

Unvalidated Redirects and Forwards



**CYBER SECURITY &
PRIVACY FOUNDATION**

Cyber Security & Privacy Foundation(CSPF)

Open URL Redirection

The vulnerability occurs when a web application takes the User Input and redirect users to the given value without doing any validation.

An Attacker can abuse this vulnerability to redirect users to a malicious webpage, especially a Phishing Page.

Requires Social Engineering

Impact

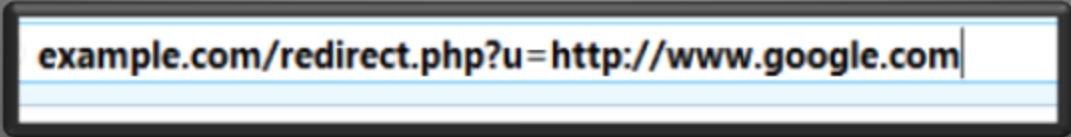
Attackers can exploit the trust a user has for a website:

- **Malware Infection:** By exploiting the Open Redirect, an attacker can redirect users to a malicious web page that infects victim's machine with a malware
- **Phishing:** Attacker can redirect users to a Phishing page – a page designed to look like legitimate website that steals user's credentials and personal information.

Example

URL Redirect

Here, we have a webpage that takes input from GET parameter “U” and redirect users to the specified value.



example.com/redirect.php?u=http://www.google.com|

The above request will redirect users to “Google.com”

Back End: PHP Code

```
$url=$_GET['u'];  
header("Location:".$url);
```

Abusing Open Redirection

An attacker can abuse this vulnerability by supplying a Phishing Page URL in the Parameter.

```
example.com/redirect.php?u=http://www.PhishingPageOfExample.com/login.php
```

Attacker then sends this crafted link via email to victims

Open URL Redirection Attack

Attacker



1. Sends a fake email with a crafted link:
[http://example.com/redirect.php?u=http://
phishingPageofExample.com/login.php](http://example.com/redirect.php?u=http://phishingPageofExample.com/login.php)

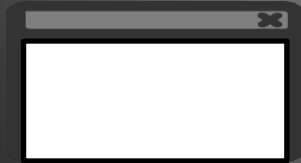
3. Requesting
[http://example.com/redirect.php?u=http://
phishingPageofExample.com/login.php](http://example.com/redirect.php?u=http://phishingPageofExample.com/login.php)

4. Response
HTTP/1.1 302 Found
Location: <http://phishingPageofExample.com/login.php>

Victim



Browser

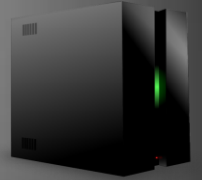


2. Victim click the link

5. Opens:

<http://phishingPageofExample.com/login.php>

Vulnerable Website



Phishing Page



In Simple English

Hades

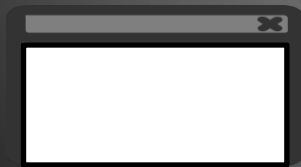


1. Congratulations Andrea!! You are today's Lucky User of Example.com, eligible to receive a Laptop. Click Here to Claim Your Prize

2. Cool..



Andrea



3. Hey Example.com, Open this URL "http://ex.."

5. Hey Evil.com, Open the "login.php" page

4. Go to "Evil.com/login.php"



Example.com

6. Here is the Page you request for..



Evil.com

He..He..a victim



Open Forward

Similar to Open URL Redirection, this vulnerability occurs when a web application takes the User Input and **forwards** users to **another part of the application** without doing any validation.

An attack can exploit this vulnerability to bypass Access control check.

