



Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul



Atividade Orientada a Ensino

Acadêmico: Gustavo Lube Machado de Melo

RGA: 2018 1905 0424

Professor: Carlos Alberto da Silva

Atividade: Atividade Orientada a Ensino sobre Segurança computacional (Kali Linux)

Introdução

As atividades orientadas a ensino tiveram foco em segurança computacional. Foram realizados testes de segurança (Pentests) e as ferramentas estudadas estão listadas abaixo, com seus respectivos comandos e vulnerabilidades encontradas.

Não será possível demonstrar resultados e sites, pois foi exigido sigilo para realização do estudo.

PENTEST

Footprinting - Coleta de informações

Nslookup:

Ferramenta Unix para saber endereço de respectivo DNS.

```
(root@kali)
# nslookup
Server:
Address:
```

Whois:

Utilizado para saber informações básicas dos sites.

```
(root@kali)
# whois www.
```



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



Google Dorking:

Foi utilizado o Google como ferramenta para pesquisa e análises de diretórios, documentos e outras coisas de interesse. Foram encontrados dados possivelmente sensíveis e diretórios mais vulneráveis.

Comandos:

site:

filetype:

host:

Comando do linux para saber qual o host do site especificado.

comandos:

```
(root@kali)-[~  
# host -t a www.
```

Nmap:

Ferramenta do KaliLinux para obter mais informações de usuários, além de mapeamento de falhas de segurança. Foram utilizados e estudados várias variações, sendo elas:

```
(root@  
# nmap
```

```
(root@ka  
# nmap -o
```

```
(root@ka  
# nmap -0
```



Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul



```
(root@kali)-[~]  
# nmap -p 1-1024
```

```
(root@kali)-[~]  
# nmap -v -A -sV
```

```
(root@kali)-[~]  
# nmap -sV
```

```
(root@kali)-[~]  
# nmap --script vuln
```

Ping:

Comando Linux utilizado para verificar comunicação do servidor e analisar possível bloqueio do mesmo, após detectar os ataques de teste.

```
(root@kali)-[~]  
# ping w
```



Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul



Nping:

Usado para análise de respostas e tempos de pacotes de dados da rede. Comando utilizado:

```
(root@kali)-[~]  
└─# nping --tcp -p 22 --flags syn --ttl 2
```

Nikto:

Scanner usado para busca de vulnerabilidades de servidores web. Site especificado reconheceu risco do uso e bloqueou sistema atacante.

```
(root@kali)-  
└─# nikto -host
```

Sslscan:

Nativo no KaliLinux, utilizado para escanear tipo de criptografia utilizada em site especificado.

```
(root@kali)-  
└─# sslscan www
```



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



Wpscan:

Ferramenta hacker utilizada para escaneamento de vulnerabilidades web. Site especificado detectou a ferramenta e bloqueou o sistema atacante. Opção utilizada:

```
(root@kali)-[~]  
# wpscan --url SITE --enumerate p
```

Whatweb:

Outro Scanner web que não deu bloqueio do site para o atacante, mas não conseguiu obter informações.

```
(root@ka  
# whatweb
```

```
(root@kali)-[~]  
# whatweb --aggression 3 -v
```

Dirb:

Outro Scanner web que não provocou bloqueio do site para o atacante, mas também não conseguiu obter informações.

```
(root@kali)-[~]  
# dirb SITE /usr/share/wordlists/dirb/common.txt
```



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



Nuclei:

Scanner web especializado que foi instalado à parte no sistema. Detectou várias vulnerabilidades como método TRACE, sistemas antigos utilizados e falta de headers.

Opções utilizadas:

```
(root@kali  
# nuclei -l
```

Foi utilizada, também, a opção **-rl num**, sendo **num** um número inteiro que representa a quantidade de testes realizados em um determinado tempo. Foram realizados diferentes números para testes de bloqueio e análises.

Alguns testes tomaram bloqueio, enquanto outros passaram e retornaram as vulnerabilidades.

Imagem de iniciação do Nuclei:

```
nuclei (C)  
v3.0.3  
projectdiscovery.io  
[INF] Current nuclei version: v3.0.3 (latest)  
[INF] Current nuclei-templates version: v9.6.9 (latest)  
[INF] New templates added in latest release: 73  
[INF] Templates loaded for current scan: 7278  
[INF] Executing 5264 signed templates from projectdiscovery/nuclei-templates  
[WRN] Executing 2028 unsigned templates. Use with caution.  
[INF] Targets loaded for current scan: 9  
[INF] Templates clustered: 1252 (Reduced 10971 Requests)
```

