راه‌اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس‌دهنده وب Lighttpd 1.4

شماره مستند APA-AMIRKABIR-13950705-1
تاریخ نگارش ..... ۵ مهر ۱۳۹۵
شماره نگارش ۱/۰
نگارش ..... آپای امیرکبیر
طبقه‌بندی ..... عادی

فهرست مطالب

۱ مقدمه

برای تأمین محرمانگی و جامعیت داده‌های مبادله شده می‌توان از پروتکل‌های استانداردی که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم‌ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری داده‌های لایه کاربرد و تأمین امنیت ارتباطات استفاده می‌شود، پروتکل SSL/TLS است. در این گزارش مراحل نصب گواهی‌نامه SSL و امن‌سازی پروتکل SSL/TLS را بر روی سرویس‌دهنده وب Lighttpd نسخه 1.4.31 بیان می‌کنیم.

۲ فعال‌سازی ارتباطات HTTPS

برای پیکربندی سرویس‌دهنده HTTPS و استفاده از این پروتکل ابتدا باید گواهی‌نامه دیجیتال مربوطه را از مراکز صدور گواهی (CA)[۱] معتبر دریافت کرد (یا گواهی خود-امضا را تولید کرد). گرفتن گواهی دارای مراحلی است که برای اطلاعات بیشتر در این زمینه می‌توانید به گزارش ارائه شده توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر که در آدرس زیر قرار دارد مراجعه کنید:

http://apa.aut.ac.ir/?p=971

در ادامه این بخش، قصد داریم تا مراحل نصب گواهی را در Lighttpd بیان کنیم:

۱. **کپی کردن فایل‌های گواهی به سرور**

ابتدا باید فایل‌های زنجیره گواهی‌های میانی و همچنین فایل گواهی اصلی (برای دامنه خودتان) را به سرور انتقال دهید.

۲. **ترکیب کردن فایل گواهی‌نامه و کلید**

شما نیاز دارید که فایل گواهی و کلید را به داخل فایلی با فرمت pem با استفاده از دستور زیر ترکیب کنید.

```
cat your_domain_name.key your_domain_name.crt > your_domain_name.pem
```

۳. **ویرایش فایل پیکربندی Lighttpd**

در این مرحله فایل lighttpd.conf را باز کنید و دستورات مورد نظر را به صورت زیر در آن اضافه کنید. توجه کنید که "DigiCertCA.crt" فایل زنجیره گواهی میانی است.

```
var.confdir = "/etc/lighttpd"
$SERVER["socket"] == "15.15.15.15:443" {
ssl.engine = "enable"
ssl.pemfile = var.confdir + "/your_domain_name.pem"
ssl.ca-file = var.confdir + "/DigiCertCA.crt"
server.name = "your.domain.com"
server.document-root = "/my/document/root/"
}
```

اطمینان حاصل کنید که var.confdir (/etc/lighttpd) با مکان قرارگیری فایل پیکربندی مطابقت داشته باشد و همچنین آدرس IP را به آدرس مورد نظر خود تغییر دهید.

۴. **Lighttpd را راه‌اندازی مجدد کنید.**

```
# /etc/init.d/lighttpd restart
```

[۱] Certificate Authority

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۳ پیکربندی امن پروتکل SSL/TLS

در این بخش چگونگی پیکربندی امن پروتکل SSL/TLS را در سرویس‌دهنده وب Lighttpd بیان می‌کنیم. مواردی همچون استثنا کردن برخی الگوریتم‌های رمزنگاری به منظور کاهش حملاتی شبیه به FREAK، CRIME و LogJAM، غیرفعال سازی نسخه‌های ناامن SSL، برقرار کردن رمزنگاری‌های قوی که از (FS) Forward Secrecy پشتیبانی می‌کنند و فعال‌سازی HSTS را بیان می‌کنیم.

برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس‌دهنده خود، می‌توانید به ابزاری که بدین منظور توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر طراحی شده و در آدرس زیر قرار دارد، مراجعه کنید.

https://sslcheck.certcc.ir

قابل ذکر است که فایل پیکربندی Lighttpd در مسیر زیر قرار دارد و برای امن سازی SSL نیاز به ویرایش این فایل است:

- `/etc/lighttpd/lighttpd.conf`

لازم به ذکر است که در این قسمت، موارد مربوط به پیکربندی lighttpd 1.4.31 از Debian Wheezy بیان می‌شود.

