Universitätsexperte

Fortgeschrittenes Web-Hacking

tech technologische universität

tech technologische universität

Universitätsexperte
Fortgeschrittenes Web-Hacking

- Modalität: **online**
- Dauer: **6 Monate**
- Qualifizierung: **TECH Global University**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: **www.techtitute.com/de/informatik/spezialisierung/spezialisierung-fortgeschrittenes-web-hacking**

Index

01

Präsentation

Im Zuge der digitalen Expansion nutzen Institutionen zunehmend Technologien, um sensible Daten zu speichern. Fortgeschrittenes *Hacking* wird so zu einer ernsten Bedrohung für die Institutionen. Wenn sich *Hacker* Zugang zu ihren Websites verschaffen, kann das schlimme Folgen haben, die von Identitätsdiebstahl bis hin zu Finanzbetrug und Erpressung reichen. Aus diesem Grund ist es für Unternehmen wichtig, Experten für fortschrittliche Sicherheitsmaßnahmen zu haben, die Maßnahmen wie *Firewalls* implementieren. Vor diesem Hintergrund startet TECH ein innovatives Programm für Studenten, um die effektivsten Techniken der Cybersicherheit zu erlernen. Darüber hinaus basiert es auf einem 100%igen Online-Modus, der Komfort und zeitliche Flexibilität garantiert.

Dank dieses Universitätsexperten werden Sie jedes Unternehmen in eine sichere Umgebung verwandeln, die frei von Cyberbedrohungen ist"

IT-Spezialisten sind ein wertvolles immaterielles Gut für die Unternehmen von heute. Einer der Hauptgründe dafür ist, dass ihre regelmäßigen Audits dazu beitragen, potenzielle Schwachstellen frühzeitig zu erkennen und zu beheben. Auf diese Weise kommen sie Verbrechen, die *Hacker* begehen könnten, zuvor und verwandeln virtuelle Umgebungen in sichere Zonen.

Auf diese Weise ist gewährleistet, dass die Nutzer sicher und frei in ihrem Netzwerk surfen und sowohl Waren als auch Dienstleistungen erwerben können. Angesichts der Zunahme dieser Praktiken stehen die Informatiker jedoch vor der Herausforderung, ihr Wissen ständig zu aktualisieren und die revolutionärsten Techniken zur Bekämpfung dieser Praktiken einzusetzen.

In diesem Zusammenhang hat TECH den umfassendsten Universitätsexperten in Fortgeschrittenes Web-Hacking auf dem akademischen Markt entwickelt. Durch dieses Programm werden die Studenten an der Spitze der Cybersicherheit stehen und über eine breite Palette von Taktiken zum Schutz vertraulicher Informationen verfügen. Darüber hinaus werden sie sich mit Strategien zur Ausnutzung raffinierter Schwachstellen befassen.

Zudem wird sich die Fachkraft auf die Implementierung effektiver Sicherheitsmaßnahmen, wie z. B. Systeme zur Erkennung von Eindringlingen, konzentrieren. Ein weiterer Schwerpunkt liegt auf dem *Switching*, um Geräte aus allen Bereichen des Unternehmens im selben Netzwerk miteinander zu verbinden. Der Kurs vermittelt auch die Grundlagen für das Verfassen von technischen Berichten und Executive Reports. In diesem Sinne werden die Möglichkeiten zur Offenlegung sensibler Daten erörtert, wobei der Schwerpunkt des Berichts auf den Kunden liegt. Schließlich werden verschiedene Methoden zur Messung der tatsächlichen operativen Sicherheit erkundet.

Um die Beherrschung der Inhalte zu festigen, wendet diese Fortbildung das innovative *Relearning*-System an, das die Assimilation komplexer Konzepte durch die natürliche und progressive Wiederholung derselben fördert. Außerdem verwendet das Programm Materialien in verschiedenen Formaten, wie z. B. Infografiken und Erklärungsvideos. All dies in einem bequemen 100%igen Online-Modus, der es jeder Person ermöglicht, ihren Zeitplan an ihre Aufgaben anzupassen.

Dieser **Universitätsexperte in Fortgeschrittenes Web-Hacking** enthält das vollständigste und aktuellste Programm auf dem Markt. Seine herausragendsten Merkmale sind:

- Die Entwicklung praktischer Fälle, die von Experten für fortgeschrittenes Web-Hacking vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren praktischen Informationen
- Die praktischen Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens durchgeführt werden kann
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Lektionen, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugriffs auf die Inhalte von jedem festen oder tragbaren Gerät mit Internetanschluss

> *Sie werden Passwörter entschlüsseln, die auf Computern gespeichert sind, und Hackerangriffe vorhersehen"*

Sie werden das OSI-Modell erforschen und die Kommunikationsprozesse in Netzwerksystemen verstehen" Und das in nur 6 Monaten!“

