**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 8a :** "NOWASP - Mutillidae"

 “OWASP Mutillidae II Web Pentest Practice Application”

Tópico no Moodle: “Tarefa 8a - Multillidae”

Data:

Tempo de Aula: 1 hora-aula

Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 <Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ASSUNTO**

**Nesta experiência, exploraremos como usar o NOWASP Mutillidae.** NOWASP (Mutillidae) is a aplicação-web “free”, open source, deliberadamente vulnerável provendo um alvo para treinamento de testes de invasão sobre web-security. NOWASP (Mutillidae) pode ser instalado em Linux (usando LAMP) e Windows (usando WAMP) ou Unix BSD (usando XAMMP) para usuários que não desejem ser administrativos de servidores web.

É pre-instalado sobre SamuraiWTF, Metasploitable 2 (Rapid 7) e OWASP-BWA. A versão existente pode ser atualizada sobre plataformas existentes. Com dezenas de vulnerabilidades e sugestões de ajuda ao usuário, é um ambiente “hacking” de fácil uso, projetado para labs, entusiastas de segurança, salas de aula, CTF, e alvos de ferramentas de avaliação de vulnerabilidades. Mutillidae tem sido usado em cursos de segurança de graduação e cursos de treinamento de segurança de web de empresas.

**REQUISITOS

VM Ubuntu 12.04**

**Mutillidae**

------------------------------------------------------------------------------------------------------------------------------
 **OBJETIVOS DA AULA**

Conhecer como fazer testes de penetração em ambientes web, como previstos no OWASP Top 10 (<https://www.owasp.org/index.php/Main_Page>), que indica as 10 formas de ataques web mais realizados:

1. Cross-Site Scripting (94%)
2. Cross-Site request forgery (Falsificação de Solicitação) (92%)
3. Information Leakage (Vazamento de Informações) (78%)
4. Broken Access Controls (Quebra de Controles de Acessos) (71%)
5. Broken Authentication (Quebra de Autenticação) (62%)
6. SQL Injection (Injeção de SQL) (32%)
7. ...
8. ...
9. ...
10. ...

**BIBLIOGRAFIA BÁSICA**

Advanced Penetration Testing for Highly-Secured Enviroments: The Ultimate Security Guide, Lee Allen, PACKT Publishing, 2012.

Release corrente: <https://sourceforge.net/projects/mutillidae/files/>

Última Release revisada: <https://sourceforge.net/projects/mutillidae/files/>

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula, com a instalação de Mutillidae numa VM Ubuntu 12.04, visando o objetivo acima, pode ser colocada como:

**MOSTRE SEU EXPERIMENTO**

**Abra o Virtualbox.**

**Execute a VM Ubuntu 11.10 ou 12.04**

**Em VM Ubuntu, abra uma janela de terminal e vá o diretório seguinte:**

Versão corrente de Mutillidae pode ser obtida de <http://sourceforge.net/projects/mutillidae/>

Atualmente, mutillidae-2.6.5 (“OWASP Mutillidae II Web Pentest Practice Application”)

**# cd /home/bosco/Downloads/**

**# unzip mutillidae-2.6.5.zip**

**# cp -r mutillidae /var/www**

**Agora, precisa-se configurar a conexão da base de dados MySQL de modo que mutillidae funcione adequadamente. Mudar no arquivo config.inc para refletir que temos uma senha MySQL para root.**

**# nano /var/www/mutillidae/config.inc // mudar a senha do MySQL**

**No diretório /var/www/mutillidae/classes/**

**No arquivo MySQLHandle.php existe a configuração de toda a base de dados MySQL usada por Mutillidae com user = “root” e senha = “ “. Estas devem ser consideradas no arquivo config.inc citado acima.**

**Abra o navegador Firefox na VM Ubuntu e entre com http://localhost/mutillidae**

**Deve aparecer o ambiente sobre Samurai WTF (Web Testing Framework)**

 **----------------------------------------------------------------------------------------------------------**

 **Mutillidae: Hack, Learn, Secure, Have Fun !!!**

 **Mutillidae: Deliberately Vulnerable PHP Scripts of OWASP Top 10**

 **-------------------------------------------------------------------------------------------**

**Neste ambiente, localize e click no link Setup/Reset the DB, após ter mudado o arquivo config.inc no diretório /var/www/mutillidae .**

**Tudo pronto! Agora é necessário dar “reboot” a VM Ubuntu e “disable the NAT connection”, de modo que esta não seja mais acessível via Internet. Estas páginas não devem estar disponíveis a usuários maliciosos na Internet.**

**Vídeos instrucionais estão disponíveis em canal You Tube,** “webpwnized” **em** <https://www.youtube.com/user/webpwnized> .

**CONCLUSÃO**

Você pode treinar várias formas de ataques como os apontados acima. Por exemplo, veja o vídeo sobre Cross-Site Scripting, SQL Injection, ou outro teste.

**Tire suas conclusões sobre como fazer um teste de penetração em ambiente web**