KHUNG CHƯƠNG TRÌNH ĐÀO TẠO WEB SECURITY

WBS	Tên nội dung đào tạo	Thông tin chi tiết nội dung đào tạo	Tài liệu học tập	Yêu cầu đánh giá chi tiết	Cách thức đánh giá	Hoạt động của mentor và sinh viên	Parttime	Fulltime
							265	**217**
1,0	**Lập trình**							
1,1	Shell script	Tối thiểu: - Setup OS - Command - Web Server - Virtual host - Linux programming Optional: - SSH Logger - HTTP Client	- Google - Linux LPIC	Đạt: PL01 (5đ) Tốt: PL01 + PL02 + PL03 (7 - dưới 8.5) XS: PL01 + PL02 + PL03 + PL04 (8.5 - 10)	Chấm báo cáo + báo cáo trực tiếp có demo, tài liệu	- Đầu ngày thứ 2 sau khi nhận bài sinh viên update về hướng tiếp cận - Sinh viên update tiến độ sau 2 ngày và đảm bảo finish deadline - Nội dung không nắm rõ sau 1 ngày tìm hiểu => mentor giải đáp	7	5
1,2	Lập trình web hoàn chỉnh	framework Laravel with DB MySQL	- http://giasutinhoc.vn/chuyen-muc/lap-trinh/lap-trinh-php-co-ban/ - https://laravel.com/	Đạt: PL05 (5đ) Tốt: PL05 + PL06 (7 - dưới 8.5) XS: như mức Tốt và code clean, dễ đọc	Chấm source code và demo trực tiếp, phản biện với mentor vào deadline	- Đầu ngày thứ 3 sau khi nhận bài sinh viên update về hướng tiếp cận - Sinh viên báo cáo trực tiếp sau 5-7 ngày để trình bày tiến độ, finish đúng deadline - Nội dung không nắm rõ sau 1 ngày tìm hiểu => mentor giải đáp	14	10
			1. Checkpoint Programming					
2,0	**Basic web vul**							
2,1	Server side vul	Authention & Access Control	Portswigger	Đạt: 50% lab các bài mức độ Apprentice & 50% các bài mức độ Practitioner Tốt: 70% lab các bài mức độ Apprentice & 70% các bài mức độ Practitioner Xuất sắc: Làm hết các lab Từ apprentice đến Expert	Số bài lab được ghi nhận là những bài có nộp wu và báo cáo trực tiếp	- Sinh viên đọc lý thuyết trên Portswigger và làm lab như yêu cầu, viết lại write up để mô tả cách làm và bản chất lỗ hổng - Deadline: hẹn gặp mentor để phản biện trực tiếp cách làm	7	5
2,2		SQL Injection	Portswigger				7	5
2,3		Directory Traversal, Command Injection, File Upload	Portswigger				7	5
2,4		Information disclosure, business logic vulnerablities	Portswigger				7	5
2,5		Race conditions, SSRF	Portswigger				7	5
2,6		XXE, NoSQL injection	Portswigger				7	5
2,7	Client side vul	XSS	Portswigger	Đạt: 50% lab các bài mức độ Practitioner Tốt: 70% lab các bài mức độ Apprentice & 70% các bài mức độ Practitioner	Số bài lab được ghi nhận là những bài có nộp wu và báo cáo trực tiếp	- Sinh viên đọc lý thuyết trên Portswigger và làm lab như yêu cầu, viết lại write up để mô tả cách làm và bản chất lỗ hổng - Deadline: hẹn gặp mentor để phản biện trực tiếp cách làm	7	5
2,8		CSRF, CORS, Clickjacking	Portswigger				7	5
2,9		Dom-based vulnerablities, Websockets	Portswigger				7	5
			2. Checkpoint Basic web vul					
3,0	**Advanced web vul**							
3,1	Các kỹ thuật khó & mới về tấn công Web	Insecure deserialization	Portswigger	Đạt: 50% lab các bài mức độ Apprentice & 50% các bài mức độ Practitioner Tốt: 70% lab các bài mức độ Apprentice & 70% các bài mức độ Practitioner Xuất sắc: Làm hết các lab Từ apprentice đến Expert	Số bài lab được ghi nhận là những bài có nộp wu và báo cáo trực tiếp	- Sinh viên đọc lý thuyết trên Portswigger và làm lab như yêu cầu, viết lại write up để mô tả cách làm và bản chất lỗ hổng - Deadline: hẹn gặp mentor để phản biện trực tiếp cách làm	7	5
3,2		Server-side template injection, Oauth, JWT	Portswigger				7	5
3,3		Web cache poisoning, Essential skills, Prototype pollution	Portswigger				7	5
3,4		GraphQL API vulnerabilities, HTTP Host attacks	Portswigger				7	5
3,5		HTTP request smuggling	Portswigger				7	5
			3. Checkpoint Advanced web vul					
4,0	**Pentest - redteam**							
4,1	Redteam	MSSQL Server and Active Directory Certificate Services (ADCS)	Hackthebox.com	Đạt: Hoàn thành yêu cầu trong thời gian quy định Tốt: Hoàn thành yêu cầu sớm 30% thời gian XS: Hoàn thành yêu cầu sớm 50% thời gian Yêu cầu: Giải và trình bày wu challenge Escape trong Hackthebox	Bài được ghi nhận hoàn thành khi sinh viên báo cáo trực tiếp kết quả kèm theo write up	Bài được ghi nhận hoàn thành khi sinh viên báo cáo trực tiếp kết quả kèm theo write up	7	5
4,2		Webshell, backdoor, tunnel	Google	Đạt: Hoàn thành yêu cầu trong thời gian quy định Tốt: Hoàn thành yêu cầu sớm 30% thời gian XS: Hoàn thành yêu cầu sớm 50% thời gian Yêu cầu: theo phụ lục Redteam Webshell	Bài được ghi nhận hoàn thành khi sinh viên báo cáo trực tiếp kèm theo video và các kết quả theo yêu cầu	Bài được ghi nhận hoàn thành khi sinh viên báo cáo trực tiếp kết quả kèm theo write up	14	10
4,3	Mobile pentest	Dựng môi trường pentest một ứng dụng Android.	Google	Đạt: Hoàn thành yêu cầu trong thời gian quy định Tốt: Hoàn thành yêu cầu sớm 30% thời gian XS: Hoàn thành yêu cầu sớm 50% thời gian Yêu cầu: theo	Bài được ghi nhận hoàn thành khi sinh viên báo cáo trực tiếp kết quả kèm theo write up	Bài được ghi nhận hoàn thành khi sinh viên báo cáo trực tiếp kết quả kèm theo write up	7	7
		Checkpoint - Full pentest	**Google**	Đạt: làm theo checklist & cover 80% lỗ hổng của hệ thống Tốt: làm theo checklist & cover 90% lỗ hổng Xuất sắc: làm theo checklist & cover 100% lỗ hổng			**28**	**20**
			4. Checkpoint trước Onjob - Hoàn thành tất cả challenge - Điểm trung bình trên 7 - Đạt chứng chỉ Portswigger					
5,0	**On job training**			**Hoàn thành xong challenge web security, nhân sự có thể onjob tại các role sử dụng web security như sau:** - Pentest - Redteam - Purple team - Web security research (điểm trung bình trên 8, không có điểm học phần < 7) - Incident Response			**90**	**90**