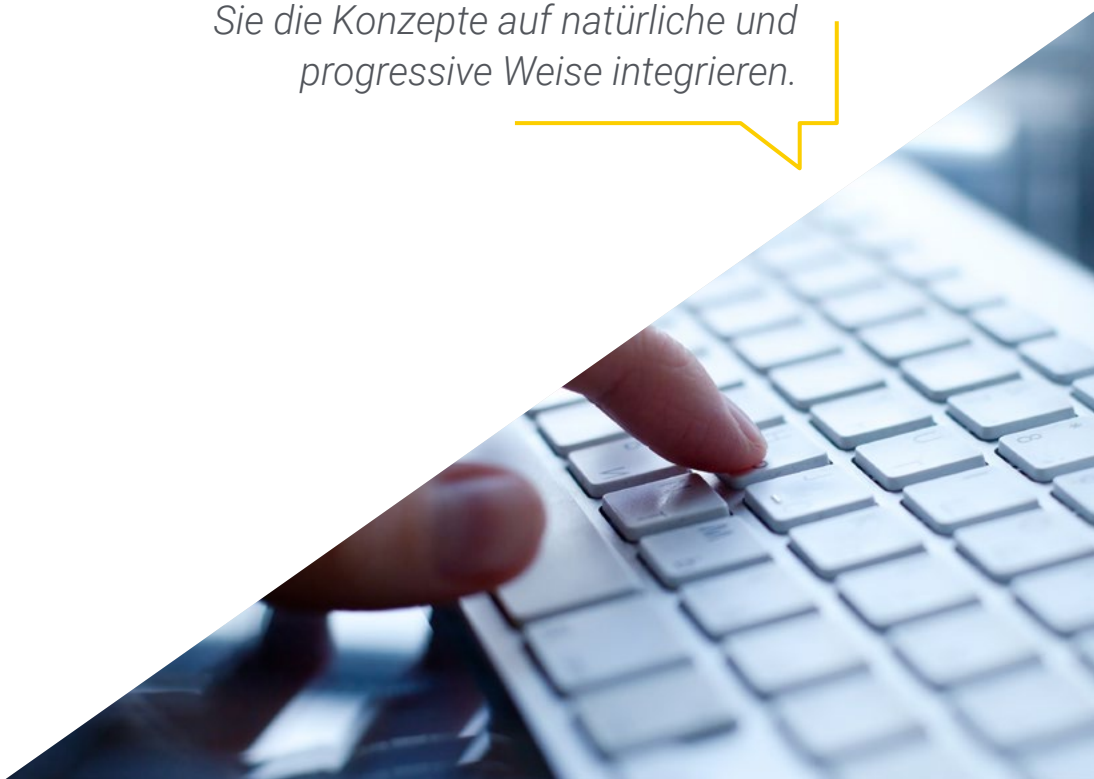
Vertiefen Sie Ihre Kenntnisse über DOM-Schwachstellen und verhindern Sie fortgeschrittene Angriffe mit den effektivsten Strategien.

Vergessen Sie das Auswendiglernen! Mit der Relearning-Methode werden Sie die Konzepte auf natürliche und progressive Weise integrieren.

Das Dozententeam des Programms besteht aus Experten des Sektors, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie aus renommierten Fachleuten von führenden Unternehmen und angesehenen Universitäten.

Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situiertes und kontextbezogenes Lernen ermöglichen, d. h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung von realen Situationen ausgerichtet ist.

Das Konzept dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.



02

Ziele

Dieser Lehrplan befasst sich mit fortgeschrittenen Hacking-Techniken, die auf Webdienste abzielen, und ermöglicht es Fachleuten, die effektivsten Strategien zu implementieren, bevor es zu Hacking-Angriffen kommt. Um dies zu erreichen, werden die grundlegenden Prinzipien des Netzwerkdesigns analysiert und gemeinsame Schwachstellen identifiziert. Auf diese Weise werden die Studenten die innovativsten Lösungen anbieten und sich in einem digitalen Sektor, der sprunghaft voranschreitet, hervorheben.

Wollen Sie das Netzwerk und die darin übertragenen Daten sichern? Meistern Sie das Switching an der laut Forbes besten digitalen Universität der Welt"

Allgemeine Ziele

- Erwerben fortgeschrittener Fähigkeiten in Penetrationstests und *Red-Team*-Simulationen, die sich mit der Identifizierung und Ausnutzung von Schwachstellen in Systemen und Netzwerken befassen
- Entwickeln von Führungsqualitäten, um auf offensive Cybersicherheit spezialisierte Teams zu koordinieren und die Durchführung von *Pentesting*- und *Red-Team*-Projekten zu optimieren
- Entwickeln von Fähigkeiten zur Analyse und Entwicklung von Malware, zum Verständnis ihrer Funktionsweise und zur Anwendung von Verteidigungs- und Aufklärungsstrategien
- Verbessern der Kommunikationsfähigkeiten durch die Erstellung von detaillierten technischen Berichten und Berichten für die Geschäftsleitung, wobei die Ergebnisse einem technischen Publikum und der Geschäftsleitung effektiv präsentiert werden
- Fördern der ethischen und verantwortungsbewussten Praxis im Bereich der Cybersicherheit, wobei ethische und rechtliche Grundsätze bei allen Aktivitäten berücksichtigt werden
- Aktualisieren der Studenten in Bezug auf neue Trends und Technologien im Bereich der Cybersicherheit

Sie werden die effektivsten Sicherheitsmaßnahmen anwenden und Schwachstellen vermeiden wie z. B. die Broken Authentication. Schreiben Sie sich jetzt ein!"

