INE5429 - Segurança em Computação
Trabalho Individual IV

16100725 - Fabíola Maria Kretzer

4 de junho de 2019

Questão 1

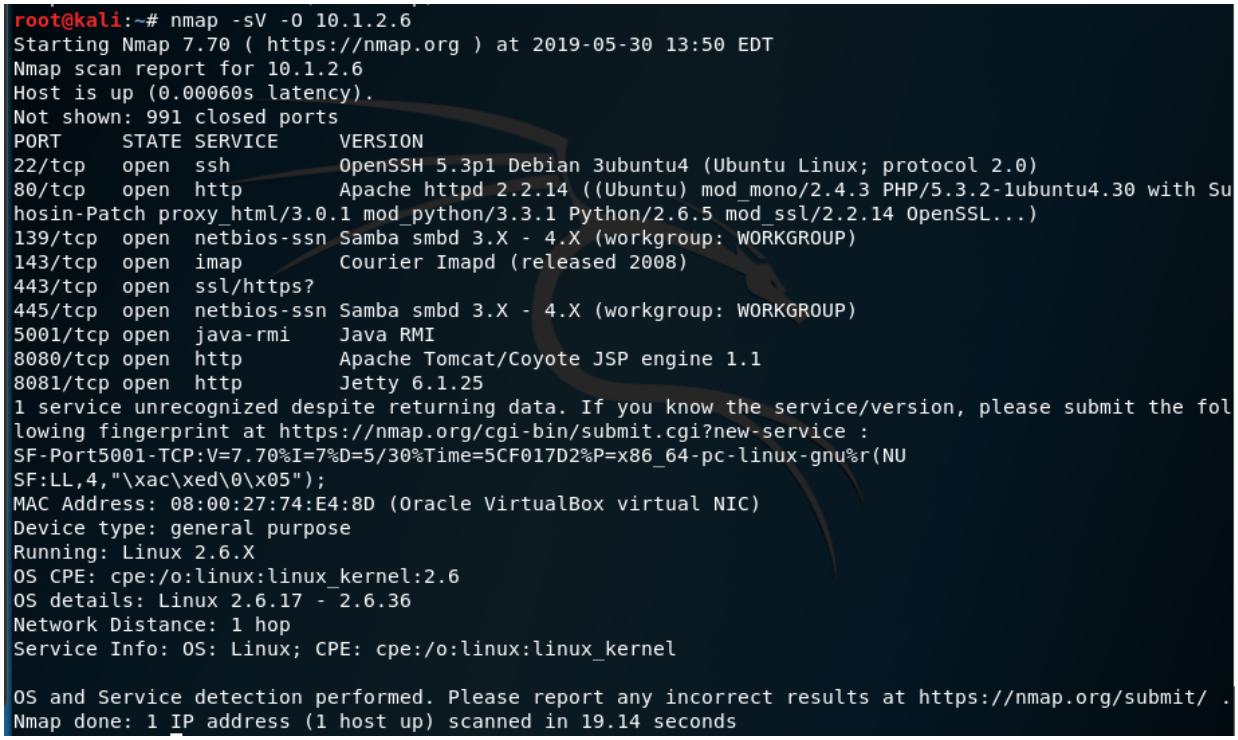


Figura 1: Tela obtida na execução do comando *nmap -sV -O 10.1.2.5*

Ao executar o comando a ferramenta nmap é inicializada, realiza uma varredura na rede até encontrar o endereço IP 10.1.2.6 e produz um relatório de verificação desse IP. No relatório são detectadas a versão e o tipo de serviço em execução em cada porta aberta, não sendo mostrados as 991 portas fechadas que a máquina com IP 10.1.2.6 possui. Essas portas fechadas são acessíveis (recebe e responde aos pacotes de sondagem do Nmap), mas não há nenhum aplicativo ouvindo nela [2]. Uma das portas abertas é a porta 80 (demostrando que a máquina está aceitando ativamente conexões TCP ou pacotes UDP nessa porta) [2]. Essa porta está diretamente ligada ao protocolo TCP, o qual é a base da *internet* e também tem relação com o protocolo HTTP, que realiza funções importantes no envio e recebimento de dados; e envolve um conexão TCP completa, portanto fica registrado nos logs da máquina remota. A versão do sistema operacional da máquina

escaneada se torna conhecido pelo comando -*O*, possuindo um *Linux 2.6.X* e um *MAC adress* 08:00:27:74:E4:8D.

Questão 2

Primeiramente a ferramenta Nmap é inicializada, carregada e inicializa os *scripts* que vão detectar serviços na rede através do NSE (*Nmap Scripting Engine*) que permite executar *scripts* de usuário. Através de um SYN enviado ao IP 10.1.2.6 é descoberto que algumas portas estao abertas, fazendo com que o SYN não seja efetivamente completado, para dificultar sua detecção. Em seguida, detecta o número de serviços realizados pelo dono do IP 10.1.2.6 (nesse caso serviço) e mostra as portas que oferecem os serviços. São mostradas os serviços e os métodos suportados por cada porta e também o cabeçalho que contém a versão do sistema operacional.

```
root@kali:~# nmap -v -A 10.1.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 14:12 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:12
Completed NSE at 14:12, 0.00s elapsed
Initiating NSE at 14:12
Completed NSE at 14:12, 0.00s elapsed
Initiating ARP Ping Scan at 14:12
Scanning 10.1.2.6 [1 port]
Completed ARP Ping Scan at 14:12, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:12
Completed Parallel DNS resolution of 1 host. at 14:12, 0.00s elapsed
Initiating SYN Stealth Scan at 14:12
Scanning 10.1.2.6 [1000 ports]
Discovered open port 139/tcp on 10.1.2.6
Discovered open port 8080/tcp on 10.1.2.6
Discovered open port 143/tcp on 10.1.2.6
Discovered open port 80/tcp on 10.1.2.6
Discovered open port 443/tcp on 10.1.2.6
Discovered open port 445/tcp on 10.1.2.6
Discovered open port 22/tcp on 10.1.2.6
Discovered open port 8081/tcp on 10.1.2.6
Discovered open port 5001/tcp on 10.1.2.6
Completed SYN Stealth Scan at 14:12, 0.11s elapsed (1000 total ports)
Initiating Service scan at 14:12
Scanning 9 services on 10.1.2.6
Completed Service scan at 14:12, 14.02s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 10.1.2.6
NSE: Script scanning 10.1.2.6.
Initiating NSE at 14:12
Completed NSE at 14:13, 90.03s elapsed
Initiating NSE at 14:13
Completed NSE at 14:13, 0.01s elapsed
Nmap scan report for 10.1.2.6
Host is up (0.00069s latency).
Not shown: 991 closed ports
```

Figura 2: Tela obtida na execução do comando *nmap -v –A 10.1.2.5* (parte 1)

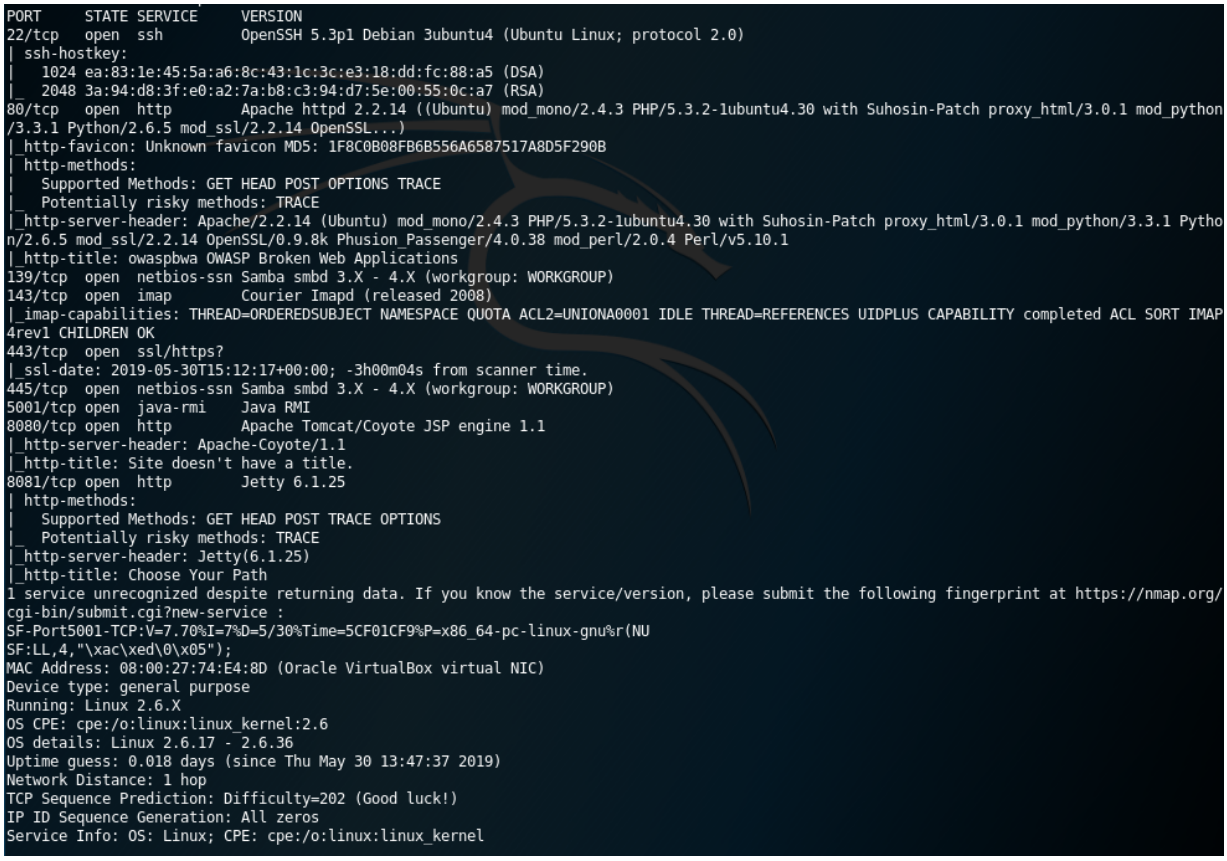


Figura 3: Tela obtida na execução do comando *nmap -v –A 10.1.2.5* (parte 2)

