Backlogの未来を見据えた、ヌーラボ社の選択。

CASE STUDY
お客様成功事例

nulab
株式会社ヌーラボ
情報統括部 品質保証課
セキュリティエンジニア
松山 保 様

EG Secure Solutions
EG セキュアソリューションズ株式会社
取締役 CTO
イー・ガーディアングループ CISO
徳丸 浩

セキュアコーディング対応強化に向けて EGセキュアソリューションズのeラーニングサービスを採用。

Backlog（バックログ）は、ガントチャートやカンバンボードで進捗状況を可視化できるプロジェクト管理ツール。有料契約数128万人超の、プロジェクト管理ツール分野の国内 TOP ランナーです。そんな Backlog の開発企業が、株式会社ヌーラボ様。今回、同社情報統括部 セキュリティエンジニアの松山様と、EG セキュアソリューションズ社 CTO 徳丸の貴重な対談をお届けします。

海外ユーザも急増中の Backlog だからこそエンジニア教育をさらに重視

〈司会〉松山さん、最近のヌーラボさんは、「BEST SOFTWARE AWARD 2024 の TOP50」や「G2's 2024 Spring Awards」、また「SaaSworthy」へのランクインなど、海外での受賞が目立ちますね。おめでとうございます。

〈松山〉ありがとうございます。Backlog をはじめとしたヌーラボサービスは英語でも展開しているため、海外での利用事例も増えてきました。言語の壁を越えて評価してもらえて嬉しいです。

〈司会〉今後、海外のユーザ数もさらに増加しますね。それにともなって、セキュリティ対策も今後ますます重要になるのではないでしょうか。

〈松山〉はい。ここまで成長した Backlog にとって、セキュアであることは大前提です。全てのお客様に安心してご利用いただけるソフトウェアでなければいけません。

〈司会〉そのようなお考えのもとで、開発エンジニアに対して様々な教育コンテンツを随時ご提供されているわけですね。

〈松山〉はい。エンジニアが学びたい時、いつでもどこからでも学べるように様々な e- ラーニングコンテンツを提供しています。それと、講師の方をお招きして行う集合研修を実施しています。徳丸さんにも、2022年に社内のエンジニアに向けて実践的な研修を行っていただきました。

米国最大級のソフトウェアレビューサイトで、プロジェクトマネジメント部門 TOP50 にランクインした Backlog

© EG Secure Solutions Inc.

Backlogの未来を見据えた、ヌーラボ社の選択。

CASE STUDY　お客様成功事例

はじまりは2021年、X のポストから

〈司会〉徳丸さんとヌーラボさんのお付き合いは、2021 年からですね。

〈徳丸〉私が、X（旧 Twitter）でポストさせていただいたことでスタートしました。当時 Web 上に、クリックジャッキング対策を解説したページが多数存在していました。しかし、実は検索して上位表示されているにも関わらず、解説内容に疑問を感じるページもありました。
そんな中、ヌーラボさんが公開されていた、クリックジャッキング対策のページは正しく解説されていました。

〈松山〉ありがとうございます。記事を取り上げていただきとても嬉しいです。

〈徳丸〉こうした有益性の高いページを、もっと多くの Web システム開発者に見てほしくてポストさせていただきました。

〈松山〉あのポストが社内で話題となりまして。徳丸さんに、ぜひ Web セキュリティをテーマに集合研修をお願いしようとなりました。貴重な研修をありがとうございました。

ヌーラボ社のクリックジャッキング攻撃対策解説ページ

2021年6月
徳丸 CTOのポスト

EG セキュアソリューションズ CTO 徳丸が全面監修した、Security Campus e-Learning

〈司会〉そして今回、集合研修に続いて EG セキュアソリューションズの「Security Campus e-Learning」も採用していただいたわけですが、採用理由として、徳丸 CTO が全編監修しているという部分は大きかったでしょうか。

〈松山〉もちろんです。ヌーラボとして、セキュアコーディング強化につながる教育施策を、さらに強化したいと考えていました。開発エンジニアのセキュリティレベルを、さらに一段階上げたいと考えています。そのためにも、セキュアコーディングを強化する研修が必要でした。徳丸さんが監修されたコンテンツを、ぜひ活用させていただきたいと考えました。

〈徳丸〉ありがとうございます。Security Campus e-Learning は、これから Web システム開発に取り組むエンジニアのみなさんに向けて「今、ちゃんと理解していただきたい Web セキュリティ」にフォーカスして構成しました。
徳丸本 * の初版から 、10 年以上経過していますし。ゼロベースで見直して、今開発に取り組んでいるエンジニアのみなさんに有用性の高い学習コンテンツをご提供する必要があると感じていました。

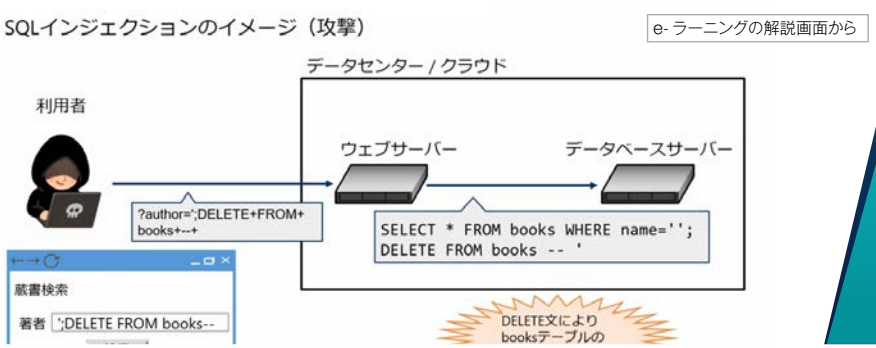
〈松山〉実際に受講したエンジニアたちのアンケートを振り返ってみると、「それぞれの動画がコンパクトにまとまっていて見やすかった」という感想が多くみられました。

〈徳丸〉そこは特に重視しました。どうすれば、忙しい Web システム開発に携わるエンジニアのみなさんがつねに関心度を持って視聴できるか重点的に考えました。短い時間で、しっかりと現在取り組むべきポイントを効率的に学ぶことができるコンテンツを目指しました。

* 徳丸本

2011年3月に刊行された「体系的に学ぶ 安全な Web アプリケーションの作り方」の別称。Web 開発の指南書として、異例のベストセラーを記録。2018年に改訂版として第2版が刊行されました。著者である徳丸の名前にちなんで、徳丸本（とくまるぼん）と呼ばれています。

© EG Secure Solutions Inc.



Backlogの未来を見据えた、ヌーラボ社の選択。

CASE STUDY お客様成功事例

今、取り組むべき脆弱性対策を重視した編成

〈司会〉お伺いしたいのですが、今回受講させていただいたウェブセキュリティエッセンシャルコースの中で SQL インジェクション攻撃が解説されていました。
SQL インジェクション攻撃にフォーカスしている理由を改めて教えてください。きっと徳丸さんならではの理由があるのではないでしょうか?

〈徳丸〉ここ2年位でしょうか、弊社の脆弱性診断サービスで、SQL インジェクションが検出されています。検出数が、明らかに増加傾向にあります。
私が危惧しているのは、実は水面下で Web セキュリティが退化している可能性があるのではないかという点です。Web エンジニアのみなさんに、ここで改めて SQL インジェクションの脆弱性と攻撃者の視点を学習してほしかった、というのが最大の理由ですね。

〈松山〉脆弱性診断サービスの結果を踏まえて、動画コンテンツの中で取り上げるテーマを精査し直したということですか?

〈徳丸〉はい。脆弱性診断や最近の事故・事件を踏まえて、3 時間の動画で説明する項目をゼロベースで見直しました。そうすると、ディレクトリトラバーサル等は有名ではあるが近年はあまり重要ではないとか、パスワードの安全な保存法は短いコンテンツでも説明しなければならないという結論になりました。

〈松山〉受講したエンジニアのアンケートには、徳丸さんが監修された e ラーニングコンテンツを見て、「新たな気づきがあった」という感想もありました。

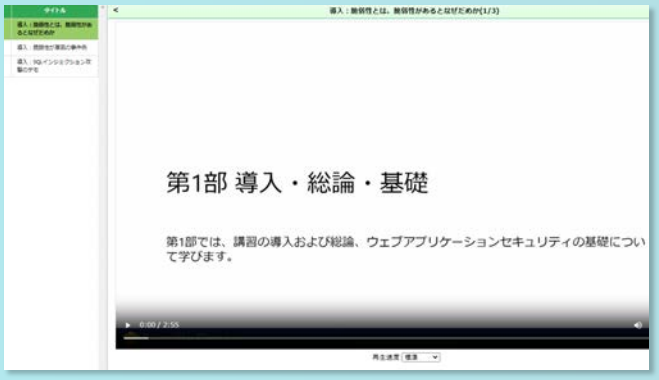
〈徳丸〉そこも大きな狙いです。例えば、すでに有名な脆弱性なので、自分は SQL インジェクション攻撃を理解していると認識している方も多いでしょう。
しかし、今回の Security Campus e-Learning という e ラーニングコンテンツを通して、改めて学習していただくことで、新たな気づきを得てほしいと思っています。こうした気づきの積み重ねがエンジニアの意識を向上させ、最終的に Web サービスのセキュリティ向上につながると思うのです。

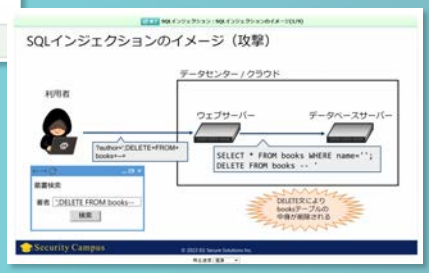
第1部：コンテンツ構成

第2部：コンテンツ構成

第3部：コンテンツ構成

Web アプリケーションセキュリティに関する、徳丸 CTO の最新解説を学習可能





SQLインジェクション放置の危険性

PHP のフレームワークが起因となった SQL インジェクションを紹介。攻撃者に「踏み台」として悪用されてしまった実例を交えながら、改めて SQL インジェクション放置の危険性を分かりやすく解説しています。

© EG Secure Solutions Inc.

Backlogの未来を見据えた、ヌーラボ社の選択。

CASE STUDY お客様成功事例

攻撃による影響範囲を理解することの大切さ

〈松山〉その他にも「攻撃者目線のアクションを解説した動画で、理解が深まった」という感想もありました。受講者の意識向上を感じることができました。

〈徳丸〉はい。一般的な脆弱性の説明ではリアリティのない説明が多いので、技術力のある方ほど「本当に危険なのか」と思ってしまいます。そこで、脆弱性の悪用で攻撃者が実際にどのような行動をとるのか、動画で解説しています。セキュアコーディングを推進する上で、まず攻撃による影響範囲の大きさを理解することは、とても重要なのです。Security Campus e-Learning は、エンジニアはもちろんなのですが、営業の方やマーケティングの方、品質管理の方でも十分理解できるように分かりやすく解説しています。より多くのみなさんに学んでいただけるコンテンツを目指して作成しました。

攻撃者目線で XSS 攻撃の実例を解説

入力フォームにスクリプト付のリンクを含む内容を入力して Web システムに罠を仕掛け、外部の不審なサイトへ誘導。その後、不審なスクリプトが実行され、最終的に個人情報が流出してしまう、それら一連の動きを、実際に画面操作を通して解説します。受講者は、XSS 攻撃の実態をリアルに学ぶことができます。

一つのサイバー攻撃に関して、EG セキュアソリューションズの Security Campus e-Learning では、以下のようなコンテンツ体系イメージで編成されています。

- XSS 攻撃解説
  - XSS 攻撃とは
  - XSS 攻撃のデモ
  - XSS 攻撃の影響範囲
  - XSS 対策方法
  - XSS 攻撃保険的対策

なぜ、「エッセンシャルコース」なのか

〈徳丸〉今回、e ラーニングコンテンツで解説している全ての脆弱性対策に関して、私自身の従来の解説をゼロベースで見直して、再構成しました。

〈司会〉なるほど。徳丸さんの解説が全て刷新されているわけですね。

〈松山〉Web システム開発者にとって、脆弱性対応は永遠の課題ですから。徳丸さんの最新解説を通して学習することは、ヌーラボが考える、セキュリティマネジメントの体制強化の面でもとても有効だと思います。

〈徳丸〉ありがとうございます。コンテンツを編成するにあたって、「何を入れないか」にもこだわりました。厳選した内容となっています。Web システム開発者にとって、いずれも必要不可欠なテーマ、ポイントです。だからこそ、エッセンシャルコースと命名しました。

チャプター最後のテストにも徳丸のこだわり

〈松山〉私も視聴して、実はチャプター最後のテストにも、他社の e ラーニングとの違いを感じました。他の受講者からも「このテストに徳丸さんらしさを感じた」という感想がありました。チャプター最後のテストの狙いを教えてください。

〈徳丸〉単に、正解／不正解の判定だけではありません。もし受講者がテストで間違った場合に、なぜ間違っているのかをしっかり補足説明しています。

私は、間違った時にこそ「気づき」が生まれるチャンスだと思うのです。

© EG Secure Solutions Inc.

クロスサイトスクリプティングのイメージ（攻撃）

e- ラーニングの解説画面から

Backlogの未来を見据えた、ヌーラボ社の選択。

CASE STUDY お客様成功事例

そのタイミングでしっかりフォローして、エンジニアの意識向上を促すことを目指しています。

〈松山〉受講したスタッフの中には、2 回、3 回と繰り返し見ているスタッフも大勢います。

〈徳丸〉ありがとうございます。みなさんが何回でも視聴できるように、e- ラーニングコンテンツというコンテンツタイプを選択しました。2 回、3 回と見ていくと、きっと新たな気づきがあります。何回でも、繰り返し見てほしいと思います。

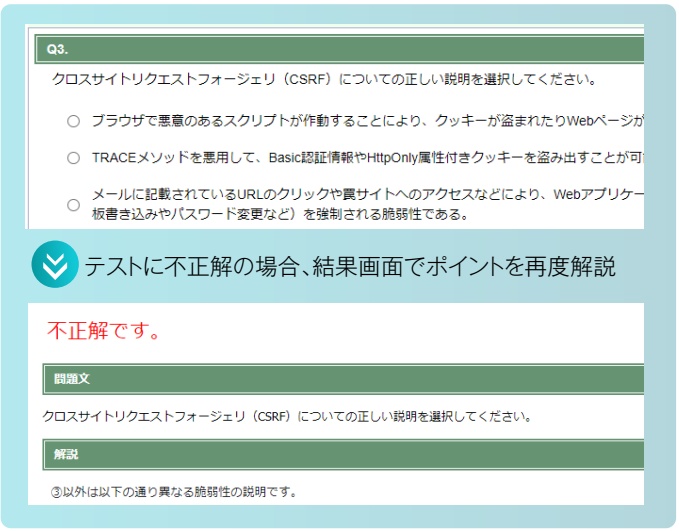
〈松山〉今回受講させていただいたのは、ウェブセキュリティエッセンシャルコースでした。さらに上のレベルのコースを受講したいという声も上がっているのですが…。

〈徳丸〉もちろん、リリースを予定しています。ご期待ください。

〈松山〉楽しみにしています!ぜひ、また集合研修もお願いします。

〈徳丸〉実のところ、徳丸本をリリースした 2011 年当時と比較しても、Web セキュリティの原理は変わっていません。ディテールが変わっていると感じます。

Web システム開発に携わるエンジニアみなさんには、原理を抑えつつ、最新のディテールを学習していただきたいと思います。最新の 2024 版集合研修もご用意したいと思います。世界中の Backlog ユーザのためにも、これからもご協力させていただきます。



徳丸 CTO が高評価する、ヌーラボ社の透明性

〈徳丸〉最後に、私がヌーラボさんの企業姿勢を評価させていただているポイントが、実はもう一つあるんです。

〈司会〉ぜひ、お聞きしたいです。

〈徳丸〉ヌーラボさんが公開している、セキュリティホワイトペーパーです。お客様情報に関して、正直に書かれています。非常に信頼できる企業だと感じました。

〈松山〉ありがとうございます。お客様情報の暗号化の部分ですね。暗号化は、アプリのパフォーマンスに影響します。それに例えば、暗号化することでユーザサポートがお客様の情報をスピーディーに確認できないなど、レスポンスにも影響が出ます。お客様に、事前にしっかりと通知させていただき、透明性を担保しています。

〈徳丸〉Web セキュリティにおいて、透明性はとても重要です。ヌーラボさんのセキュリティホワイトペーパーには、透明性や誠実さを感じます。ヌーラボさんのお考えに賛同します。

〈松山〉ありがとうございます。今後ともよろしくお願いします。

徳丸CTO全面監修による2つの e- ラーニングコンテンツ

Security Campus e-Learning
〈ウェブセキュリティエッセンシャルコース〉

セキュアコーディングのために取り組むべきポイントを分かりやすく解説した、Web エンジニア向けの e- ラーニングコンテンツ。CTO 徳丸浩が全面監修した、EG セキュアソリューションズ社の完全オリジナルです。いつでも、どこでも、繰り返し学習することが可能。非エンジニアへのセキュリティ研修コンテンツとしても活用できます。

最新 Security Campus e-Learning
〈発注者向けウェブセキュリティコース〉

2024 年 5 月 13 日にリリースした、最新の e- ラーニングコンテンツ。ウェブサイトの企画・開発に携わる人に不可欠な、「発注側のスキル」を解説しています。発注者がセキュリティの理解を深めることで、開発におけるムダ発生の抑止効果も高めることができます。広報部やサービス提供事業部でウェブサイトの企画・開発に関わる担当者にぜひ受講いただきたいコンテンツです。もちろん、EG セキュアソリューションズ CTO 徳丸浩が全面監修しています。

EGセキュアソリューションズ株式会社
〒105-0001 東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー 8F
https://www.eg-secure.co.jp/
© EG Secure Solutions Inc.