به نام خدا

امنیت داده و شبکه

نیم‌سال دوم ۱۴۰۴-۱۴۰۳

دانشکده‌ی مهندسی کامپیوتر

دانشگاه صنعتی شریف

موضوع **آسیب‌پذیری برنامه‌های کاربردی وب**

موعد تحویل **ساعت ۲۳:۵۹ شنبه ۶ اردی‌بهشت ۱۴۰۴**

طراحی تمرین توسط **محمد حدادیان**

اقتباس بخشی از `CS155, Spring 2020, Stanford University`

مقدمه

در این تمرین شما در چهار بخش، اقدام به شناسایی آسیب‌پذیری‌های برنامه‌های کاربردی تحت وب می‌کنید. بخش اول در سیستم خودتان پیاده‌سازی و اجرا می‌شود اما بخش‌های بعد را باید در یک محیط واقعی انجام دهید.

۱ بخش اول

در این بخش شما با یک برنامه وب به نام Bitbar روبرو هستید که در زبان Node.js پیاده‌سازی شده است و به کاربران این امکان را می‌دهد که Bitbar ها، یک ارز دیجیتال بسیار ایمن، را مدیریت کنند. هر کاربر هنگام ثبت‌نام در سایت، ۱۰۰ بیت‌بار دریافت می‌کند. آن‌ها می‌توانند بیت‌بارها را از طریق رابط وب به کاربران دیگر انتقال دهند و همچنین پروفایل کاربران دیگر را ایجاد و مشاهده کنند.

شما کد منبع برنامه Bitbar را در اختیار دارید. حمله‌کنندگان واقعی به طور عمومی چنین دسترسی‌ای ندارند، اما برای فهم بهتر آسیب‌پذیری‌ها در این بخش تمرین دسترسی به کد منبع برای شما فراهم شده است. Bitbar توسط یک مجموعه از بسته‌های Node اداره می‌شود که شامل چارچوب برنامه‌نویسی وب Express.js، پایگاه داده SQLite و EJS برای قالب‌بندی HTML است. لیست منابع در بخش بعدی شامل پیوندهایی برای اطلاعات بیشتر در مورد این بسته‌ها و همچنین اطلاعات دیگری است که می‌توانید به عنوان مرجع استفاده کنید.

شما برنامه Bitbar را در یک کانتینر Docker که در اختیارتان قرار گرفته‌است اجرا می‌کنید. هنگامی که سرور در حال اجراست، با رفتن به آدرس `http://localhost:3000` به سایت دسترسی دارید.

مرورگر

ما در این تمرین از نسخه ۹۳ فایرفاکس برای امتیازدهی استفاده خواهیم کرد و توصیه می‌شود که حملات خود را در فایرفاکس تست کنید. مرورگر کروم چون بعضی حفاظت‌های اضافه برای XSS دارد، ممکن است برخی از حملات را غیرممکن کند.

دستورالعمل‌های نصب دقیق:

سرور وب شما در یک کانتینر Docker اجرا خواهد شد. دستورالعمل‌های زیر شما را در نصب Docker و کانتینر کمک خواهند کرد.

۱. اگر از ویندوز یا مک استفاده می‌کنید، دستورالعمل‌های موجود در لینک۱ و لینک۲ را دنبال کنید تا Docker Desktop را نصب کنید[۱]. اگر از لینوکس استفاده می‌کنید، توزیع لینوکس خود را در `https://docs.docker.com/engine` انتخاب کنید و دستورالعمل‌ها برای نصب Docker Engine را دنبال کنید.

۲. بعد از دانلود فایل‌های تمرین به پوشه‌ی `hw2-1` رفته و دستور `bash build_image.sh` را بزنید. این دستور داکر ایمیج مربوط به این سوال را می‌سازد.

۳. برای شروع به کار برنامه، دستور `bash start_server.sh` را بزنید. پس از این کار، با رفتن به آدرس `http://localhost:3000` به وب‌اپلیکیشن دسترسی خواهید داشت.

می‌توانید سرور را با فشار دادن Ctrl+C در ترمینال ببندید. **هر بار که سرور را خاموش می‌کنید، سرور به طور کامل بازنشانی خواهد شد.**

برای راه‌اندازی مجدد سرور با یک پایگاه داده پاک، فقط دستور `bash start_server.sh` را دوباره اجرا کنید.

[۱] برای راهنمای گام به گام برای ویندوز، به `https://www.youtube.com/watch?v=IwLQ92XRiGg` مراجعه کنید.

