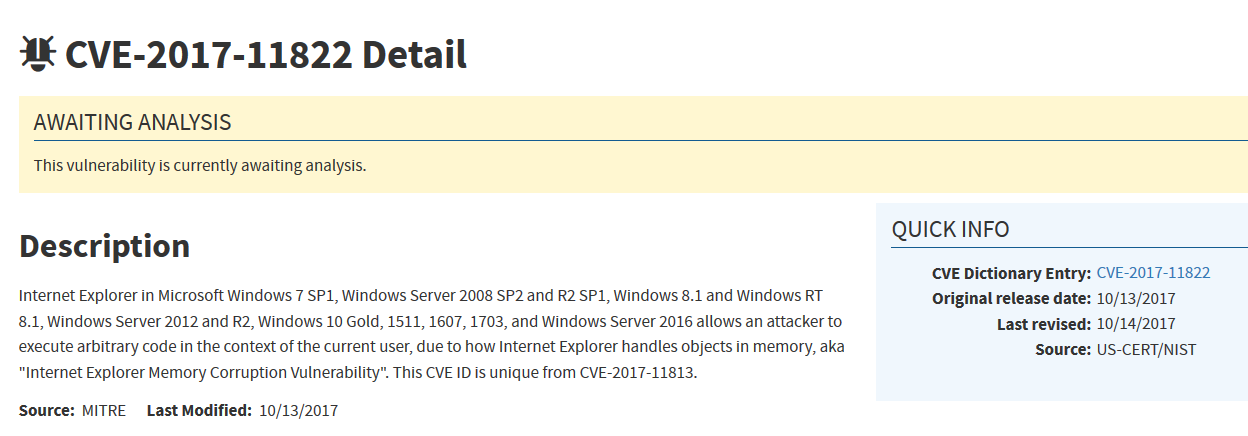
Esta vulnerabilidade, permite que o atacante execute o código que pretender com efeito na máquina do utilizador e com os privilégios do mesmo. Deve-se ao facto como estes sistemas operativos gerem os objetos que estejam em memória.

Ainda não foi encontrada qualquer solução para esta CVE.

* CVE-2017-8694

Esta vulnerabilidade, permite uma elevação de estatutos no momento em que falha no tratamento de objetos em memória. Afeta apenas os sistemas operativos acima mencionados.

Ainda não foi encontrada qualquer solução para esta CVE.

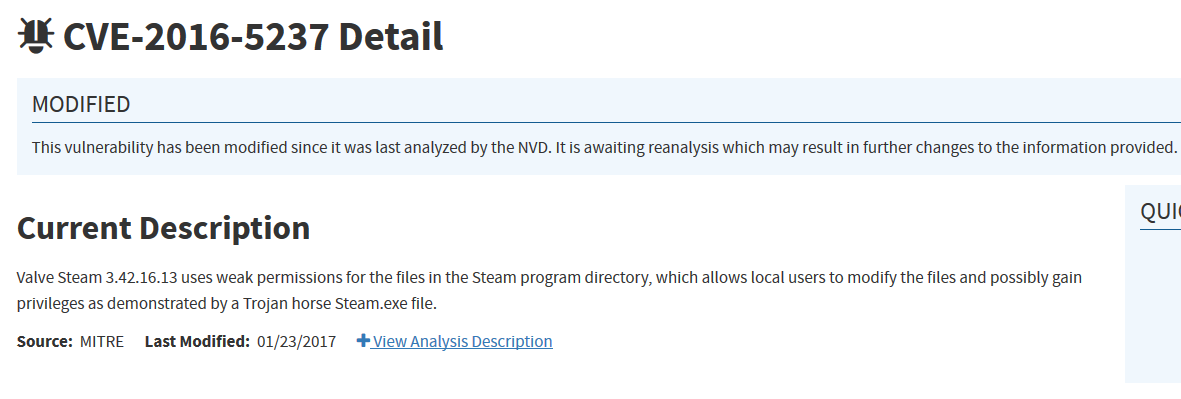
* CVE-2017-11822

Esta vulnerabilidade permite a um atacante, a execução do código que pretenda, sobre os privilégios de um utilizador com uma máquina a operar sobre os sistemas operativos acima referidos. Deve ao facto de como o Internet Explorer (Browser pré-definido nestes sistemas operativos) falha em tratar dos objetos em memória.

