With just a search engine and a cup of coffee: hunting vulnerabilities on the web

Jan Kopřiva
jan.kopriva@alef.com
ALEF CSIRT

SANS Pen Test Hackfest Europe 2019
Security research seems difficult to get into…

• Articles about highly technical vulnerabilities („I couldn‘t do that…“)

• All low-hanging fruit seems to have been found already („It‘s too late…“)
...but is finding vulnerabilities really that hard?
Open Directories – directory listing in action

### Index of /kali-images

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>kali-2017.2/</td>
<td>2017-09-18 11:50</td>
<td>-</td>
</tr>
<tr>
<td>kali-2017.3/</td>
<td>2017-11-20 07:28</td>
<td>-</td>
</tr>
<tr>
<td>kali-2018.1/</td>
<td>2018-02-13 00:33</td>
<td>-</td>
</tr>
<tr>
<td>kali-2018.2/</td>
<td>2018-04-30 01:01</td>
<td>-</td>
</tr>
<tr>
<td>kali-2018.3/</td>
<td>2018-08-27 06:19</td>
<td>-</td>
</tr>
<tr>
<td>kali-2018.3g</td>
<td>2018-09-14 12:33</td>
<td>-</td>
</tr>
<tr>
<td>kali-weekly/</td>
<td>2018-09-15 21:10</td>
<td>-</td>
</tr>
<tr>
<td>project/</td>
<td>2014-12-04 06:11</td>
<td>-</td>
</tr>
</tbody>
</table>

### Index of /cz

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>info-centrum/</td>
<td>2017-04-18 14:04</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>kontakty/</td>
<td>2017-04-18 14:04</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>o-nas/</td>
<td>2017-04-18 14:04</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>produktv-a-sluzby/</td>
<td>2017-04-18 14:04</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>tiskove-zpravy/</td>
<td>2017-04-18 14:04</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>volna-mista/</td>
<td>2017-04-18 14:04</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
Analysis in CZ and SK TLDs

- Timeframe: Q3 2018
- Thousands of open directories analysed (mostly manually)
- Sensitive data found on 185 domains
Analysis in CZ and SK TLDs

- CZ: 86%
- SK: 14%
Personal and Highly Sensitive Data

- Personal data: 22%
- Highly Sensitive Data: 15%
SW/Warez and Audiovisual Content

SW/Warez

18%

Audiovisual Content

14%
Music and e-Books

Music

- 23%

e-Books, audiobooks

- 9%
Photography and Pornography

Photos: 16%

Pornography: 5%
Passwords and Databases

Passwords: 3%

Databases: 1%
Hic sunt leones
What was there?
Redirection Mechanism


www.newsite.com
Redirection Mechanism

• Unsafe (Open)
  • www.mysite.com/redirect?url=www.newsite.com

• Safe(r)
  • www.mysite.com/redirect?url=22
Open Redirection

- www.yourbank.com/redirect?url=ebanking.yourbank.com
- www.yourbank.com/redirect?url=%77%77%77%2e%66%61%6b%65%2d%65%62%61%6e%69%6e%67%2e%6e%65%74
- www.yourbank.com/%72%65%64%69%72%65%63%74%3f%75%72%6c%3d%77%77%77%2e%66%61%6b%65%2d%65%62%61%6e%6b%69%6e%67%2e%6e%65%74%0a
Analysis of „Czech“ Redirects

• Timeframe: Q4 2018

• Hundreds of „redirectors“ analyzed (mostly manually)

• Open redirection found on 114 sites
Where were they?
Which might have been useful? (CZ)

- Banks
- E-shops
- TV and radio stations with national coverage
- One ministry and couple of local governmental sites
- News sites
- Hospitals
Which might have been useful? (non-CZ)

- OpenSubtitles
- CompTIA
- EC-Council
- Oracle
- Wiley
- Washington Post
How fast was response/fix

- Washington Post – 4 hours/within 2 months
- OpenSubtitles – 6 hours/within 24 hours
- EC-Council – 2 days/3 months
- TV station – 18 hours/18 hours
- Banks – 2x hours/within 2x hours
How many are left?

Directory listing:
- Accessible: 73%
- Closed: 27%

Open redirect:
- Open: 62%
- Patched: 38%
Babel – CMSMS multi-language module

Babel – CMSMS multi-language module

```php
if(!isset($_GET["newurl"])) {
    /* code not important for our purposes removed here*/
} else{
    /* code not important for our purposes removed here*/
    header("location: ".$_GET["newurl"]");
}
```
Babel – CMSMS multi-language module

<table>
<thead>
<tr>
<th>TLD</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>COM</td>
<td>1590</td>
</tr>
<tr>
<td>BE</td>
<td>448</td>
</tr>
<tr>
<td>FR</td>
<td>408</td>
</tr>
<tr>
<td>NL</td>
<td>227</td>
</tr>
<tr>
<td>PT</td>
<td>226</td>
</tr>
<tr>
<td>CH</td>
<td>207</td>
</tr>
<tr>
<td>DE</td>
<td>142</td>
</tr>
<tr>
<td>CZ</td>
<td>96</td>
</tr>
<tr>
<td>LV</td>
<td>78</td>
</tr>
<tr>
<td>AT</td>
<td>46</td>
</tr>
</tbody>
</table>
Youtube – half-closed (but still fun 😊) redirect

• Links under videos use redirection mechanism

• https://www.youtube.com/redirect?q=[link]&redir_token=[token]&event=video_description&v=[video]

• Tokens last for ~24 hours and are valid for any redirection…
Results

• Contact of affected subjects
  • Help from CZ.NIC (and others)
  • OpenBugBounty
• One CVE – CVE-2019-1010290 (R.I.P. DWF)
• HoF mentions
• This presentation…😊
Methodology – Directory listing

- site:cz, site:interesting_urls, site:top_companies/inurl:top_companies,…
- intitle:"index of /" + "last modified" + "parent directory"
- finance, accounting, students, id, private, secret, photos, books, sw, torrents, e-mail,…
Methodology – Open redirection

- site:cz, site:bank_urls, site:top_cz_companies/inurl:top_cz_companies,…
- inurl:
  - link
  - newurl
  - redir
  - redirect
  - redirectto
- redirecturl
  - returnurl
  - url
  - …
Why not try it yourself?

• Good opportunity to get into „the game“ (and possibly BBs, HoFs,…😊)

• Giving just 10 minutes a week can help someone a lot

• Be ready for lack of response to your findings

• CSIRTs, registrars and hosting providers can sometimes help
Thank you for your attention