

## Exam Report: 12.2.10 Practice Questions

Date: 5/11/2020 1:37:23 pm  
Time Spent: 2:10

Candidate: Garsteck, Matthew  
Login: mGarsteck

## Overall Performance

Your Score: 29%



View results by: ☐ Objective Analysis ☒ Individual Responses

## Individual Responses

### ▼ Question 1:

**Incorrect**

Which type of web application requires a separate application to be installed before you can use the app?

- ☐ Browser-based web app
- ☒ ~~Server-based web app~~
- ➡ ☐ Client-based web app
- ☐ Mobile apps

### Explanation

Client-based apps are run in a separate client-side application that needs to be installed before the web app can be used.

Browser-based web applications are run in a web browser.

Mobile apps are similar to other applications but are designed to work on mobile operating systems such as Apple iOS or Android.

Server-based computing is when you run applications on a server while forwarding their output to the clients.

### References

TestOut Ethical Hacker Pro - 12.2 Web Applications  
[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_SERVER\_01\_EH1]

### ▼ Question 2:

**Incorrect**

Which of the following best describes a web application?

- ☒ ~~Web applications need to be developed for every operating system.~~
- ☐ A web application taxes the client's processor and storage space.
- ☐ Web applications require special administration because they involve updates on client computers.
- ➡ ☐ A web application is software that has been installed on a web server.

### Explanation

A web application is software that has been installed on a web server. These applications process, store, and distribute information on demand.

A web application does not tax the client's processor and storage space as much as a locally installed application would.

Administration is easier because there are fewer installations and updates on client computers.

If the app can run over a browser, there is no need to develop the application for every operating system.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications  
[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_SERVER\_02\_EH1]

### ▼ Question 3: Correct

Upload bombing and poison null byte attacks are designed to target which of the following web application vulnerabilities?

- ☐ Flawed web design
- ☐ Buffer overflow
- ➡ ☒ Scripting errors
- ☐ Input validation

## Explanation

Upload bombing and poison null byte attacks are designed to target possible errors in scripting. Upload bombing loads tons of files onto a server, hoping to fill up the server's drives and crash the system. A poison null byte attack sends special characters to the script. If the script is unable to handle the characters, the script may provide access that it wouldn't otherwise.

As data is entered into an application, an input validation feature verifies the data. When there is no restriction on the data type, it's easy to make mistakes. This may seem like a small concern, but extreme errors can make data useless or crash a system.

A buffer should be limited in how much it can hold. It will stop accepting data when it hits a cap. However, if a developer forgot to place the necessary restrictions, the buffer will overflow when an application or process tries to send more data than a buffer is able to hold, resulting in corrupt or lost data.

Because web developers sometimes assume that their code is for their eyes only, sometimes they'll leave themselves notes in the code that serve as reminders, but are not intended for public viewing. Because it's so easy to access a web page's source code, developers should be cautious not to include information that could be valuable to an attacker.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications  
[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_VULNERABILITIES\_01\_EH1]

### ▼ Question 4: Correct

Which of the following statements is true regarding cookies?

- ☐ They load tons of files onto a server, hoping to fill up the server's drives and crash the system.
- ➡ ☒ They were created to store information about user preferences and web activities.
- ☐ They will overflow when an application or process tries to send more data than they are able to hold.
- ☐ They assign session IDs, encryption, and permissions to a specific client for a period of time.

## Explanation

Cookies are a necessary part of web applications; they are also a notable vulnerability. Because HTTP was not designed to save state information, cookies were created to store information about user preferences and web activities.

When a client effectively connects to a server, a session is created. This session assigns session IDs, encryption, and permissions to a specific client for a period of time.

Upload bombing and poison null byte attacks are designed to target possible scripting errors. Upload bombing loads tons of files onto a server, hoping to fill up the server's drives and crash the system. A

poison null byte attack sends special characters to the script. If the script is unable to handle the characters, the script may provide access that it wouldn't otherwise.

A buffer should have limits on how much it can hold. It will stop accepting data when it hits a cap. However, if a developer forgot to place the necessary restrictions, the buffer will overflow when an application or process tries to send more data than a buffer is able to hold, resulting in corrupt or lost data.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_VULNERABILITIES\_02\_EH1]

### ▼ Question 5:

Incorrect

Gathering information about a system, its components, and how they work together is known as \_\_\_\_\_?

☐ Spoofing

➡ ☐ Footprinting

☐ Attacking

☒ Analyzing

## Explanation

Footprinting is the process of gathering information about the system, its components, and how they work together.

Analyzing is examining the methodology and structure of a concept or feature, typically for purposes of explanation and interpretation.

Spoofing is when a hacker impersonates another device or user on a network in order to steal data, spread malware, or bypass access controls.