Spezifische Ziele

Modul 1. Fortgeschrittenes Web-Hacking

- Entwickeln von Fähigkeiten zur Identifizierung und Bewertung von Schwachstellen in Webanwendungen, einschließlich SQL-Injektionen, Cross-Site Scripting (XSS) und anderen gängigen Angriffsvektoren
- Lernen, wie man Sicherheitstests für moderne Webanwendungen durchführt
- Erwerben von Kompetenzen in fortgeschrittenen Web-Hacking-Techniken, wobei Strategien zur Umgehung von Sicherheitsmaßnahmen und zur Ausnutzung ausgeklügelter Schwachstellen erforscht werden
- Kennenlernen der Bewertung der Sicherheit von APIs und Webdiensten, Identifizierung potenzieller Schwachstellen und Stärkung der Sicherheit von Programmierschnittstellen
- Entwickeln von Fähigkeiten zur Implementierung effektiver Abhilfemaßnahmen in Webanwendungen, um die Anfälligkeit für Angriffe zu verringern und die Sicherheit zu erhöhen
- Teilnehmen an praktischen Simulationen, um die Sicherheit in komplexen Webumgebungen zu bewerten und das Wissen auf reale Szenarien anzuwenden
- Entwickeln von Kompetenzen bei der Formulierung effektiver Verteidigungsstrategien zum Schutz von Webanwendungen vor Cyberbedrohungen
- Lernen, fortgeschrittene Web-Hacking-Praktiken mit den relevanten Sicherheitsvorschriften und -standards in Einklang zu bringen, um die Einhaltung rechtlicher und ethischer Rahmenbedingungen zu gewährleisten
- Fördern einer effektiven Zusammenarbeit zwischen Entwicklungs- und Sicherheitsteams

Modul 2. Netzwerkarchitektur und -sicherheit

- Erwerben fortgeschrittener Kenntnisse der Netzwerkarchitektur, einschließlich Topologien, Protokollen und wichtigen Komponenten
- Entwickeln von Fähigkeiten zur Identifizierung und Bewertung spezifischer Schwachstellen in Netzwerkinfrastrukturen unter Berücksichtigung potenzieller Bedrohungen
- Lernen, wie man effektive Netzwerksicherheitsmaßnahmen implementiert, einschließlich Firewalls, *Intrusion Detection Systems* (IDS) und Netzwerksegmentierung
- Kennenlernen neuer Netzwerktechnologien wie *Software-defined Networking* (SDN) und Verstehen ihrer Auswirkungen auf die Sicherheit
- Entwickeln von Fähigkeiten zur Sicherung der Netzwerkkommunikation, einschließlich des Schutzes vor Bedrohungen wie *Sniffing* und *Man-in-the-Middle*-Angriffen
- Lernen, wie man Sicherheitskonfigurationen in Unternehmensnetzwerken bewertet und verbessert, um einen angemessenen Schutz zu gewährleisten
- Entwickeln von Fähigkeiten zur Implementierung effektiver Maßnahmen zur Abwehr von Bedrohungen in Unternehmensnetzwerken, von internen Angriffen bis hin zu externen Bedrohungen
- Fördern der effektiven Zusammenarbeit mit Sicherheitsteams, um Strategien und Bemühungen zum Schutz der Netzwerkinfrastruktur zu integrieren
- Fördern ethischer und rechtlicher Praktiken bei der Implementierung von Netzwerksicherheitsmaßnahmen und gewährleisten die Einhaltung ethischer Grundsätze bei allen Aktivitäten

Modul 3. Technischer Bericht und Executive Report

- Entwickeln von Fähigkeiten zur Erstellung detaillierter technischer Berichte, in denen Ergebnisse, verwendete Methoden und Empfehlungen klar und umfassend dargestellt werden
- Lernen, effektiv mit technischen Zielgruppen zu kommunizieren und dabei eine präzise und angemessene Sprache zu verwenden, um komplexe technische Informationen zu vermitteln
- Entwickeln von Fähigkeiten, um umsetzbare und praktische Empfehlungen zu formulieren, die darauf abzielen, Schwachstellen zu entschärfen und die Sicherheitslage zu verbessern
- Lernen, die potenziellen Auswirkungen identifizierter Schwachstellen unter Berücksichtigung technischer, betrieblicher und strategischer Aspekte zu bewerten
- Kennenlernen der Best Practices für die Berichterstattung an Führungskräfte, um technische Informationen für ein nicht technisches Publikum aufzubereiten
- Entwickeln von Kompetenzen, um Ergebnisse und Empfehlungen mit den strategischen und operativen Zielen des Unternehmens in Einklang zu bringen
- Lernen, wie man Datenvisualisierungstools verwendet, um die in Berichten enthaltenen Informationen grafisch darzustellen und so das Verständnis zu erleichtern
- Fördern der Aufnahme relevanter Informationen über die Einhaltung von Vorschriften und Standards in Berichte, um die Einhaltung rechtlicher Anforderungen zu gewährleisten
- Fördern der effektiven Zusammenarbeit zwischen technischen und leitenden Teams, um Verständnis und Unterstützung für die im Bericht vorgeschlagenen Verbesserungsmaßnahmen sicherzustellen

03

Kursleitung

Mit dem Ziel, eine exzellente Fortbildung zu bieten, hat TECH ein Dozententeam zusammengestellt, das über einen breiten beruflichen Hintergrund im Bereich der Cybersicherheit verfügt. Mit mehr als 13 Jahren Erfahrung bieten diese Spezialisten den umfassendsten Ansatz und die neuesten Tools zur Entwicklung sicherer virtueller Umgebungen. Auf diese Weise erhalten die Studenten die Garantien, die sie brauchen, um sich in einem digitalen Sektor zu spezialisieren, der zahlreiche Möglichkeiten bietet.