Example

Forwarding a Page

Here, we have a web page that forwards **Users** to the value specified in “returnurl” parameter after successful login.

```
example.com/UserLogin.php?returnurl=index.php
```

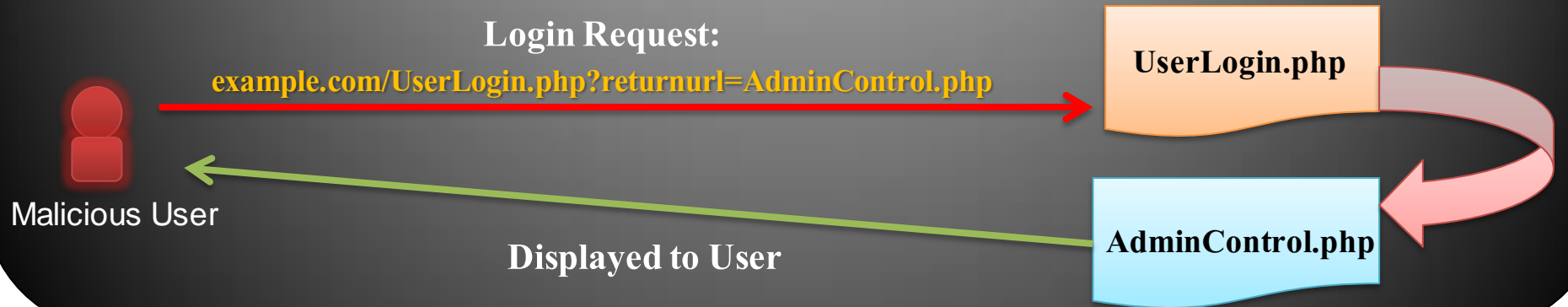
As you can see, the “returnurl” is an user-controllable parameter.

Access Control Bypass

An attacker can exploit the Open Forward vulnerability to gain access to administrator's panel

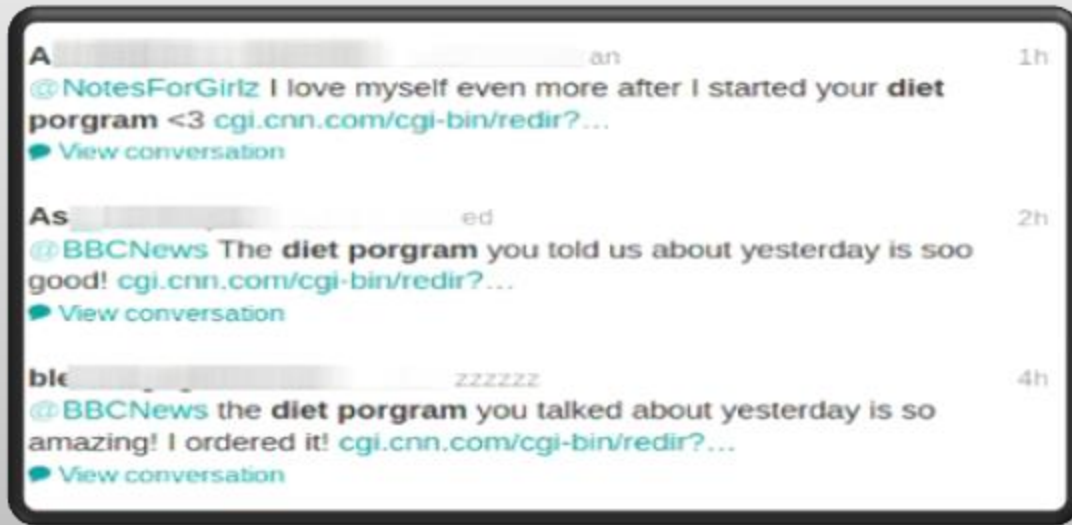
```
example.com/UserLogin.php?returnurl=admincontrol.php|
```

Attacker who has user-level access to the website will be forwarded to the admin Panel.



Real World “Open URL Redirection” Attacks

In 2013, We reported that Cyber Criminals had abused an open redirection vulnerability in CNN Website – one of the World’s largest News organizations. Opening the crafted Links lead to the spammer’s website.



Attackers also leveraged Open Redirection bug in one of the Yahoo’s Subdomain to spread a Diet spam tweets in Twitter.

In 2012, Symantec reported that Spammers had abused open redirection vulnerability in Government Websites. Victims are redirected to work-at-home scam website.