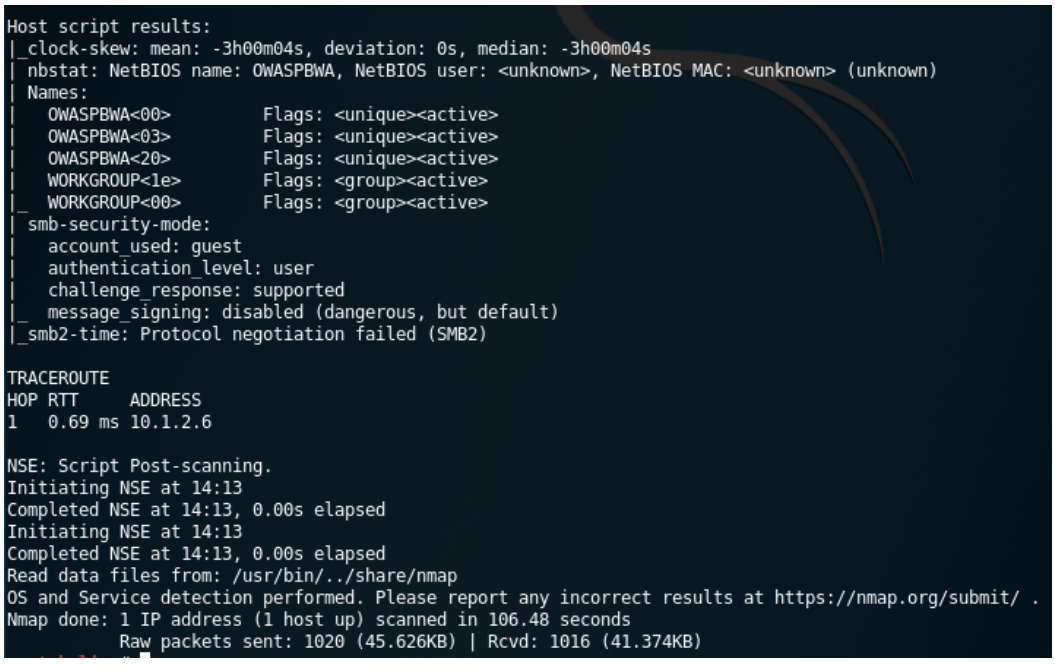


Figura 4: Tela obtida na execução do comando *nmap -v –A 10.1.2.5* (parte 3)

Questão 3

Quando a ferramenta Nmap é inicializada, esta procura o *Ping* que corresponde ao endereço www.ufsc.br e converte os endereços IP em nomes de domínio através da re-

solução de DNS. Em seguida envia um SYN e realiza um *scan* da rede de forma que a conexão não chegue a ser efetivamente completado, dificultando a sua detecção. O resultado do *scan* será aproximadamente metade das portas abertas para os protocolos TCP e UDP. Estão listadas as portas encontradas, seu estado, o serviço que oferecem e a resposta ao SYN enviado anteriormente. Pode-se observar que as portas 80 e 443 estão abertas e as outras portas que estão listadas na imagem estão em estado filtrado. Ou seja, o Nmap não pode determinar se a porta está aberta porque a filtragem de pacotes impede o alcance a porta [2].

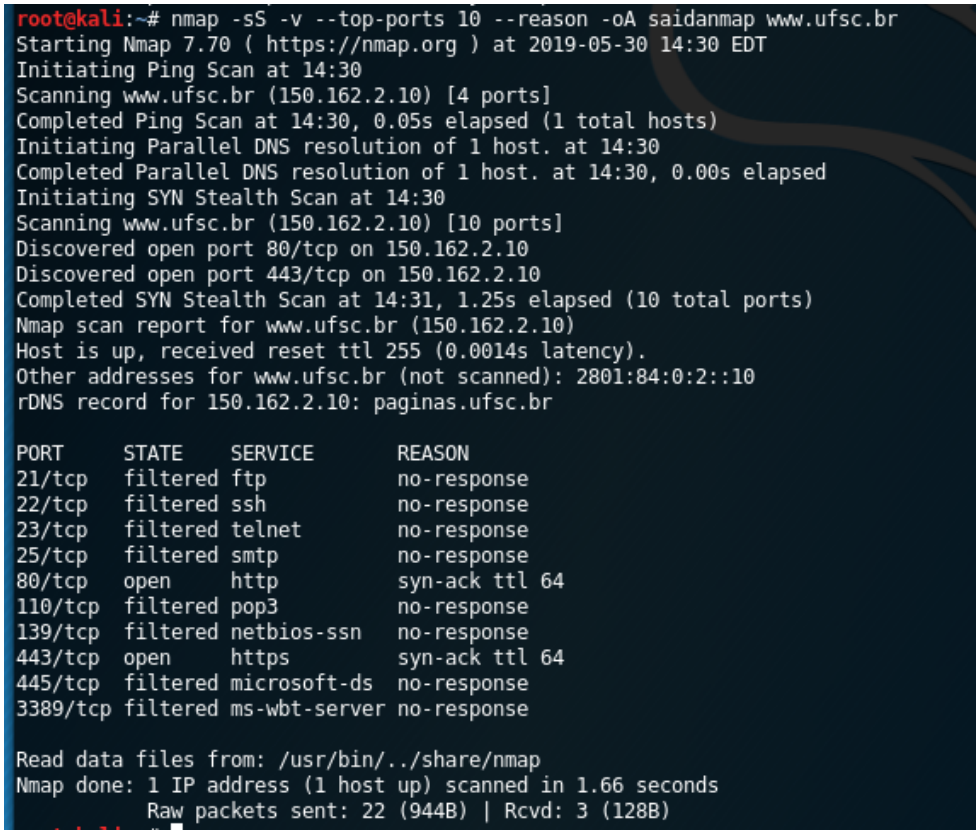


Figura 5: Tela obtida na execução do comando *nmap -sS -v –top-ports 10 –reason -oA saidanmap www.ufsc.br*

Questão 4

Depois de inicializada, a ferramenta Nmap converte os endereços IP em nomes de domínio através da resolução de DNS. Envia um SYN ao IP 10.1.2.6 e descobre que algumas portas estão abertas, fazendo com que o SYN não seja efetivamente completado. Em seguida mostra uma lista com os serviços que realizados pelo dono do IP 10.1.2.6 e o seu sistema operacional.

Figura 6: Tela obtida na execução do comando *nmap -v -O 10.1.2.5*

Questão 5

- **Letra A:** *Scan* de conexão TCP a ativação necessita de uma conexão TCP completa, portanto fica registrado nos logs da máquina remota [3]. Enquanto que *SYN scan* uma vez que ele nunca completa uma conexão TCP [3].

- **Letra B:** A Questão 3 utiliza *SYN scan* e a Questão 1 utiliza o *scan* de conexão TCP.

- **Letra C:** Inicialmente se envia um pacote SYN, como se fosse abrir uma conexão real e então espera uma resposta [3]. Um SYN/ACK indica que a porta está ouvindo (aberta), enquanto um RST (reset) é indicativo de uma não-ouvinte [3]. Se nenhuma resposta é recebida após diversas retransmissões, a porta é marcada como filtrada [3]. Assim a porta permanece aberta e vulnerável exploração, porém se o servidor responder com um pacote RST (reset) de uma porta específica, isso indica que a

porta está fechada e não pode ser explorada [4]. A vulnerabilidade é identificada pelo código CVE-2006-6411.

Questão 6

- **Letra A:**

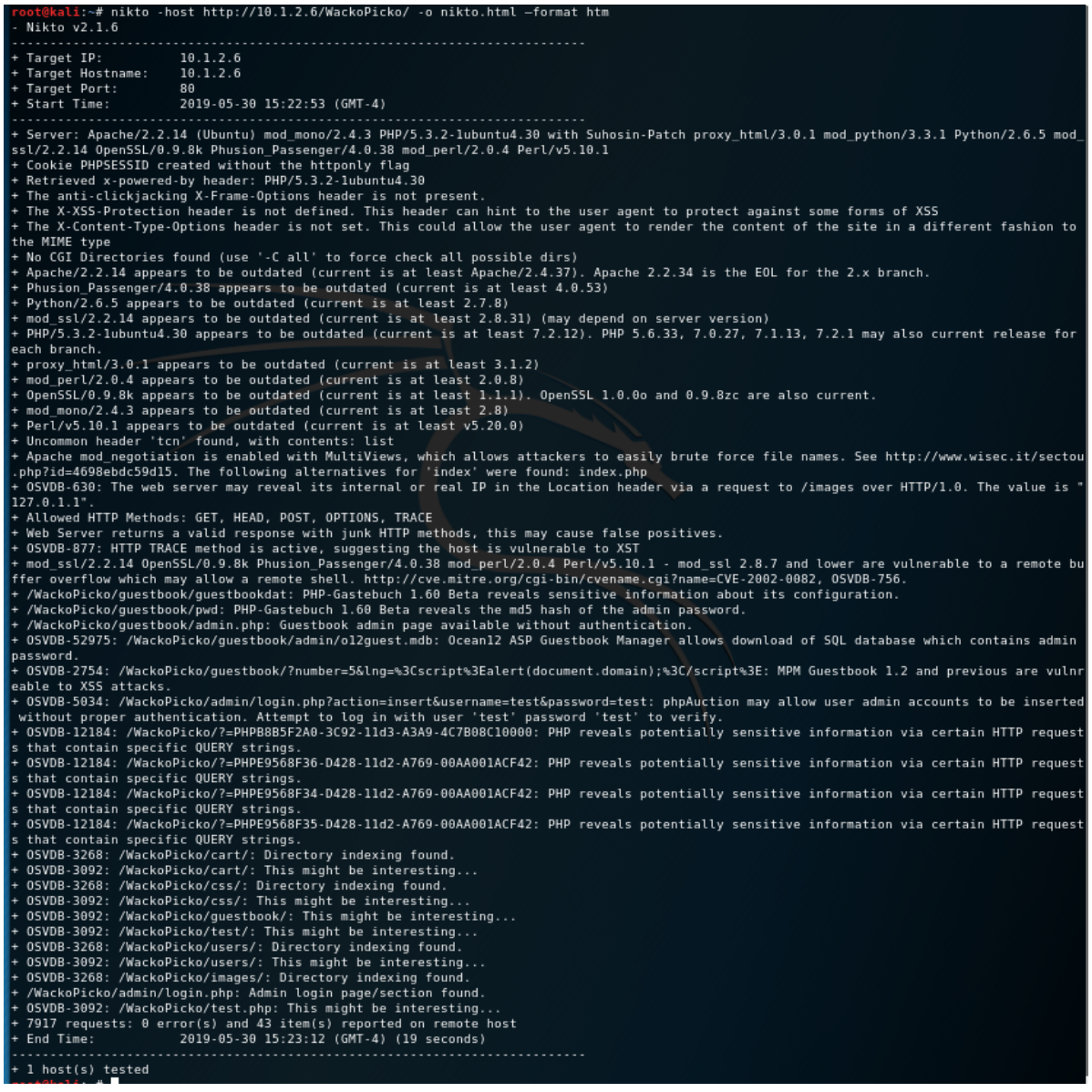
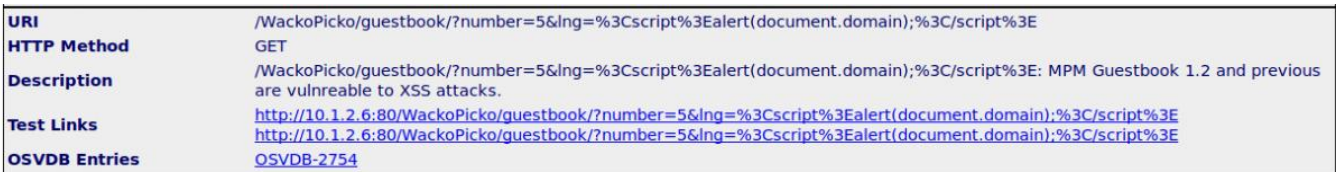


Figura 7: Tela obtida na execução do comando *nikto -host http://10.1.2.7/WackoPicko/ –o nikto.html –format htm*

- **Letra B:** O Nikto consegue capturar algumas aplicações disponíveis na máquina e faz um comparativo entre a versão disponível e a última versão, permitindo que o atacante procure vulnerabilidades nos pacotes desatualizados. Uma vulnerabilidade encontrada foi o XSS (*Cross-Site Scripting*) e pode ser observado na imagem abaixo. Outros detalhes e vulnerabilidades encontrados pelo Nikto podem ser estão nikto.html disponível no final do trabalho.



URI	/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E
HTTP Method	GET
Description	/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are vulnreable to XSS attacks.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E
OSVDB Entries	OSVDB-2754

Figura 8: Tela obtida em nikto.html

Questão 7

- **A2:** A autenticação é o processo para garantir que uma pessoa esteja acessando sua conta e os dados, geralmente é realizado através do nome do usuário e senha. Isso pode gerar uma vulnerabilidade chamada *Broken Authentication*, na qual acontece devido ao *design* e implementação da maioria dos controles de identidade e acesso [1]. O gerenciamento de sessões é a base dos controles de autenticação e acesso, estando presente em todos os aplicativos [1]. Os atacantes podem detectar uma quebra autenticação usando meios manuais, ferramentas automatizadas ou uma lista de nomes de usuários e senhas válidos [1]. Os atacantes podem ter acesso apenas a algumas contas, ou apenas um administrador conta para comprometer o sistema [1]. Uma maneira de evitar esse ataque é a implementação verificações de senhas fracas [1].

- **A3:** *Sensitive Data Exposure* ocorre quando um atacante que roubar dados confidenciais, como números de cartão de crédito. A falha mais comum é simplesmente não criptografar dados confidenciais ou são empregados geração e gerenciamento de chaves fracas ou um fraco algoritmo [1]. Assim, muitas vezes, os invasores não atacam diretamente a criptografia, eles roubam chaves, executam ataques intermediários ou roubam texto claro do servidor durante envios na *internet* [1]. Com o intuito de prevenir ataques, identifique quais dados são sensíveis de acordo com as leis de privacidade, requisitos regulatórios ou necessidades comerciais e não armazene esses dados confidenciais desnecessariamente [1].

- **A7:** O *Cross-Site Scripting* permite que códigos mal-intencionados sejam adicionados a uma página da Web ou aplicativo. Esse ataque pode via comentários ou envios de formulários usados para definir a ação subsequente. Um arquivo HTML normalmente mistura instruções com dados. Assim, um ataque bem-sucedido pode permitir que o invasor execute HTML e *JavaScript* arbitrários no navegador da vítima, no qual pode conter código que muda o comportamento padrão da página [1]. Prevenir *Cross-Site Scripting* requer separação de dados não confiáveis de conteúdo do navegador e uma das maneiras de prevenção é a utilizaçao de *frameworks* ou APIs [1].

Questão 8

- **Letra A:**

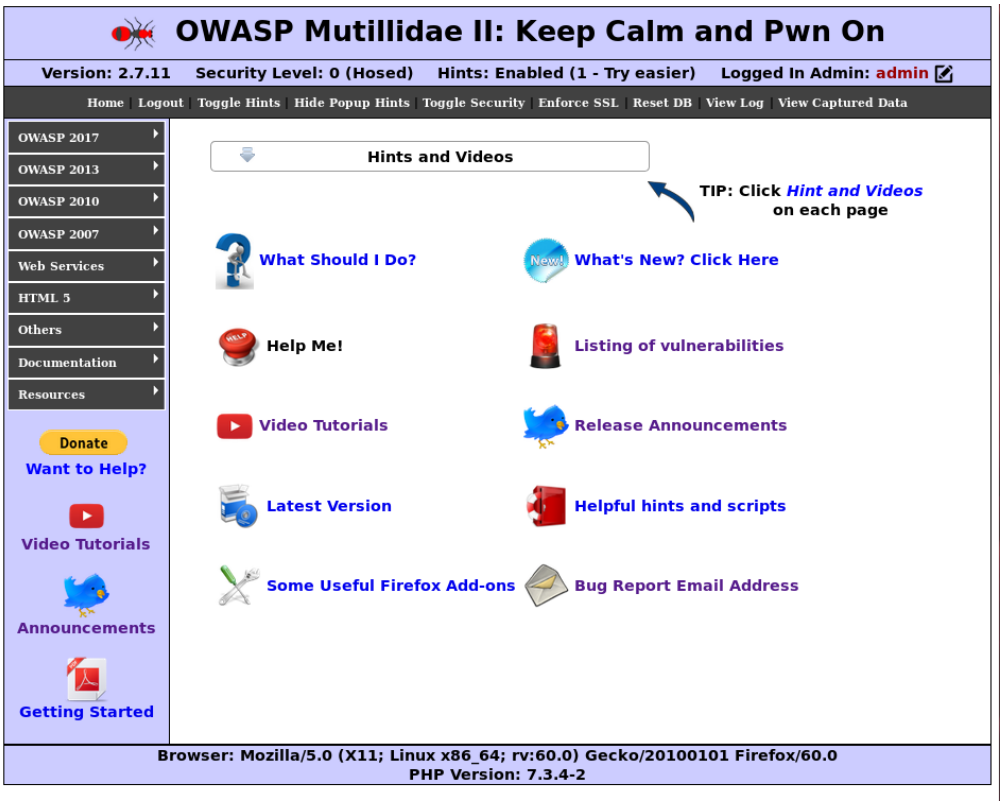


Figura 9: Tela obtida na execução string ' or 1=1 – ' no campo *Username*

- **Letra B:** Neste caso o ocorre o *Login* no usuário "admin". A vulnerabilidade é *Injection*, que acontece ao inserir "carga útil"diretamente na entrada mencionada *Login*. Como não há um mecanismo de validação dos dados de entrada o servidor procura por "' or 1=1 – "". *Injection* ocorre quando um invasor executa comandos no banco de dados que inicializa um script ou outro aplicativo. O invasor também pode adicionar, alterar ou excluir dados.