نکات Docker

شما نیازی به آشنایی با Docker برای تکمیل این تکلیف ندارید. با این حال، چند نکته ممکن است مفید باشد:

- `docker ps -a` تمام کانتینرهای شما را لیست می‌کند.
- `docker images` ایمیج‌های شما را لیست می‌کند.
- `docker system prune -a` ایمیج‌ها و کانتینرهای بی‌استفاده از ماشین شما را حذف می‌کند.
- اسکریپت‌های `build_image` و `start_server` به طور ساده دستورات Docker یک خطی برای ساخت یک ایمیج Docker و ایجاد یک کانتینر موقت از آن ایمیج هستند.
- تنها فایلی که از ماشین محلی شما به کانتینر Docker در حال اجرا منتقل می‌شود `code/router.js` است. پس اگر شروع به اصلاح فایل‌های دیگر کنید و تغییرات نمایان نشود، نگران نباشید. شاید برای اعمال تغییرات لازم باشد کانتینر خود را پس از اصلاح `code/router.js` دوباره راه‌اندازی کنید. اگر تصمیم به اصلاح فایل‌های دیگر کنید، باید ایمیج Docker را بازسازی کنید تا تغییرات شما در ایمیج جای گیرند.
- مستندات: https://docs.docker.com/

در ادامه‌ی این بخش شما باید سه سری حمله علیه برنامه Bitbar توسعه دهید. برای هر حمله، در ادامه شرح می‌دهیم که دقیقاً باید چه‌کار کنید. برای دریافت امتیاز، باید نتیجه‌ای که در هر حمله توصیف شده را به دست آورید. تمامی حملات شما باید فرض کنند که سایت به آدرس http://localhost:3000 قابل دسترس است.
شما نمی‌توانید از کتابخانه‌های خارجی استفاده کنید و همچنین نمی‌توانید به برنامه وب خود دست بزنید. به خصوص نمی‌توانید از jQuery استفاده کنید. شما می‌توانید از منابع آنلاین استفاده کنید، اما لطفاً آن‌ها را در `README.txt` ارسالی‌تان ذکر کنید.

۱.۱ اکسپلویت آلفا: دزدیدن کوکی

در حمله اول، هدف شما دزدیدن کوکی جلسه (session) کاربر وارد شده به سیستم و ارسال آن به یک URL تحت کنترل مهاجم است. شما باید یک URL ایجاد کنید که با `http://localhost:3000/profile?username=` شروع شود و زمان بازدید از این آدرس، کوکی دزدیده شده را به
`http://localhost:3000/steal_cookie?cookie=stolen_cookie_here`
ارسال کند. زمانی که حمله موفق باشد، سرور کوکی دزدیده شده را در خروجی ترمینال ثبت خواهد کرد.
توجه! حمله باید به شکل نامحسوس برای کاربر باشد. این به این معناست که نباید تغییراتی در ظاهر سایت ایجاد شود و متن اضافی دیگری قابل مشاهده نباشد. به جز نوار مکان مرورگر (که ممکن است متفاوت باشد)، کاربر باید صفحه‌ای را ببیند که هنگام بازدید از پروفایل خود به نظر معمولی برسد. اجتناب از متن آبی هشدار دهنده که یک کاربر یافت نشد راه مهمی از حمله است. اگر تعداد بیت‌بارها یا محتوای پروفایل صحیح نباشد (تا جایی که "معمولی" به‌نظر بیاید)، مشکل ندارد.
تحویل و امتیازدهی. شما باید یک فایل به نام `a.txt` را تحویل دهید که فقط آدرس URL مخرب شما را دربردارد. مصحح به عنوان `user1` وارد Bitbar شده و در تب پروفایل قرار دارد. از این مکان، مصحح آدرس URL شما را از نوار آدرس کپی می‌کند و به آنجا می‌رود. مصحح باید با انتخاب "Containers/Apps" در Docker، سپس "bitbar-container" و کلیک بر روی "LOGS"، کوکی دزدیده شده را ببیند.

۲.۱ اکسپلویت براوو: جعل درخواست راه دور (CSRF)

در حمله دوم، شما باید یک حمله جعل درخواست از راه دور (CSRF) بسازید که از یک کاربر دیگر ۱۰ بیت‌بار به حساب مهاجم انتقال دهد.