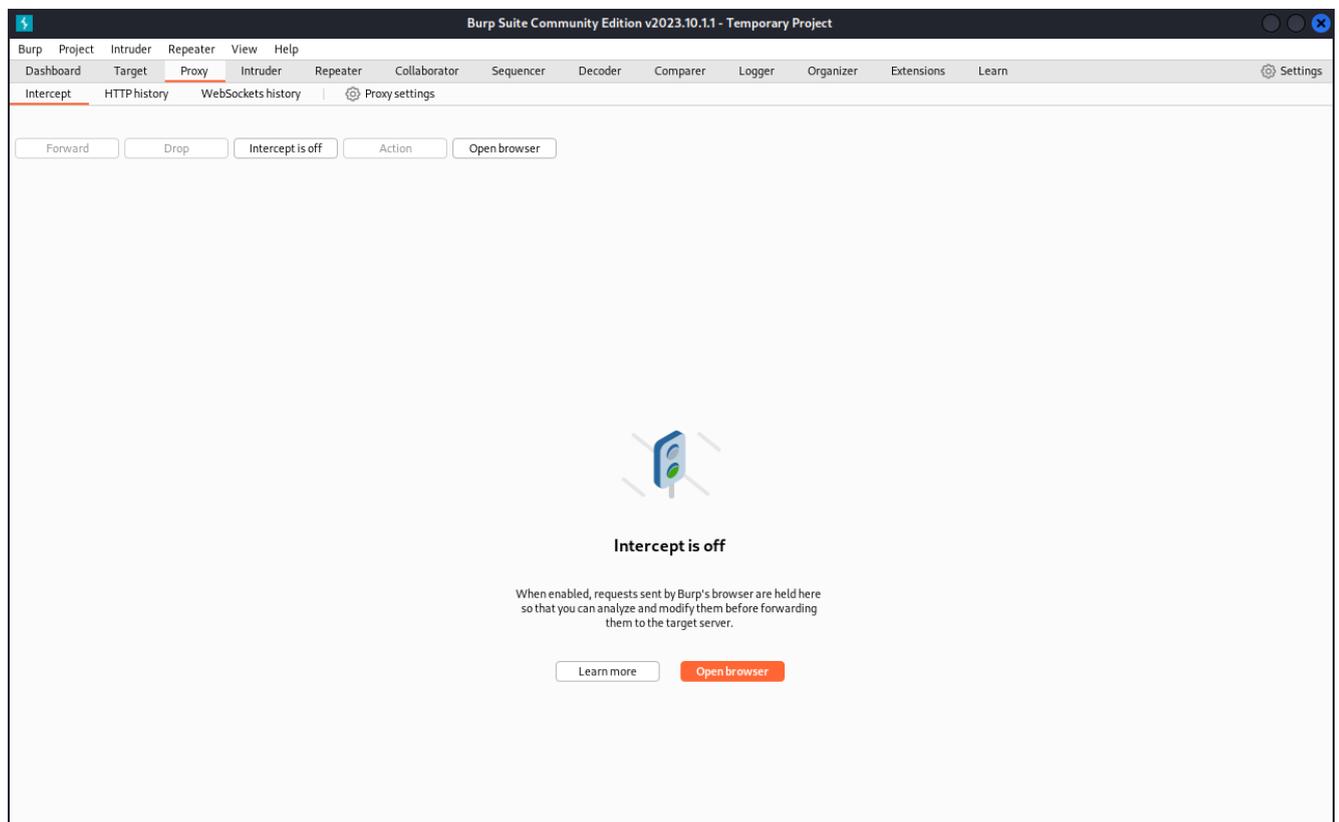


Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul



Burp Suite:

Multiferramenta para análise, ataque e muito mais para códigos na web. Foi utilizada para validação de vulnerabilidades, testes de injection, obtenções de informações, além de estudos de ataques à força bruta pelo mesmo. Foram obtidas a validação do método TRACE, informações sobre os sistemas utilizados e códigos com possíveis vulnerabilidades. As tentativas de HTML injection foram reconhecidas e não validadas nos testes.





Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

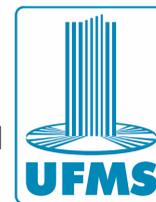


A captura de tela mostra a interface do Burp Suite Community Edition. O menu superior inclui 'Burp', 'Project', 'Intruder', 'Repeater', 'View' e 'Help'. Abaixo, há uma barra de ferramentas com opções como 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Organizer', 'Extensions' e 'Learn'. O painel principal está dividido em 'Positions', 'Payloads', 'Resource pool' e 'Settings'. O modo 'Intruder' está selecionado, com o tipo de ataque definido como 'Sniper'. A seção 'Payload positions' permite configurar posições para inserção de payloads em uma solicitação HTTP. O exemplo de solicitação mostra um POST para '/example?p1=\$p1val\$&p2=\$p2val\$' com cabeçalhos de cookie e conteúdo. O status da interface indica '5 payload positions' e 'Length: 107'.



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



CONCLUSÃO:

Nessas atividades orientadas a ensino foram realizadas vários testes de websites e estudos importantes na análise de segurança de dados e vulnerabilidades existentes. O estudo da gravidade das vulnerabilidades encontradas também foram realizadas, e junto com essa, a análise de consequências foi obtida. Como a gravidade e as consequências encontradas não foram baixas, essa atividade ressalta a importância da cibersegurança no mundo contemporâneo e da constante atualização dos sistemas, pentests e estudos. Dessa forma, é possível manter a estrutura dos servidores afastada de ataques maliciosos.

Assim, o estudo foi essencial para conhecimento pessoal e para a formação acadêmica e profissional.

Campo Grande, 27 de Novembro de 2023.

Gustavo Lube Machado de Melo
Acadêmico