

OPEN REDIRECT SCANNER

**2003A53010 Mahankali . Koushik**

To

**Dr. Sampath Kumar Tallapally**

Assistant Professor

in

School of Computer Science And Engineering

**01 . ABSTRACT :-**

Open redirect is a security defect in an app or a web page that causes it to fail to properly authenticate URLs. When apps and web pages have requests for URLs, they are supposed to prove that those URLs are part of the expected page’s domain. To test the web-based application manually for Open Redirection is very difficult. So we need an automated script that can make the task of manual testing easier and save the time of the penetration tester. OpenRedireX is an automated script developed in the Python language which tests the single URL and Multiple URLs or Open Redirection Vulnerability by inserting the payload of open redirection into the URL parameter and analyzing the response from the server. OpenRedireX supports customizing the payload list and also allows users to use their payload list. OpenRedireX tool is open-source and free to use. These can be done in linux , kali finder tools in the linux operating system.

**02 . INTRODUCTION :-**

To know better about the Open Redirect Scanner Let’s get some questions about it to know briefly about them :-

a) What is DNS Open Redirect Scanner?

b) What is meant by Open Redirect Scanner?

c) Why is Open Redirect Scanner is a problem?

d) How to prevent a Open Redirect Scanner?

e) Explain some example attacks of Open Redirect Scanner?

First of all what we know about the “ Open Redirect Scanner ” is a vulnerability that can be used to manipulate the application to redirect the users to a different URL other can be the one that’s intended , this can be done by manipulating the URL to include the parameters that redirects the user to different URL’s .

Open Redirect Scanner is a problem if the same redirect doesn’t features filtered or validated then it becomes unsafe as there is a possibility of an attacker inserting malicious content into the input ensures the high amount of risk into it .

Open Redirect Scanner uses the various types of methods to prevent into it they are :-

1. HTTP Location Header :- It specifies the new browser location , is the most common redirection method

Eg :- Location : https://www.attacker.com/

1. Meta tag redirects :- it uses the HTML meta tag to navigate the new locations .

Eg :- <meta http-equiv = “refresh” content = “0:url=https://www.attacker.com/” />

1. DOM – based redirects the use JavaScript to manipulate the DOM window properties .

Eg :- window.location = ‘https://www.attacker .com’

There are different types of scenarios for exploiting the Open Redirect Scanner / vulnerabilities are :-

1. Phishing Attacks – it is used for the malicious URL is in phishing attempts . if a legitimate site exposes the Open Redirect Scanner endpoint , attackers might send the phishing emails with a link that seems the point at original site redirects the attacker - controlled URL

Eg :- <https://example.com/redirect>.php? Redrecturl =http://attacker .com/phish/

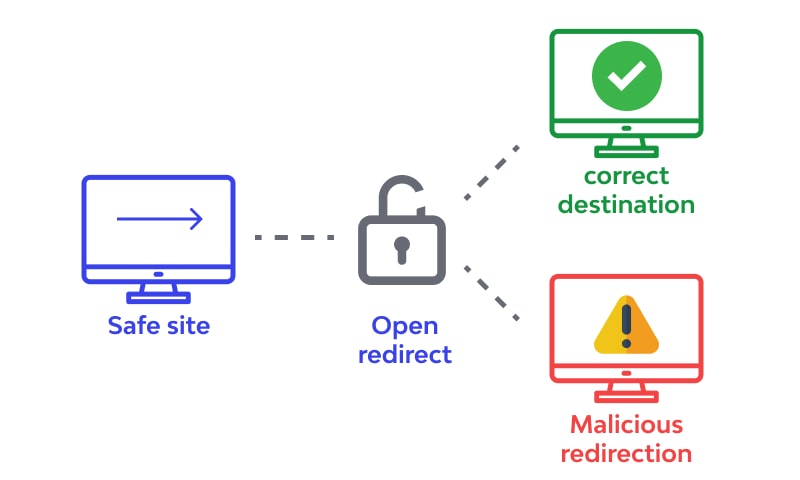
1. Token Theft Scenario - Open Redirect Scanner makes the steal user tokens of single sign-on(SSO) & is vulnerable to Open Redirection authentication follows

* Login page URL opens
* The authentication server checks the login page URL is whitelisted
* User provides their passwords and username
* If credentials are valid. Server sends the authentication and access tokens to specifies target by calling any different URL to the user.

1. If URL exposes the Open Redirect attack may be possible the

* Attacker supplies the login URL
* Target server’s hostname is URL so authentication server allows it
* User provides the username and passwords
* Access tokens sent by authentication server is redirect to attacker by calling the URL

**03. Architecture / model (fixed inputs and outputs):-**



Open Redirect Scanner / vulnerabilities arises the application incorporates the controllable data into targets the redirection of an unsafe way . An attacker can create a URL within the application that causes the redirection to an arbitrary external domain . these process can be done while the data seen as :-

* When safe site URL has entered the login(username, passwords) credentials the open redirect navigates into the correct destination or malicious redirection says into it .
* When data sends the data by open redirect into the correct navigation site .

**04 . SURVEY :-**

We have done the survey on the Open Redirect Scanner that what the common have altered or accessed while there URL has been used for irrelevant works from them to have their access to their malicious content in their websites are they are :

1. This article was published by “Uber.com by InfoSec Write -ups” says about the unvalidated redirects & forwards are possible when a web application

* that domain redirects the URL
* that sends the evil URL with a payload(that obfuscate the url for cheat the user with any encode that available)
* code executes their part of execution to follow requests the final destination & sees that if open redirect scanner works or not .
* scanner loads a list of subdomains an add a payload to final url sees what it does .

1. This article was published by “Google Dork – Bug Bounty by InfoSec Write -ups” says about their param scanner will reflects the swag modifying the scanner PSFuzz , so that it can also scan open redirect the scanner will improves the over time .

* The Burp suite will redirects the links which makes the searching for bugs easier.
* After investigating the simple security holes it actually finds the XSS stuff by Google Dorks

for eg:- “site:\*redacted.cominurl:target “ => and has the result to see that suitable the open redirect

* Different steps are used for reproducing of theopen redirect of the scanner are:-
* Behind the google search result the login page of website notices the parameter target contained a whole URL , which was very valid data into it & no longer jumps the subdomain of [www.subdomain](http://www.subdomain)
* So they have tested it out and replaced the URL
* Now they submit the website information to the server that redirects the website that enables the payload and founds the good open redirect .
* These whole impacts the redirected targeted URL that application causes the external domain into .

1. This article was published by “Common Weakness Enumeration” that says about the web application accepts the user-controlled input that specifies the link on external site and uses the link to redirect these simplifies the phishing attack into it. And these whole can be executed in the using programming platforms like “JAVA , Python” that references the deletion of content history in the anonymous tool vendor (under the NDA)
2. This article was published by “<https://learn.snyk.io>” Open redirect the scanner is a vulnerability that occurs the when application allows the user to control a redirect or forward to another URL , if application does not validate the untrusted user input an attacker could supply a URL that redirects the unsuspecting the victim from a legitimate domain to be an attacker’s phishing site on the attacker side.

* There are different types of examples on open redirect scanner that provides the arbitrary location are provided the application are “goodexample.com/redir.php?q=badexample.com” these application redir php is accepting the query string .
* There are different types of vulnerabilities of open redirect scanner are to an attacker manipulating the user and redirects them from one site to another .

1. This article was published by “https://PortSwigger.net” that says about the open redirection (reflected) that has the vulnerabilities that redirects the application from redirected the URL function to receiver user: controllable input and incorporate into redirection should be minimized the attacks are:-

* Application should use URL is an all that redirects the function should strictly validate the receiver’s URL to relative URL
* The application should use web root for all that redirects the function should validate with a slash(#) character to pretend into it for eg:-

<http://yourdomainname.com> to the URL before issuing the redirect

* The application should absolute URL for redirects the function should verify the user-supplied URL begins with

<http://yourdomainname.com/> before issuing the redirect.