- **Letra C:** Evitar *Injection* requer manter os dados separados dos comandos e consultas [1]. Uma opção é para qualquer consulta dinâmica residual, não deixe o usuário digitar caracteres especiais [1]. Usar um mecanismo para validação de entrada do lado do servidor [1]. A opção preferida é usar uma API segura, que evite o uso do interpretador por completo e assim parametrizar os dados de entrada [1].

- **Letra D:** O usuário "admin"sai de sua conta e volta para a tela de *Login*.

Questão 9

- **Letra A:** O *Cross-Site Scripting* permite que códigos mal-intencionados sejam adicionados a uma página da Web ou aplicativo [1]. Quando uma página utiliza conteúdo inserido pelo usuário como parte de uma página sem verificar as coisas ruins, um usuário mal-intencionado pode inserir conteúdo (arquivo com código malicioso) que muda o comportamento padrão da página. Neste caso são listados nomes de usuário e suas senhas, mudando o comportamento padrão dessa página.

- **Letra B:**

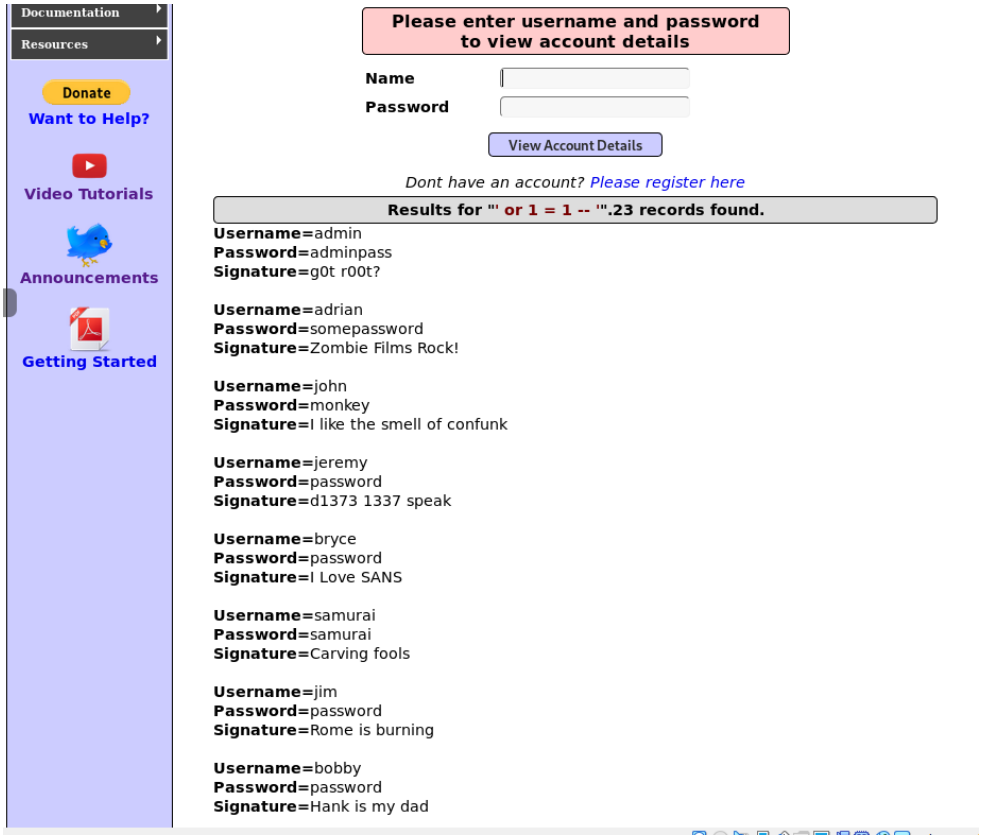


Figura 10: Tela obtida na execução string ' or 1=1 – ' no campo *Name*

- **Letra C:** Evitar a exploração dessa vulnerabilidade envolve a separação de dados não confiáveis do conteúdo do navegador ativo através do uso de estruturas que escapam automaticamente do XSS, aprendendo as limitações da proteção XSS de cada estrutura e manipule apropriadamente os casos de uso não cobertos [1]. Ative uma política de segurança de conteúdo, na qual é eficaz se não existirem outras vulnerabilidades que permitam a colocação de códigos maliciosos através de inclusão de arquivos locais [1]. Utilize APIs semelhantes as aplicadas ao navegador [1].

Questão 10

- **Letra A:** Execução da ferramenta OWASP ZAP.
- **Letra B:** A ferramenta gerou um relatório que descreve algumas vulnerabilidades encontradas na máquina e com resolvê-las. Também classifica as vulnerabilidades por nível de risco (alto, médio e alto). O relatório pode ser encontrado no final do trabalho.

Questão 11

No primeiro ataque foi explorada a vulnerabilidade *SQL Injection*, deletando a tabela de contas do sistema utilizando o seguinte link: http://localhost/mutillidae/index.php?page=user-info.php.

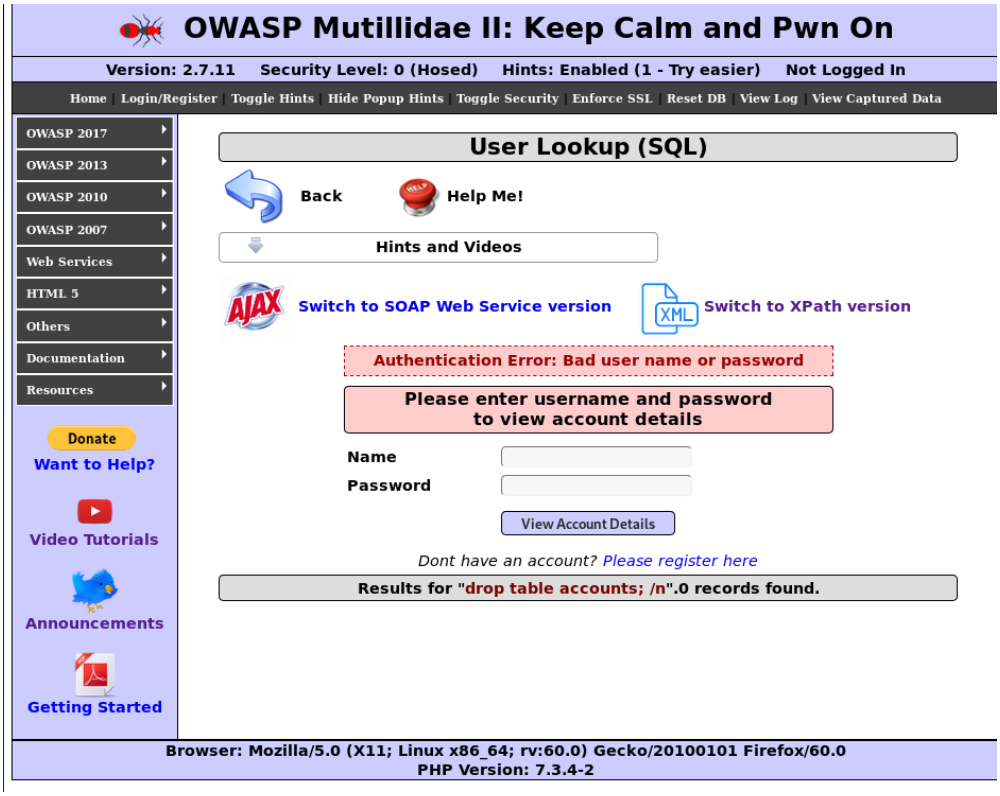


Figura 11: Tela obtida na execução string drop table accounts; \n no campo *Name*

No segundo ataque foi explorada a vulnerabilidade *Sensitive Data Exposure*. Essa vulnerabilidade ocorre pois alguns dados que deveriam estar protegidos foram expostos. O link http://localhost/mutillidae/index.php?page=./robots.txt mostra os arquivos que não devem ser divulgados, mas é possível ter acesso.

