

به نام خدا



امنیت داده و شبکه

نیمسال اول ۱۴۰۴-۱۴۰۳

دانشکده‌ی مهندسی کامپیوتر

دانشگاه صنعتی شریف

موضوع آسیب‌پذیری برنامه‌های کاربردی وب
موعد تحویل ساعت ۲۳:۵۹ دوشنبه ۲۸ آبان ۱۴۰۳
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، 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 گرفته است اجرا می‌کنید. هنگامی که سرور در حال اجراست، با رفتن به آدرس <http://localhost:3000> به سایت دسترسی دارید.

مروگر

ما در این تمرین از نسخه ۹۳ فایرفاکس برای امتیازدهی استفاده خواهیم کرد و توصیه می‌شود که حملات خود را در فایرفاکس تست کنید. مروگر 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 [لينك ۱](#) و [لينك ۲](#) را دنبال کنید تا 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 ۱-۲ hw2.sh رفته و دستور bash build_image را بزنید. این دستور داکر ایمیج مربوط به این سوال را می‌سازد.

۳. برای شروع به کار برنامه، دستور bash start_server 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 بینید. هر بار که سرور را خاموش می‌کنید، سرور به طور کامل بازنشانی خواهد شد.

برای راه اندازی مجدد سرور با یک پایگاه داده پاک، فقط دستور bash start_server 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:

- تمام کانتینرهای شما را لیست می‌کند. `docker ps -a`
- ایمیج‌های شما را لیست می‌کند. `docker images`
- docker system prune -a ایمیج‌ها و کانتینرهای بی‌استفاده از ماشین شما را حذف می‌کند.
- اسکریپت‌های `start_server` و `build_image` 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 راه اندازی 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 چه کار 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 ارسالی تان ذکر کنید.

۱.۱ اکسپلوبیت 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 `=username` شروع شود و زمان بازدید از این آدرس، کوکی دزدیده شده را به

`http://localhost:3000/steal_cookie?cookie=stolen_cookie_here`

ارسال کنند. 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 یافته نشد راه مهمی از حمله است. اگر تعداد بیتبارها یا محتوای پروفایل صحیح نباشد (تا جایی که "معمولی" به نظر 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 کند و به آنجا می‌رود. مصحح باید با انتخاب "Containers/Apps" در "Containers/Apps" سپس "bitbar-container" و کلیک بر روی "LOGS"، "کوکی دزدیده شده را ببینند.

۲.۱ اکسپلوبیت 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 لایگین شده به حساب کاربر attacker منتقل می‌کند. به محض اتمام انتقال، حمله شما باید بلافضله 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 `hw1.html` را تحویل دهید که حاوی حمله شما باشد. باز کردن این صفحه توسط کاربری که از قبل در سامانه لایگین است، باید ۱) ده بیتبار از حساب او به حساب مهاجم منتقل شود، ۲) سایت حمله به سایت CE441 به سرعت منتقل شود و ۳) هیچ‌گاه آدرس localhost:3000 مشخص نشود.

۳.۱ اکسپلولیت گاما: حمله زمانی

حمله زمانی یک نوع حمله جانبی است که مهاجم 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 حمله کننده 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` بسازید که 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 بدھید و آن را هم در دایرکتوری `hw2-1` قرار دهید.
- برای هر بخش، راه حل 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 بخش دوم با یک وبسایت روبرو هستید که در آن می‌توان یوزرهای جدید ساخت و با یوزرهای لاتین کرد. این سوال دو صفحه مختلف را در بر می‌گیرد. روی پورت ۵۰۰۱ سرویس اصلی در حال اجراست و روی پورت ۵۰۰۲ مخزن اسرار بالا آمده است. برای دسترسی به پرچم این بخش باید مخزن اسرار را بگیرید اما این مخزن چک می‌کند که فقط آدرس‌های خاصی اجازه دسترسی به آن داشته باشند. در واقع اگر شما با آیپی سایت بخواهید پورت ۵۰۰۲ را ببینید خطای خطا می‌خورد و باید با هاست لوکال یا دیگر هاست‌های مجاز به پرچم دست پیدا کنید.

همچنین این بخش فقط با کاربر ادمین قابل مشاهده هست پس باید به سطح ادمین دسترسی پیدا کنید. برای دسترسی به این سایت به آدرس <http://ce441-web.spchallenge.ir:5001> رفته و برای گرفتن پرچم به پورت ۵۰۰۲ از این آدرس باید بروید. قالب پرچم این بخش به شکل {CE441{xxx}} است.

راهنمایی: دسترسی شما به پرچم این سوال در دو مرحله انجام می‌شود. نخست سعی کنید با استفاده از آسیب‌پذیری‌های نسبتاً رایج در کد این سایت که به زبان پایتون نوشته شده است دسترسی ادمین بگیرید، و در مرحله بعد از طریق یوزر ادمین به پرچم محافظت‌شده دسترسی پیدا کنید.

راهنمایی: ممکن است روی مرورگر فایرفاکس به مشکل بخورد، ترجیحاً از مرورگر گوگل کروم استفاده کنید.
راهنمایی: در شبکه داخلی داکر می‌توان با نام هر سرویس در فایل docker-compose.yml به آن سرویس دسترسی پیدا کرد!

۳ بخش سوم

در این بخش، با یک حمله‌ی ترکیبی XSS و CSRF به سمت یک سایت که بروی 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 docker compose up و زدن دستور hw2-3 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://ce441-web.spchallenge.ir:8080> است. قالب پرچم این سوال هم به شکل {CE441{xxx}} است.

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 به روز می‌شود. بعد از ارسال این URL، ربات ادمین سایت به آن آدرس درخواست می‌زند. پس برای حل این سوال باید به گونه‌ای 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 اکسپلوبیت خود را در یک آدرس دسترسی‌پذیر از سمت ربات ادمین قرار دهید. از این روش می‌توانید از ابزارهایی که کدها و صفحات

شما را به صورت موقت میزبانی کرده و لاغ درخواست‌های ارسالی به سمت آن‌ها را ذخیره می‌کند استفاده کنید.

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

۴ بخش چهارم

در آخرین بخش این تمرین، مجدداً با یک سایت روپرو 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 دسترسي 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 دسترسي به این وبسایت به آدرس <http://ce441-web.spchallenge.ir:8000> بروید.

در ادامه از دو طریق می‌توانید راه حل را دنبال کنید: یا به نحوی توکن ادمین را به دست 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: احتمالاً برای حل این بخش هم نیاز داشته باشید تا محتوای اکسپلوبیت 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 باید را می‌توانید ببینید. البته شاید این سایت به تنها‌ی 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.

تحویل بخش‌های دو تا چهار

برای این بخش شما باید کد اکسپلوبیت خود را به همراه یک ویدیو ۵ دقیقه‌ای که قدم به قدم تا رسیدن به پرچم راه حل 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.

در نهایت تحویل دادنی‌های شما باید یک فایل zip با نام گذاری <STUDENT_ID> 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 (Mثلا HTML) اکسپلوبیت خود را بنویسید):

```

1 ce441-hw2-99101234:
2   hw2-1:
3     README.txt
4     a.txt
5     b.html
6     g.txt
7     report.pdf
8   hw2-2:
9     exploit.py
10    url.txt
11   hw2-3:
12     exploit.py
13     url.txt
14   hw2-4:
15     exploit.py
16     url.txt

```