| | |
|---|---|
| **Состояние** | Завершены |
| **Тест начат** | воскресенье, 23 ноября 2025, 15:22 |
| **Завершен** | воскресенье, 23 ноября 2025, 15:34 |
| **Затраченное время** | 11 мин. 14 сек. |
| **Баллы** | 41,00/45,00 |
| **Оценка** | **9,11** из 10,00 (**91,11**%) |

**Вопрос 1**

Верно

Баллов: 1,00 из 1,00

Как называется механизм безопасности (политика) браузера, который позволяет бороться с XSS, CSRF и другими атаками за счет определения политики – с каких доменов могут подгружаться ресурсы, политика в отношении заголовков origin, политика в отношении использования безопасного протокола и т.п.? Полное название, 3 слова

Ответ: Content Security Policy

**Вопрос 2**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода, создающего HTML с внедрением пользовательского ввода из $searchQuery. К пользовательскому вводу применено кодирование HTML Encoding. Является ли данное приложение безопасным для встраивания xss?
<td>< ?php echo htmlentities($searchQuery); ?></td>

a. Да

b. Нет

Обратная связь: в данном примере кодирования HTML Encoding достаточно, тк это самый простой контекст внедрения, достаточно обезопасить базовые служебные символы.

**Вопрос 3**

Верно

Баллов: 1,00 из 1,00

Вид XSS при котором злоумышленник получает возможность сохранить вредоносный код на сервере, и код отдается в ответ на последующие запросы к этой или другой странице

- a. Reflected
- b. Blind stored ✓
- c. DOM based
- d. Stored ✓

Обратная связь: такой вид XSS называется stored (к нему же относится и слепая атака, blind stored)

**Вопрос 4**

Верно

Баллов: 1,00 из 1,00

Для защиты от XSS лучшим способом является экранирование. Вы анализируете код, и видите, что все потенциально небезопасные элементы перед отправкой в браузер кодируются при помощи HTML Entity Encoding. Можно ли сказать, что данное приложение защищено от XSS?

- a. Да
- b. Нет ✓

Обратная связь: для разных контекстов внедрения пользовательского ввода на странице на странице нужно использовать разные контексты встраивания, просто HTML Entity Encoding не будет достаточно

**Вопрос 5**

Верно

Баллов: 1,00 из 1,00

Может ли вредоносное js приложение, внедренное в ответ на запрос атакуемого сайта с помощью XSS, делать запросы на сторонние сайты из браузера пользователя?

- a. Да, но только если атакуемое приложение не использует специальные заголовки для запрета запросов к сторонним сайтам ✓
- b. Нет
- c. Да, при любых условиях, так как Same Origin Policy разрешает такие запросы

Обратная связь: SOP позволяет приложению делать запросы к сторонним доменам. Для настройки политики загрузки контента таким образом, чтобы эти запросы были запрещены, рекомендуется использовать Content-Security-Policy

**Вопрос 6**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода страницы создающего HTML с внедрением пользовательского ввода из $searchQuery.
<A href="<?php echo htmlentities($searchQuery); ?>">some link text</a>
Как можно встроить выполнение команды js в данном случае?

Ответ: javascript:alert('XSS')

**Вопрос 7**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода (встраивание пользовательского ввода $searchParams в javascript). К $searchParams применено Unicode кодирование. Является ли такое приложение безопасным для встраивания вредоносного xss?
< script>< ?php echo json_encode($searchParams) ?>< /script>

a. Да
b. Нет

Обратная связь: нет, т.к. встраивание непосредственно между тегами script (не внутри строки программы js) не будет безопасным при таком экранировании.

**Вопрос 8**

Верно

Баллов: 1,00 из 1,00

Как называется http заголовок, в котором передается тип контента ответа?

Ответ: Content-Type

**Вопрос 9**

Верно

Баллов: 1,00 из 1,00

Какой безопасный http заголовок позволяет предотвратить XSS атаку за счет установки разрешенных типов и источников контента на странице?

a. X-Frame-Options
b. Strict-Transport-Security (HSTS)
c. X-XSS-Protection
d. Content-Security-Policy (CSP)

**Вопрос 10**

Верно

Баллов: 1,00 из 1,00

Как называется http заголовок, который задает политику в отношении cross-origin запросов (сервер может полностью запретить такие запросы)

Ответ: Cross-Origin-Resource-Policy

**Вопрос 11**

Неверно

Баллов: 0,00 из 1,00

В системе настроено ведение системных журналов с отображением в формате HTML на административной части сайта. К какой атаке потенциально уязвим данный сайт, если данные системных журналов недостаточно экранируются (три слова, по-английски, … … xss)?

Ответ: Persistent Cross-site Scripting

**Вопрос 12**

Верно

Баллов: 1,00 из 1,00

К какой группе уязвимостей согласно OWAST Top 10 относят XSS

a. A03 Injection
b. A08 Software and data integrity failures
c. A10 Server Side Request Forgery
d. A01 Broken Access Control
e. A02 Cryptographic failures

**Вопрос 13**

Верно

Баллов: 1,00 из 1,00

Перед часть HTML страницы, на которую попал пользовательский ввод. Какой метод кодирования для экранирования достаточен при внедрении небезопасного ввода в простой HTML контекст («между обычными тегами», пример <td>%USER_INPUT%</td>)? Три слова (на английском языке)

Ответ: HTML Entity Encoding

**Вопрос 14**

Верно

Баллов: 1,00 из 1,00

Как называется http заголовок, который сообщает браузеру, что он должен использовать только HTTPS протокол. Он защищает от атак с использованием понижением уровня защиты (HTTPS-> HTTP), cookie hijacking

Ответ: Strict-Transport-Security

**Вопрос 15**

Верно

Баллов: 1,00 из 1,00

Что из следующего является наиболее вероятным вектором для встраивания reflected xss атаки?

a. База данных сервера
b. Пользовательский ввод в input элементе на форме поиска
c. Клиентская часть приложения (штатный js)
d. Http заголовки запроса

**Вопрос 16**

Верно

Баллов: 1,00 из 1,00

Верно ли утверждение: из-за same origin policy браузер не позволит загрузить js со стороннего сайта, так как выполнение приложения, загруженного со стороннего сайте, будет заблокировано

a. Нет
b. Да

Обратная связь: SOP позволяет встраивать в атрибут src тега script ссылки на сторонние сайты, и при этом код, загруженный с таких сайтов, будет выполнен с правами того приложения, с которого пришел исходный html с тегом < script src=...>. Для того, чтобы это запретить, приложение должно использовать специальные безопасные заголовки.

**Вопрос 17**

Верно

Баллов: 1,00 из 1,00

Вид XSS при котором в ответе с сервера исходно нет работающего кода вредоносного XSS, но после выполнения штатных клиентских скриптов приложения вредоносный код внедряется на страницу непосредственно в браузере клиента (три слова, по-английски, ... ... xss).

Ответ: DOM Based XSS

**Вопрос 18**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода с генерацией HTML в javascript приложении на стороне клиента

Select your language:
< select>< script>

document.write("< OPTION value=1>"+decodeURIComponent(document.location.href.substring(document.location.href.indexOf("default=")+8))+"< /OPTION>");

document.write("< OPTION value=2>English< /OPTION>");

< /script>< /select>

К какому типу инъекции потенциально уязвим этот сайт (3 слова, по-английски)?

Ответ: DOM Based XSS

**Вопрос 19**

Верно

Баллов: 1,00 из 1,00

Может ли вредоносное приложение, внедренное на атакуемый сайт с помощью XSS, получить доступ к хранилищу local storage данного сайта?

a. Да
b. Нет
c. Да, но только если приложение присылает нужный CORS заголовок
d. Да, но только при работе по безопасному протоколу

Обратная связь: javascript приложение может получить доступ к хранилищу local storage, для этого не требуется дополнительных ограничений.

**Вопрос 20**

Верно

Баллов: 1,00 из 1,00

Может ли вредоносное приложение, внедренное на атакуемый сайт с помощью XSS, делать запросы на атакуемый сайт и обрабатывать ответ сервера?

a. Да, но только если приложение присылает нужный CORS заголовок
b. Да ✓
c. Нет
d. Да, но только при работе по безопасному протоколу

Обратная связь: javascript приложение может делать запросы к своему сайту и обрабатывать ответы, для этого не требуется дополнительных ограничений.

**Вопрос 21**

Верно

Баллов: 1,00 из 1,00

Является ли безопасным выстраивание механизмов безопасности на базе использования фильтрации по черному списку

a. Да
b. Нет ✓
c. Да, но только при работе по безопасному протоколу

Обратная связь: механизмы безопасности на базе фильтров могут и должны использоваться, но только как вспомогательные, т.к. фильтры можно обойти и не всегда можно запретить все опасные символы.

**Вопрос 22**

Неверно

Баллов: 0,00 из 1,00

Приведен пример кода страницы создающего HTML с внедрением пользовательского ввода из $searchQuery. Является ли данное приложение безопасным для встраивания xss?
<a href=http://www.somesite.com?test=<?php echo htmlentities(urlencode($searchParams), ENT_QUOTES); ?> >link</a >

a. Да
b. Нет ✗

**Вопрос 23**

Верно

Баллов: 1,00 из 1,00

Как сервер может запретить браузеру выполнять javascript программы, загруженные со сторонних сайтов (что он должен отправить в ответе на запрос)

a. Отправить заголовок Only-First-Party-Scripts: true
b. Отправить заголовок Strict Transport Security
c. Никак не может
d. Установить только свой домен в настройках (в заголовках) Content-Security-Policy для script-src ✓
e. Такие программы и так запрещены, браузер их не выполнит

Обратная связь: для настройки политики загрузки скриптов, рекомендуется использовать Content-Security-Policy

**Вопрос 24**

Верно

Баллов: 1,00 из 1,00

Существует несколько способов встроить вредоносный код в атрибут src. Один из них – использование специального псевдопротокола для втраивания непосредственно js команд. Как называется этот псевдопротокол (одно слова, без двоеточия)

Ответ: javascript ✓

**Вопрос 25**

Верно

Баллов: 1,00 из 1,00

Какой метод кодирования для экранирования достаточен при внедрении небезопасного ввода в значения атрибутов HTML ( < td class=USER_INPUT>)?

a. URL Encoding
b. HTML Encoding всех символов
c. HTML Entity Encoding
d. HTML Encoding + обрамление строки встраивания кавычками ✓
e. HTML Entity Encoding + URL encoding

**Вопрос 26**

Верно

Баллов: 1,00 из 1,00

Существует ли возможность встроить javascript в каскадные таблицы стилей?

a. Нет
b. Да ✓

**Вопрос 27**

Верно

Баллов: 1,00 из 1,00

Пришел ответ от сервера, и в нем нет заголовков или данных, которые подсказали бы браузеру, что аз тип содержимого содержится в ответе. Браузер попытается сам определить тип переданного контента. Как называется этот процесс (слово по-английски)?

Ответ: sniffing ✓

**Вопрос 28**

Верно

Баллов: 1,00 из 1,00

Верно ли утверждение: используя XSS атаку, злоумышленник может украсть идентификатор сеанса пользователя из хранилища cookie

a. Нет
b. Да, но только при использовании незащищенного протокола http
c. Да ✓

**Вопрос 29**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода, где $searchQuery – небезопасный пользовательский ввод. Какое экранирование можно применить к searchQuery, чтобы обезопасить страницу?
<img src=https://mysite.com?action=<?php echo $searchQuery; ?> >

a. Unicode encoding
b. URL encoding
c. Никакое, данный код не является безопасным ✓
d. HTML Entity Encoding

Обратная связь: в данном случае, отсутствие кавычек при встраивании значения атрибута тега не позволяет гарантировать безопасность.

**Вопрос 30**

Неверно

Баллов: 0,00 из 1,00

Приведен пример кода, создающего HTML с внедрением пользовательского ввода из $searchQuery. К пользовательскому вводу применено кодирование HTML Encoding. Является ли данное приложение безопасным для встраивания xss?
< td class=< ?php echo htmlentities($searchQuery); ?> >

a. Нет
b. Да ⊗

Обратная связь: в данном примере кодирования HTML Encoding недостаточно, т.к. поскольку строка не обрамлена кавычками, легко можно встроить дополнительный атрибут (пример ввода: “class onload=….” )

**Вопрос 31**

Верно

Баллов: 1,00 из 1,00

Как называется процедура преобразования опасных (прежде всего, служебных) символов в escape-последовательности, так, чтобы они потеряли свое служебное значение. Одно слово на русском.

Ответ: Экранирование ✓

**Вопрос 32**

Верно

Баллов: 1,00 из 1,00

Может ли злоумышленник использовать сторонний сайт для хранения вредоносного js приложения и загружать основной код атакующего приложения со стороннего сайта

a. Да ✓
b. Нет

Обратная связь: SOP позволяет встраивать в атрибут src тега script ссылки на сторонние сайты, и при этом код, загруженный с таких сайтов, будет выполнен с правами того приложения, с которого пришел исходный html с тегом < script src=…>. Для того, чтобы это запретить, приложение должно использовать специальные безопасные заголовки.

**Вопрос 33**

Верно

Баллов: 1,00 из 1,00

Вид XSS, при котором вредоносный код передается в запросе и возвращается в ответе сервера на этот же запрос

a. Blind stored
b. DOM based
c. Stored
d. Reflected ✓

Обратная связь: это отраженная атака (или reflected)

**Вопрос 34**

Верно

Баллов: 1,00 из 1,00

Можно ли встроить javascript на страницу пользователя, не используя тег < script>

a. Да ✓
b. Нет

**Вопрос 35**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода, создающего HTML с внедрением пользовательского ввода из $searchQuery. К пользовательскому вводу применено кодирование HTML Encoding. Является ли данное приложение безопасным для встраивания xss?
< script src="< ?php echo htmlentities($searchQuery, ENT_QUOTES); ?>">< / script>

a. Нет ✓
b. Да

Обратная связь: в данном примере кодирования HTML Encoding недостаточно, т.к. встраивание происходит в атрибут src и требует другого способа защиты.

**Вопрос 36**

Верно

Баллов: 1,00 из 1,00

Как называется http заголовок, который запрещает отображать сайт в iframe. Это помогает защищать сайт от атак типа clickjacking

Ответ: X-Frame-Options ✓

**Вопрос 37**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода, создающего HTML с внедрением пользовательского ввода из $searchQuery. К пользовательскому вводу применено кодирование HTML Encoding. Является ли данное приложение безопасным для встраивания xss?
< td class="< ?php echo htmlentities($searchQuery); ?>" >

a. Да
b. Нет

Обратная связь: в данном примере кодирования HTML Encoding достаточно, т.к. поскольку строка обрамлена кавычками, и встроить дополнительный атрибут так просто не получится.

**Вопрос 38**

Неверно

Баллов: 0,00 из 1,00

При встраивании вредоносного скрипта в параметры запроса (через ссылку), пользователь может заподозрить подвох и не перейти по подозрительной ссылке. Какой способ может использовать злоумышленник, чтобы скрыть подозрительно выглядящую ссылку (название способа или название сервиса, одно слово)

Ответ: HTML Encoding

**Вопрос 39**

Верно

Баллов: 1,00 из 1,00

Может ли вредоносное приложение, внедренное на атакуемый сайт с помощью XSS, изменять элементы страницы (например, создавать новые формы и разделы на странице)?

a. Да, но только если приложение присылает нужный CORS заголовок
b. Нет
c. Да

Обратная связь: javascript приложение может модифицировать DOM страницы, для этого не требуется дополнительных ограничений.

**Вопрос 40**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода, создающего HTML с внедрением пользовательского ввода из $searchQuery. К пользовательскому вводу применено кодирование HTML Encoding. Является ли данное приложение безопасным для встраивания xss?
< script> var name = < ?php echo htmlentities($searchQuery); ?>; < /script>

a. Нет
b. Да

**Вопрос 41**

Верно

Баллов: 1,00 из 1,00

Может ли вредоносное приложение, внедренное на атакуемый сайт с помощью XSS, получить доступ к хранилищу cookie данного сайта?

a. Да, но только при работе по безопасному протоколу
b. Да, но только если приложение присылает нужный CORS заголовок
c. Нет
d. Да

Обратная связь: javascript приложение может получить доступ к хранилищу cookie, для этого не требуется дополнительных ограничений.

**Вопрос 42**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода страницы создающего HTML с внедрением пользовательского ввода из $searchQuery. Является ли данное приложение безопасным для встраивания xss?
<a href=http://www.somesite.com?test=<?php echo htmlentities($searchParams, ENT_QUOTES); ?> >link</a >

a. Нет
b. Да

**Вопрос 43**

Верно

Баллов: 1,00 из 1,00

Приведен пример кода, создающего HTML с внедрением пользовательского ввода из $searchQuery. К пользовательскому вводу применено кодирование Javascript Encoding (кодирование в unicode). Является ли данное приложение безопасным для встраивания xss?
< script> var name = "< ?php echo json_encode($searchQuery); ?>"; < /script>

a. Да
b. Нет

**Вопрос 44**

Верно

Баллов: 1,00 из 1,00

Как называется атака, при которой злоумышленник открывает атакуемый сайт на невидимом слое (например внутри фрейма) и отображает другую страницу поверх с наложением элементов контроля, так что при клике на форму на видимой странице, пользователь одновременно не осознавая кликает по форме, которая скрытаот отображения и создает запрос к атакуемому сайту.

Ответ: Clickjacking

**Вопрос 45**

Верно

Баллов: 1,00 из 1,00

Верно ли утверждение: используя XSS атаку, злоумышленник может сделать серию последовательных запросов от лица пользователя к атакуемому приложению, например для обхода защиты csrf token

a. Нет
b. Да, но только при использовании незащищенного протокола http
c. Да

Служба поддержки сайта

Вы зашли под именем Новиков Виталий Сергеевич (Выход)