

Nginx ssl??????

1

? ? ? ? ? ? ? ?

1. SSL ?????

```
ssl_stapling on;
ssl_stapling_verify on;
ssl_session_cache shared:SSL:10m;
ssl_session_timeout 10m;
resolver 119.29.29.29 182.254.116.116 valid=300s;
resolver_timeout 5s;
```

```
? ssl_stapling on
```

HTTPS

```
? ssl_stapling_verify on
```

☐ OSCP ☐

```
? ssl session cache shared:SSL:10m
```

SSL [][][][][][][][]

```
? ssl session timeout 10m
```

10 ☐ ☐ ☐

? DNS ?????? OSCP ??

```
resolver 119.29.29.29 182.254.116.116 valid=300s;
resolver_timeout 5s;
```

☐ OCSP Stapling ☐

DNS ☐

OCSP ☐

2. HTTP ??????????

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload";
add_header X-Frame-Options SAMEORIGIN;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "strict-origin-when-cross-origin";
add_header Set-Cookie "Path=/; HttpOnly; Secure; SameSite=Strict";
```

? HSTS??? HTTPS?

Strict-Transport-Security

☐

☐

HTTPS ☐

? ?? iframe ????

X-Frame-Options SAMEORIGIN

☐ Clickjacking ☐

? ?? MIME ??

X-Content-Type-Options nosniff

? ???????

Referrer-Policy strict-origin-when-cross-origin

☐ referrer ☐

? ?? Cookie

```
Set-Cookie "Path=/; HttpOnly; Secure; SameSite=Strict";
```

cookie

- HttpOnly JavaScript
- Secure HTTPS
- SameSite=Strict cookie CSRF

?????? ??????????

????? ?? server{} ?????? HTTPS ?
server ??

```
server {  
    listen 443 ssl http2;  
    server_name example.com;  
  
    ssl_certificate /path/to/fullchain.pem;  
    ssl_certificate_key /path/to/privkey.pem;  
  
    #  
    ssl_stapling on;  
    ssl_stapling_verify on;  
    ssl_session_cache shared:SSL:10m;  
    ssl_session_timeout 10m;  
    resolver 119.29.29.29 182.254.116.116 valid=300s;  
    resolver_timeout 5s;  
  
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload";  
    add_header X-Frame-Options SAMEORIGIN;  
    add_header X-Content-Type-Options "nosniff" always;  
    add_header Referrer-Policy "strict-origin-when-cross-origin";  
    add_header Set-Cookie "Path=/; HttpOnly; Secure; SameSite=Strict";
```

```
root /var/www/html;  
}
```

? ?????

1. add_header ??? HTTPS ? server {} ?

??????

2. ????????? location ???

?? server{} ?????? location{} ?? ?

3. ? HTTP?80? ? server ???????????

??

- HSTS ?? HTTPS ??
- cookie ? Secure ?? HTTPS
- OCSP Stapling ?? HTTPS ???

? ?????

???	???
SSL OCSP / session ??	server { listen 443 ssl; }
HTTP ??? add_header?	?? HTTPS server{} ??
resolver	?? server{}

????? Nginx ??????

```
/etc/nginx/sites-available/xxx.conf
```

????????? ????????? ?