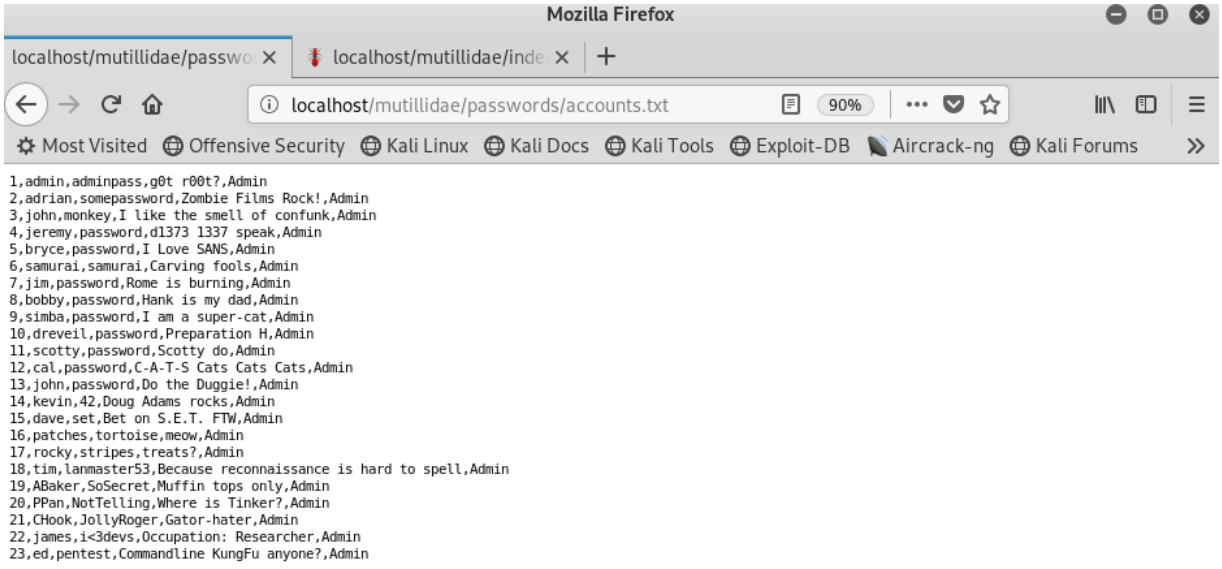


Figura 12: Captura de tela de um documento exposto

Questão 12

- **Letra A:** *Shodan* é um scanner que encontra e informa a localização física de dispositivos conectados pela *internet* [7]. Semáforos, câmeras de segurança, dispositivos de aquecimento doméstico e monitores de bebês, podem ser encontrados pelo *Shodan* [7]. Este scanner também pode encontrar o sistema SCADA como estações de gás, usinas nucleares [7]. *Shodan* pode criar violação na privacidade dos usuários, porque consegue encontrar o *ping* de qualquer dispositivo conectado através da *internet* sem levar a permissão dos usuários [7].

- **Letra B:**

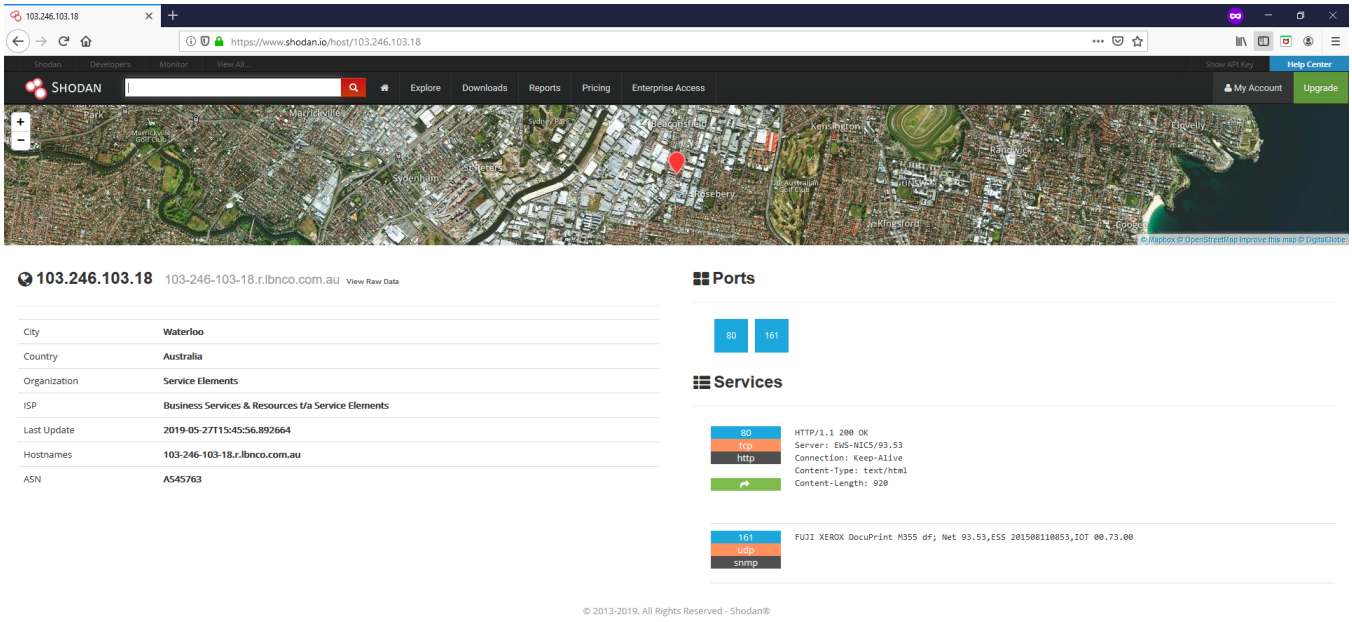


Figura 13: Dispositivo IoT encontrado

Questão 13

- **Letra A:** É uma câmera de segurança colocada em frente a *outdoor* e também é possível visualisar os carros e as pessoas que passam naquela rua.

- **Letra B:** Pode-se observar as pessoas e os carros que passam no local,e também os horários para possíveis furtos.

Questão 14

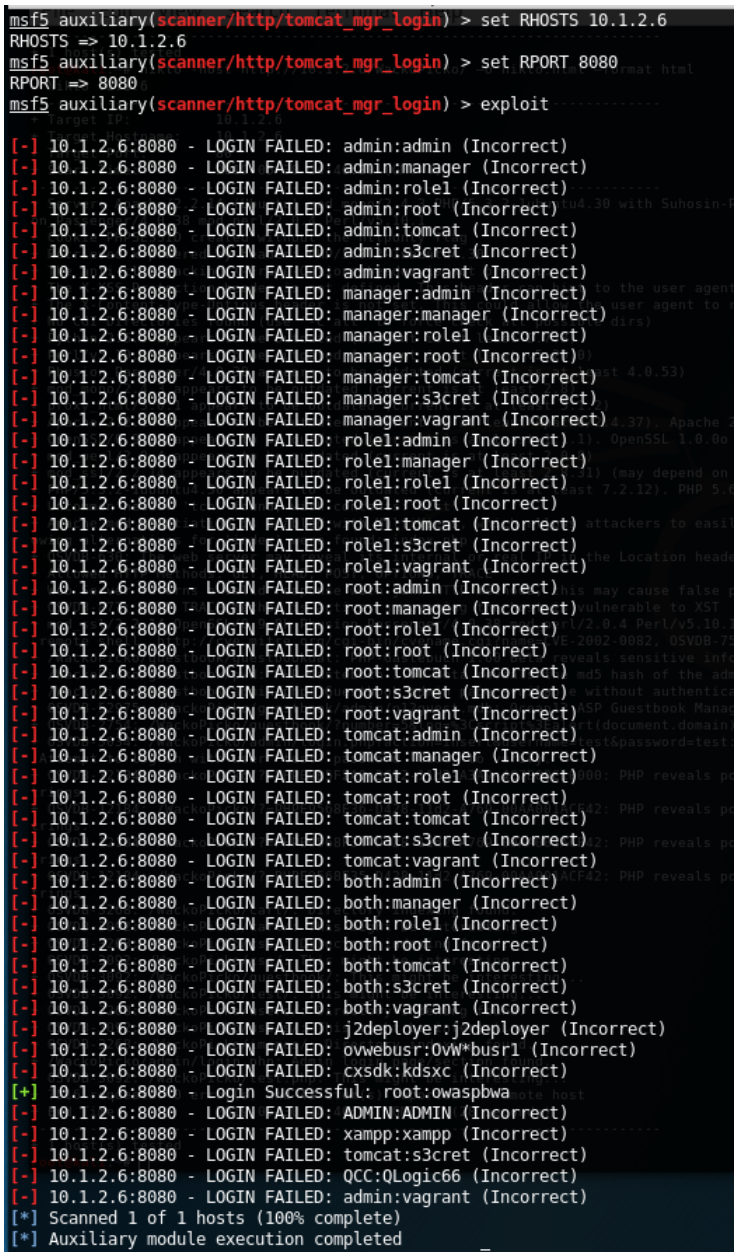


Figura 14: Tela obtida após a sequência de comandos

- **Letra A:** Um ataque de dicionário é uma técnica usada para violar a segurança do computador de uma máquina ou servidor protegido por senha [5]. Um ataque de dicionário tenta derrotar um mecanismo de autenticação, inserindo sistematicamente cada palavra em um dicionário como uma senha ou tentando determinar a chave de descriptografia de uma mensagem ou documento criptografado [5]. Os ataques de dicionário geralmente são bem-sucedidos porque muitos usuários e empresas usam palavras comuns como senhas [5].
- **Letra B:** O usuário e a senha para autentificação no IP 10.1.2.6.
- **Letra C:** A vulnerabilidade explorada foi a utilização de usuário e senha padrão.

- **Letra D:** O atacante pode logar no sistema com o usuário e a senha e ter o controle da máquina.

