



Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER -
SECURITY IMPLEMENTATION

Progresso do curso

Módulo 11. Session Hijacking

Módulo 12. Evading IDS, Firewalls, and Honeypots

Módulo 13. Hacking Web Servers

Módulo 14. Hacking Web Applications

Módulo 15. SQL Injection

Conceitos de Aplicações WEB:

As aplicações web são as aplicações que são executadas no servidor web. Tecnologias Web 2.0 são utilizadas por todos os aplicativos baseados em servidores web, tais como a comunicação com os usuários, clientes etc. A aplicação web é composta de muitas camadas de funcionalidades. No entanto, considera-se uma arquitetura de três camadas que consiste em camadas de apresentação, lógica e de dados.

O HTTP é o meio de comunicação entre o servidor e o cliente. Normalmente, ele opera através da porta TCP 80, mas também pode se comunicar através de uma porta não padrão. Aplicações web fornecem uma interface entre os usuários finais e servidores web através do conjunto de páginas web que são geradas pelo servidor.

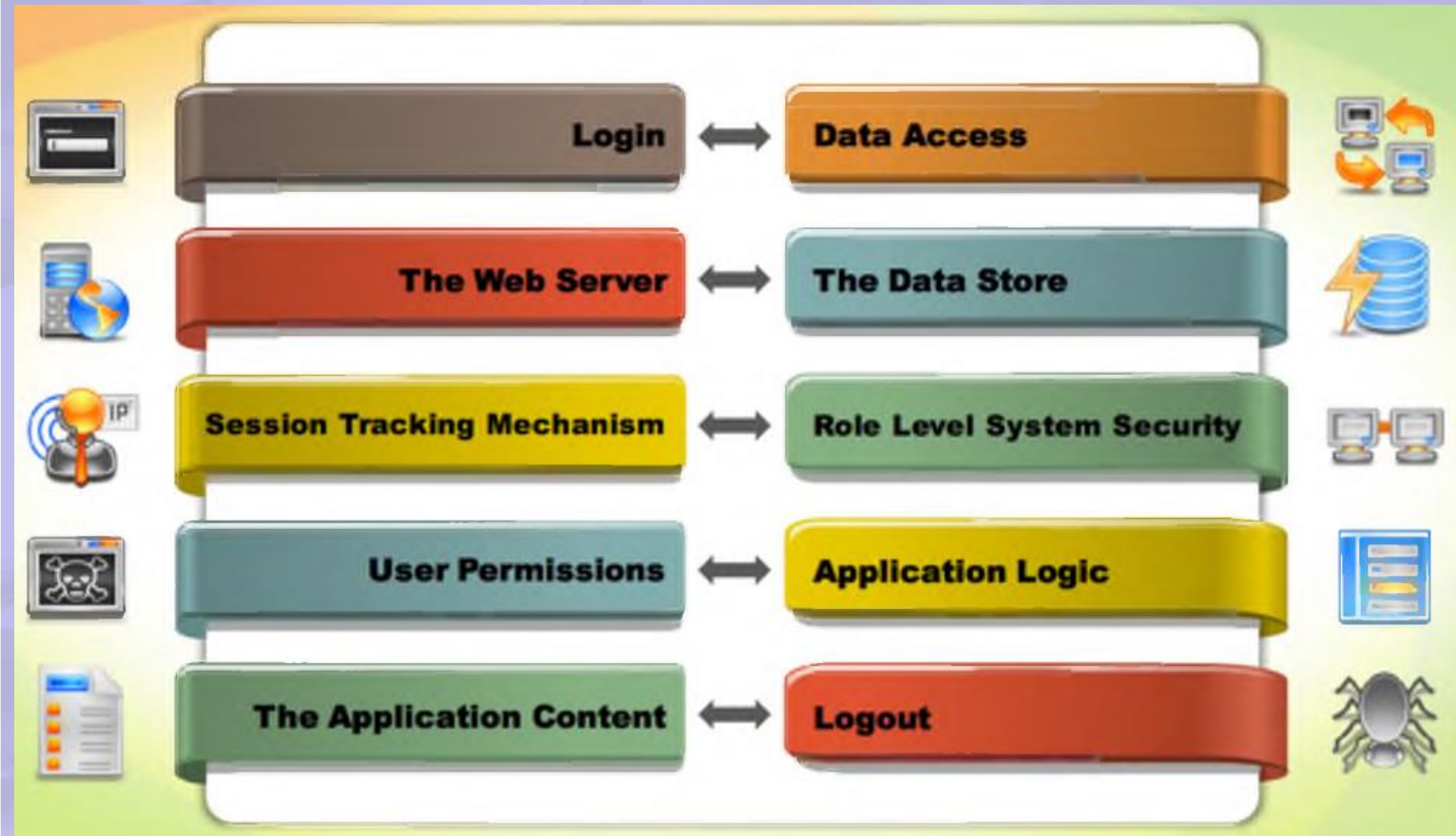


CEHv12 (ANSI)