حمله ارسالی شما یک صفحه HTML است که ۱۰ بیت‌بار را از کاربر لاگین‌شده به حساب کاربر attacker منتقل می‌کند. به محض اتمام انتقال، حمله شما باید بلافاصله کاربر را به
http://sharif.edu/~kharrazi/courses/40441-011/
هدایت کند. این کار باید به گونه‌ای سریع انجام شود که کاربران عادی آن را متوجه نشوند.
تحویل و امتیازدهی. شما باید یک فایل HTML مستقل به نام b.html را تحویل دهید که حاوی حمله شما باشد. با باز کردن این صفحه توسط کاربری که از قبل در سامانه لاگین است، باید ۱) ده بیت‌بار از حساب او به حساب مهاجم منتقل شود، ۲) سایت حمله به سایت CE441 به‌سرعت منتقل شود و ۳) هیچ‌گاه آدرس localhost:3000 مشخص نشود.

۳.۱ اکسپلویت گاما: حمله زمانی

حمله زمانی یک نوع حمله جانبی است که مهاجم با تجزیه و تحلیل زمانی که یک سیستم برای انجام یک عمل صرف می‌کند، سعی در استخراج داده می‌کند. به عنوان مثال، یک سرور وب ممکن است زمان بیشتری برای پاسخ به یک درخواست ورود که حاوی یک گذرواژه صحیح است، نسبت به یک درخواست حاوی گذرواژه نامعتبر صرف کند. حتی اگر قوانین سایت یک حمله‌کننده را از مشاهده مستقیم پاسخ HTML به یک درخواست ورود جلوگیری کند، مقدار زمانی که سرور برای پاسخ دادن به درخواست زمان می‌برد ممکن است اطلاعاتی در مورد اینکه گذرواژه ارائه شده صحیح یا نادرست بوده باشد را لو دهد. در این قسمت شما باید یک حمله انجام دهید که گذرواژه کاربر دیگر را با بهره‌گیری از چنین کانال جانبی زمانی استخراج کنید. شما به ویژه با تحلیل مقدار زمانی که صفحه ورود به Bitbar به یک گذرواژه صحیح در مقابل گذرواژه‌های نادرست پاسخ می‌دهد، گذرواژه قربانی را پیدا خواهید کرد.
شما باید یک نام کاربری مخرب بسازید که شامل یک اسکریپت باشد که گذرواژه userx را با تست گذرواژه‌ها در یک لغتنامه ارائه شده و اندازه زمان پاسخ سرور برای هر گذرواژه‌ای که ارائه می‌شود اندازه‌گیری کند. اسکریپت شما باید زمان پاسخ سرور را برای تمام گذرواژه‌های موجود در لیست ارائه شده تحلیل کرده، گذرواژه صحیح را تشخیص دهد و آن را به

```
http://localhost:3000/steal_password?password=[password]&timeElapsed=[time_elapsed]
```

ارسال کند.
می‌توانید از کد proj2/code/gamma_starter.html به عنوان نقطه شروع برای حمله خود استفاده کنید. این قطعه کد شامل لغتنامه‌ای از گذرواژه‌ها برای تست است.
تحویل و امتیازدهی. شما باید یک فایل به نام g.txt حاوی اسکریپت نام کاربری مخرب را تحویل دهید. برای امتیازدهی حمله، ما به عنوان attacker وارد شده و به صفحه انتقال می‌رویم، اسکریپت نام کاربری مخرب را که در حلقه اجرا مشخص کرده‌اید را در فیلد username وارد می‌کنیم و ۱۰ بیت‌بار به آن منتقل می‌کنیم.
اگر مصحح بعد از انجام حمله به عنوان userx وارد شده باشد، مشکلی نیست، و حمله ممکن است چند ثانیه به طول بیانجامد. مصحح در حین اجرای حمله کلیکی انجام نخواهد داد و یا از صفحه انتقال خارج نخواهد شد. تغییرات قابل مشاهده در وب‌سایت نباید وجود داشته باشد و پیام خطای آبی در صفحه انتقال باید "کاربر یافت نشد" باشد.
راهنمایی: مطمئن شوید که برای این حمله از علامت backtick به جای quote استفاده می‌کنید. کانال‌های جانبی زمانی ممکن است حساس باشند.

