

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ



Návrh, správa a bezpečnost počítačových sítí
2020/2021

4. laboratorne cvičenie

1 Zadanie

Cieľom tejto laboratórnej úlohy je zoznámenie sa s manuálnym penetračným testovaním webových aplikácií. Celé zadanie laboratórnej úlohy je možné nájsť v e-learningu na karte predmetu alebo na Dropboxe¹.

- Seznámení se s manuálním testováním bezpečnosti webových aplikací.
- Metodologie OWASP.
- Průzkum prostředí:
 - Identifikace OS webového serveru (hlavičky, case senzitivní, chybové stránky atd.), zajištění verze Apache (př. icons).
 - Identifikace programovacího jazyka.
 - Identifikace aplikace.
 - Vyhledání zranitelností.
- Použití nástroje BurpSuite (základ manuálního testování).
- Trénovací obraz OWASP BWA a příklad testování vstupů.
- Psaní reportu, co má obsahovat, jak se má psát.

2 Nastavenie pracoviska

Príklad pre pracovisko	Kali	OWASP
IP	192.168.17.139	192.168.17.140
MAC	00:0c:29:b7:9b:a1	00:0C:29:CF:AF:36

Tabuľka 1: Nastavenie pracoviska

¹<https://paper.dropbox.com/doc/5-CV-4BzOY01AIIG5171iEWHoM>

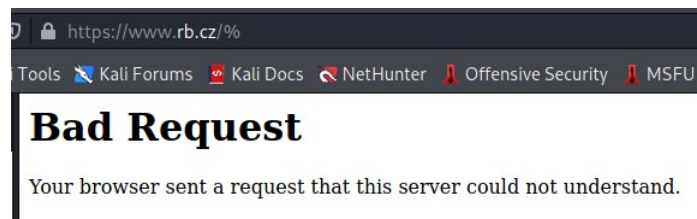
3 Průzkum prostředí - první krok penetračního testování

3.1 1. Identifikace OS webového serveru

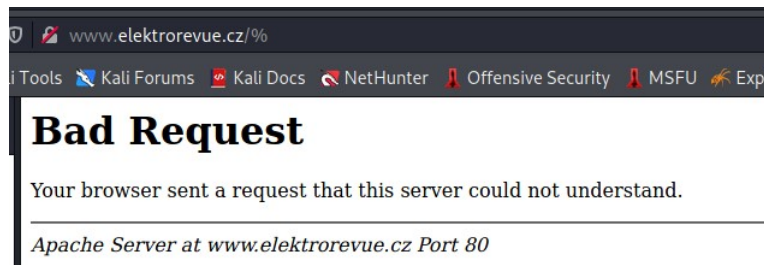
3.1.1 Výchozí chybové stránky 400, 403



Obr. 1: `http://linux.cz`



Obr. 2: `www.kb.cz`



Obr. 3: `www.elektrorevue.cz`

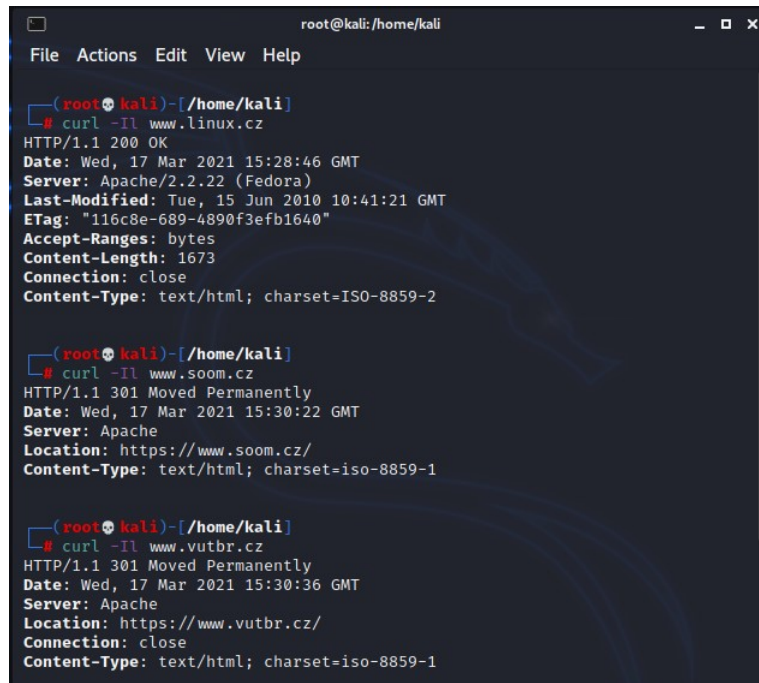
Vzpomínáte si na spojitost s minulým cvičením, nastavení výchozích chybových stránek a Security Prod? Jaká byla výchozí hlavička Apache server ?