Questão 15

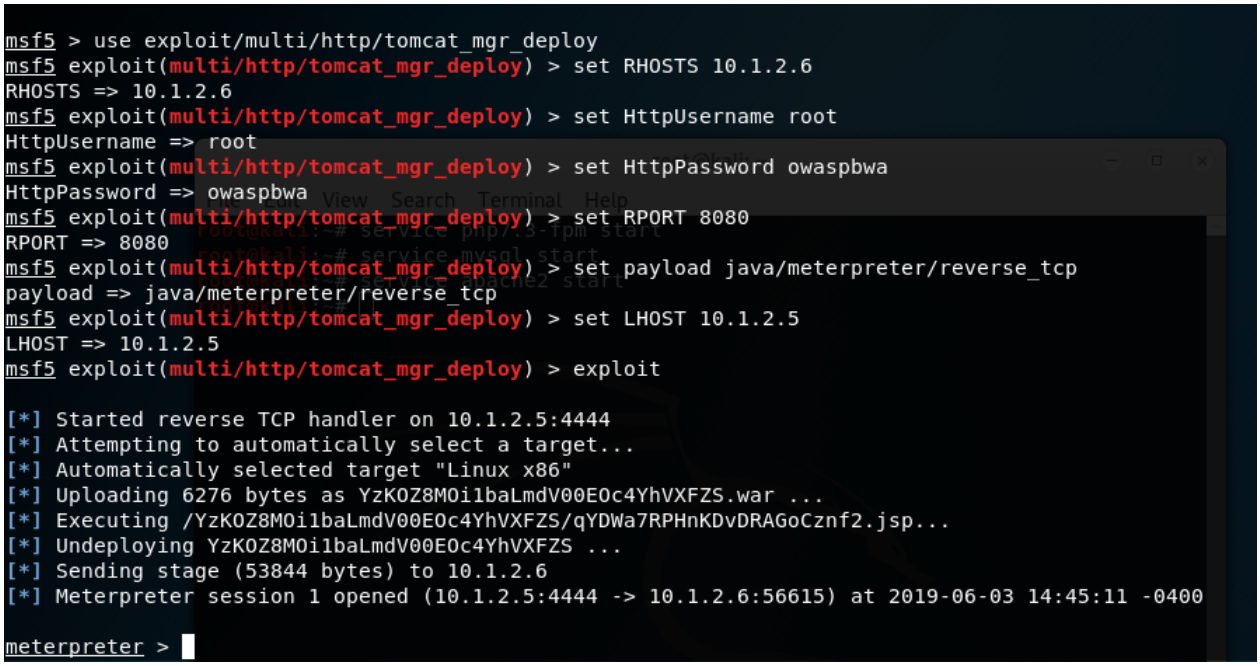


Figura 15: Tela obtida após a sequência de comandos

- **Letra A:** a vulnerabilidade é a mesma da questão anterior. Na questão anterior o usuário e a senha foram descobertos e nesta questão esses valores foram configurados na ferramenta para realizar o ataque.
- **Letra B:** O *exploit* conecta a máquina *localhost* na outra máquina através do protocolo TCP.
- **Letra C:** O *Meterpreter* é uma carga útil avançada, extensível dinamicamente, que usa injeção de DLL na memória e é espanhado pela rede em tempo de execução [6]. Ele se comunica através do soquete e fornece uma abrangente API do lado do cliente. Ele apresenta histórico de comandos, conclusão de guias, canais e muito mais [6].
- **Letra D:** Depois de executar o comando *exploit* é possível alterar dados e executar comandos.

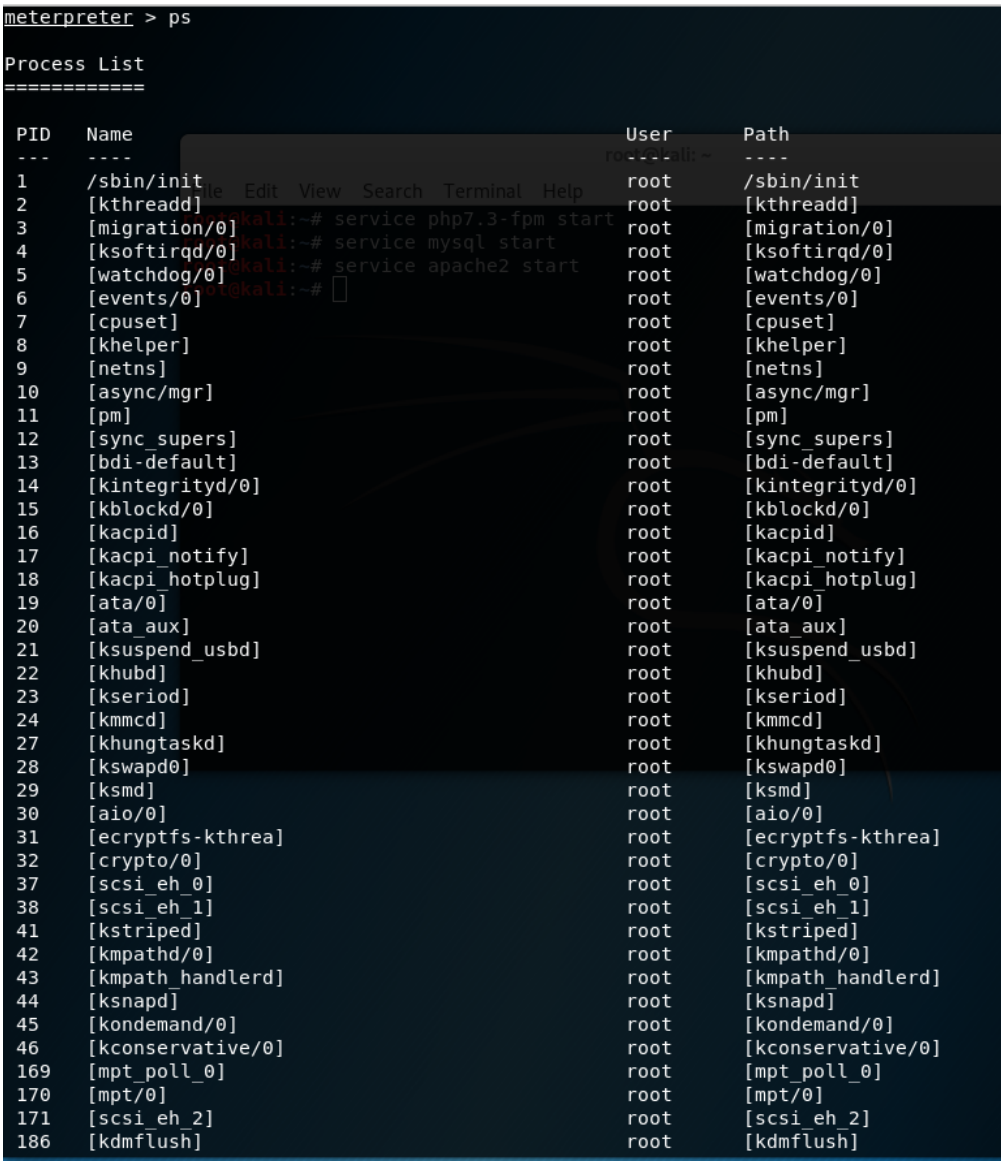


Figura 16: O comando *ps* retorna os processos que estão rodando na máquina com IP 10.1.2.6

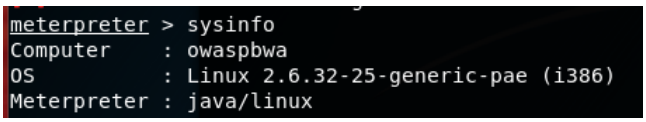


Figura 17: O comando *sysinfo* informa algumas características da máquina com IP 10.1.2.6, incluindo a versão do sistema operacional

Referências

[1] OWASP. OWASP Top 10 - 2017. Disponível em: <https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf>. Acessado em 26 de Maio de 2019.

[2] Nmap. Nmap Network Scanning. Disponível em: <https://nmap.org/book/port-scanning.html>. Acessado em 26 de Maio de 2019.

[3] Nmap. Nmap Network Scanning. Disponível em: <https://nmap.org/man/pt_BR/man-port-scanning-techniques.html>. Acessado em 26 de Maio de 2019.

[4] Margaret Rouse. SYN scanning. Disponível em: <https://searchnetworking.techtarget.com/definition/SYN-scanning>. Acessado em 26 de Maio de 2019.

[5] Techopedia. Dictionary Attack. Disponível em: <https://www.techopedia.com/definition/1774/dictionary-attack>. Acessado em 26 de Maio de 2019.

[6] Offensive Security. About the Metasploit Meterpreter. Disponível em: <https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/>. Acessado em 26 de Maio de 2019.

[7] Information Security Newspaper. Find webcams, databases, boats in the sea using Shodan. Disponível em: <https://www.securitynewspaper.com/2018/11/27/find-webcams-databases-boats-in-the-sea-using-shodan/>. Acessado em 26 de Maio de 2019.