In a computer network, an attack is any attempt to expose, alter, disable, destroy, steal, or gain unauthorized access to or make unauthorized use of an asset.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_HACKING\_METHOD\_01\_EH1]

### ▼ Question 6:

Incorrect

Which of the following footprinting methods would you use to scan a web server to find ports that the web server is using for various services?

➡ ☐ Service discovery

☐ Detect firewalls

☐ Port scanning

☒ Detect proxy servers

## Explanation

Service discovery is a method of scanning a web server to find ports that are being used by services. These services can be used as pathways for application hacking.

Port scanning attempts to connect to TCP or UDP ports to determine what service is running on the server.

Proxy servers frequently include headers in the response header field, so it is possible to determine whether a target is using a proxy.

Web application firewalls (WAFs) analyze HTTP traffic to prevent web application attacks. To determine if the target is running a WAF, the cookie responses can be checked. Most WAFs include their own cookies in the response.


## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_HACKING\_METHOD\_02\_EH1]

### ▼ Question 7: Incorrect

You are analyzing the web applications in your company and have newly discovered vulnerabilities. You want to launch a denial-of-service (DoS) attack against the web server. Which of the following tools would you most likely use?

-  ☐ WebInspect
- ☒ WebScarab
- ☐ Wireshark
- ☐ Burp Suite

## Explanation

Denial-of-service (DoS) attacks are against a web server. Tools that can be used during this step include UrlScan, Nessus, and WebInspect. WebInspect is a web application security assessment tool that helps identify known and unknown vulnerabilities within the Web Application layer.

Burp Suite is a web spidering application that can be used as a local proxy. Once you have browsed every link and URL that you can find and completed every form and application available, Burp Suite provides a site map and identifies hidden application content or functions that it can find.

WebScarab is a tool for analyzing applications that use HTTP and HTTPS protocols.

Wireshark is one of the most well-known packet analyzers.


## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_HACKING\_METHOD\_03\_EH1]

### ▼ Question 8: Incorrect

HTTP headers can contain hidden parameters such as user-agent, host headers, accept, and referrer. Which of the following tool could you use to discover hidden parameters?

- ☐ Hackalert
- ☒ WinDump
-  ☐ Burp Suite
- ☐ Wikto

## Explanation

HTTP headers can contain hidden parameters such as user-agent, host headers, accept, and referrer. Tools used during this step include Burp Suite, HttPrint, and WebScarab. Burp Suite is a web spidering application that can be used as a local proxy. Once you have browsed every link and URL that you can find and completed every form and application available, Burp Suite provides a site map and identifies hidden application content or functions that it can find.

Wikto is a security scanner for Windows web servers. It checks for errors in code and monitors HTTP requests and responses.

Hackalert is a service that detects hidden malware in websites and advertisements.

WinDump is the Windows version of TCPdump.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_HACKING\_METHOD\_04\_EH1]

**Question 9:** Incorrect

Web applications use sessions to establish a connection and transfer sensitive information between a client and a server. Attacking an application's session management mechanisms can help you get around some of the authentication controls and allow you to use the permissions of more privileged application users. Which of the following type of attacks could you use to accomplish this?

- ☐ Web script injection
- ☐ Buffer overflow
- ➡ ☐ Cookie parameter tampering
- ☒ Hash stealing

**Explanation**

In a cookie parameter tampering attack, an attacker collects cookies and analyzes them to determine how the cookies are being generated. The attacker then uses tools to tamper with the parameters and replay them to the application.

In a web script injection attack, if user input is used in executed code, entries can be crafted to ignore the original data and execute commands on the server.

Buffer overflow injects large amounts of invalid data beyond the input field's capacity.

Hash stealing occurs when an attacker replaces a data source parameter value with a rogue SQL server that is running a sniffer. The attacker will use the sniffer to obtain password hashes when the application attempts to connect to the rogue server.

**References**

TestOut Ethical Hacker Pro - 12.2 Web Applications  
[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_HACKING\_METHOD\_05\_EH1]

**Question 10:** Correct

Which of the following types of injections can be injected into conversations between an application and a server to generate excessive amounts of spam email?

- ☐ SQL injection
- ➡ ☒ SMTP injection
- ☐ XPath injection
- ☐ LDAP injection

**Explanation**

With an SMTP injection, SMTP commands can be injected into conversations between an application and an SMTP server to generate excessive amounts of spam email.

An LDAP injection targets non-validated web application input vulnerabilities to get past LDAP filters and gain access to the database.

With SQL injection, a series of SQL queries are entered into the input fields to manipulate the database.

With XPath injection, altered strings are entered into input fields and are used to manipulate the XPath query in a way that interferes with the application's logic.

**References**

TestOut Ethical Hacker Pro - 12.2 Web Applications  
[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_HACKING\_METHOD\_06\_EH1]

**Question 11:** Incorrect

An attacker is attempting to connect to a database using a web application system account instead of user-provided credentials. Which of the following methods is the attacker attempting to use?

- ☒ Hijacking web credentials
- ☒ Password attacks
- ☐ Cookie exploitation
- ☐ Cookie parameter tampering

## Explanation

With the hijacking web credentials method, an attacker attempts to connect to the database using a web application system account instead of user-provided credentials.

With the cookie parameter tampering method, an attacker collects cookies and analyzes them to determine how the cookies are being generated. The attacker then uses tools to tamper with the parameters and replays them to the application.

With the password attacks method, passwords can be exploited using the change password, forgot password, or remember me functions. In some instances, passwords can be guessed.

With the cookie exploitation method, attackers can use script injection and eavesdropping techniques to collect this data from the cookies.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APPS\_HACKING\_METHOD\_07\_EH1]

### ▼ Question 12: Incorrect

Which of the following best describes the countermeasures you would take against a cross-site request forgery attack?

- ☒ Log off immediately after using a web application. Clear the history after using a web application, and don't allow your browser to save your login details.
- ☐ Set the secure flag on all sensitive cookies. Ensure that certificates are valid and are not expired. All non-SSL web page requests should be directed to the SSL page.
- ☒ ~~Use SSL for all authenticated parts of an application. Verify whether user information is stored in a hashed format. Do not submit session data as part of a GET or POST.~~
- ☐ Avoid using redirects and forwards. If you must use them, be sure that the supplies values are valid and the user has appropriate authorization.

## Explanation

The countermeasures for a cross-site request forgery attack are to log off immediately after using a web application. Clear the history after using a web application, and don't allow your browser to save your login details.

The countermeasures for an unvalidated redirects and forwards attack are to avoid using redirects and forwards. If you must use them, be sure that the supplies values are valid and the user has appropriate authorization.

The countermeasures for a broken authentication and session management attack are to use SSL for all authenticated parts of an application. Verify whether user information is stored in a hashed format. Do not submit session data as part of a GET or POST.

The countermeasures for an insufficient transport layer protection attack are to set the secure flag on all sensitive cookies. Ensure that certificates are valid and are not expired. All non-SSL web page requests should be directed to the SSL page.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APP\_COUNTER\_ATTACK\_01\_EH1]

### ▼ Question 13: Correct

The following are countermeasures you would take against a web application attack:

- Secure remote administration and connectivity testing.
- Perform extensive input validation.
- Configure the firewall to deny ICMP traffic.
- Stop data processed by the attacker from being executed.

Which of the following attacks would these countermeasures prevent?

- ☐ Directory traversal
- ☐ XSS attacks
- ☐ Web services attack

➡ ☒ DoS attacks

## Explanation

The countermeasures for a DoS attack are to:

- Secure remote administration and connectivity testing.
- Perform extensive input validation.
- Configure the firewall to deny ICMP traffic.
- Stop the attacker's data processing from being executed.

The countermeasures for an XSS attack are to:

- Validate all headers, cookies, query strings, hidden fields, and form fields against rigid specifications.
- Use a web application firewall.
- Do not trust all websites that use HTTPS.
- Encode input and output filters and filter all meta characters.
- Use testing tools during the design phase to detect and prevent errors in the application before it's put into production.
- Design standard scripts using private and public keys that will check for authenticated scripts.

The countermeasures for a web services attack are to:

- Configure WSDL access control permissions.
- Use multiple security credentials.
- Configure firewalls and IDS systems to filter SOAP and ZML syntax and detect web service anomalies.
- Maintain an updated, secure store of XML schemas.
- Implement centralized in-line requests and response schema validation.

The countermeasures for a directory traversal are to:

- Update web servers with security patches on a regular basis.
- Limit access to the secure areas of the website.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APP\_COUNTER\_ATTACK\_02\_EH1]

▼ Question 14: Incorrect

You are looking for a web application security tool that runs automated scans looking for vulnerabilities susceptible to SQL injection, cross-site scripting, and remote code injection. Which of the following web application security tools would you most likely use?

- ☒ ~~VampireScan~~
- ☐ N-Stalker

➡ ☐ Netsparker

☐

 dotDefender

## Explanation

Netsparker runs automated scans looking for vulnerabilities susceptible to SQL injection, cross-site scripting, and remote code injection.

N-Stalker is a suite of assessment checks that can improve the overall security of your web applications. It contains assessment checks for code injection, cross-site scripting, parameter tampering, and web server vulnerabilities.

VampireScan is a tool that allows users to test their web infrastructure and application for vulnerabilities. It provides insight about addressing risk vulnerabilities on a low, medium, or high scale.

dotDefender is a software web application firewall that inspects HTTP and HTTPS traffic. It also detects and blocks SQL injection attacks.

## References

TestOut Ethical Hacker Pro - 12.2 Web Applications

[e\_web\_apps\_eh1.exam.xml Q\_WEB\_APP\_COUNTER\_SECURE\_TOOLS\_01\_EH1]