

Forum:[Hack Forums](#)

Thread: [How to redirect page content \(External service interaction \(HTTP\)\)](#)

TheWaxBear - June 10, 2024, 4:25 pm

Hi, I was wondering how it is possible to redirect the content of a page to another service(DNS or server) with the External service interaction (HTTP) vulnerability. I want something that doesn't need port forwarding.

Example:

GET /secret HTTP/1.1

Host: (Domain or server or whatever that can work)

Thanks guys for the help !

G.P.D. - June 10, 2024, 5:37 pm

Can you explain more about what you want to do?

SSRF is not a redirection; it involves making a request from the server to another server or resource instead of you making the request directly.

This can be used to access internal systems that are otherwise protected or to retrieve information from services that the server can communicate with but you cannot.

To achieve SSRF, there are multiple ways to do so.

Exploiting URL parsing is one common method, where if a web application accepts a URL as input, it might be possible to manipulate the input to make the server request an internal resource.

For example, submitting `http://localhost/admin` might cause the server to request an internal admin page.

Another technique involves manipulating headers; certain HTTP headers, such as Host, X-Forwarded-For, or X-Original-URL, can sometimes be manipulated to induce the server to make requests to unintended destinations.

Additionally, file inclusion vulnerabilities can be exploited when applications include files or resources based on user input, allowing to include internal network files or external URLs, causing the server to fetch and include them.

DNS rebinding is another advanced technique, where manipulating DNS responses can make the server think it is contacting a legitimate external resource when it is actually contacting an internal resource.

Even when the attacker does not see the response, blind SSRF can still be exploited to perform actions like internal port scanning, triggering internal services, or exploiting internal vulnerabilities.

Do you have any specific scenario or context in which you are looking to understand or exploit SSRF?

TheWaxBear - June 10, 2024, 6:24 pm

(Jun 10, 2024 05:37 PM)G.P.D. Wrote: [CITE](#) Can you explain more about what you want to do?

SSRF is not a redirection; it involves making a request from the server to another server or resource instead of you making the request directly.

This can be used to access internal systems that are otherwise protected or to retrieve information from services that the server can communicate with but you cannot.

To achieve SSRF, there are multiple ways to do so.

Exploiting URL parsing is one common method, where if a web application accepts a URL as input, it might be possible to manipulate the input to make the server request an internal resource.

For example, submitting `http://localhost/admin` might cause the server to request an internal admin page.

Another technique involves manipulating headers; certain HTTP headers, such as `Host`, `X-Forwarded-For`, or `X-Original-URL`, can sometimes be manipulated to induce the server to make requests to unintended destinations.

Additionally, file inclusion vulnerabilities can be exploited when applications include files or resources based on user input, allowing to include internal network files or external URLs, causing the server to fetch and include them.

DNS rebinding is another advanced technique, where manipulating DNS responses can make the server think it is contacting a legitimate external resource when it is actually contacting an internal resource.

Even when the attacker does not see the response, blind SSRF can still be exploited to perform actions like internal port scanning, triggering internal services, or exploiting internal vulnerabilities.

Do you have any specific scenario or context in which you are looking to understand or exploit SSRF?

Hi ! Sorry if i wasn't clear, the vulnerability is External service interaction (HTTP). So when I change the host header's value for a dns from the burp collaborator like `havpvj565h0ed3eup5rrd9n9y04tsqgf.oastify.com` the request works well. I think is related to ssrf but i'm not 100% sure.

Thanks for the help

G.P.D. - June 11, 2024, 4:31 am

When you change the Host header to your domain (like `havpvj565h0ed3eup5rrd9n9y04tsqgf.oastify.com`), it's normal for the server to make a request to your domain; This is expected behavior.

However, SSRF vulnerabilities can occur when the Host header is manipulated in specific ways. For instance, using two Host headers can create ambiguous requests, or you can craft headers like `example.com:evil.com` to trick the server.

SSRF is often exploited through headers like `X-Forwarded-For` or `X-Original-URL`, which the server might trust for making internal or external requests.