10.1.2.6 / 10.1.2.6 port 80

Target IP	10.1.2.6
Target hostname	10.1.2.6
Target Port	80
HTTP Server	Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Site Link (Name)	http://10.1.2.6:80/WackoPicko/
Site Link (IP)	http://10.1.2.6:80/WackoPicko/

URI	/WackoPicko/
HTTP Method	GET
Description	Cookie PHPSESSID created without the httponly flag
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	HEAD
Description	Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	HEAD
Description	Python/2.6.5 appears to be outdated (current is at least 2.7.8)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	HEAD
Description	proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/

OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/index
HTTP Method	GET
Description	Uncommon header 'tcn' found, with contents: list
Test Links	http://10.1.2.6:80/WackoPicko/index http://10.1.2.6:80/WackoPicko/index
OSVDB Entries	OSVDB-0
URI	/WackoPicko/index
HTTP Method	GET
Description	Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
Test Links	http://10.1.2.6:80/WackoPicko/index http://10.1.2.6:80/WackoPicko/index
OSVDB Entries	OSVDB-0

URI	/WackoPicko/images
HTTP Method	GET
Description	The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
Test Links	http://10.1.2.6:80/WackoPicko/images http://10.1.2.6:80/WackoPicko/images
OSVDB Entries	OSVDB-630
URI	/WackoPicko/
HTTP Method	OPTIONS
Description	Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	BLOTVQPF
Description	Web Server returns a valid response with junk HTTP methods, this may cause false positives.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	TRACE
Description	HTTP TRACE method is active, suggesting the host is vulnerable to XST
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-877
URI	/WackoPicko/
HTTP Method	GET
Description	mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. CVE-2002-0082, OSVDB-756.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/guestbookdat
HTTP Method	GET
Description	/WackoPicko/guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive information about its configuration.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/guestbookdat http://10.1.2.6:80/WackoPicko/guestbook/guestbookdat
OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/pwd
HTTP Method	GET
Description	/WackoPicko/guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of the admin password.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/pwd http://10.1.2.6:80/WackoPicko/guestbook/pwd
OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/admin.php
HTTP Method	GET
Description	/WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/admin.php http://10.1.2.6:80/WackoPicko/guestbook/admin.php
OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/admin/o12guest.mdb
HTTP Method	GET
Description	/WackoPicko/guestbook/admin/o12guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains admin password.

Test Links	http://10.1.2.6:80/WackoPicko/guestbook/admin/o12guest.mdb http://10.1.2.6:80/WackoPicko/guestbook/admin/o12guest.mdb
OSVDB Entries	OSVDB-52975
URI	/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E
HTTP Method	GET
Description	/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are vulnreable to XSS attacks.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E
OSVDB Entries	OSVDB-2754
URI	/WackoPicko/admin/login.php?action=insert&username=test&password=test
HTTP Method	GET
Description	/WackoPicko/admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify.
Test Links	http://10.1.2.6:80/WackoPicko/admin/login.php?action=insert&username=test&password=test http://10.1.2.6:80/WackoPicko/admin/login.php?action=insert&username=test&password=test
OSVDB Entries	OSVDB-5034
URI	/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
HTTP Method	GET
Description	/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 http://10.1.2.6:80/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42
HTTP Method	GET
Description	/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42 http://10.1.2.6:80/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
HTTP Method	GET
Description	/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42 http://10.1.2.6:80/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42
HTTP Method	GET
Description	/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42 http://10.1.2.6:80/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/cart/
HTTP Method	GET
Description	/WackoPicko/cart/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/cart/ http://10.1.2.6:80/WackoPicko/cart/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/cart/
HTTP Method	GET

Description	/WackoPicko/cart/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/cart/ http://10.1.2.6:80/WackoPicko/cart/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/css/
HTTP Method	GET
Description	/WackoPicko/css/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/css/ http://10.1.2.6:80/WackoPicko/css/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/css/
HTTP Method	GET
Description	/WackoPicko/css/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/css/ http://10.1.2.6:80/WackoPicko/css/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/guestbook/
HTTP Method	GET
Description	/WackoPicko/guestbook/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/ http://10.1.2.6:80/WackoPicko/guestbook/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/test/
HTTP Method	GET
Description	/WackoPicko/test/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/test/ http://10.1.2.6:80/WackoPicko/test/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/users/
HTTP Method	GET
Description	/WackoPicko/users/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/users/ http://10.1.2.6:80/WackoPicko/users/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/users/
HTTP Method	GET
Description	/WackoPicko/users/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/users/ http://10.1.2.6:80/WackoPicko/users/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/images/
HTTP Method	GET
Description	/WackoPicko/images/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/images/ http://10.1.2.6:80/WackoPicko/images/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/admin/login.php
HTTP Method	GET
Description	/WackoPicko/admin/login.php: Admin login page/section found.
Test Links	http://10.1.2.6:80/WackoPicko/admin/login.php http://10.1.2.6:80/WackoPicko/admin/login.php
OSVDB Entries	OSVDB-0
URI	/WackoPicko/test.php
HTTP Method	GET
Description	/WackoPicko/test.php: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/test.php http://10.1.2.6:80/WackoPicko/test.php
OSVDB Entries	OSVDB-3092

Host Summary

Start Time	2019-05-30 15:18:13
End Time	2019-05-30 15:18:39
Elapsed Time	26 seconds
Statistics	7916 requests, 0 errors, 43 findings

Scan Summary

Software Details	Nikto 2.1.6
CLI Options	-host http://10.1.2.6/WackoPicko/ -o nikto.html –format htm
Hosts Tested	1
Start Time	Thu May 30 15:18:12 2019
End Time	Thu May 30 15:18:39 2019
Elapsed Time	27 seconds

10.1.2.6 / 10.1.2.6 port 80

Target IP	10.1.2.6
Target hostname	10.1.2.6
Target Port	80
HTTP Server	Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Site Link (Name)	http://10.1.2.6:80/WackoPicko/
Site Link (IP)	http://10.1.2.6:80/WackoPicko/

URI	/WackoPicko/
HTTP Method	GET
Description	Cookie PHPSESSID created without the httponly flag
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	GET
Description	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0

URI	/WackoPicko/
HTTP Method	HEAD
Description	Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	Python/2.6.5 appears to be outdated (current is at least 2.7.8)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	HEAD
Description	mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/

HTTP Method	HEAD
Description	Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/index
HTTP Method	GET
Description	Uncommon header 'tcn' found, with contents: list
Test Links	http://10.1.2.6:80/WackoPicko/index http://10.1.2.6:80/WackoPicko/index
OSVDB Entries	OSVDB-0
URI	/WackoPicko/index
HTTP Method	GET
Description	Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
Test Links	http://10.1.2.6:80/WackoPicko/index http://10.1.2.6:80/WackoPicko/index
OSVDB Entries	OSVDB-0
URI	/WackoPicko/images
HTTP Method	GET
Description	The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
Test Links	http://10.1.2.6:80/WackoPicko/images http://10.1.2.6:80/WackoPicko/images
OSVDB Entries	OSVDB-630
URI	/WackoPicko/
HTTP Method	OPTIONS
Description	Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	LWQWRNXK
Description	Web Server returns a valid response with junk HTTP methods, this may cause false positives.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/
HTTP Method	TRACE
Description	HTTP TRACE method is active, suggesting the host is vulnerable to XST
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-877
URI	/WackoPicko/
HTTP Method	GET
Description	mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. CVE-2002-0082, OSVDB-756.
Test Links	http://10.1.2.6:80/WackoPicko/ http://10.1.2.6:80/WackoPicko/
OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/guestbookdat
HTTP Method	GET
Description	/WackoPicko/guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive information about its configuration.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/guestbookdat http://10.1.2.6:80/WackoPicko/guestbook/guestbookdat

OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/pwd
HTTP Method	GET
Description	/WackoPicko/guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of the admin password.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/pwd http://10.1.2.6:80/WackoPicko/guestbook/pwd
OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/admin.php
HTTP Method	GET
Description	/WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/admin.php http://10.1.2.6:80/WackoPicko/guestbook/admin.php
OSVDB Entries	OSVDB-0
URI	/WackoPicko/guestbook/admin/o12guest.mdb
HTTP Method	GET
Description	/WackoPicko/guestbook/admin/o12guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains admin password.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/admin/o12guest.mdb http://10.1.2.6:80/WackoPicko/guestbook/admin/o12guest.mdb
OSVDB Entries	OSVDB-52975
URI	/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E
HTTP Method	GET
Description	/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are vulnreable to XSS attacks.
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E http://10.1.2.6:80/WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E
OSVDB Entries	OSVDB-2754
URI	/WackoPicko/admin/login.php?action=insert&username=test&password=test
HTTP Method	GET
Description	/WackoPicko/admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify.
Test Links	http://10.1.2.6:80/WackoPicko/admin/login.php?action=insert&username=test&password=test http://10.1.2.6:80/WackoPicko/admin/login.php?action=insert&username=test&password=test
OSVDB Entries	OSVDB-5034
URI	/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
HTTP Method	GET
Description	/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 http://10.1.2.6:80/WackoPicko/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42
HTTP Method	GET
Description	/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42 http://10.1.2.6:80/WackoPicko/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
HTTP Method	GET

Description	/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42 http://10.1.2.6:80/WackoPicko/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42
HTTP Method	GET
Description	/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
Test Links	http://10.1.2.6:80/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42 http://10.1.2.6:80/WackoPicko/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42
OSVDB Entries	OSVDB-12184
URI	/WackoPicko/cart/
HTTP Method	GET
Description	/WackoPicko/cart/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/cart/ http://10.1.2.6:80/WackoPicko/cart/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/cart/
HTTP Method	GET
Description	/WackoPicko/cart/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/cart/ http://10.1.2.6:80/WackoPicko/cart/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/css/
HTTP Method	GET
Description	/WackoPicko/css/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/css/ http://10.1.2.6:80/WackoPicko/css/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/css/
HTTP Method	GET
Description	/WackoPicko/css/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/css/ http://10.1.2.6:80/WackoPicko/css/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/guestbook/
HTTP Method	GET
Description	/WackoPicko/guestbook/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/guestbook/ http://10.1.2.6:80/WackoPicko/guestbook/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/test/
HTTP Method	GET
Description	/WackoPicko/test/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/test/ http://10.1.2.6:80/WackoPicko/test/
OSVDB Entries	OSVDB-3092
URI	/WackoPicko/users/
HTTP Method	GET
Description	/WackoPicko/users/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/users/ http://10.1.2.6:80/WackoPicko/users/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/users/
HTTP Method	GET
Description	/WackoPicko/users/: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/users/ http://10.1.2.6:80/WackoPicko/users/