Sie werden die Grenzen von Pentester mit der Unterstützung der besten Lehrkräfte erkunden. Ihre Aktivitäten werden zu 100% gesetzlich abgesichert sein!“

Leitung

Hr. Gómez Pintado, Carlos

- Manager für Cybersicherheit und Red Team Cipherbit bei Grupo Oesía
- Geschäftsführender *Advisor & Investor* bei Wesson App
- Hochschulabschluss in Software Engineering und Technologien der Informationsgesellschaft an der Polytechnischen Universität von Madrid
- Zusammenarbeit mit Bildungseinrichtungen bei der Entwicklung von höherstufigen Ausbildungszyklen im Bereich Cybersicherheit

Professoren

Hr. Siles Rubia, Marcelino

- Cibersecurity Engineer
- Ingenieur für Cybersicherheit von der Universität Rey Juan Carlos
- Kenntnisse: Wettbewerbsorientierte Programmierung, *Web-Hacking*, *Active Directory* und *Malware Development*
- Gewinner des AdaByron-Wettbewerbs

Hr. Redondo Castro, Pablo

- Pentester bei Grupo Oesía
- Ingenieur für Cybersicherheit von der Universität Rey Juan Carlos
- Umfangreiche Erfahrung als *Cybersecurity Evaluator Trainee*
- Er sammelt Lehrerfahrung, indem er Fortbildungen im Zusammenhang mit Capture The Flag-Turnieren gibt

04

Struktur und Inhalt

Dieses Programm umfasst 3 umfassende Module: Fortgeschrittenes Web-Hacking, Netzwerkarchitektur und -sicherheit sowie Technischer Bericht und Executive Reporting. Mit der Unterstützung erfahrener Dozenten werden fortgeschrittene Taktiken zur Sicherung von Unternehmensnetzwerken durch die Implementierung von *Firewalls* behandelt. Die Erkennung von Eindringlingen, einschließlich HHTP *Request Smuggling*, wird ebenfalls behandelt. Darüber hinaus wird die Bedeutung von VLANs für die Trennung des Datenverkehrs in derselben virtuellen Umgebung erörtert und der Berichterstattungsprozess für eine genaue und detaillierte Berichterstattung erforscht.

Sie werden Zugang zu einem Lernsystem haben, das auf Wiederholung basiert, mit natürlichem und progressivem Unterricht während des gesamten Lehrplans"

Modul 1. Fortgeschrittenes Web-Hacking

1.1. Wie eine Website funktioniert
- 1.1.1. Die URL und ihre Bestandteile
- 1.1.2. HTTP-Methoden
- 1.1.3. Die Kopfzeilen
- 1.1.4. Wie man Webanfragen mit Burp Suite betrachtet

1.2. Sitzungen
- 1.2.1. Die *Cookies*
- 1.2.2. *Tokens* JWT
- 1.2.3. *Session-Hijacking*-Angriffe
- 1.2.4. JWT-Angriffe

1.3. *Cross Site Scripting* (XSS)
- 1.3.1. Was ist ein XSS
- 1.3.2. Arten von XSS
- 1.3.3. Ausnutzen eines XSS
- 1.3.4. Einführung in *XSLeaks*

1.4. Datenbank-Injektionen
- 1.4.1. Was ist eine *SQL-Injection*?
- 1.4.2. Exfiltrieren von Informationen mit *SQLi*
- 1.4.3. *SQLi Blind, Time-Based* und *Error-Based*
- 1.4.4. NoSQLi-Injektionen

1.5. *Path Traversal* und *Local File Inclusion*
- 1.5.1. Was sie sind und ihre Unterschiede
- 1.5.2. Übliche Filter und wie man sie umgeht
- 1.5.3. *Log Poisoning*
- 1.5.4. LFIs in PHP

1.6. *Broken Authentication*
- 1.6.1. *User Enumeration*
- 1.6.2. *Password Bruteforce*
- 1.6.3. *2FA Bypass*
- 1.6.4. *Cookies* mit sensiblen und änderbaren Informationen

1.7. *Remote Command Execution*
- 1.7.1. *Command Injection*
- 1.7.2. *Blind Command Injection*
- 1.7.3. *Insecure Deserialization* PHP
- 1.7.4. *Insecure Deserialization* Java

1.8. *File Uploads*
- 1.8.1. CERs über *Webshells*
- 1.8.2. XSS in Dateiuploads
- 1.8.3. XML *External Entity* (XXE) *Injection*
- 1.8.4. *Path Traversal* bei Dateiuploads

1.9. *Broken Acess Control*
- 1.9.1. Uneingeschränkter Zugang zu den Panels
- 1.9.2. *Insecure Direct Object References* (IDOR)
- 1.9.3. Filter-*Bypass*
- 1.9.4. Unzureichende Autorisierungsmethoden

1.10. DOM-Schwachstellen und weitergehende Angriffe
- 1.10.1. *Regex Denial of Service*
- 1.10.2. DOM *Clobbering*
- 1.10.3. *Prototype Pollution*
- 1.10.4. HTTP *Request Smuggling*

Modul 2. Netzwerkarchitektur und -sicherheit

2.1. Computer-Netzwerke
- 2.1.1. Grundlegende Konzepte: LAN, WAN, CP, CC-Protokolle
- 2.1.2. OSI-Modell und TCP/IP
- 2.1.3. *Switching:* Grundlegende Konzepte
- 2.1.4. *Routing:* Grundlegende Konzepte

2.2. *Switching*
- 2.2.1. Einführung in VLANs
- 2.2.2. STP
- 2.2.3. *EtherChannel*
- 2.2.4. Angriffe auf Schicht 2

