دوره تسلط به OWASP TOP10 and More

درباره این دوره

با توجه به درخواست‌های متعددی که برای برگزاری کلاس داشتم، تصمیم گرفتم یک دوره با محوریت آشنایی و تسلط به آسیب‌پذیری‌هایی که روزانه در شرکت‌های بزرگ کشف و گزارش می‌شه رو تدوین کنم. برای همین سراغ OWASP رفتم، ولی ۱۰ آسیب‌پذیری برتر این بنیاد امنیتی تمامی موارد رو پوشش نمی‌ده برای همین موارد دیگه رو هم اضافه کردم. این موارد رو می‌تونید توی سیلابس مشاهده کنید. به طور کلی در یک جمله هدف این دوره انتقال دانش کشف آسیب‌پذیری‌های رایج به‌صورت اصولی هست.

مزیت این کلاس

موردی که همیشه توی ذهن من بوده، کاربردی نبودن کلاس‌های امنیت هست. معمولا یه سری تئوری به شاگردان گفته میشه و روی یک محیط مصنوعی، یه سری آسیب‌پذیری به‌صورت عملی نشون داده می‌شه. من احساس می‌کنم که جای پیکارهایی که شاگردان بعد از تفهیم درس تئوری،به سراغ اونا برن و حلشون کنن کم هست. برای همین سعی کردم در دوره پیش رو این مورد رو لحاظ کنم.

مدت زمان دوره

این دوره به مدت ۵ هفته در ۵ جلسه ۶ ساعته در روزهای جمعه بین ساعت ۱۰ تا ۱۶ برگزار میشه، محل برگزاری یا Skype یا Google meet است. در صورت نیاز، یک جلسه اضافه‌تر نیز برگزار خواهد شد.

پیشنیازهای این دوره

از پیشنیازهای دوره به موارد زیر میشه اشاره کرد:

- آشنایی نسبی با JavaScript
- آشنایی نسبی با یک زبان برنامه‌نویسی
- آشنایی نسبی با ابزار BurpSuite
- علاقه‌مندی زیاد به امنیت

با توجه به اینکه این دوره قرار هست از سطح پایین تا متوسط رو به‌صورت کامل پوشش بده (البته در برخی موارد پیکارها سطح بسیار بالایی دارند)، نگران نداشتن دانش کافی نباشید

کیا برای این دوره مناسبن؟

افراد زیر برای این دوره مناسب هستن:

- برنامه‌نویس‌های علاقه‌مند به امنیت
- امنیت‌کارهای تازه کار

- افراد علاقه‌مند به امنیت با پشتکار
- افرادی که در آینده میخوان باگ‌بانتی کار کنن

آیا امکان تهیه ضبط شده کلاس هست؟

خیر، چرا که اصل این دوره پیکارهای رفع اشکال‌ها هست. البته شرکت‌کننده‌ها میتونن دوره رو برای استفاده شخصی خودشون ضبط کنن.

پیکارها

پیکارهای این دوره اکثرا از صفر کد زده شده و تنوع زبان در آنها وجود داره. نصف بیشتر پیکارها بر اساس آسیب‌پذیری واقعی که پیشتر رخ داده هست. در طول هفته بین دو جلسه کلاس، آدرس آی.پی سرور روی اینترنت به شرکت‌کنندگان داده میشه و می‌تونن روی پیکارها کار کنند.

نقش شما در این دوره

اولا شما باید تا روز برگزاری کلاس، موارد مشخص شده در سیلابس رو مطالعه کنید، این بتون کمک می‌کنه خیلی راحت‌تر با کلاس ارتباط برقرار کنید. دوما، در بین جلسات کلاس که ۱ هفته هست، فعال باشید و روی پیکارها کار کنید، این باعث میشه اگر هم نتونید پیکار رو حل کنید، بعد از اینکه من توی کلاس حل کردم، توی ذهنتون ثبت بشه.

امتحان دوره

امتحان دوره برای اینکه شرکت‌کننده‌ها بتونن ارزیابی از خودشون داشته باشن در جلسه آخر برگزار میشه. پیکار آخر شامل یک سوال واقعی استخدامی در یک شرکت امنیتی در انگلستان است که شامل چندین آسیب‌پذیری است و کشف و اکسپلویت موفق همه اونها به منزله حل چالش است.

سیلابس

Web Application Security - OWASP TOP10 and More

Description

The syllabus has been designed based on the OWASP top10 and more security concepts (Inspired by ELearnSecurity courses). The course consists of various challenges which make the participant get involved and realize the vulnerabilities, learn the exploitation and make patches.