۴.۱ تحویل بخش اول

- فایل تحویلی برای هر حمله را داخل یک دایرکتوری به نام hw2-1 قرار دهید.
- یک README.txt بسازید تا منابع آنلاین مورد استفاده خود را نقل قول کرده و یادداشت‌های خاصی را به مصحح بدهید و آن را هم در دایرکتوری hw2-1 قرار دهید.
- برای هر بخش، راه‌حل خود را گام به گام توضیح دهید و تصاویر مرتبط را در گزارش خود قرار دهید و آن را به عنوان یک فایل به نام report.pdf ارسال کنید.
- زمانی که فایل تحویلی شما را دانلود می‌کنیم، انتظار داریم که پنج فایل زیر داخل 'hw2-1' باشد:

```
README.txt -
report.pdf -
a.txt -
b.html -
g.txt -
```

۲ بخش دوم

در این بخش، با یک حمله‌ی ترکیبی XSS و CSRF به سمت یک سایت که برروی سیستم خود میزبانی نمی‌شود روبرو هستیم. مشابه تمرین گذشته، در این بخش هم به شما تنظیمات داکر مربوط به سوال داده شده است که با رفتن به پوشه‌ی hw2-2 و زدن دستور `docker compose up` می‌توانید سایت مدنظر را به صورت لوکال بالا بیاورید. هرچند گرفتن نمره‌ی این تمرین منوط به گرفتن پرچم موجود در سایت اصلی به آدرس http://65.174:8080.201.109/ است. قالب پرچم این سوال هم به شکل CE441{xxx} است (چنان‌چه دسترسی به سرور از داخل ایران مسدود شود، این موضوع تاثیری بر زمان تحویل تمرین ندارد و ضمن اطلاع موضوع از روش‌های جایگزین برای اتصال استفاده کنید).

در فایل‌های این سوال، می‌توانید کدهای مربوط به سایت را ببینید هرچند در واقعیت شما به کد منبع اهداف خود دسترسی ندارید.

کار خود در این سوال را با بررسی کد منبع سایت و دیدن اسکریپت‌های JS موجود در آن شروع کنید. صفحه‌ی اصلی این سایت هدف به شما اجازه‌ی ارسال یک آدرس به عنوان کتاب اهدایی به سایت را می‌دهد. شما در این بخش می‌توانید URL موردنظر خود را ارسال کنید.

همچنین آمار مربوط به تعداد کتاب‌های اهدایی به کتاب‌خانه هم از طریق ایجاد یک ارتباط وب‌سوکت به‌روز می‌شود.

بعد از ارسال این URL ، ربات ادمین سایت به آن آدرس درخواست می‌زند. پس برای حل این سوال باید به‌گونه‌ای آدرس موردنظر خود را بسازید که بعد از ارجاع ربات ادمین به این آدرس، به‌نوعی به پرچم دست پیدا کنید.

راهنمایی: تفاوت این بخش با بخش اول، این است که چون ربات ادمین روی سیستم شما در حال اجرا نیست، باید محتویات اکسپلویت خود را در یک آدرس دسترس‌پذیر از سمت ربات ادمین قرار دهید. از این رو می‌توانید از ابزارهایی که کدها و صفحات شما را به صورت موقت میزبانی کرده و لاگ درخواست‌های ارسالی به سمت آن‌ها را ذخیره می‌کنند استفاده کنید.

راهنمایی: برای راهنمایی بیشتر، حملات جعل درخواست از راه دور در وب‌سوکت‌ها را بررسی کنید.

راهنمایی: ممکن است در ارسال دستورات وب‌سوکت به خطای http/s بخورید. برای رفع عیب از خطاها همواره کنسول مرورگر را بررسی کنید.

۳ بخش سوم

در سومین بخش این تمرین، با یک سایت روبرو هستیم که در آن هر شخص می‌تواند ثبت‌نام کرده و پروفایل خود را با پشتیبانی از زبان مارک‌داون داشته باشد. هدف این بخش هم مانند بخش‌های قبل دسترسی به پرچم است. با دقت در کد متوجه خواهید شد که پرچم در صورتی به شما داده می‌شود که با استفاده از توکن ادمین، به آدرس دریافت فلگ درخواستی ارسال کنید.

برای دسترسی به این وبسایت به آدرس http://65.174:8000.201.109 بروید.

در ادامه از دو طریق می‌توانید راه‌حل را دنبال کنید: یا به نحوی توکن ادمین را به‌دست بیاورید (ممکن است شدنی نباشد) یا ادمین را مجبور کنید تا با استفاده از توکن خود، پرچم را گرفته و برای شما ارسال کند!

پس تا اینجا باید متوجه شده باشید که گزینه‌ی ریپورت در صفحه پروفایل باید مورد استفاده قرار بگیرد تا ادمین را وادار به ارسال پرچم برای خود کنید.

قالب پرچم این بخش هم به شکل CE441{xxx} است و ادامه‌ی راه به عهده‌ی شما.