- Parameter `ServerToken` nastavoval množství informací, které o sebe webový server prezradí.
- Na minulom cvičení sme sa stretli s dvoma hodnotami a to **full** a **prod**. V prípade full o sebe server prezradza všetky dostupné informácie. V prípade prod len obmedzené množstvo.

3.1.2 Informace z HTTP response hlaviček

Diskuze reportu, lze podvrhnout informace v hlavičce ?

- Áno, tieto údaje môžu byť podvrhnuté za účelom zmätenia útočníka.



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali) - [/home/kali]
# curl -I www.linux.cz
HTTP/1.1 200 OK
Date: Wed, 17 Mar 2021 15:28:46 GMT
Server: Apache/2.2.22 (Fedora)
Last-Modified: Tue, 15 Jun 2010 10:41:21 GMT
ETag: "116c8e-689-4890f3efb1640"
Accept-Ranges: bytes
Content-Length: 1673
Connection: close
Content-Type: text/html; charset=ISO-8859-2

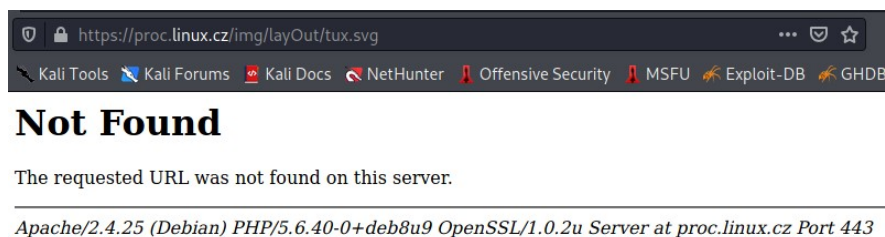
(root@kali) - [/home/kali]
# curl -I www.soom.cz
HTTP/1.1 301 Moved Permanently
Date: Wed, 17 Mar 2021 15:30:22 GMT
Server: Apache
Location: https://www.soom.cz/
Content-Type: text/html; charset=iso-8859-1

(root@kali) - [/home/kali]
# curl -I www.vutbr.cz
HTTP/1.1 301 Moved Permanently
Date: Wed, 17 Mar 2021 15:30:36 GMT
Server: Apache
Location: https://www.vutbr.cz/
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Obr. 4: HTTP Response hlavičky

3.1.3 Využití case-sensitive

Na obázku 5 je vidieť, že po modifikovaní url, na seba server prezradil citlivé informácie.



Obr. 5: case-sensitive check

- `www.gopas.cz` - Windows
- `www.lsbyc.cz` - Linux
- `www.linux.cz` - Linux
- `www.kb.cz` - Windows
- `www.csob.cz` - Linux
- `www.rb.cz` - Linux
- `www.elektrorevue.cz` - Linux

3.1.4 Podle složky icons

- www.fio.cz - Apache 2.4
- www.elektrorevue.cz - Apache 2.2
- www.kb.cz - Windows, verzia sa nepodarila zistiť
- www.csob.cz - nepodarilo sa nič zistiť
- www.airbank.cz - nepodarilo sa nič zistiť
- www.vutbr.cz - Apache 2.2
- www.rb.cz - nepodarilo sa nič zistiť

3.2 Identifikace programovacího jazyka

- www.zvut.cz - PHP
- www.unob.cz - .NET
- elektrorevue.cz - PHP
- www.gopas.cz - .NET

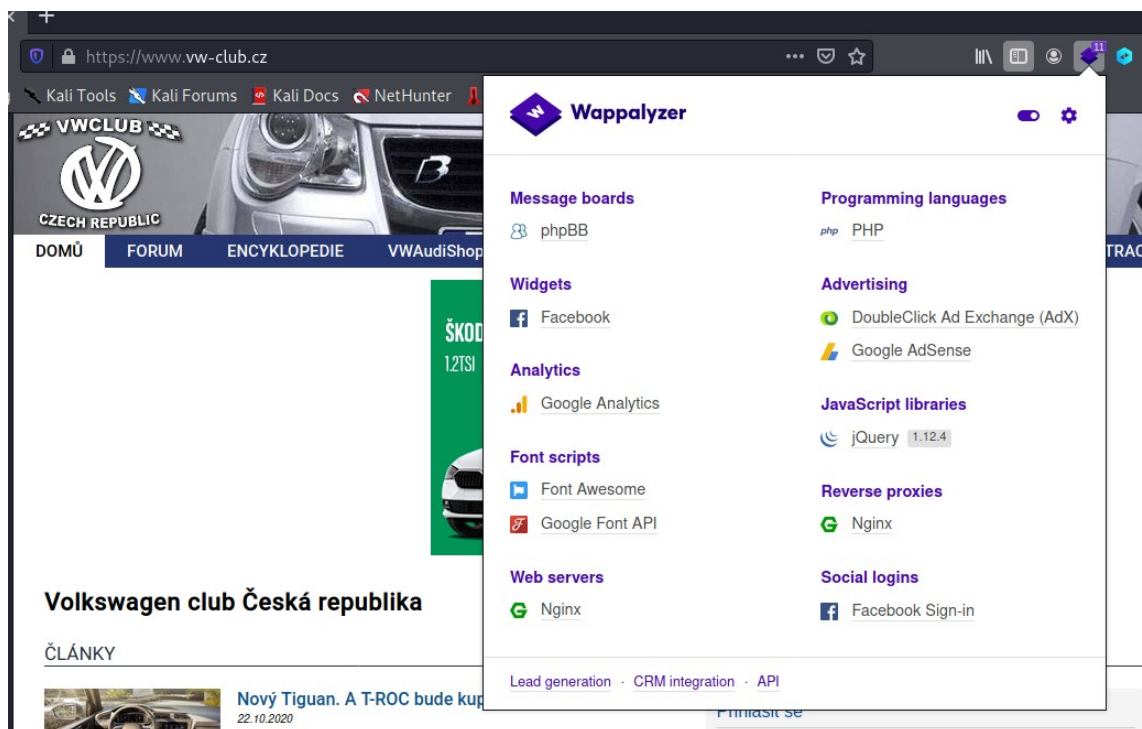
3.3 Identifikace aplikace

3.3.1 Analýza zdrojového kódu

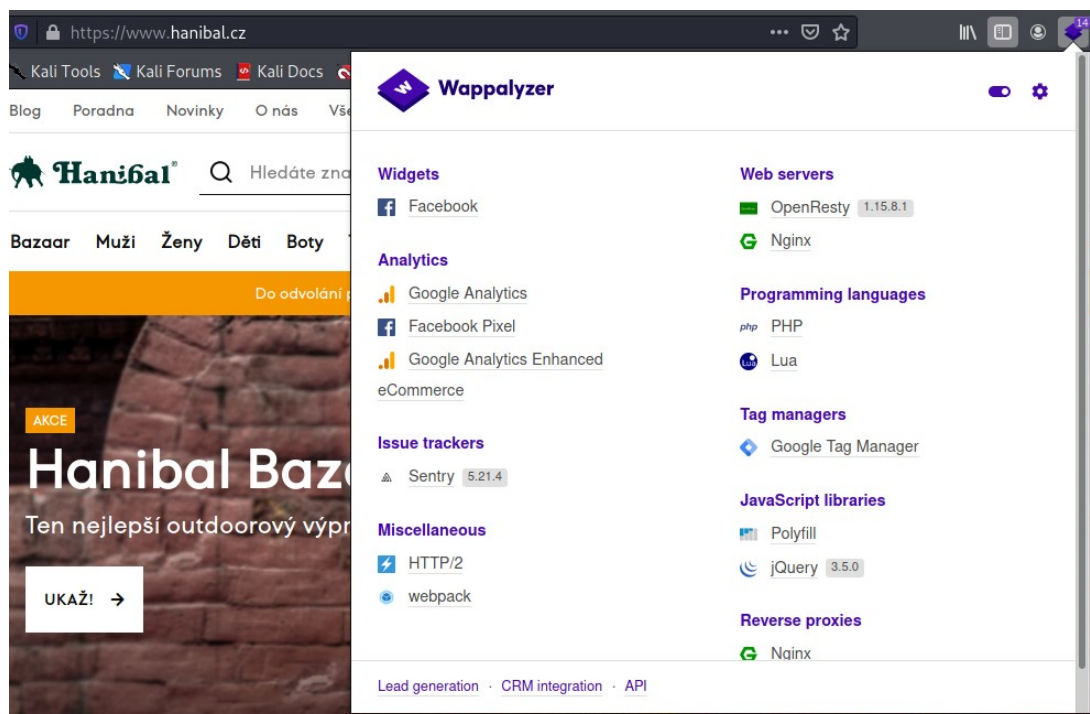
```
149 <script type='text/javascript' src='http://domeg.cz/wp-content/themes/dt-the7/'>
150 <script type='text/javascript' src='http://domeg.cz/wp-includes/js/jquery/ui/c
151 <script type='text/javascript' src='http://domeg.cz/wp-content/plugins/Ultimat
152 <link rel='https://api.w.org/' href='http://domeg.cz/wp-json/' />
153 <link rel='EditURI' type='application/rsd+xml' title='RSD' href='http://domeg.
154 <link rel='wlwmanifest' type='application/wlwmanifest+xml' href='http://domeg.
155 <meta name='generator' content='WordPress 4.7.19' />
156 <link rel='canonical' href='http://domeg.cz/' />
157 <link rel='shortlink' href='http://domeg.cz/' />
158 <link rel='alternate' type='application/json+oembed' href='http://domeg.cz/wp-
159 <link rel='alternate' type='text/xml+oembed' href='http://domeg.cz/wp-json/oem
160 <meta name='generator' content='WPML ver:3.4.1 stt:3,9;' />
161 <meta property='og:site_name' content='Domeg' />
```

Obr. 6: www.domeg.cz source code

3.3.2 Pomocí doplňku Wappalyzer



Obr. 7: www.vw-club.cz



Obr. 8: www.hanibal.cz

4 Mapování aplikace

4.1 Zjišťování Vhostů

Reverse IP results for vutbr.cz (147.229.2.90)
=====

There are 19 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
bces.cz	2021-03-15
but.cz	2021-03-15
chytrebrno.cz	2021-03-15
chytrej.cz	2021-03-16
generacevut.cz	2021-03-15
milujitemevut.cz	2021-03-15

Obr. 9: www.vutbr.cz

Reverse IP results for domeg.cz (37.9.175.3)
=====

There are 4,846 domains hosted on this server.
The first 1000 of these are listed below.

[Download The Full Report for \\$27](#)

Domain	Last Resolved Date
21centuryprojects.eu	2021-03-16
21centuryprojects.sk	2021-03-12
24-pay.sk	2021-03-16
24stundenpflegeat.at	2021-03-15
2s2.sk	2021-03-12
32.sk	2021-03-12
3cko.com	2021-03-16
3dloga.sk	2021-03-12

Obr. 10: www.domeg.cz

Reverse IP results for novezamky.sk (78.156.158.91)
=====

There are 24 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
brandysko.cz	2021-03-15
csne.cz	2021-03-15
hradeckralove.eu	2021-03-16
hradeckralove.org	2021-03-16
mb-net.cz	2021-03-16
mesto-most.cz	2021-03-16
mestorokycany.eu	2021-03-16

Obr. 11: www.novezamky.sk

4.2 Zjišťování subdomén

Subject Alt Names	
DNS Name	www.csobam.cz
DNS Name	www.csobpb.cz
DNS Name	csobam.cz
DNS Name	csobpb.cz
DNS Name	www.csobpremium.cz
DNS Name	csobpremium.cz
DNS Name	csob.cz
DNS Name	www.csob.cz

Obr. 12: www.csob.cz

Subject Alt Names	
DNS Name	vut.cz
DNS Name	zvut.cz
DNS Name	zpravyzvut.cz
DNS Name	but.cz
DNS Name	navut.cz
DNS Name	vutbrno.cz
DNS Name	vutbr.cz
DNS Name	www.vutbr.cz
DNS Name	sgt.vut.cz
DNS Name	sgq.vut.cz
DNS Name	sgp.vut.cz
DNS Name	sap.vutbr.cz
DNS Name	sap.vut.cz
DNS Name	ra.vutbr.cz
DNS Name	poptavka.vutbr.cz
DNS Name	office365.vutbr.cz
DNS Name	office365.vut.cz
DNS Name	skolenispisovka.vutbr.cz
DNS Name	office.vutbr.cz
DNS Name	office.vut.cz