۳–۱ غیرفعال سازی SSL Compression

با وجود SSL Compression، حمله CRIME ممکن است انجام شود و ما باید آن را غیرفعال کنیم. دستور زیر، SSL compression را غیرفعال می‌کند.

```
ssl.use-compression = "disable"
```

۳–۲ غیرفعال سازی الگوریتم‌های رمزنگاری ضعیف

Forward Secrecy اطمینان می‌دهد که صحت[۱] یک کلید جلسه[۲] حتی وقتی که کلیدهای زیادی مورد مخاطره قرار گرفتند، حفظ می‌شود. FS کامل[۳] این مورد را با استخراج یک کلید جدید برای هر جلسه، به انجام می‌رساند. این بدان معناست که زمانی که کلید خصوصی به مخاطره افتاد، نمی‌تواند برای رمزگشایی ترافیک SSL مورد استفاده قرار گیرد.

پیشنهاد می‌شود دستور زیر را برای استفاده از الگوریتم‌های رمزنگاری قوی و غیرفعال سازی رمزنگاری‌های ضعیف در فایل پیکربندی وارد کنید. اگر نسخه OpenSSL شما قدیمی باشد، الگوریتم‌های غیرقابل دسترس به صورت خودکار دور انداخته می‌شوند. دقت کنید که همیشه از کل الگوریتم‌ها استفاده کنید و اجازه دهید تا OpenSSL، آنهایی را که پشتیبانی می‌کند انتخاب کند.

---

۱ Integrity
۲ Session Key
۳ Perfect Forward Secrecy

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

```
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM:ECDHE-RSA-AES128-GCM-
SHA256:AES256+EECDH:AES256+EDH:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-
AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-
SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA:DHE-
RSA-AES128-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES256-GCM-
SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:AES256-SHA:AES128-
SHA:DES-CBC3-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4"
```

ترتیب الگوریتم‌ها خیلی مهم است زیرا الگوریتم‌ها به ترتیب انتخاب می‌شوند. لیست نوشته شده در بالا الگوریتم‌هایی که PFS را فراهم می‌آورند را در اولویت قرار داده است. نسخه‌های قدیمی‌تر OpenSSL ممکن است بعضی از الگوریتم‌های بالا را شامل نشود.

۳–۳ امن سازی پارامترهای دیفی هلمن

ما نیاز داریم تا یک پارامتر دیفی هلمن قوی را تولید کنیم، که می‌توانیم با دستور زیر این کار را انجام دهیم:

```
cd /etc/ssl/certs
openssl dhparam -out dhparam.pem 4096
```

و سپس باید به lighttpd بگوییم که از این پارامترها برای تغییر کلید دیفی هلمن[۱] استفاده کند:

```
ssl.dh-file = "/etc/ssl/certs/dhparam.pem"
ssl.ec-curve = "secp384r1"
```

۴–۳ اضافه کردن سرآیند HSTS

در صورت امکان شما باید ویژگی HSTS[۲] را فعال کنید برای اینکه مرورگرها فقط با پروتکل HTTPS بتوانند با سایت شما ارتباط برقرار کنند.

برای فعال‌سازی HSTS باید دستور زیر را در فایل پیکربندی Lighttpd که در زیر بیان شده است، اضافه کنید.

- /etc/lighttpd/lighttpd.conf

```
server.modules += ( "mod_setenv" )
$HTTP["scheme"] == "https" {
    setenv.add-response-header  = ( "Strict-Transport-Security" =>
"max-age=63072000; includeSubdomains; ")
}
```

و سپس Lighttpd را راه‌اندازی مجدد کنید.

توجه: برای اعمال تغییرات بالا، باید بعد از تغییرات مورد نظر، به صورت زیر سرویس‌دهنده Lighttpd راه‌اندازی مجدد شود:

```
/etc/init.d/lighttpd restart
```

[۱] DHE key-exchange

[۲] HTTP Strict Transport Security

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۵–۳ غیرفعال کردن SSLv2 و SSLv3

SSLv2 و SSLv3 ناامن هستند و باید غیرفعال شوند. برای غیرفعال سازی آنها، فایل مخصوص پیکربندی را به صورت زیر ویرایش می‌کنیم:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
```

۴ منابع

1 https://redmine.lighttpd.net/projects/1/wiki/docs_ssl

2 https://www.digicert.com/ssl-certificate-installation-lighttpd.htm

3 https://raymii.org/s/tutorials/HTTP_Strict_Transport_Security_for_Apache_NGINX_and_Lighttpd.html

4 https://raymii.org/s/tutorials/Strong_SSL_Security_On_lighttpd.html

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir