קורס סייבר באטל רויאל – שיעור ניסיון

פריצת סיסמאות

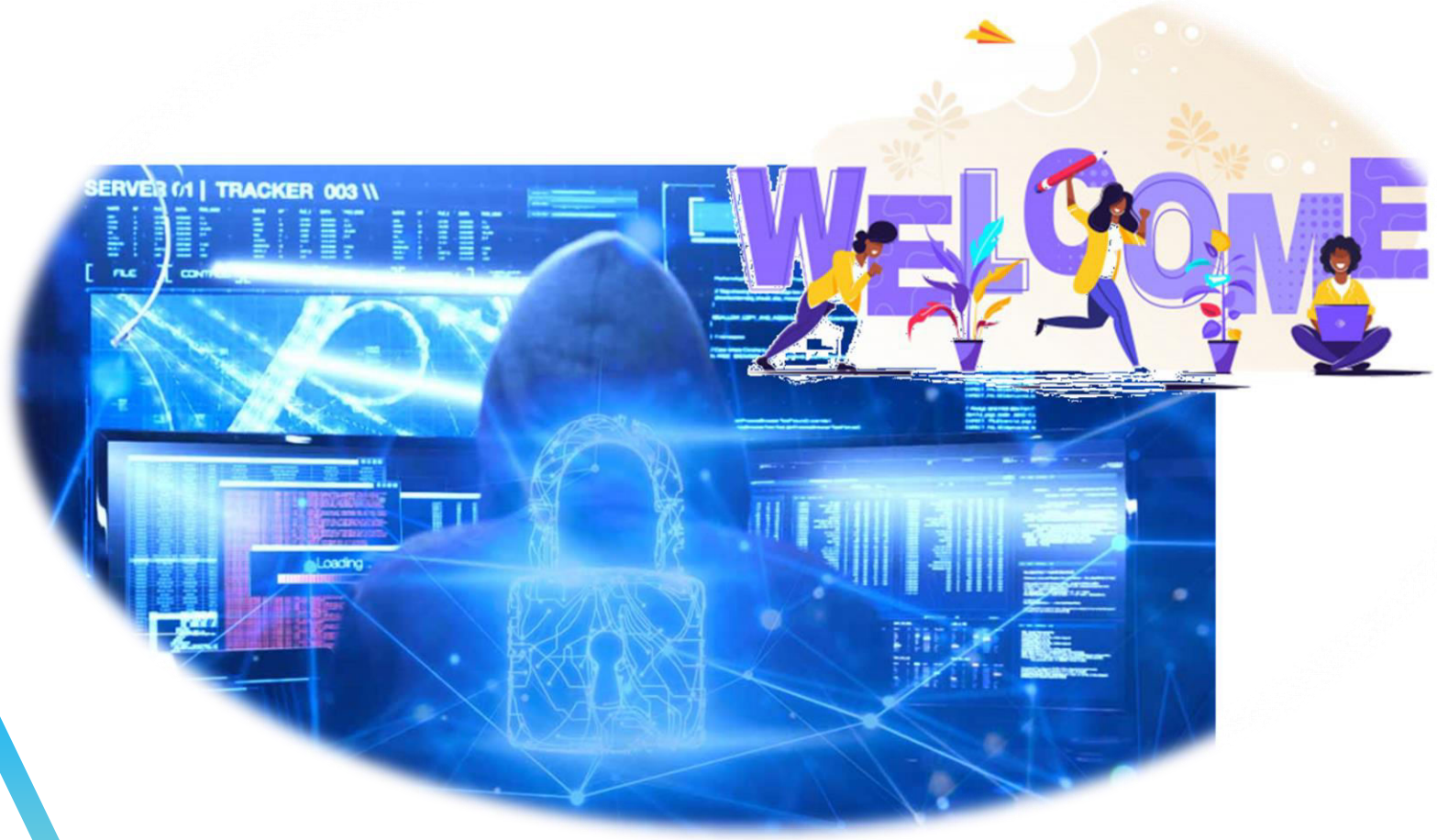
CYBER SCHOOL

ברוכים הבאים

שלום לכולם, שמחים לראותכם!

אנחנו מניחים שבאתם לכאן כי אתם רוצים ללמוד על עולם הסייבר, ההאקינג והאינטרנט...

מצוין! זה בדיוק מה שאנחנו הולכים ללמוד ביחד.



CYBER SCHOOL

תכנית הקורס

אז מה זה קורס סייבר באטל רויאל?

תפקידו של קורס סייבר באטל רויאל הוא להכיר לנו את עולם הסייבר, הרשת והאינטרנט. ביחד נלמד על מושגי מחשוב, רשתות ואבטחת מידע, וכל מה שנוגע לאינטרנט.

השיעורים מציגים בפניכם את יסודות הרשת והפעילות בה, מערכות ההפעלה, פקודות בסיסיות ופרוטוקולי תקשורת מחשבים.

בקורס נתרגל תקיפות סייבר אמיתיות, אמצעי הגנה מתקדמים, ונשתמש בכלים עוצמתיים וייחודיים מעולם ההאקינג והסייבר!

CYBER SCHOOL

מטרות השיעור

אז מה נעשה היום ביחד?

- נלמד על פרצות אבטחה
- נבין מהו קובץ מקור
- נחשוב כמו האקרים – ונפתור אתגרי פריצת סיסמאות!
- בסוף השיעור נקדיש זמן לשאלות ומידע על הקורס.

CYBER SCHOOL

סיסמאות

גניבת סיסמאות ופריצה לחשבונות פרטיים הן מגיפות של ממש בעולם האינטרנט של ימינו!

כולנו משתמשים בסיסמאות על בסיס קבוע, ולכן הן מהוות יעד מועדף לתקיפה.

CYBER SCHOOL

CYBER SCHOOL

קורס סייבר באטל רויאל

פירצת אבטחה

עולם הפרצות – נעים להכיר

לפני שנבין כיצד למצוא ולהתגונן מפני פרצות בעולם האינטרנט, חשוב שנבין מהן אותן פרצות וחולשות שקיימות ברשת.

פירצה מתייחסת למנגנון מסוים בשירות כלשהו, שניתן לקבל באמצעותו גישה למידע מסוים באותו השירות, בדרך שהיוצר לא התכוון אליה.

חשבו: מהי "דרך שהיוצר לא התכון אליה?"

CYBER SCHOOL

קטגוריות התקיפה

פגיעה ישירה בזדון	VS	כשל מערכתי/פנימי	VS	פרצות
DOS (תקיפה של שרתי האתר)		שרת האתר נפל כתוצאה מתקלה טכנית		הכנסת תו מסוים (נגיד "@") בשדה הסיסמא, והוא משבש את מערכת האימות
השתלת וירוס במכוון		הפסקת חשמל ללא מערכת גיבוי UPS		מערת זיהוי פנים שנותנת אישור זיהוי גם אם הפנים מוצגות מתמונה ולא באמת
ריגול (אחרי אדם או ארגון)		אנטנות הסלולר לא עובדות, ובתוצאה מכך אין קליטה ואין שירות		הזרקות XSS או SQL

CYBER SCHOOL

CYBER SCHOOL

קורס סייבר באטל רויאל

קוד מקור

פירצות באתרי אינטרנט

היום אתרי אינטרנט בנויים מעשרות ואף מאות אלפי שורות קוד.

כל הקוד הזה מיועד לבניה של מנגנונים ענקיים ומסובכים (כמו רשתות חברתיות, מנועי חיפוש, צפייה בסרטונים, העברות בנקאיות, שליחת מיילים וכו')

האם לדעתכם כל אתר בעולם כיסה את עצמו מכל פירצה אפשרית בקוד שלו?

CYBER SCHOOL

פירצות באתרי אינטרנט

שליפת סיסמאות

פריצה לחשבונות

מידע רגיש - האם הוא נמצא בצד השרת או בצד הלקוח?

הרשאות גישה - האם לכולם בארגון יש הרשאות גישה למידע מסויים?

CYBER SCHOOL

סיסמאות

ללא ספק קו ההגנה החזק ביותר של כל שירות/אתר הוא סיסמאות (ושמות משתמש).

אם מישהו השיג את שם המשתמש והסיסמא שלכם לשירות מסוים, הוא יכול לעשות במעט הכל. לכן כיום קיימות אין ספור טכנולוגיות ושיטות בדי להקשות על תוקפים להשיג את המידע הזה.

CYBER SCHOOL

קוד המקור

מחקר קוד המקור הוא הדרך היעילה ביותר להבין איך אתר אינטרנט עובד, והיכן נמצאות החולשות שלו. האקרים משקיעים זמן רב במחקר קוד מקור כשלב מקדים לביצוע תקיפות, ובדי לאסוף מודיעין.

```
<!doctype html>

<html lang="he" id="htmlHead" xmlns:fb="http://www.facebook.com/2008/fbml" xmlns:og="http://opengraphprotocol.org/schema/">
<head id="ctl00_ctl00_Head1">
<script id="vad-hb-snippet" data-publisher="globes">var _0x3656=['text/javascript','top','async','//cdn.valuad.cloud/hb/','pus
<script async src="https://securepubads.g.doubleclick.net/tag/js/gpt.js"></script>

<script>
    window.googletag = window.googletag || { cmd: [] };

      var domain= window.location.hostname;
      var rand=Math.floor(10*Math.random());
      var script=document.createElement("script");
      script.src= 'https://stag-core.tfla.xyz/serve_onetag?pub_id=33&domain=' + domain + '&rand=' + rand;
      document.head.append(script);
</script>


    <meta http-equiv="X-UA-Compatible" content="IE=edge" /><link rel="manifest" href="/news/manifest.json" />
    <script src="//apis.google.com/js/platform.js" type="text/javascript" async></script>


    <script type="text/javascript">var _sf_startpt = (new Date()).getTime()</script>
    <!-- OutputCache at:1/4/2022 8:17:26 AM template: /news/templates/master_35_default.master // --><title>
    אלה היכולות המלאות של הווירוס שהושתל נגד איראן - גלובס
</title><meta charset="utf-8" /><meta property="fb:pages" content="128641160502301" /><meta property="og:site_name" content="t
    <link href="/news/passmadadim/css/pass.css?v=3" rel="stylesheet" type="text/css" />

    <!-- IE Pinned Sites -->
    <link rel="icon" type="image/png" href="https://images.globes.co.il/globes/icons/favicon2019-he.png" sizes="64x64" /><link
    <!-- START ZOOMD -->
    <script async="async" src="//zdwidget3-bs.sphereup.com/zoomd/SearchUi/Script?clientId=96326701"></script>
    <script type='text/javascript'>
        var searchType = '100';
        var flagOpenWidget = true;
```

CYBER SCHOOL

קובץ המקור- ולמה הוא חשוב להאקרים?

קובץ המקור בד"כ מכיל את הלוגיקה של האתר/שירות.

מידע רגיש לא יאוחסן בקוד המקור עצמו, אך ניתן בכל זאת ללמוד ממנו הרבה, למשל:

ביצד האתר שומר את המידע שאנו שולחים לו, ביצד הוא מתקשר עם השרתים שלו.

עם אילו טכנולוגיות ושפות תכנות האתר עובד (php, node.js, ruby, python ועוד..), ואיזה תהליך ולידציה (אימות) עובר המידע שלנו.

בדרך כלל המנגנון של בדיקת הסיסמה נמצא בקובץ המקור של האתר.

CYBER SCHOOL

נסו בעצמכם!

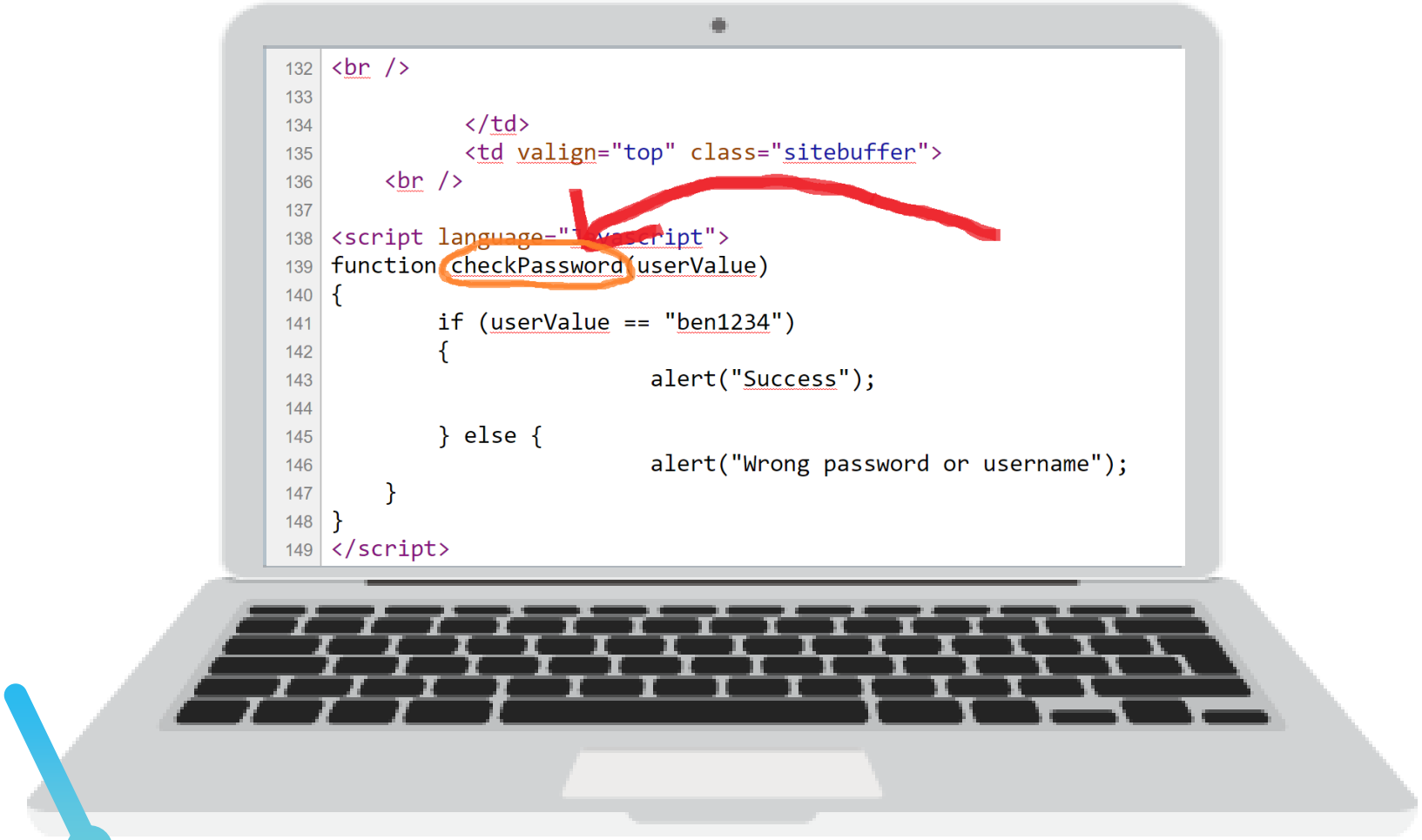
כניסה לקובץ מקור וצפייה בו נעשית על ידי לחיצה על הכפתורים:
Ctrl+U במקלדת

נסו בעצמכם - כנסו לאתר מסויים והביטו בקובץ המקור שלו.

CYBER SCHOOL

קובץ המקור- מציאת חולשה

לא ניתן לדעת היכן נמצא מנגנון בדיקת הסיסמא, לכן צריך לחפש משהו "חשוד".
בדוגמא זו, ניתן לראות כי בשורה מס' 139, ישנו קטע קוד "חשוד".
מדוע דווקא קטע קוד זה "תפס לנו את העין"? מה קורה בשורה זו?



CYBER SCHOOL

מונחים חשודים

מונחים חשודים בקוד המקור הם כאלו שקשורים לתהליך ולידציה (אימות) של סיסמאות, למשל.

Function – פונקציה

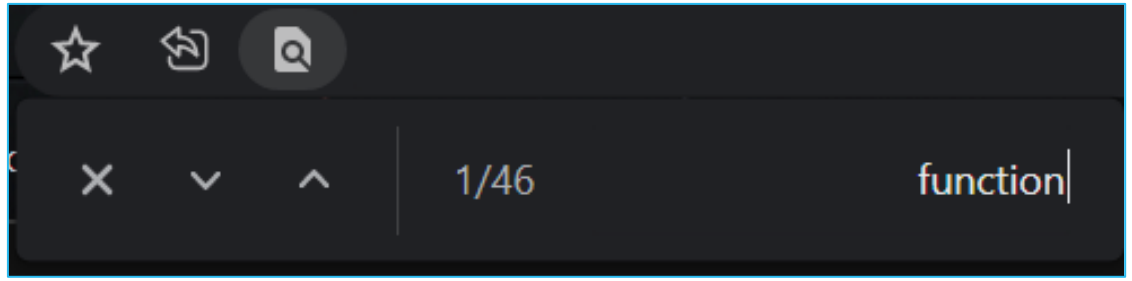
Check – בדיקה

Value – ערך

Alert – התראה

Password – סיסמא

ניתן לחפש מונחים אלו בתוך קוד המקור על ידי שימוש בקיצור המקשים Ctrl+F:



CYBER SCHOOL

CYBER SCHOOL

קורס סייבר באטל רויאל

אתגרי פריצה

בואו נתחיל!

כעת נתנסה בפריצת סיסמאות.

בתרגילים השונים תיתקלו באתגרים ובשיטות שונות אשר יקשו עליכם לפצח את הסיסמאות שלפניכם.

אלו הן שיטות אשר בעבר היו משמשות אתרים אמיתיים להגנה על סיסמאות!
אל תשכחו להשתמש בכלי למפתחים וקובץ המקור!

בהצלחה!

CYBER SCHOOL

תרגול פריצת סיסמאות

במו האקרים!

20-30 דק'

המשימה

ללמוד כיצד האקרים פורצים סיסמאות על ידי שימוש בקוד המקור

השלבים

- היכנסו לאתר https://cyber-school.co.il/jshack/1/
- נסו להבין מהי הסיסמא על ידי שימוש בקוד המקור. הקלידו את הסיסמא במקום המיועד לכך.
- הצלחתם? עברו לשלב הבא!

כלים

דפדפן

קבצים קשורים

- https://cyber-school.co.il/jshack/1/

שאלות?

- מהו אורך הקורס?
- באיזה שעות וימים מתקיים הקורס?
- מה לומדים בקורס?
- האם יש הפסקות?
- האם יש שיעורי בית?
- איפה נרשמים?
- ועוד...