Explorando falha SQLi com Sqlmap METODO GET

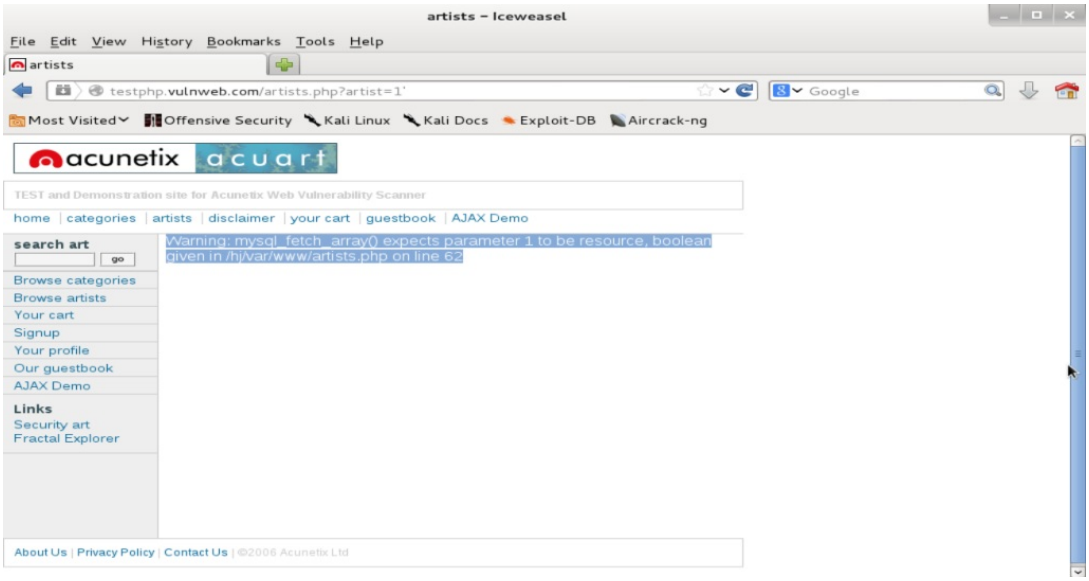
7 de maio de 201517 de setembro de 2015 / s0ph0s

A falha SQLi é muito mais comum que você pensa, sendo listada como principal vulnerabilidade na lista da OWASP anualmente, para explorar essa falha usaremos o ***Sqlmap.*** Primeiramente precisamos entender o conceito teórico da falha antes de introduzir a parte técnica do ataque, para quem não conhece a falha SQLi está relacionado a falha de programação no banco de dados onde o atacante pode enviar requisições maliciosas a ele retornando dados as quais não poderiam ser extraídos (informações no banco que só deveriam ser acessada por usuário com privilégios).

Para quem já possui ela instalada em sua distro (como no exemplo usaremos o Kali Linux) siga os seguintes passos ou simplesmente baixe a ferramenta.

Para buscar sites com falha de SQLi podemos simplesmente usar a técnica do Google Hacking ou passa alguma ferramenta de scanning no alvo (Acunetix, Nessus, Vega, entre outras). No caso de hoje pegaremos um site próprio para fazer esse tipo de ataque, sendo o da Acunetix. Para verificarmos a falha de SQLi pelo moto GET (falha explorada via URL) inserimos algum caracter especial como aspas simples (‘) no final da tag (como *id*= , *produto*= , *cat*= , e nosso caso a tag *artist*=) do site ficando dessa maneira:

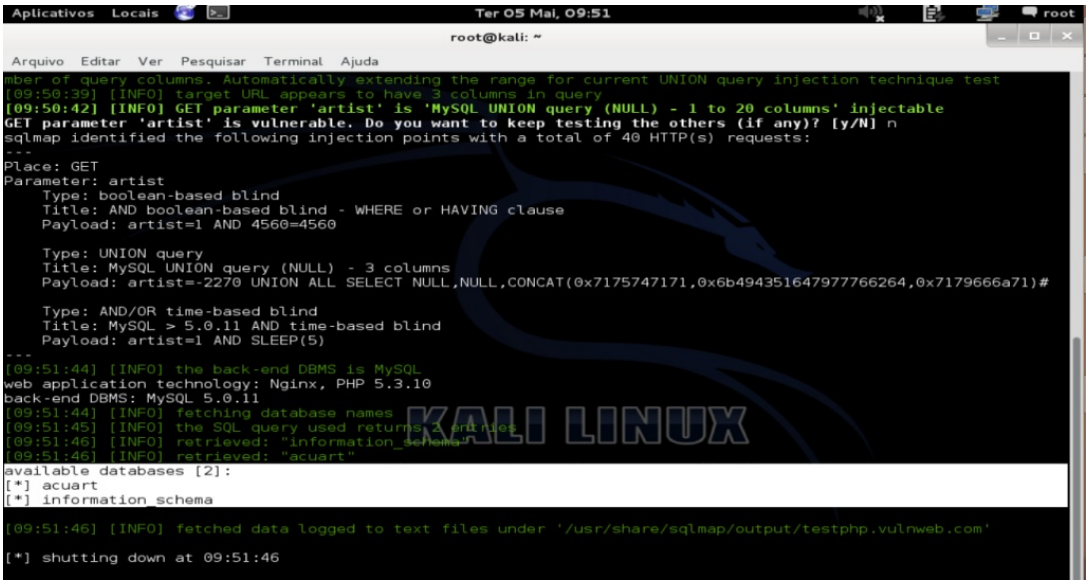
http://testphp.vulnweb.com/artists.php?artist=1′



A qual estará retornando um erro no banco de dados, a qual exploraremos a falha de SQLi. Agora abra o terminal e executaremos a ferramenta Sqlmap a qual nós permite enviar requisição Query (ao banco de dados) e nos retorne dados sensíveis do alvo como contas de logins, relatórios da empresa, dados de clientes, entre outras coisas.

Primeiro comando que damos é para listar o banco de dados existentes, para acessar os database contido nele.

```
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
```



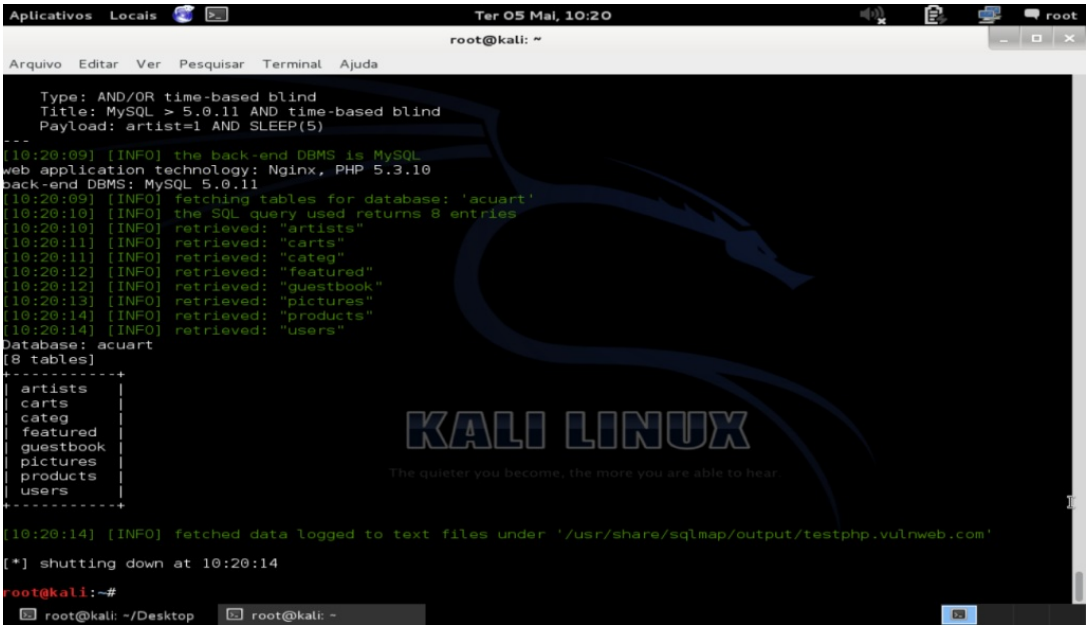
Após listar o banco de dados deparamos com dois banco de dados:

* acuart

* information_schema

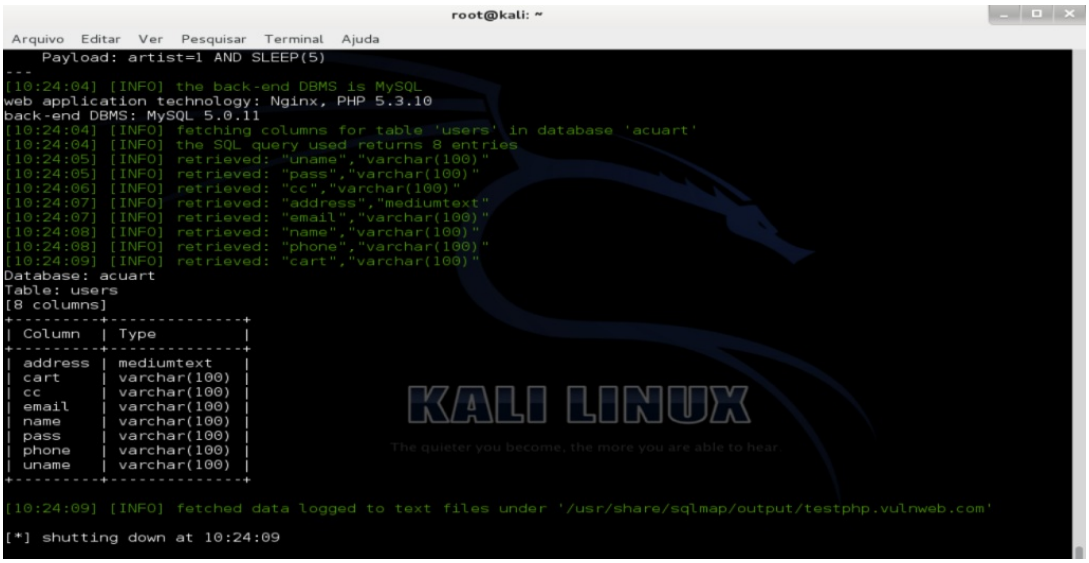
Escolhemos o Acuart por padrão pois geralmente os dados dos usuários cadastrados no sistema estão nele (mas pode selecionar o outro sem problema, mas nesse caso nós retornará dados referente a estrutura do site). E então geramos suas tabelas:

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart –tables



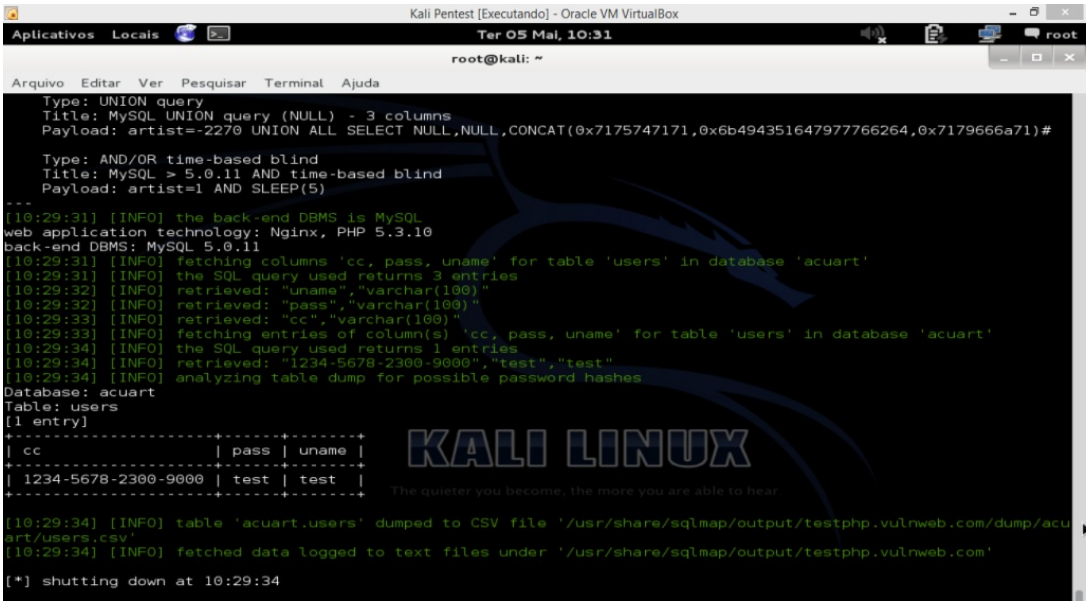
Deparamos com diversas tabelas (*artists, carts, categ, featured, guestbook, pictures, products, users*) a qual nos interessa é a tabela *users* a qual está cadastrado os usuários com suas respectiva senhas.

```
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns
```

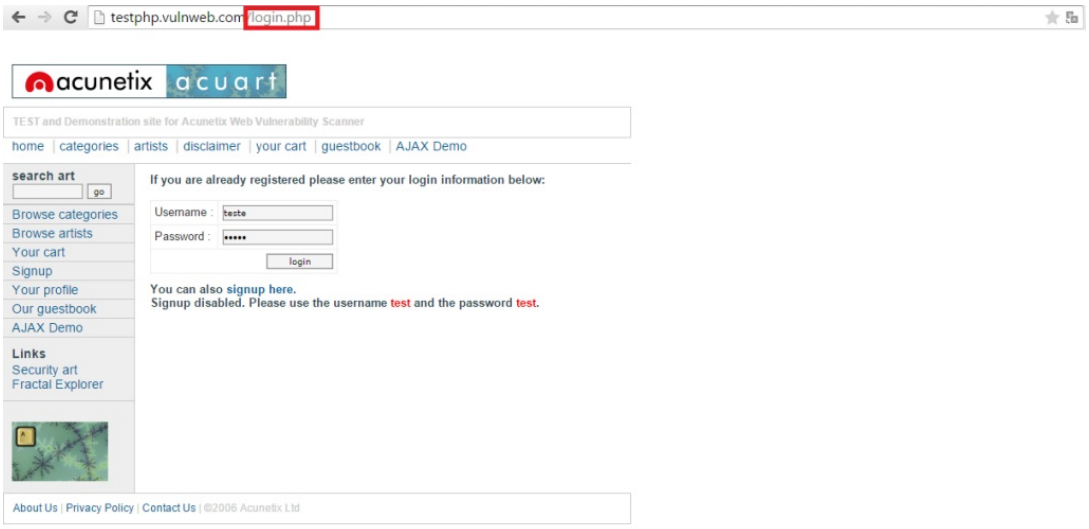


Agora podemos ver as colunas listada de nossa tabela *users* (*address,cart,cc,email,name,pass,phone,uname*), a qual extrairemos dados mais revelante a nós com usuário e senha ou até um cartão de crédito vinculado (sendo um dado falso obviamente).

```
#sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname,pass,cc --dump
```



Agora podemos ver o nome de usuário e senha dele, agora só entrar no painel do administrador e logar o usuário.



Nota: Com Sqlmap podemos extrair qualquer dado do banco de dados, sendo assim você não precisa se limitar na busca apenas de usuário e senhas, e sim de relatórios ou informações que é essencial a

empresa como no caso de uma utilização para um relatório de um pentest.