OSVDB Entries	OSVDB-3092
URI	/WackoPicko/images/
HTTP Method	GET
Description	/WackoPicko/images/: Directory indexing found.
Test Links	http://10.1.2.6:80/WackoPicko/images/ http://10.1.2.6:80/WackoPicko/images/
OSVDB Entries	OSVDB-3268
URI	/WackoPicko/admin/login.php
HTTP Method	GET
Description	/WackoPicko/admin/login.php: Admin login page/section found.
Test Links	http://10.1.2.6:80/WackoPicko/admin/login.php http://10.1.2.6:80/WackoPicko/admin/login.php
OSVDB Entries	OSVDB-0
URI	/WackoPicko/test.php
HTTP Method	GET
Description	/WackoPicko/test.php: This might be interesting...
Test Links	http://10.1.2.6:80/WackoPicko/test.php http://10.1.2.6:80/WackoPicko/test.php
OSVDB Entries	OSVDB-3092

Host Summary

Start Time	2019-05-30 15:22:53
End Time	2019-05-30 15:23:12
Elapsed Time	19 seconds
Statistics	7917 requests, 0 errors, 43 findings

Scan Summary

Software Details	Nikto 2.1.6
CLI Options	-host http://10.1.2.6/WackoPicko/ -o nikto.html –format htm
Hosts Tested	1
Start Time	Thu May 30 15:22:52 2019
End Time	Thu May 30 15:23:12 2019
Elapsed Time	20 seconds

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	4
Low	4
Informational	0

Alert Detail

High (Medium)	Cross Site Scripting (Reflected)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	POST
Parameter	comment
Attack	<script>alert(1);</script>
Evidence	<script>alert(1);</script>
URL	http://10.1.2.6/WackoPicko/pictures/search.php?query=%22%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
Method	GET
Parameter	query
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://10.1.2.6/WackoPicko/guestbook.php?query=%3C%2Fp%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cp%3E
Method	GET
Parameter	query
Attack	<script>alert(1);</script>
Evidence	<script>alert(1);</script>
URL	http://10.1.2.6/WackoPicko/guestbook.php?query=%3C%2Fp%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cp%3E
Method	POST
Parameter	query
Attack	<script>alert(1);</script>
Evidence	<script>alert(1);</script>
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	POST
Parameter	name
Attack	<script>alert(1);</script>
Evidence	<script>alert(1);</script>
Instances	5
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8

Source ID	1

Medium (Medium)	Directory Browsing
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files , backup source files etc which can be accessed to read sensitive information.
URL	http://10.1.2.6/WackoPicko/cart/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/upload/doggie/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/upload/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/upload/waterfall/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/upload/house/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/users/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/pictures/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/css/blueprint/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/upload/toga/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/css/
Method	GET
Attack	Parent Directory
URL	http://10.1.2.6/WackoPicko/upload/flowers/
Method	GET
Attack	Parent Directory
Instances	11
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html
CWE Id	548
WASC Id	48
Source ID	1

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://10.1.2.6/WackoPicko/passcheck.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559318725
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/cart/review.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/users/login.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/pictures/recent.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/passcheck.php
Method	POST
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/calendar.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/tos.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/pictures/search.php?query=ZAP
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559405125
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/users/sample.php?userid=1

Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	POST
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559491525
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	POST
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559577925
Method	GET
Parameter	X-Frame-Options
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	POST
Parameter	X-Frame-Options
Instances	20
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Medium (Medium)	**Buffer Overflow**
Description	Buffer overflow errors are characterized by the overwriting of memory spaces of the background web process, which should have never been modified intentionally or unintentionally. Overwriting values of the IP (Instruction P
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	POST
Parameter	page
Attack	POST http://10.1.2.6/WackoPicko/admin/index.php? page=EmBGKvwXpRjQkfsAFQZCOPhRGSmeXnrLFwPoMxGRSwjUZVnfURNpFMZVCqcimxpJMKKBRWRTmrvMtvpjCCoCUYOFvCHZCUkBAmuFsiesacKRZkbILwcoaKwULYvbywnCkZcCjPFSeadDbcCHiswWEBMdDZC HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Pragma: no-cache Cache-Control: no-cache Content-Type: application/x-www-form-urlencoded Content-Length: 26 Refer
URL	http://10.1.2.6/WackoPicko/admin
Method	GET
Parameter	query
Attack	GET http://10.1.2.6/WackoPicko/admin? query=AlGoLpCcsyNjFucsFHAVsbnfNuvRlsRiaERPUtmvlXRTmglQpJhxJqZNVhGGTsiHlCRKyCZsYRHCFOoDiLTJHjaRRLQhKgkhNjwyrQsptxfQDejtoKUkeJYEDqeJDsergrDCGmLqLSGHLqJdJJNKtLdfxUxDaLOHJevsqfV Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Pragma: no-cache Cache-Control: no-cache Referer: http://10.1.2.6/WackoPicko/ Cookie: PHPSESSID=nue7t6ssojki2rc5721d4to9p4 Content-L
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	GET
Parameter	page
Attack	GET http://10.1.2.6/WackoPicko/admin/index.php? page=ZKdRMKlcCKFAUmfQcHJRMMoLuHKgtdmamJLQPDdMncJyYouJRQswKacQbTTOWSQUBjriOlXtsqXysCxDiVINNdqGZFdVbyMECLSvrDAlxMfZtWstFhKnkydbMhrdgMhVLBdsVMNuFljEcXKtvmXfKkeuZZxiBZGSImi (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Pragma: no-cache Cache-Control: no-cache Content-Length: 0 Referer: http://10.1.2.6/WackoPicko/ Cookie: PHPSESSID=nue7t6ssojki2rc5721d4to9p4 Ho
Instances	3
Solution	Rewrite the background program using proper return length checking. This will require a recompile of the background executable.
Other information	Potential Buffer Overflow. The script closed the connection and threw a 500 Internal Server Error
Reference	https://www.owasp.org/index.php/Buffer_overflow_attack
CWE Id	120
WASC Id	7
Source ID	1

Medium (Medium)	**Format String Error**
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	http://10.1.2.6/WackoPicko/admin/index.php? page=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n
Method	GET
Parameter	page
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://10.1.2.6/WackoPicko/admin? query=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25
Method	GET
Parameter	query
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://10.1.2.6/WackoPicko/admin/index.php? page=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n
Method	POST
Parameter	page
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
Instances	3
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.
Other information	Potential Format String Error. The script closed the connection on a /%s
Reference	https://www.owasp.org/index.php/Format_string_attack
CWE Id	134
WASC Id	6
Source ID	1

Low (Medium)	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://10.1.2.6/WackoPicko/

Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/tos.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/pictures/search.php?query=ZAP
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/css/blueprint/screen.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559577925
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/css/stylings.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559405125
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/css/blueprint/print.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/pictures/recent.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	POST
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/css/blueprint/ie.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/users/sample.php?userid=1
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/calendar.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/upload/doggie/Dog.jpg.128_128.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/upload/toga/togasfs.128_128.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/upload/house/hodjjgld.128_128.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/upload/flowers/flweofoee.128_128.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/users/login.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	POST
Parameter	X-Content-Type-Options
Instances	33
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://10.1.2.6/WackoPicko/
Method	GET
Parameter	PHPSESSID
Evidence	Set-Cookie: PHPSESSID
Instances	1
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3

Low (Medium)	Password Autocomplete in Browser
Description	The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	POST
Parameter	password
Evidence	<input type="password" name="password" />
URL	http://10.1.2.6/WackoPicko/passcheck.php
Method	POST
Parameter	password
Evidence	<input type="password" name="password" />
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	GET
Parameter	password
Evidence	<input type="password" name="password" />
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	POST
Parameter	password
Evidence	<input type="password" name="password" />
URL	http://10.1.2.6/WackoPicko/users/login.php
Method	GET
Parameter	password
Evidence	<input type="password" name="password" />
URL	http://10.1.2.6/WackoPicko/passcheck.php
Method	GET
Parameter	password
Evidence	<input type="password" name="password" />
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	GET
Parameter	password
Evidence	<input type="password" name="password" />
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	GET
Parameter	againpass
Evidence	<input type="password" name="againpass" />
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	POST
Parameter	againpass
Evidence	<input type="password" name="againpass" />
Instances	9
Solution	Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.
Reference	http://www.w3schools.com/tags/att_input_autocomplete.asp https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx
CWE Id	525
WASC Id	15
Source ID	3

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://10.1.2.6/WackoPicko/users/login.php
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/calendar.php
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/users/sample.php?userid=1
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	POST
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/passcheck.php
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/guestbook.php
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/passcheck.php
Method	POST
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559318725
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/pictures/search.php?query=ZAP
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559405125
Method	GET
Parameter	X-XSS-Protection

URL	http://10.1.2.6/WackoPicko/calendar.php?date=1559491525
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/tos.php
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/robots.txt
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	GET
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/pic'%20+%20'check'%20+%20'.php
Method	POST
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/users/register.php
Method	POST
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/admin/index.php?page=login
Method	POST
Parameter	X-XSS-Protection
URL	http://10.1.2.6/WackoPicko/pictures/recent.php
Method	GET
Parameter	X-XSS-Protection
Instances	23
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3