نام: _____ تاریخ: _____ نمره: _____

نشت گذرواژه و امنیت اعتبارنامه

پر کردن اعتبارنامه، نقض داده‌ها، الگوریتم‌های هش، احراز هویت چندعاملی و امنیت گذرواژه.

مرور آموزشی نشت گذرواژه

خوش آمدید! این بستهٔ فعالیت شما را در بررسی نشت گذرواژه و امنیت اطلاعات کاربری راهنمایی می‌کند. با حملات تکرار اعتبارنامه (credential stuffing)، نقض داده، الگوریتم‌های درهم‌سازی، احراز هویت چندعاملی و مدیران گذرواژه آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- ☐ **بخش 1-4: بر امنیت سایبری و پیشگیری از تهدید مسلط شوید.**
- ☐ **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- ☐ **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- ☐ **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- ☐ **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- ☐ **تکمیلی: چالش سریع فکر کن**

ایمن‌شده

رمزگذاری داده

استاندارد AES 256 بیتی

منطبق

استانداردهای جهانی

چارچوب‌های GDPR و CCPA

اعتماد صفر

سیاست دسترسی

احراز هویت چندعاملی

باز کردن راهنمای امنیت سایبری VPN.com

URL: https://www.vpn.com/cybersecurity/passwords-leak/

نقشهٔ راه یادگیری امنیت گذرواژه شما

- خطرهای افشای اطلاعات ورود در انجمن‌های وب تاریک را درک کنید.
- احراز هویت چندعاملی (MFA) و پایش اطلاعات ورود لو رفته را پیاده‌سازی کنید.
- دفاع‌های امنیتی سازمانی را در برابر کلاهبرداری‌های مهندسی اجتماعی هدفمند طراحی کنید.

راهنمای دستورالعمل‌های نشت گذرواژه

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره حفاظت از اعتبارنامه‌ها به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

نشت گذرواژه و امنیت اعتبارنامه (مقدمه)

نشت گذرواژه، اعتبارنامه‌های کاربران را در سایت‌های عمومی و وب تاریک آشکار می‌کند. گذرواژه‌های منحصربه‌فرد از مدیر گذرواژه، بررسی گذرواژه‌های نشت‌یافته و احراز هویت چندعاملی (MFA) خطر پر کردن اعتبارنامه را کاهش می‌دهند، و درهم‌سازی کند و نمک‌دار گذرواژه در صورت سرقت پایگاه داده گذرواژه، آسیب را محدود می‌کند.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. پر کردن اعتبارنامه (credential stuffing) چیست؟

- A. استفاده از خودکارسازی برای آزمایش ترکیب‌های نام کاربری/گذرواژهٔ نشت‌یافته در چند سایت
- B. رمزگذاری فایل‌های ذخیره‌سازی پایگاه دادهٔ محلی
- C. اشباع وب‌سرورها با درخواست‌های ترافیک شبکه
- D. پایش پنهانی ورودی‌های صفحه‌کلید

2. OWASP امروز کدام الگوریتم را به‌عنوان انتخاب اول برای ذخیرهٔ گذرواژه‌ها فهرست می‌کند؟

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3. احراز هویت چندعاملی (MFA) چگونه ریسک نشت گذرواژه را کاهش می‌دهد؟

- A. عامل تأیید اضافی می‌خواهد، بنابراین گذرواژهٔ دزدیده‌شده به‌تنهایی کافی نیست
- B. گذرواژه را هر ساعت به‌طور خودکار تغییر می‌دهد
- C. نام کاربری را هنگام انتقال رمزگذاری می‌کند
- D. دفتر اعتبارسنجی را از درخواست‌های متقلبانه آگاه می‌کند

4. دامپ نقض داده چیست؟

- A. مجموعه‌ای از اعتبارنامه‌های نشت‌یافتهٔ کاربران که آنلاین منتشر یا در انجمن‌های هکرها فروخته می‌شود
- B. نسخهٔ پشتیبان فایل‌های پایگاه داده که در خارج از محل نگهداری می‌شود
- C. حافظهٔ نهان موقت لاگ‌های سرور وب
- D. ابزار مدیریتی برای بازنشانی گذرواژه‌های کاربران

5. نقش مدیر گذرواژه چیست؟

- A. تولید و ذخیرهٔ گذرواژه‌های یکتا و قوی برای هر حساب
- B. پایش ترافیک شبکه برای یافتن نشت گذرواژه
- C. مسدود کردن حملات خودکار جست‌وجوی فراگیر (brute-force) در دروازه
- D. اسکن بلوک‌های ذخیره‌سازی پایگاه داده برای یافتن گذرواژه‌های رمزنگاری‌نشده

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. استفادهٔ مجدد از گذرواژه در چند حساب خطر credential stuffing را افزایش می‌دهد.

○ درست ○ نادرست

7 پرسش 7

7. SHA-1 یک تابع درهم‌ساز توصیه‌شده برای ذخیره‌سازی مدرن گذرواژه است.

○ درست ○ نادرست

8 پرسش 8

8. اعمال پیچیدگی گذرواژه به‌تنهایی (بدون MFA) به‌طور کامل جلوی پر کردن اعتبارنامه را می‌گیرد.

○ درست ○ نادرست

9 پرسش 9

9. ابزارهای پایش وب تاریک، اینترنت را برای یافتن اعتبارنامه‌های لورفتهٔ شرکتی اسکن می‌کنند.

○ درست ○ نادرست

10 پرسش 10

10. درهم‌سازی‌های نمک‌دار پیش از درهم‌سازی داده‌های تصادفی یکتا به گذرواژه‌ها می‌افزایند تا حمله‌های جدول رنگین‌کمان را بی‌اثر کنند.

○ درست ○ نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. آزمودن اعتبارنامه‌های لورفته روی برنامه‌های وب بسیار، حملهٔ _____ اعتبارنامه است.
2. یک الگوریتم هش کند و تطبیقی گذرواژه که هنوز مورد پذیرش OWASP است، _____ نام دارد.
3. افشای فایل‌های محرمانهٔ پایگاه داده در اینترنت، یک _____ داده است.
4. افزودن مقادیر تصادفی به گذرواژه‌ها پیش از هش‌کردن _____ نام دارد.
5. یک پایگاه داده محلی امن برای اعتبارنامه‌های کاربر، یک _____ گذرواژه است.
6. افزودن گام دوم تأیید ورود از _____ استفاده می‌کند.

بانک واژگان

احراز هویت چندعاملی | انباشت | رنگین‌کمان | فیشینگ | مدیر | نقض | نمک‌گذاری | bcrypt

پاسخ‌های خود را اینجا بنویسید:

1.
2.
3.
4.
5.
6.

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

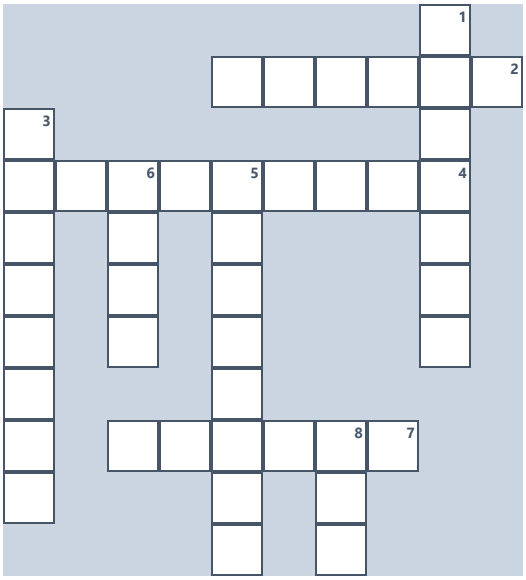
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. انباشت اعتبارنامه	A	جدول از پیش محاسبه‌شدهٔ درهم‌سازهای گذرواژه.
2. bcrypt	B	بررسی ورود چندعاملی.
3. نقض امنیتی	C	ابزار ذخیرهٔ اعتبارنامه.
4. نمک‌افزایی	D	افشای غیرمجاز پایگاه داده.
5. مدیر	E	مهندسی اجتماعی برای سرقت اطلاعات ورود.
6. احراز هویت چندعاملی (MFA)	F	آزمودن اطلاعات ورود افشاشده.
7. رنگین‌کمان	G	افزودن salt تصادفی به درهم‌ساز گذرواژه.
8. فیشینگ	H	الگوریتم کند هش‌کردن گذرواژه.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

2. مهندسی اجتماعی برای سرقت اطلاعات ورود. (6)

4. جدول از پیش محاسبه‌شدهٔ هش گذرواژه‌ها. (9)

7. آزمودن اعتبارنامه‌های لورفته. (6)

عمودی

1. الگوریتم هش کند گذرواژه. (7)

3. بررسی ورود با چند عامل. (8)

5. افزودن نمک تصادفی به هش گذرواژه. (8)

6. ابزار نگهداری اعتبارنامه. (4)

8. افشای غیرمجاز پایگاه داده. (3)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

2 افقی: مهندسی اجتماعی برای سرقت اطلاعات ورود. (6 حرف):

4 افقی: جدول از پیش محاسبه‌شدهٔ هش گذرواژه‌ها. (9 حرف):

7 افقی: آزمودن اعتبارنامه‌های لورفته. (6 حرف):

عمودی

1 عمودی: الگوریتم هش کند گذرواژه. (7 حرف):

3 عمودی: بررسی ورود با چند عامل. (8 حرف):

5 عمودی: افزودن نمک تصادفی به هش گذرواژه. (8 حرف):

6 عمودی: ابزار نگهداری اعتبارنامه. (4 حرف):

8 عمودی: افشای غیرمجاز پایگاه داده. (3 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ح	ظ	گ	س	ت	غ	ذ	ح	ص	غ	ش	ظ	ن	ع	ض
ت	ک	ن	ف	ق	ج	ژ	ر	ب	پ	ا	ب	پ	ط	و
ژ	ز	ی	و	ژ	ن	ک	ز	ث	ی	ع	ش	ر	ث	ذ
ص	ش	ت	ش	ب	ا	ن	ا	ژ	ک	ع	ظ	خ	ش	
ی	ش	ی	ع	غ	ر	ف	ک	ک	خ	پ	ر	ف	ظ	ض
ل	د	ف	ف	پ	ن	م	ن	ث	ق	ه	گ	ی	ت	ی
م	م	ح	ز	خ	گ	ی	ث	م	ص	ث	ع	ن	پ	ظ
ا	پ	گ	ب	ا	ی	ی	ض	ث	ک	ژ	ض	ا	ث	ت
ع	ض	ث	چ	خ	ن	ذ	ث	غ	ع	گ	ش	ق	چ	ذ
د	ف	ی	ق	چ	ک	ع	ل	چ	ا	ا	ذ	ع	ن	ط
ن	ص	ظ	ک	و	م	ع	ز	غ	ک	ر	ف	ا	ت	ص
چ	ه	پ	ح	ف	ا	ن	م	ر	ی	ا	غ	ی	ر	ه
ه	ژ	ح	ذ	ش	ن	غ	ز	د	س	س	ق	ط	خ	ی
ظ	ع	خ	ی	ا	ض	ل	م	ح	گ	پ	ه	ف	ه	ب
خ	س	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی	ه	ح	و