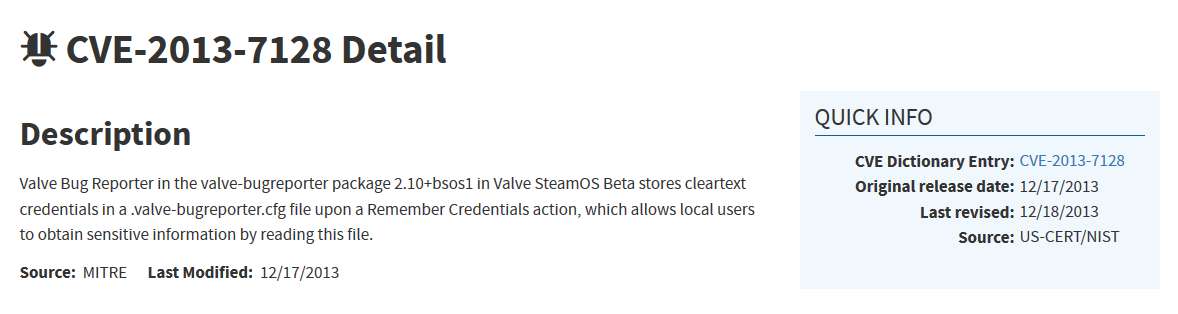
Ainda não foi encontrada qualquer solução para esta CVE.

## **Steam**

* CVE-2016-5237

Esta vulnerabilidade afetou a versão 3.42.16.13 do programa Valve Steam. Permitia, por usar permissões fracas, que os utilizadores modificassem os ficheiros do programa, de maneira a ganhar privilégios e criar executáveis indesejáveis.

Esta CVE foi resolvida na atualização seguinte da Steam.

* CVE-2013-7128

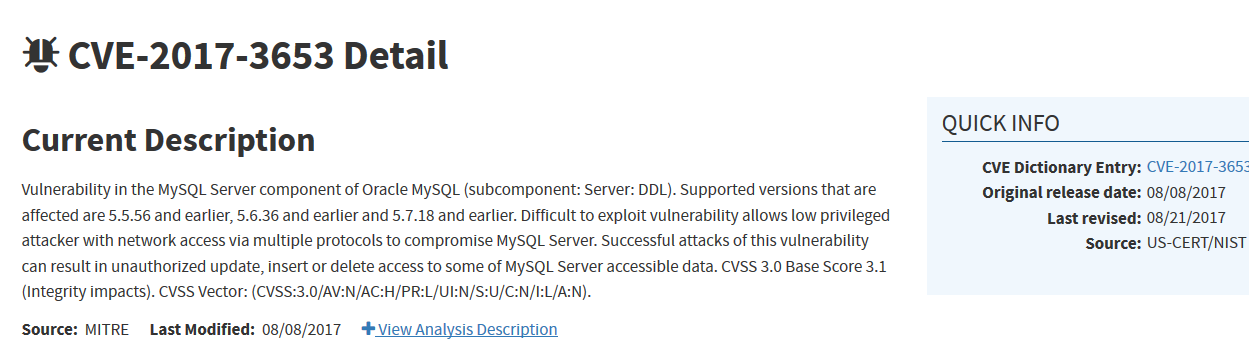
Esta vulnerabilidade permitia aos utilizadores locais, lerem informações sensíveis guardadas no ficheiro valve-bugreporter.cfg. Afetava os utilizadores do Valve SteamOS Beta.

A vulnerabilidade foi resolvida após a atualização da versão do Valve SteamOS.

# Vulnerabilidades em ferramentas relacionadas com serviços Web

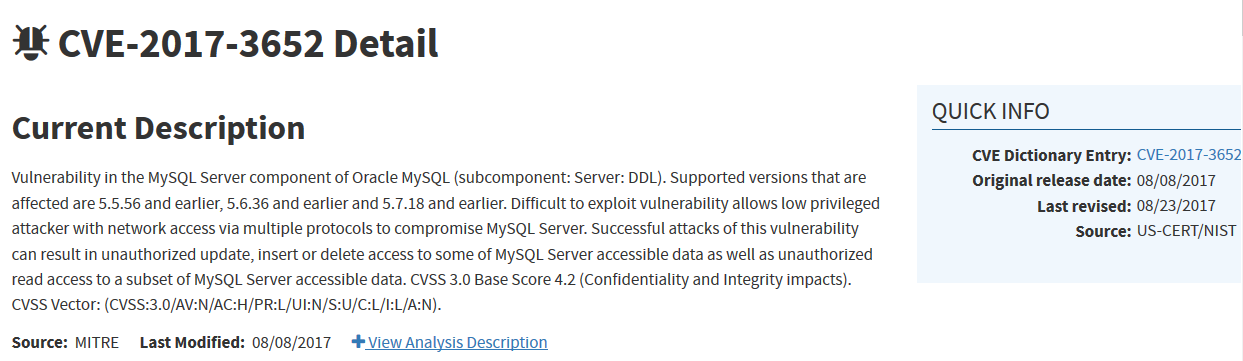
## MySQL

* CVE-2017-3653



Esta vulnerabilidade, permitia operações de INSERT, DELETE e UPDATE em tabelas das bases de dados Oracle MySQL, por parte de utilizadores com poucos privilégios com acesso à rede. As versões 5.5.56 e mais recente, 5.6.36 e mais recente, 5.7.18 e mais recente, foram aquelas afetadas por esta CVE.