2.3. VLAN´s
- 2.3.1. Bedeutung von VLANs
- 2.3.2. Schwachstellen in VLANs
- 2.3.3. Häufige Angriffe auf VLANs
- 2.3.4. Abhilfemaßnahmen

2.4. *Routing*
- 2.4.1. IP-Adressierung - IPv4 und IPv6
- 2.4.2. Routing: Wichtige Konzepte
- 2.4.3. Statisches Routing
- 2.4.4. Dynamisches Routing: Einführung

2.5. IGP-Protokolle
- 2.5.1. RIP
- 2.5.2. OSPF
- 2.5.3. RIP vs OSPF
- 2.5.4. Analyse des Topologiebedarfs

2.6. Perimeter-Schutz
- 2.6.1. DMZs
- 2.6.2. *Firewalls*
- 2.6.3. Gemeinsame Architekturen
- 2.6.4. Zero Trust Network Access

2.7. IDS und IPS
- 2.7.1. Merkmale
- 2.7.2. Implementierung
- 2.7.3. SIEM und SIEM CLOUDS
- 2.7.4. Auf *HoneyPots* basierende Erkennung

2.8. TLS und VPNs
- 2.8.1. SSL/TLS
- 2.8.2. TLS: Häufige Angriffe
- 2.8.3. VPNs mit TLS
- 2.8.4. VPNs mit IPSEC

2.9. Sicherheit für drahtlose Netzwerke
- 2.9.1. Einführung in drahtlose Netzwerke
- 2.9.2. Protokolle
- 2.9.3. Wichtige Elemente
- 2.9.4. Häufige Angriffe

2.10. Unternehmensnetzwerke und der Umgang mit ihnen
- 2.10.1. Logische Segmentierung
- 2.10.2. Physische Segmentierung
- 2.10.3. Zugangskontrolle
- 2.10.4. Andere zu berücksichtigende Maßnahmen

Modul 3. Technischer Bericht und Executive Report

3.1. Prozess der Berichterstattung
- 3.1.1. Aufbau eines Berichts
- 3.1.2. Prozess der Berichterstattung
- 3.1.3. Wichtige Konzepte
- 3.1.4. Executive vs. technisch

3.2. Leitfäden
- 3.2.1. Einführung
- 3.2.2. Arten von Leitfäden
- 3.2.3. Nationale Leitfäden
- 3.2.4. Anwendungsbeispiele

3.3. Methoden
- 3.3.1. Bewertung
- 3.3.2. *Pentesting*
- 3.3.3. Überprüfung der gemeinsamen Methoden
- 3.3.4. Einführung in nationale Methodologien

3.4. Technischer Ansatz für die Berichtsphase
- 3.4.1. Die Grenzen von *Pentester* verstehen
- 3.4.2. Sprachgebrauch und Stichwörter
- 3.4.3. Präsentation von Informationen
- 3.4.4. Häufige Fehler

3.5. Executive-Ansatz für die Berichtsphase
- 3.5.1. Anpassen des Berichts an den Kontext
- 3.5.2. Sprachgebrauch und Stichwörter
- 3.5.3. Standardisierung
- 3.5.4. Häufige Fehler

3.6. OSSTMM
- 3.6.1. Verstehen der Methodik
- 3.6.2. Anerkennung
- 3.6.3. Dokumentation
- 3.6.4. Erstellen des Berichts

3.7. LINCE
- 3.7.1. Verstehen der Methodik
- 3.7.2. Anerkennung
- 3.7.3. Dokumentation
- 3.7.4. Erstellen des Berichts

3.8. Meldung von Schwachstellen
- 3.8.1. Wichtige Konzepte
- 3.8.2. Quantifizierung des Umfangs
- 3.8.3. Schwachstellen und Beweise
- 3.8.4. Häufige Fehler

3.9. Fokussierung des Berichts an den Kunden
- 3.9.1. Bedeutung von Arbeitstests
- 3.9.2. Lösungen und Abhilfemaßnahmen
- 3.9.3. Sensible und relevante Daten
- 3.9.4. Praktische Beispiele und Fälle

3.10. Berichterstattung über *Retakes*
- 3.10.1. Wichtige Konzepte
- 3.10.2. Verstehen von Altdaten
- 3.10.3. Fehlerprüfung
- 3.10.4. Hinzufügen von Informationen

05

Methodik

Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: ***das Relearning***.
Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem ***New England Journal of Medicine*** als eines der effektivsten angesehen.

Entdecken Sie Relearning, ein System, das das herkömmliche lineare Lernen hinter sich lässt und Sie durch zyklische Lehrsysteme führt: eine Art des Lernens, die sich als äußerst effektiv erwiesen hat, insbesondere in Fächern, die Auswendiglernen erfordern"

Fallstudie zur Kontextualisierung aller Inhalte

Unser Programm bietet eine revolutionäre Methode zur Entwicklung von Fähigkeiten und Kenntnissen. Unser Ziel ist es, Kompetenzen in einem sich wandelnden, wettbewerbsorientierten und sehr anspruchsvollen Umfeld zu stärken.

Mit TECH werden Sie eine Art des Lernens erleben, die an den Grundlagen der traditionellen Universitäten auf der ganzen Welt rüttelt"

Sie werden Zugang zu einem Lernsystem haben, das auf Wiederholung basiert, mit natürlichem und progressivem Unterricht während des gesamten Lehrplans.

