**Relatório de Auditoria Forense**

**Web Aplicações**

**Jorge Almeida**

**Vulnerabilidades Web das aplicações**

* WebGoat.Net (Injection Attacks - File Download Patch Manipulation )
* DVWA ( Requisição de Senhas, com sqlmap)
* WebGoat ( ﻿Malicious File Execution )

**Sumário**

* Executivo Descrição das atividades Findings (classificados por nível de risco)
* Recomendações (com criticidade e esforço de implementação)

**Web Aplicação WebGoat.Net (** Injection Attacks - File Download Patch Manipulation )

**Executivo Descrição das atividades Findings**

﻿ É um ataque que combina [segmentos de caminho da URL](https://translate.googleusercontent.com/translate_c?depth=1&hl=pt-PT&prev=search&rurl=translate.google.pt&sl=en&sp=nmt4&u=http://stackoverflow.com/questions/2163803/what-is-the-semicolon-reserved-for-in-urls&xid=25657,15700002,15700023,15700186,15700190,15700256,15700259,15700262,15700265,15700271,15700283&usg=ALkJrhhlqzb1BvcSGeujrTUoLgaND5QtEw), onde realiza-se ﻿**Download** do arquivo, ﻿com páginas que refletem as entradas do usuário na resposta. Contudo através deste ataques conseguimos visualizar e baixar todo o Web.Conf onde trará nele informações necessárias para outras acessos e colhimentos de dados. O Arquivo que foi coletado atrves de uma outra ferramenta chamada Burpe Suite, consegue intercepta com o proxy o arquivo, com o botão direito você acionar a opção **send to repeater**, ao qual ira descodificar todo o seu ficheiro trazendo as informações crucias que necessita.

Está falha é bem utilizada dentro dos API que não tem aplicabilidade de segurança ativa, onde o jsan injection trará informações essências para invasão.

Em relação ao seu nível de risco, é de grande proporção pois traz todas as informações crucias para um devido ataque, tais eles como :

**<authentication mode="Forms">**

**<forms name="customer\_login" timeout="30" loginUrl="~/WebGoatCoins/CustomerLogin.aspx" requireSSL="false" protection="All" path="/">**

**<credentials passwordFormat="Clear">**

**<user name="admin" password="admin" />**

**<user name="mario" password="luigi" />**

**<user name="bob" password="password" />**

**</credentials>**

**Logins e password como está na coleta do script logo acima.**

Bom ressaltar que este tipo de ataque nos dias de hoje está descontinuado, através das correções de segurança na área de Engenharia de software, já existe métodos que conseguem inibir esse tipo de ações .

**Recomendações**

﻿

* higienizar a entrada da sua (nesse caso, eles devem apenas permitir alfanuméricos); escapar não é suficiente
* adicione `Disposição de conteúdo: anexo; filename = "Whatever.txt" `nas que não serão renderizadas.
* adicione o cabeçalho `X-Content-Type-Options: nosniff` às respostas da
* Tratamento nas Entradas de acessos
* Redireccionamento através de tocken pra confirmação de acesso.

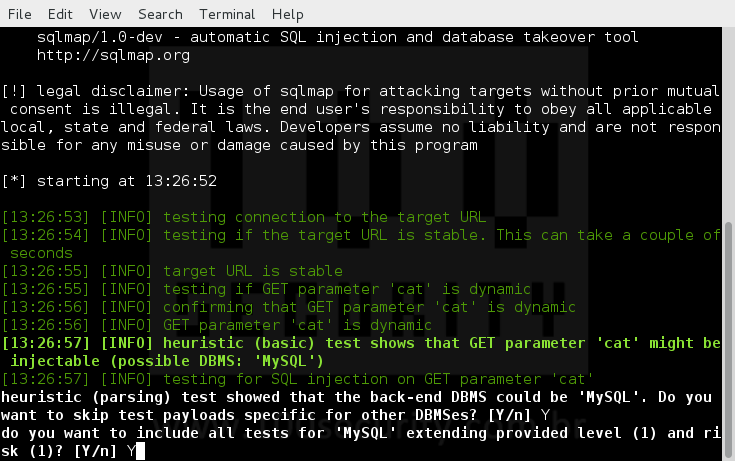
**DVWA ( Requisição de Senhas, com sqlmap)**