**05. EXISTING SYSTEM:-**

The existing system of websites and applications is a complex networks of connection between internet , URL’s, interconnected technologies & services allowed by the users to access and interact with digital content and services on the internet . some key components are existing system that includes are :-

1. Use fast scan to find open redirect vulnerabilities : that they used the vulnerabilities that writes the url to scan and click stat button to proceed the process into it . but it ha some limitations Into it are:-

* If we want to scan parameters of form used the page of HTML form parser
* To get fast scan allows the parameter in query using HTTP GET method
* Use expert mode if application accepts the data using HTTP methods are:
* POST
* PUT
* DELETE
* If application requires the authentication from web access page should be scan uses the expert mode from authentication mode into it.

1. HTML from parser are to scan web page from parameters that has many forms to submit then data to server by means of login , contact , search forms into it. The URL enters into the HTML format parser area uses analyze button to popup the select form to scan into it. Some hints are:-

* Use authentication header if web page needs authentications
* We can set HTTP methods & use any valid header as we want
* Request body can be set with any HTTP methods

1. Uses the expert mode are ability to alter the aspect of HTTP request that includes the choosing of HTTP methods are:-

* GET
* POST
* PUT
* DELETE

Selecting the HTTP headers , as well as deciding the request body into it.

**06. PROPOSED SYSTEM:-**

Different kinds of Open Redirects are:-

* Header based:-

Header-based is a location header sent from the server. The benefit with this, from an attacker's perspective, is that the redirect always works even if JavaScript is not interpreted. A server-side function that gets a URL as input will follow the redirect and end up somewhere else.

* JavaScript based:-

When the redirect instead happens in Javascript it only works in scenarios where Javascript is executed. It might not work for server-side functions, but it will work in the victim's web browser.

* If the redirect happens in Javascript it might also be possible to cause a redirect to javascript: something(), which would be an XSS in itself.
* Our main motive is to find the website is having any malicious content that having any access of the main in the middle attack that can captures the data into it.

**07. SUMMARIZE :-**

While using these methodology we can easily find the occurs of the web page is being redirected the another URL in another domain via a user – controlled input , an attacker can use this vulnerabilities to redirect the users to other malicious websites, which can be used for phishing attack and similar attacks into it . DOM based arises the when a script writes controllable data into the targeted of a redirection in an unsafe manner.

**08. ADVANTAGES OF NEW PROPOSED METHODOLGY:-**

* Improves the website security by implementing these type of security parameters that measures the improvement of security of website or web application that reduces the risk of unauthorized access or data theft into it.
* Project has the high efficiency that any developer can access and performs the security parameters for better experiences of their ensuring the data and personal data / information are secure into it.
* They especially dangerous the because an attacker knows the were trying of the specific websites , which makes the vulnerabilities to a phishing attack .

**09. DISADVANTAGES OF NEW PROPOSED METHODOLOGY:-**

* That vulnerabilities website security measures the significances of the improve security of web application or website that reduces the risk of unauthorized access or data theft.
* Maintenance and updates that web application requires the ongoing maintenance and updates the remain secure and functional of time consuming and especially for large or complex systems.
* Compatibility issues that websites and web applications must be compatible with various browsers, search engines , operating systems and devices which can compatibility issues and there requirements for additional developments and requirements and testing efforts .