A vulnerabilidade foi ultrapassada em versões mais recentes do MySQL Server.

* CVE-2017-3652

Esta vulnerabilidade, permitia o acesso a dados inseridos nas tabelas das bases de dados Oracle MySQL e com uma componente MySQL Server, por parte de utilizadores com privilégios limitados e com acesso à rede. As versões 5.5.56 e mais recente, 5.6.36 e mais recente, 5.7.18 e mais recente, foram aquelas afetadas por esta CVE.

A vulnerabilidade foi ultrapassada em versões mais recentes do MySQL Server.

## PHP

* CVE-2017-12868

Esta vulnerabilidade, permite aos atacantes conduzir ataques de *session fixation,* ou até mesmo saltar o passo de autenticação de programas que se serviam do método secureMethod, da livraria lib/SimpleSAML/Utils/Crypto.php in SimpleSAML.php 1.14.13 e mais recente, num programa desenvolvido na linguagem de programação PHP numa versão anterior à 5.6.

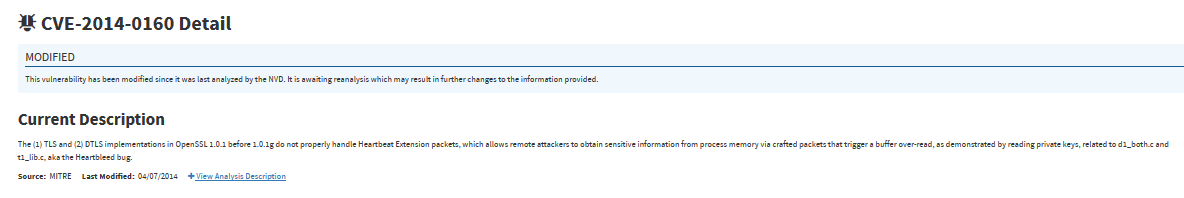
Após a versão 5.6 do PHP, a vulnerabilidade foi ultrapassada.

* CVE-2017-12934

Esta vulnerabilidade, implica que surja um impacto na integridade do PHP, quando usados os métodos e data types acima referidos.

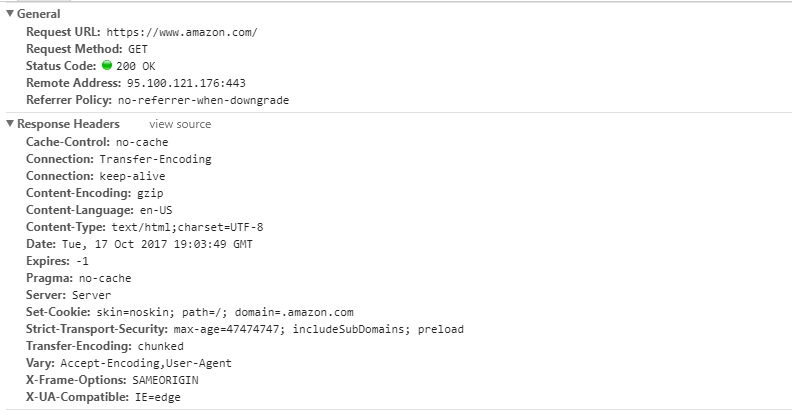
Após as atualizações mais recentes do PHP esta vulnerabilidade foi ultrapassada.

# Falha *Heartbleed* (CVE-2014-0160)

Nesta vulnerabilidade, as implementações TLS e DTLS são incapazes de tratar os pacotes *Heartbeat Extension,* esta incapacidade, permite aos prevaricadores lerem chaves privadas e outros tipos de informação sensível, ao processarem memória via pacotes alterados e desenhados por eles próprios, que ativam buffers over-read, ou seja buffers que ultrapassam as barreiras até onde devem ler, e tentam ler memória adjacente que não lhes diz respeito.

# Análise aos domínios web

## Amazon.com





## Reddit.com



Supostamente, através desta informação (extraída seguindo as instruções do ponto 5 do enunciado), deveríamos ser capazes de extrair todas as vulnerabilidades associadas aos serviços Web dos respetivos domínios. Infelizmente, ambos os domínios por nós escolhidos no decorrer do TP1 (amazon.com e reddit.com), protegem a versão do seu servidor, sendo impossível destrinçar a mesma e consequentemente, usar a ferramenta “expoit”, para pesquisar todas as vulnerabilidades que poderiam estar associadas a essa versão. Amazon apresenta o campo server preenchido, simplesmente, com “Server”, enquanto que Reddit apresenta o campo server preenchido com “snooserv”.