راهنمایی: احتمالا برای حل این بخش هم نیاز داشته باشید تا محتوای اکسپلویت خود را در یک صفحه میزبانی کنید تا ربات ادمین به آن درخواست بفرستد. یک گزینه برای این کار سایت https://webhook.site/ است که به شما یک آدرس یکتا می‌دهد و هر درخواستی به سمت آن بیاید را می‌توانید ببینید. البته شاید این سایت به تنهایی برای حل این سوال کافی نباشد!
راهنمایی: اگر موفق شدید اسکریپتی در صفحه تزریق کنید اما آن اسکریپت اجرا نشد، به این فکر کنید که چه چیزهایی ممکن است جلوی اجرای اسکریپت را گرفته باشند.

۴ بخش چهارم

در چهارمین بخش این تمرین، نیاز به بررسی دقیق و خلاقیت و تفکر خارج از چارچوب دارید. ممکن است نمره‌ی این بخش بیشتر از بخش‌های قبل تعیین شود!

در این بخش هم به شما تنظیمات داکر و کد منبع مربوط به سوال داده شده است که با رفتن به پوشه‌ی hw2-4 و زدن دستور docker compose up می‌توانید سرویس مدنظر را به صورت لوکال بالا بیاورید.

در این چالش با یک سرویس به زبان پایتون روبرو هستید که هم پرچم را در آدرس secret/نگهداری می‌کند و هم یک درخواست http به پارامتر url ورودی شما که به آدرس proxy/ فرستاده می‌شود ارسال می‌کند. اما در ارسال این درخواست، شرط‌هایی وجود دارند که باید رعایت شوند و دامنه‌های در دسترس فقط به دو دامنه محدود شده‌اند.

دسترسی به آدرس پرچم فقط با استفاده از آی‌پی لوکال امکان‌پذیر است. از این رو شما باید سرویس پروکسی را مجبور کنید تا به آدرس پرچم درخواست زده و خروجی را به شما بازگرداند.

برای دسترسی به این بخش به آدرس http://65.174:5004.201.109 مراجعه کرده و کار حل خود را با بررسی کد منبع‌ها شروع کنید تا با شرط‌هایی که باید دور بزنید آشنا شوید. برای لذت بردن از این مرحله، باقی جزئیات را خود کشف کنید!
راهنمایی: حل این سوال به‌نوعی به تفاوت پردازش url در زبان‌های پایتون و جاوااسکریپت مربوط است.
راهنمایی: برای حل این سوال حتماً به سرور شخصی نیاز دارید. پیشنهاد می‌شود تمام سناریوی حل خود را ابتدا به صورت تئوری بررسی کرده و بعد در محیط لوکال خود تست کنید و در نهایت برای اجرای نهایی از سرورهای ساعتی دسترسی بگیرید.
راهنمایی: حتماً توجه داشته باشید که احتمال کمی وجود دارد راه‌حل درست شما روی سیستم لوکال شما اجرا نشود. پس همیشه حتما یک بار روی سرور هم تست کنید.
راهنمایی: اگر به‌نظر خود تا حدی خوبی در حل سوال پیش رفته بودید، می‌توانید شانس خود را برای گرفتن راهنمایی بیشتر با ایمیل زدن امتحان کنید!

تحویل بخش‌های دو تا چهار

برای این بخش شما باید کد اکسپلویت خود را به همراه یک ویدیو ۵ دقیقه‌ای (برای هر بخش) که قدم به قدم تا رسیدن به پرچم راه‌حل را توضیح می‌دهد در پوشه‌ی hw2-2,hw2-3,hw2-4 از فایل‌های تحویلی خود قرار دهید. ویدیو خود را در سرویس‌های میزبانی فایل بارگذاری کرده و آدرس آن به همراه هش فیلم را در فایل url.txt قرار دهید.

فراموش نکنید که دسترسی فایل در سرویس گوگل‌درایو برای عموم آزاد باشد. در غیر این صورت ممکن است به دلیل عدم دسترسی نمره تمرین را کامل از دست بدهید.

در نهایت تحویل‌دادنی‌های شما باید یک فایل zip با نام‌گذاری ce441-hw2-<STUDENT_ID> باشد که به ترتیب شامل پوشه‌ها و فایل‌های زیر است (در اینجا به عنوان نمونه زبان پایتون قرار گرفته است اما شما می‌توانید با هر زبانی (مثلا HTML) اکسپلویت خود را بنویسید):

```
ce441-hw2-99101234:
   hw2-1:
      README.txt
      a.txt
      b.html
      g.txt
      report.pdf
   hw2-2:
```

```
    exploit.py
    url.txt
  hw2-3:
    exploit.py
    url.txt
  hw2-4:
    exploit.py
    url.txt
```