Obr. 13: www.vutbr.cz

Subject Alt Names	
DNS Name	admin.administrativ.cz
DNS Name	administrativ.cz
DNS Name	ccuminn.cz
DNS Name	irc.soom.cz
DNS Name	pravo.soom.cz
DNS Name	soom.cz
DNS Name	www.administrativ.cz
DNS Name	www.ccuminn.cz
DNS Name	www.soom.cz

Obr. 14: www.soom.cz

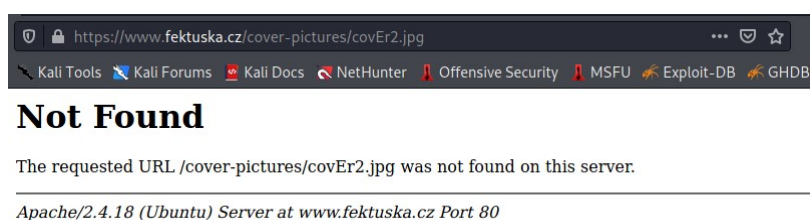
5 Samostatný úkol

```
root@kali: /home/kali
File Actions Edit View Help

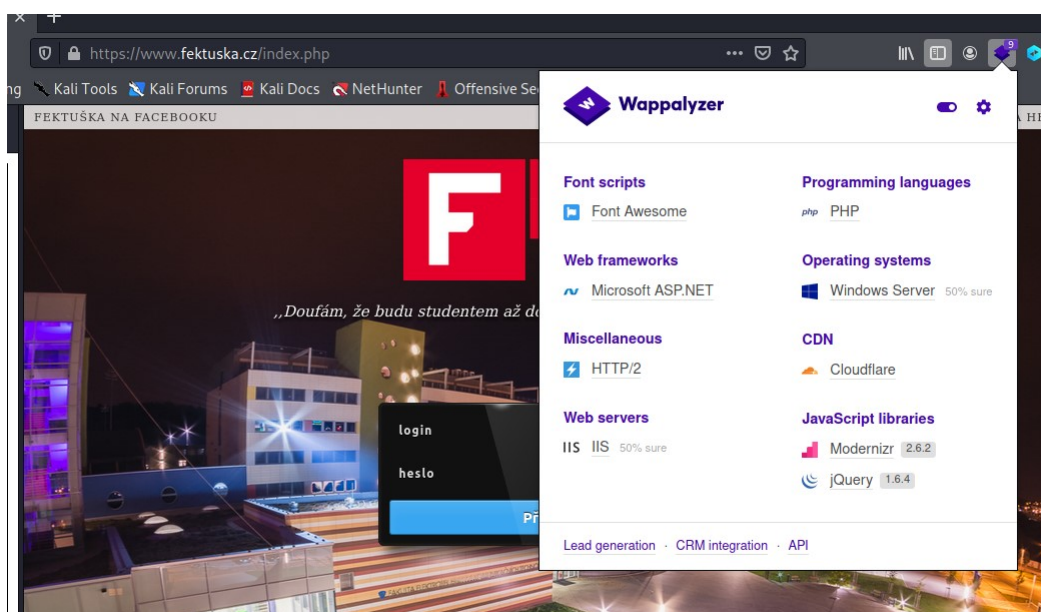
(root@kali)-[/home/kali]
# curl -I www.fektuska.cz
HTTP/1.1 301 Moved Permanently
Date: Wed, 17 Mar 2021 20:13:07 GMT
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Wed, 17 Mar 2021 21:13:07 GMT
Location: https://www.fektuska.cz/
cf-request-id: 08e36b21ed000278c328ff000000001
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?s=vi%2FV00M6czIN4bpaufKPZk3mQcJsTe5bcSf2UpVXICGoZQuPEHGpUBZIFKbbpYKMvazSR1jy%2BDV1iNPSzbbaTpChivfdXRtaLpkwfc0IX3D"}],"max_age":604800,"group":"cf-nel"}
NEL: {"max_age":604800,"report_to":"cf-nel"}
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 6318e1497d24278c-PRG
alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400

(root@kali)-[/home/kali]
```

Obr. 15: Terminálový výpis



Obr. 16: Webový server je Apache 2.4.18



Obr. 17: Bežiacie aplikácie, taktiež je v url vidieť že programovací jazyk je php