**Executivo Descrição das atividades Findings**

﻿ E um aplicativo da web PHP / MySQL que é extremamente vulnerável. Seu principal objetivo é ajudar os profissionais de segurança a testar suas habilidades e ferramentas em um ambiente legalmente permitido ser atacado, ajudar os desenvolvedores Web a entender melhor os processos de proteção de aplicativos da Web.

**Seu principal objetivo é :** ﻿ praticar algumas das vulnerabilidades da Web mais comuns, com vários níveis de dificuldade, com uma interface simples e direta

O mesmo é praticado da seguinte maneira: ativamos através de autenticação por url, os logins e senhas tais eles como root e senha roote( exemplo) logo em seguida, seguimos para o Burp Suite, ao qual interceptamos as informações pelo proxy, procuramos o link de endereçamento url, chamos a ferramenta **SQLMAP, ao qual através de linhas de comando iremos fazer um injection na url, depois seguiremos os passos do login, ao qual iremos buscar na informação coletada pelo proxy do PHPIDSSESION, onde iremos informa na linha de comando como demonstra na figura abaixo.**

﻿

**Onde iremos extrair informações através da tabela de dados, tais elas como os logins dos usuários e senhas necessárias para acesso.**

**Recomendações**

* ﻿Verifique as configurações de segurança de seu banco de dados
* Monitoramento através de Firewall Inteligentes.
* Utilização de Fremaworks para mitigação destas ações.

**WebGoat ( ﻿Malicious File Execution )**

**Executivo Descrição das atividades Findings**

﻿ A ferramenta acima permite fazer upload de uma imagem que será exibida nesta página. Recursos como esse são frequentemente encontrados em fóruns de discussão na Web e sites de redes sociais. Esse recurso é vulnerável à execução de arquivo mal-intencionado.

Irei demonstrar por etapas as suas funcionalidades:

﻿

1 - Inicie o WebGoat e navegue até a seção Execução de arquivo malicioso.

Etapa 2 - Para concluir esta lição, precisamos fazer o upload no local acima ( pode ser arquivo ou imagem)

Etapa 3 - Vamos criar um arquivo jsp de forma que o arquivo, seja criado na execução do jsp. A Nomeação do jsp não tem nenhum papel a desempenhar nesse contexto, pois estamos executando o conteúdo do arquivo jsp. ﻿

﻿ Etapa 4 - Agora faça o upload do arquivo jsp e copie o local do link após o upload. O upload está esperando uma imagem, mas estamos enviando um jsp.

Etapa 5 - Navegando para o arquivo jsp, não haverá nenhuma mensagem para o usuário.

Etapa 6 - Agora atualize a sessão em que você enviou o arquivo jsp e você receberá a mensagem "Parabéns! Você concluiu a lição com sucesso".

**Torna-se um processo simples e menos complexo que na utilização dos outros métodos expostos logo acima, é algo muito utilizado e comum para coletar informações no mundo WEB.**

﻿

**Recomendações**

* Proteger sites usando permissões de sites.
* Adote contramedidas para segurança de aplicativos da web.
* Entenda as contas internas de usuários e grupos no IIS 7.0.

Conclusão

Concluímos que está praticas acimas mencionadas algumas hoje tornando em desuso, contudo outras sempre bem comum no cotidiano do mundo web, faz necessários sempre aplicabilidade de ferramentas que possam sempres gerenciar e mitigar tipos tentativas que desejem coletar informações ou qualquer suspeitas de ações estranhas dentro de uma rede.

Observamos a real necessidade de uma auditoria continuam, não só quando existir um incidente, para tal corrigirmos, mas para sempre analisar possíveis falhas que possam ocorrer nos acessos das redes web.