Der Student wird durch gemeinschaftliche Aktivitäten und reale Fälle lernen, wie man komplexe Situationen in realen Geschäftsumgebungen löst.

Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist ein von Grund auf neu entwickeltes, intensives Lehrprogramm, das die anspruchsvollsten Herausforderungen und Entscheidungen in diesem Bereich sowohl auf nationaler als auch auf internationaler Ebene vorsieht. Dank dieser Methodik wird das persönliche und berufliche Wachstum gefördert und ein entscheidender Schritt in Richtung Erfolg gemacht. Die Fallmethode, die Technik, die diesem Inhalt zugrunde liegt, gewährleistet, dass die aktuellste wirtschaftliche, soziale und berufliche Realität berücksichtigt wird.

> *Unser Programm bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein"*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Informatikschulen der Welt, seit es sie gibt. Die Fallmethode wurde 1912 entwickelt, damit Jurastudenten das Recht nicht nur auf der Grundlage theoretischer Inhalte erlernen. Sie bestand darin, ihnen reale komplexe Situationen zu präsentieren, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen konnten, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard etabliert.

Was sollte eine Fachkraft in einer bestimmten Situation tun? Mit dieser Frage konfrontieren wir Sie in der Fallmethode, einer handlungsorientierten Lernmethode. Während des gesamten Kurses werden die Studenten mit mehreren realen Fällen konfrontiert. Sie müssen ihr gesamtes Wissen integrieren, recherchieren, argumentieren und ihre Ideen und Entscheidungen verteidigen.

Relearning Methodology

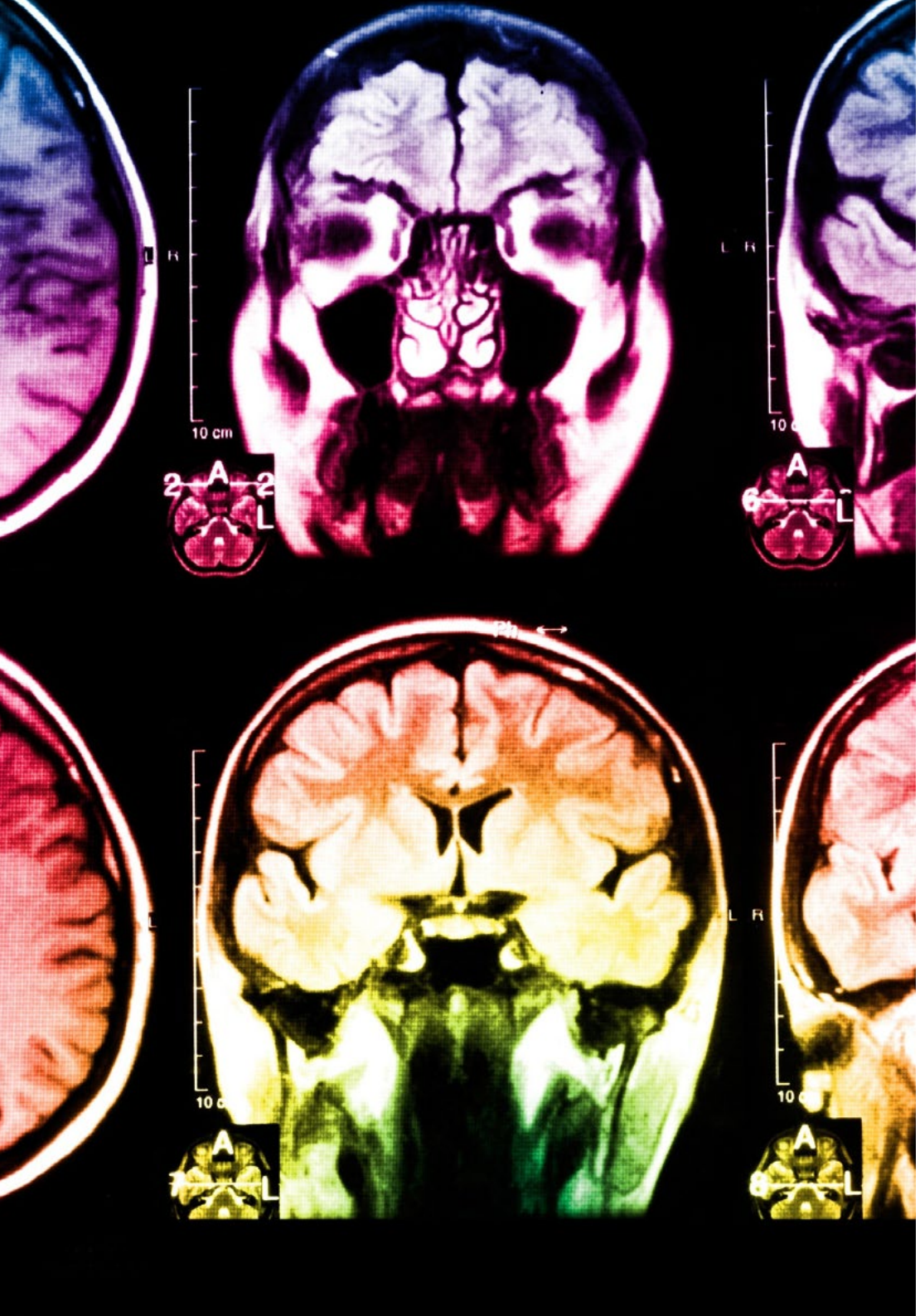
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

Wir ergänzen die Fallstudie mit der besten 100%igen Online-Lehrmethode: Relearning.