فهرست واژگان

انباشت
بیکریپت
نقض
نمکگذاری
مدیر
چندعاملی
رنگینکمان
فیشینگ

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان	تعاریف و فیلدهای تطبیق
A. انباشت	1. مهندسی اجتماعی برای سرقت اطلاعات ورود.
B. بیکریپت	2. افشای غیرمجاز پایگاه داده.
C. نقض	3. الگوریتم هش کند گذرواژه.
D. نمک‌گذاری	4. جدول از پیش محاسبه‌شدهٔ هش گذرواژه‌ها.
E. مدیر	5. آزمودن اعتبارنامه‌های لورفته.
F. چندعاملی	6. افزودن نمک تصادفی به هش گذرواژه.
G. رنگین‌کمان	7. ابزار نگهداری اعتبارنامه.
H. فیشینگ	8. بررسی ورود با چند عامل.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی امنیت سایبری آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ب ا ا ش ت ن _____
2. ض ق ن _____
3. ر م ی د _____
4. ن ن ا ی م ک ر ن گ _____
5. ی ت ر ک ب پ ی _____
6. ر ی گ ا ن ذ م ک _____
7. چ ی ا م ل ن ع د _____
8. ش گ ف ن ی ی _____

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
2	قواعد یک گذرواژهٔ قوی		
3	مدیرهای گذرواژه که می‌شناسید		
4	ابزارهای امنیتی که می‌شناسید		
5	نشانه‌های هشدار در یک ایمیل		
6	واژه‌های جالب برای یک عبارت‌عبور بلند		
7	روش‌های ورود بدون گذرواژه		
8	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
9	دلایل به‌روزرسانی نرم‌افزار		
10	کارهایی که وقتی گذرواژه‌ای نشت می‌کند باید انجام داد		
11	حساب‌هایی که به MFA نیاز دارند		
12	جاهایی که گذرواژه‌ها هرگز نباید در آن‌ها ذخیره شوند		
13	نشانه‌های آلوده بودن رایانه		
14	گذرواژه‌های ضعیفی که مردم استفاده می‌کنند		
15	چیزهایی که پشتیبان می‌گیرید		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: رفع نشت اعتبارنامه‌های سازمانی



سناریو: یک سرویس پایش وب تاریک به یک سازمان هشدار می‌دهد که یک dump پایگاه داده حاوی گذرواژه‌های مدیران سیستم شرکت به‌صورت آنلاین منتشر شده است.

پرسش برای بحث: ریسک‌های نشت اعتبارنامه‌ها را تحلیل کنید و یک راهبرد بازنشانی مدیریتی پیشنهاد دهید.

مطالعهٔ موردی 2: پیاده‌سازی استانداردهای درهم‌سازی گذرواژه



سناریو: یک پایگاه داده سازمانی اکنون گذرواژه‌های کاربران را با هش‌های قدیمی MD5 و بدون salt رمزنگاری ذخیره می‌کند، که آن‌ها را در برابر استخراج سریع آسیب‌پذیر می‌کند.

پرسش برای بحث: یک راهبرد مهاجرت برای ارتقای الگوریتم هش پایگاه داده طراحی کنید.

ایستگاه بررسی 9: رمزگشایی

متخصص امنیت سایبری از دارایی‌های شبکه در برابر عوامل تهدید آنلاین محافظت می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

ا=1 ب=2 پ=3 ت=4 ث=5 ج=6 چ=7 ح=8 خ=9 د=10 ذ=11

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

1	12		31	4	23	12		30	27		13	28	12
10	32	29	25		32	27	28	1	21	10	29	7	

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش A)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q1: نشت گذرواژه چیست؟

نشت گذرواژه زمانی رخ می‌دهد که اعتبارنامهٔ ورود کاربر از طریق نقض داده یا پیکربندی نادرست سرور افشا شود.

Q2: هکرها چگونه گذرواژه‌های نشت‌یافته را پیدا می‌کنند؟

هکرها انجمن‌های دارک وب، مجموعه‌های منتشرشدهٔ پایگاه‌داده و سایت‌های paste را که داده‌های نقض‌شده در آنها منتشر می‌شود اسکن می‌کنند [8].

Q3: آیا استفادهٔ مجدد از گذرواژه خطرناک است؟

بله، زیرا اگر یک سایت به خطر بیفتد، هکرها می‌توانند همان اعتبارنامه‌ها را روی هزاران پلتفرم دیگر آزمایش کنند [3].

Q4: نمک رمزنگاری چیست؟

salt داده‌ای تصادفی است که پیش از درهم‌سازی به گذرواژه افزوده می‌شود و حملات جستجوی از پیش محاسبه‌شده را بی‌اثر می‌کند [2].

Q5: چرا MD5 منسوخ شده است؟

MD5 یک هش همه‌منظورهٔ سریع و منسوخ است، بنابراین مهاجمان می‌توانند حدس‌های گذرواژه را بسیار سریع آزمایش کنند، به‌ویژه وقتی هش‌ها بدون نمک باشند [2].

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش B)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q6: مدیر گذرواژه چگونه از کاربران محافظت می‌کند؟

برای هر سایت اطلاعات ورود پیچیده و یکتا به‌طور خودکار تولید می‌کند و خطاهای حافظهٔ انسانی و استفادهٔ مجدد را کاهش می‌دهد.

Q7: حملهٔ brute force چیست؟

حمله‌ای که به‌طور نظام‌مند هر ترکیب نویسه را آزمایش می‌کند تا گذرواژهٔ درست پیدا شود [4].

Q8: قفل شدن حساب چه کمکی می‌کند؟

قفل‌شدگی یا محدودسازی نرخ، حدس‌زدن‌های مکرر آنلاین را کند می‌کند و همراه با پایش و MFA خطر حمله جست‌وجوی فراگیر (brute-force) را کاهش می‌دهد [4].

Q9: آیا گذرواژه‌های اصلی امن هستند؟

اگر عبارت‌های عبور با آنتروپی بالا باشند و هرگز در سامانه‌های وب دیگر دوباره استفاده نشوند، امن هستند.

Q10: آیا گذرواژه‌ها باید مرتب تغییر کنند؟

NIST می‌گوید تغییرهای دوره‌ای را تحمیل نکنید؛ در صورت شواهد افشا تغییر دهید و به طول، فهرست‌های مسدودسازی و MFA اولویت دهید [1].

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q1: Argon2 چه تفاوتی با bcrypt دارد؟

OWASP الگوریتم Argon2id را انتخاب اول خود معرفی می‌کند؛ تنظیمات حافظه‌سخت آن در برابر شکستن با GPU و ASIC بهتر از bcrypt مقاومت می‌کند [2].

Q2: کشش کلید (key stretching) چیست؟

تکنیکی که الگوریتم درهم‌سازی را هزاران بار تکرار می‌کند تا فرایند تأیید گذرواژه را کند کند و شکستن آن را پرهزینه سازد [2].

Q3: جدول‌های رنگین‌کمان چگونه کار می‌کنند؟

آن‌ها جدول‌های جست‌وجوی از پیش محاسبه‌شده‌ای هستند که گذرواژه‌های متن ساده را به هش‌هایشان پیوند می‌دهند و برای وارونه کردن سریع هش‌های بدون نمک به کار می‌روند [2].

Q4: بازیافت اعتبارنامه چیست؟

استفادهٔ مجدد از جفت‌های نام کاربری/گذرواژهٔ دزدیده‌شده از یک نشت برای تلاش در دسترسی به سرویس‌های دیگر، به‌ویژه جایی که افراد گذرواژه‌ها را تکرار کرده‌اند [3].

Q5: آیا مدیران گذرواژه هک می‌شوند؟

بله. بسیاری از آن‌ها از رمزگذاری دانش‌صفر استفاده می‌کنند، بنابراین نفوذ به سرور فقط گاوصندوق‌های رمزگذاری‌شده را افشا می‌کند، اما گذرواژه‌های اصلی ضعیف همچنان می‌توانند به‌صورت آفلاین شکسته شوند.

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q6: حملهٔ دیکشنری چیست؟

گونه‌ای از حملهٔ brute-force که به‌جای حروف تصادفی، واژه‌ها، عبارت‌ها و گذرواژه‌های نشت‌یافتهٔ قبلی رایج را آزمایش می‌کند.

Q7: چرا عبارت‌های عبور ترجیح داده می‌شوند؟

عبارت‌های گذر از چند واژهٔ تصادفی استفاده می‌کنند و آنتروپی بالایی ایجاد می‌کنند که برای انسان به‌یادماندنی است اما شکستن آن از نظر محاسباتی پرهزینه است [1].

Q8: ورود یکپارچه (SSO) چگونه بر نشت گذرواژه اثر می‌گذارد؟

SSO پراکندگی گذرواژه‌ها را کاهش می‌دهد، اما ارائه‌دهندهٔ هویت به هدفی با ارزش بالا تبدیل می‌شود که به MFA قوی و ترجیحاً مقاوم در برابر فیشینگ نیاز دارد [6].

Q9: ربایش نشست چیست؟

مهاجم توکن نشست معتبری را به دست می‌آورد یا از آن سوءاستفاده می‌کند تا بدون نیاز دوباره به گذرواژه، خود را جای کاربر واردشده جا بزند [5].

Q10: چگونه حملهٔ پاشش گذرواژه را تشخیص می‌دهید؟

با جست‌وجوی چند گذرواژهٔ یکسان که در حساب‌های بسیار آزموده می‌شوند، اغلب به‌آهستگی تا زیر آستانهٔ قفل شدن بمانند [7].

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ امنیت سایبری

واقعیت‌های دنیای واقعی دربارهٔ نقض‌های امنیتی، سازوکارهای دفاعی و استانداردهای انطباق را مرور کنید.

1. بینش امنیت

NIST SP 800-63B الزام می‌کند گذرواژه‌های جدید با فهرست‌های مسدودسازی گذرواژه‌های رایج و افشاشده بررسی شوند [1].

2. بینش امنیت

نشت 'Collection #1' در سال 2019 داده‌های بسیاری از نقض‌های پیشین را در یک فایل عظیم از جفت‌های ایمیل و گذرواژه ادغام کرد [8].

3. بینش امنیت

NIST اکنون الزام می‌کند گذرواژه‌هایی که تنها عامل احراز هویت هستند دست‌کم 15 نویسه باشند [1].

4. بینش امنیت

سخت‌افزار ASIC می‌تواند میلیاردها درهم‌ساز SHA-256 را در ثانیه محاسبه کند و درهم‌سازی خام SHA را برای گذرواژهٔ کاربران ناایمن می‌سازد [2].

5. بینش امنیت

نمک‌های یکتا یعنی دو کاربر با گذرواژهٔ کاملاً یکسان هش‌های متفاوتی در پایگاه داده دارند [2].

6. بینش امنیت

بسیاری از مدیران گذرواژه داده‌های گاوصندوق را به‌صورت محلی با رمزنگاری قوی مشتق‌شده از گذرواژهٔ اصلی کاربر رمزگذاری می‌کنند.

7. بینش امنیت

پر کردن اعتبارنامه کار می‌کند چون بسیاری از افراد از گذرواژهٔ یکسان در حساب‌های تجارت الکترونیک، بانکی و ایمیل استفاده می‌کنند [3].

8. بینش امنیت

NIST SP 800-63B می‌گوید راستی‌آزماها نباید تغییر دوره‌ای گذرواژه را الزامی کنند، بلکه فقط پس از شواهد افشا لازم است [1].

9. بینش امنیت

افزودن یک حرف بزرگ و یک نماد به گذرواژهٔ کوتاه مانع حملات فرهنگ‌لغتی خودکار مدرن مبتنی بر GPU نمی‌شود [1].

10. بینش امنیت

MFA می‌تواند بسیاری از تلاش‌های پر کردن اعتبارنامه (credential stuffing) را حتی پس از نشت گذرواژه مسدود کند؛ MFA مقاوم در برابر فیشینگ از کدهای SMS قوی‌تر است [3].

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردهای جهانی NIST، OWASP و انطباق با حریم خصوصی داده گردآوری شده‌اند.

منابع علمی و صنعتی

[1] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1 — پاسخ درست: **A**

نکتهٔ آموزشی

Credential stuffing با خودکارسازی، جفت‌های نام کاربری/گذرواژهٔ نشت‌کرده را در سایت‌های دیگر امتحان می‌کند [3].

