

## Atividade – Capture a bandeira

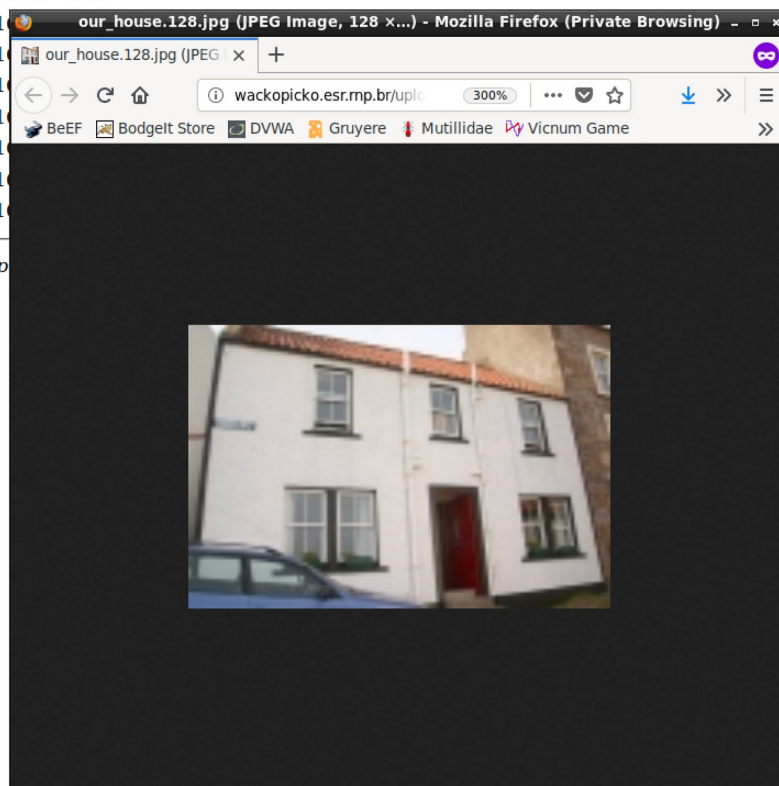
### Demonstração de acesso direto a recursos e acesso ao sistema com usuário admin

A aplicação <http://wackopicko.esr.mp.br/> permite acesso sem autenticação aos recursos conforme a imagem abaixo.

## Index of /upload/house

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">My_House</a>	09-Oct-2011 10:40	122K	
<a href="#">My_House.128.jpg</a>	09-Oct-2011 10:40	13K	
<a href="#">My_House.128_128.jpg</a>	09-Oct-2011 10:40	13K	
<a href="#">My_House.550.jpg</a>	09-Oct-2011 10:40	174K	
<a href="#">hodjigld</a>	09-Oct-2011 10:40	75K	
<a href="#">hodjigld.128.jpg</a>	09-Oct-2011 10:40	13K	
<a href="#">hodjigld.128_128.jpg</a>	09-Oct-2011 10:40	13K	
<a href="#">hodjigld.550.jpg</a>	09-Oct-2011 10:40	174K	
<a href="#">our_house</a>	09-Oct-2011 10:40	122K	
<a href="#">our_house.128.jpg</a>	09-Oct-2011 10:40	13K	
<a href="#">our_house.128_128.jpg</a>	09-Oct-2011 10:40	13K	
<a href="#">our_house.550.jpg</a>	09-Oct-2011 10:40	174K	

Apache/2.2.17 (Fedora) Server at wackop



Para simular esta vulnerabilidade, foi realizado login com os usuários cedidos e anotado as urls das postagens. Foi possível após o logout acessar os arquivos estáticos do sistema pois a navegação de diretórios está habilitada. Posteriormente executei a ferramenta nikto para ver se há vulnerabilidades comuns em servidores Web.

```

esruser@kali:~$ nikto -C all -host http://wackopicko.esr.rnp.br -port 80
- Nikto v2.1.6
-----
- ERROR: The -port option cannot be used with a full URI
esruser@kali:~$ nikto -C all -host wackopicko.esr.rnp.br -port 80
- Nikto v2.1.6
-----
+ Target IP: 192.168.213.200
+ Target Hostname: wackopicko.esr.rnp.br
+ Target Port: 80
+ Start Time: 2024-10-05 09:35:31 (GMT-3)
-----
+ Server: Apache/2.2.17 (Fedora)
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.8
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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 M
E type
+ Apache/2.2.17 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper
thentication. Attempt to log in with user 'test' password 'test' to verify.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain s
cific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain s
cific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain s
cific QUERY strings.
+ OSVDB-3268: /cart/: Directory indexing found.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /users/: Directory indexing found.
+ OSVDB-3092: /users/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /README, inode: 149167, size: 3416, mtime: Sun Oct 9 10:40:37 2011
+ OSVDB-3092: /README: README file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /admin/login.php: Admin login page/section found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 9560 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time: 2024-10-05 09:35:53 (GMT-3) (22 seconds)
-----
+ 1 host(s) tested

```

A análise detectou um arquivo README <http://wackopicko.esr.rnp.br/README> revelando várias informações sensíveis como as credenciais de alguns usuários, entre eles os admins do sistema a qual foi possível obter acesso de administrador.