Im Jahr 2019 erzielten wir die besten Lernergebnisse aller spanischsprachigen Online-Universitäten der Welt.

Bei TECH lernen Sie mit einer hochmodernen Methodik, die darauf ausgerichtet ist, die Führungskräfte der Zukunft zu spezialisieren. Diese Methode, die an der Spitze der weltweiten Pädagogik steht, wird Relearning genannt.

Unsere Universität ist die einzige in der spanischsprachigen Welt, die für die Anwendung dieser erfolgreichen Methode zugelassen ist. Im Jahr 2019 ist es uns gelungen, die Gesamtzufriedenheit unserer Studenten (Qualität der Lehre, Qualität der Materialien, Kursstruktur, Ziele...) in Bezug auf die Indikatoren der besten spanischsprachigen Online-Universität zu verbessern.



In unserem Programm ist das Lernen kein linearer Prozess, sondern erfolgt in einer Spirale (lernen, verlernen, vergessen und neu lernen). Daher wird jedes dieser Elemente konzentrisch kombiniert. Mit dieser Methode wurden mehr als 650.000 Hochschulabsolventen mit beispiellosem Erfolg in so unterschiedlichen Bereichen wie Biochemie, Genetik, Chirurgie, internationales Recht, Managementfähigkeiten, Sportwissenschaft, Philosophie, Recht, Ingenieurwesen, Journalismus, Geschichte, Finanzmärkte und -instrumente fortgebildet. Dies alles in einem sehr anspruchsvollen Umfeld mit einer Studentenschaft mit hohem sozioökonomischem Profil und einem Durchschnittsalter von 43,5 Jahren.

Das Relearning ermöglicht es Ihnen, mit weniger Aufwand und mehr Leistung zu lernen, sich mehr auf Ihre Spezialisierung einzulassen, einen kritischen Geist zu entwickeln, Argumente zu verteidigen und Meinungen zu kontrastieren: eine direkte Gleichung zum Erfolg.

Nach den neuesten wissenschaftlichen Erkenntnissen der Neurowissenschaften wissen wir nicht nur, wie wir Informationen, Ideen, Bilder und Erinnerungen organisieren, sondern auch, dass der Ort und der Kontext, in dem wir etwas gelernt haben, von grundlegender Bedeutung dafür sind, dass wir uns daran erinnern und es im Hippocampus speichern können, um es in unserem Langzeitgedächtnis zu behalten.

Auf diese Weise sind die verschiedenen Elemente unseres Programms im Rahmen des so genannten Neurocognitive Context-Dependent E-Learning mit dem Kontext verbunden, in dem der Teilnehmer seine berufliche Praxis entwickelt.

Dieses Programm bietet die besten Lehrmaterialien, die sorgfältig für Fachleute aufbereitet sind:

Studienmaterial

Alle didaktischen Inhalte werden von den Fachleuten, die den Kurs unterrichten werden, speziell für den Kurs erstellt, so dass die didaktische Entwicklung wirklich spezifisch und konkret ist.

Diese Inhalte werden dann auf das audiovisuelle Format angewendet, um die Online-Arbeitsmethode von TECH zu schaffen. All dies mit den neuesten Techniken, die in jedem einzelnen der Materialien, die dem Studenten zur Verfügung gestellt werden, qualitativ hochwertige Elemente bieten.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

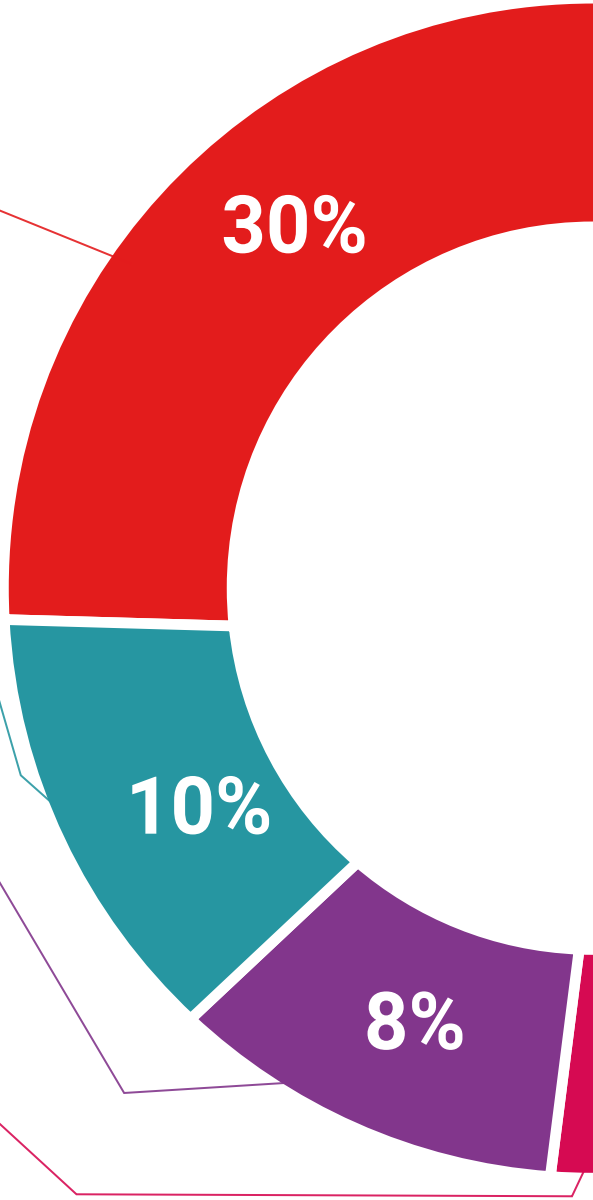
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

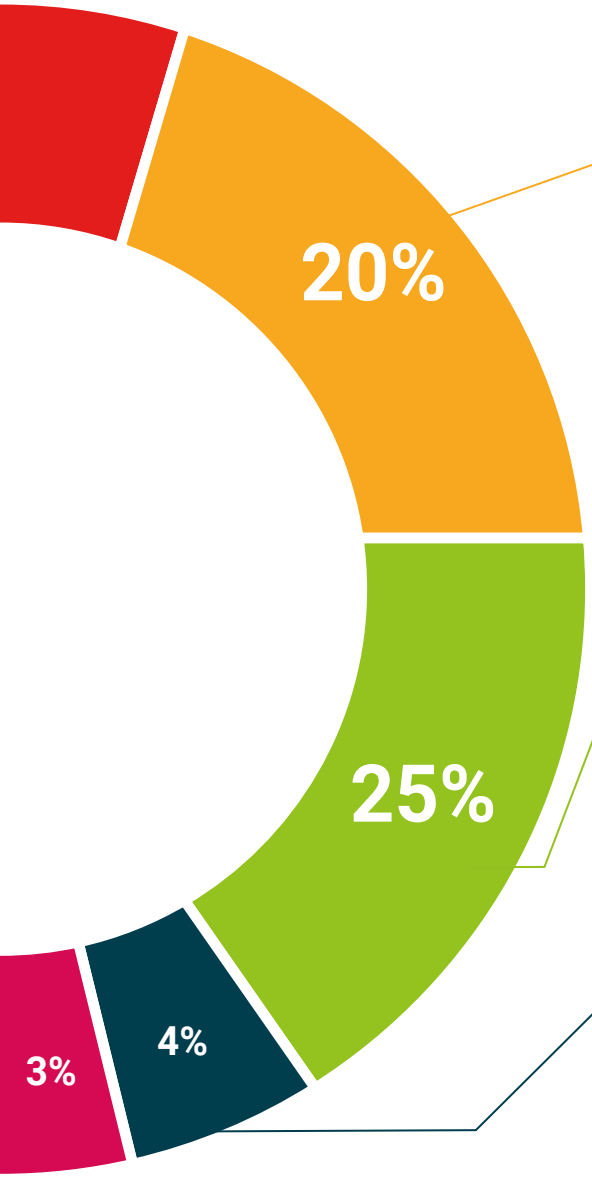
Übungen für Fertigkeiten und Kompetenzen

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein Spezialist im Rahmen der Globalisierung, in der wir leben, entwickeln muss.

Weitere Lektüren

Aktuelle Artikel, Konsensdokumente und internationale Leitfäden, u. a. In der virtuellen Bibliothek von TECH hat der Student Zugang zu allem, was er für seine Fortbildung benötigt.





Case Studies

Sie werden eine Auswahl der besten Fallstudien vervollständigen, die speziell für diese Qualifizierung ausgewählt wurden. Die Fälle werden von den besten Spezialisten der internationalen Szene präsentiert, analysiert und betreut.

Interaktive Zusammenfassungen

Das TECH-Team präsentiert die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, die Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu vertiefen.

Dieses einzigartige Bildungssystem für die Präsentation multimedialer Inhalte wurde von Microsoft als "Europäische Erfolgsgeschichte" ausgezeichnet.

Testing & Retesting

Die Kenntnisse des Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass der Student überprüfen kann, wie er seine Ziele erreicht.

06

Qualifizierung

Der Universitätskurs in Fortgeschrittenes Web-Hacking garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Technologischen Universität ausgestellten Diplom.

Schließen Sie dieses Programm erfolgreich ab und erhalten Sie Ihren Universitätsabschluss ohne lästige Reisen oder Formalitäten"

Dieser **Universitätskurs in Fortgeschrittenes Web-Hacking** enthält das vollständigste und aktuellste Programm auf dem Markt.

Sobald der Student die Prüfungen bestanden hat, erhält er/sie per Post* mit Empfangsbestätigung das entsprechende Diplom, ausgestellt von der **TECH Technologischen Universität.**

Das von **TECH Technologische Universität** ausgestellte Diplom drückt die erworbene Qualifikation aus und entspricht den Anforderungen, die in der Regel von Stellenbörsen, Auswahlprüfungen und Berufsbildungsausschüssen verlangt werden.

Título: **Universitätsexperte in Fortgeschrittenes Web-Hacking**

Modalität: **online**

Dauer: **6 Monate**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

UNIVERSITÄTSKURS

in

Fortgeschrittene Red-Team-Übungen

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 150 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

TECH ist eine private Hochschuleinrichtung, die seit dem 28. Juni 2018 vom Ministerium für öffentliche Bildung anerkannt ist.

Zum 17. Juni 2020

Tere Guevara Navarro
Rektorin

einzigartiger Code TECH: AFWOR23S techtitute.com/titel

*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH EDUCATION die notwendigen Vorkehrungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

tech technologische universität

Universitätsexperte

Fortgeschrittenes Web-Hacking

- Modalität: **online**
- Dauer: **6 Monate**
- Qualifizierung: **TECH Global University**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Universitätsexperte
Fortgeschrittenes Web-Hacking

tech technologische universität