2 پرسش 2 — پاسخ درست: **A**

نکتهٔ آموزشی

OWASP ابتدا Argon2id را توصیه می‌کند؛ bcrypt بیشتر برای سامانه‌های قدیمی است که Argon2id یا scrypt در آن‌ها در دسترس نیست [2].

3 پرسش 3 — پاسخ درست: **A**

نکتهٔ آموزشی

MFA یک عامل اضافی می‌خواهد، بنابراین گذرواژهٔ دزدیده‌شده به‌تنهایی نمی‌تواند حساب را باز کند [3].

4 پرسش 4 — پاسخ درست: **A**

نکتهٔ آموزشی

Breach dumpها مجموعه‌های اعتبارنامهٔ نشت‌کرده هستند، مانند مجموعهٔ Collection #1 [8] 2019.

5 پرسش 5 — پاسخ درست: **A**

نکتهٔ آموزشی

مدیر گذرواژه برای هر حساب یک گذرواژهٔ قوی و یکتا تولید و ذخیره می‌کند و از استفادهٔ مجدد جلوگیری می‌کند [3].

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: درست

نکتهٔ آموزشی

درست: گذرواژه‌های تکراری به مهاجمان اجازه می‌دهند اعتبارنامه‌های نشت‌کرده از یک سایت را روی سایت‌های دیگر دوباره امتحان کنند [3].

7 پرسش 7

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: SHA-1 یک هش سریع است؛ OWASP به‌جای آن bcrypt، scrypt، Argon2id یا PBKDF2 را توصیه می‌کند [2].

8 پرسش 8

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: قواعد پیچیدگی به‌تنهایی نمی‌توانند جلوی stuffing با گذرواژه‌های نشت‌کردهٔ تکراری را بگیرند؛ MFA لازم است [3].

9 پرسش 9

پاسخ درست: درست

نکتهٔ آموزشی

درست: سرویس‌های پایش، breach dumpها و منابع دارک‌وب را برای اعتبارنامه‌های افشاشده جست‌وجو می‌کنند [8].

10 پرسش 10

پاسخ درست: درست

نکتهٔ آموزشی

درست: salt یکتا برای هر گذرواژه، جدول‌های rainbow از پیش محاسبه‌شده را بی‌اثر می‌کند [2].

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

F 1. انباشت اعتبارنامه	H 2. bcrypt	D 3. نقض امنیتی	G 4. نمک‌افزایی
C 5. مدیر	B 6. احراز هویت چندعاملی (MFA)	A 7. رنگین‌کمان	E 8. فیشینگ

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 انباشت	2 bcrypt	3 نقض	4 نمک‌گذاری
5 مدیر	6 احراز هویت چندعاملی		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 H – فیشینگ	2 C – نقض	3 B – بیکریپت	4 G – رنگینکمان
5 A – انباشت	6 D – نمکگذاری	7 E – مدیر	8 F – چندعاملی

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند انباشت اعتبارنامه، bcrypt و نقض امنیتی را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

ح	ظ	گ	س	ت	غ	ذ	ح	ص	غ	ش	ظ	ن	ع	ض
ت	ک	ن	ف	ق	چ	ژ	ر	ب	پ	ا	ب	پ	ط	و
ژ	ز	ی	و	ژ	ن	ک	ز	ث	ی	ع	ش	ر	ث	ذ
ص	ص	ش	ت	ش	ا	ب	ن	ا	ژ	ک	ع	ظ	خ	ش
ی	ش	ی	ع	غ	ر	ف	ک	ک	خ	پ	ر	ف	ظ	ض
ل	د	ف	پ	ف	ن	م	ن	ث	ق	ه	گ	ی	ت	ی
م	م	ح	خ	ز	گ	ی	ث	م	ص	ن	ع	پ	ظ	
ا	پ	گ	ب	ا	ی	ی	ض	ث	ک	ژ	ض	ث	ا	ت
ع	ض	چ	خ	ث	ن	ذ	ث	غ	ع	گ	ش	ق	چ	ذ
د	ف	ی	ق	چ	ک	ع	ل	ا	ا	ذ	ع	ن	ط	
ن	ص	ظ	ک	و	م	ع	ز	غ	ک	ر	ف	ا	ت	ص
چ	ه	پ	ح	ف	ا	ن	م	ر	ی	ا	غ	ی	ر	ه
ه	ژ	ح	ذ	ش	ن	غ	ز	د	ص	س	ق	ط	خ	ی
ظ	ع	خ	ی	ا	ض	ل	م	ح	گ	پ	ه	ف	ه	ب
خ	ص	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی	ه	ح	و