OWASP TOP 10

1. Injection (NoSQL, SQL, code and command Injection)
    a. SQL injection
        i. Concept
        ii. Code example
        iii. Real world examples
        iv. Discovery and exploitation
        v. SQLmap (tool)
        vi. 7 levels Challenges (Hands on lab)
        vii. Bonus (Out of band technique)
    b. NoSQL Injection
        i. Concept
        ii. Types
        iii. A challenge (Hands on lab)
    c. Command injection
        i. Concept
        ii. Real world examples
        iii. Commix (tool)
        iv. 4 levels challenges (Hands on lab)
        v. Reverse shell
        vi. DNS data exfiltration
    d. Code injection
        i. Concept
        ii. Real world examples
        iii. 3 levels challenges (Hands on lab)
    e. Server-Side template injection (SSTI)
        i. Concept
        ii. Code examples
        iii. Real world examples
        iv. Tplmap (tool)
        v. 3 levels challenge (Hands on lab)
2. Broken Authentication
    a. Authentication and authorization

b. Various implementation models (cookie, token and etc)
c. Cookie based authentication
    i. Implementation
    ii. Weaknesses
d. Token based authentication
    i. Json Web Token
    ii. Attack on JWT
e. Open Authorization
    i. Protocol
    ii. Weaknesses
f. Single Sign On
    i. Implementations
    ii. Cross Origin resource Sharing
    iii. JSONP (implementation and attack)
g. Parked domains authentication
h. Real world examples
i. Common vulnerabilities in authentications
j. A challenge (Hands on lab)

3. Sensitive Data Exposure
    a. Concept
    b. Real world examples
    c. Gobuster, ffuf, wfuzz (tools)
    d. Fuzzing web paths (dirs and execution paths) (Hands on lab)
4. XML External Entities (XXE)
    a. Concepts
    b. Various scenarios
    c. Exploitation
        i. Reading file
        ii. CDATA method
        iii. Base64 method
        iv. DTD files
    d. Combination by SSRF
    e. Out of band technique
    f. 2 levels challenge (Hands on lab)
5. Broken Access Control
    a. Concepts
    b. Real world examples
    c. Discovery by BurpSuite

    d. Insecure Direct Object Reference (IDOR) scenario (Hands on lab)
6. Security Misconfiguration
    a. Concepts
    b. Real world examples
    c. Default credentials/Stack trace errors scenario (Hands on lab)
7. Cross-Site Scripting
    a. Concepts
        i. Critical path rendering
        ii. Document object model
        iii. Same origin policy **(in action)**
        iv. Cross origin resource sharing **(in action)**
        v. Preflight request
    b. Cross site request forgery
        i. Discovery and exploit
        ii. Same site cookies
    c. Cross origin resource sharing flaw
        i. Discovery and exploit
    d. Cross site scripting
        i. Types (HTML and DOM)
        ii. Discovery and exploit
    e. Shell upload in WordPress website by XSS (Hands on lab)
    f. Cross-Site Resource Sharing (CORS) scenario (Hands on lab)
8. Insecure Deserialization
    a. Concepts
    b. PHP deserialization
        i. Modifying object attributes
        ii. Magic methods
        iii. Discovery and exploit
    c. NodeJs object deserialization to RCE
    d. PHP object deserialization to RCE (Hands on lab)
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

Extras:

1. Open Redirect
    a. Concept
    b. 11 levels attack scenario (Hands on lab)
2. Server-Side Request Forgery
    a. Concept

    b. Real world examples
    c. Code examples
    d. Detection
    e. Filters to prevent
    f. Bypasses
        i. Domain
        ii. Redirect method
        iii. Whitelist bypass
        iv. Parse URL flaws
    g. 3 levels challenges
3. Business Logic Vulnerability
    a. Real world examples
4. API security
    a. Some tricks in security test
    b. Fuzzing on the API endpoint
    c. Mass assignment exploitation
    d. Different content types
5. Apple bug bounty lesson learned
6. A UK company challenge (Hands on lab)

Session 1

- Injection

Session 2

- Cross Site Scripting
- Using Components with Known Vulnerabilities
- Security Misconfiguration (CORS)

Session 3

- Broken Authentication
- Sensitive Data Exposure

Session 4

- Open Redirect
- Server Side Request Forgery
- External XML Entity

Session 5

- Broken Access Control
- API Security
- Insecure Deserialization
- Business Logic Vulnerability
- Insufficient Logging & Monitoring