**10. TOOLS / ALGORITHMS USED FOR PREVENT ATTACK:-**

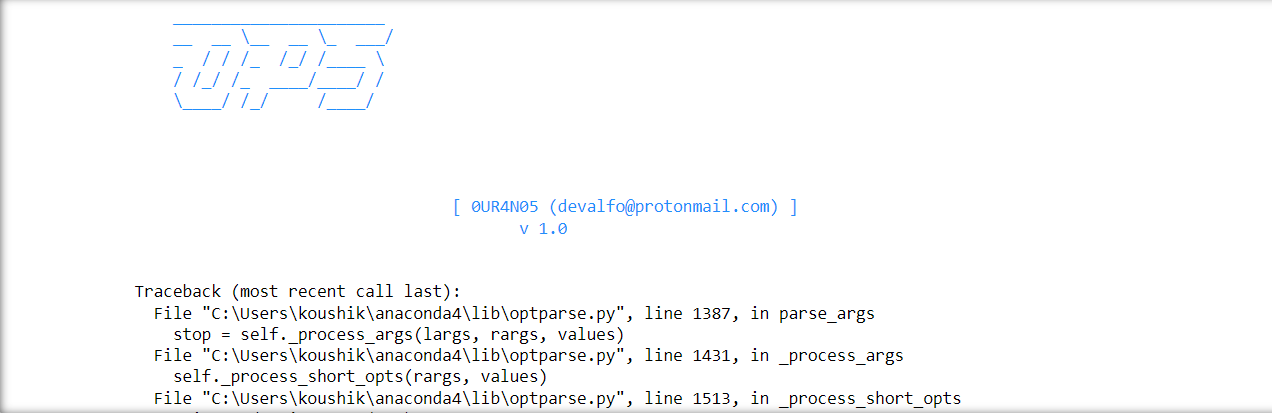
Tools used for open redirect scanner are:-

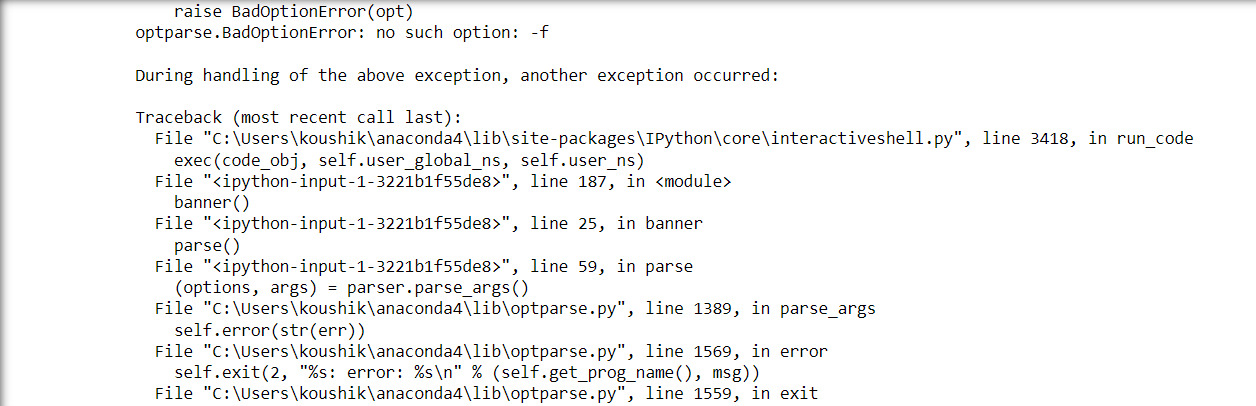
* Oralyzer : is the tool used for the web based application for CRLF injection flaw that tool is fully automated tool is a fully automated tool developed in the python language it supports the proxy , custom payload use and extracting URL’s from Wayback machine.
* DOM : DOM based the open redirection arises when a script writes the controllable data into the target of a redirection in an unsafe way .

An attacker may able to uses the vulnerabilities to construct URL that visited by another application user, will cause redirection to arbitrary external domain.

* Append >> uses the operator adds the output to existing content instead of overwriting the allows the redirect the output from multiple commands to a signal file.

**11. RESULT:-**

****

****

**12.CONCLUSION:-**

We now know how harmful an open redirect vulnerability can be and why it is so important to prevent it. The easiest and the most effective way to prevent it is by not letting your user have control of where the page redirects them to. It is only necessary to provide users with the authority to enter short keywords and map them to the target URL or simply allow them to confirm before being redirected to the destination.

**13.REFERENCES:-**

* <https://learn.snyk.io/lessons/open-redirect/javascript/>
* <https://brightsec.com/blog/open-redirect-vulnerabilities/>
* https://secnhack.in/open-redirection-vulnerability exploiting-and-mitigation