پاسخ جدول‌کلمات

									ب					
					گ	ن	ی	ش	ی	ف				
									ک					
چ														
ن	ا	م	ک	ن	ی	گ	ن	ر						
د		د		م				ی						
ع		ی		ک				پ						
ا		ر		گ				ت						
م				ذ										
ل		ت	ش	ا	ب	ن	ا							
ی				ر		ق								
				ی		ض								

راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

2 افقی: فیشینگ مهندسی اجتماعی برای سرقت اطلاعات ورود. (6 حرف)

4 افقی: رنگین‌کمان جدول از پیش محاسبه‌شدهٔ هش گذرواژه‌ها. (9 حرف)

7 افقی: انباشت آزمودن اعتبارنامه‌های لورفته. (6 حرف)

عمودی

1 عمودی: بیکریپت الگوریتم هش کند گذرواژه. (7 حرف)

3 عمودی: چندعاملی بررسی ورود با چند عامل. (8 حرف)

5 عمودی: نمک‌گذاری افزودن نمک تصادفی به هش گذرواژه. (8 حرف)

6 عمودی: مدیر ابزار نگهداری اعتبارنامه. (4 حرف)

8 عمودی: نقض افشای غیرمجاز پایگاه داده. (3 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. بااشتن — انباشت
2. ضقن — نقض
3. رمید — مدیر
4. ننایمکرنگ — رنگینکمان
5. یترکبپی — بیکریپت
6. ریگانذمک — نمکگذاری
7. چیاملنعد — چندعاملی
8. شگفنیی — فیشینگ

کلید چالش رمز مخفی

"رمز لو رفته را چندعاملی کنید"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: رفع نشت اعتبارنامه‌های سازمانی

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک سرویس پایش وب تاریک به یک سازمان هشدار می‌دهد که نشتی پایگاه داده حاوی گذرواژه‌های مدیران سیستم سازمانی به‌صورت آنلاین منتشر شده است.
- راهبرد و راه‌حل پیشنهادی: همهٔ نشست‌های فعال مدیر را لغو کنید و اعتبارنامه‌ها را با یک مولد پرآنتروپی بازنشانی کنید. MFA مقاوم در برابر فیشینگ را روی پورتال‌های مدیریت اعمال کنید [6]، کلیدهای API آسیب‌دیده را بچرخانید، گزارش‌های ورود را بررسی کنید، نخستین نقطهٔ افشا را بیابید و سایر حساب‌های دارای دسترسی ویژه را بررسی کنید.

B مطالعهٔ موردی 2: پیاده‌سازی استانداردهای درهم‌سازی گذرواژه

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک پایگاه دادهٔ سازمانی هنوز گذرواژه‌های کاربران را با هش‌های قدیمی MD5 و بدون salt رمزنگاری‌شده ذخیره می‌کند و همین باعث می‌شود در برابر استخراج سریع آسیب‌پذیر باشد.
- راهبرد و راه‌حل توصیه‌شده: Argon2id (یا bcrypt در سیستم‌های قدیمی) را با نمک یکتا برای هر کاربر به کار ببرید [2]. هش‌های MD5 موجود را اکنون در الگوریتم جدید بپوشانید، در ورود بعدی هر کاربر مستقیماً دوباره هش کنید و برای حساب‌های مدت‌ها غیرفعال بازنشانی را اجباری کنید.