14.Hacking Web Applications

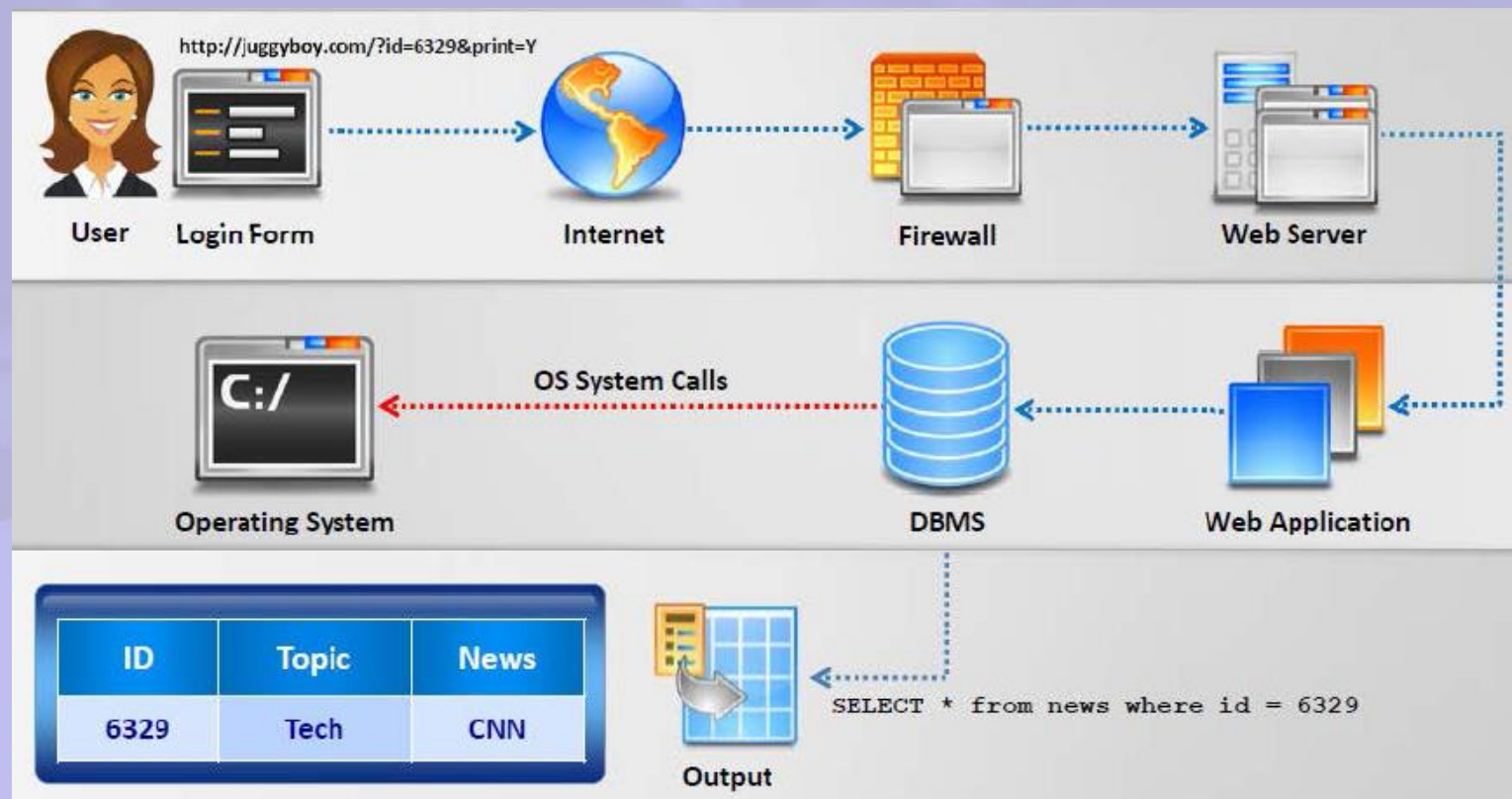
Componentes de uma aplicação web

- Login
- Acesso de dados
- O servidor Web
- O armazenamento de dados
- Mecanismo de rastreamento de sessão
- Nível de Função da Segurança do Sistema
- Permissão do usuário
- Lógica de Aplicação
- O conteúdo da aplicação
- Logout



Funcionamento de uma aplicação web

- Primeiro o usuário digita o nome do site no navegador e a solicitação é enviada para o servidor web.
- Ao receber o pedido, o servidor web verifica a extensão de arquivo.
- Se o usuário solicita uma página web simples com uma HTM ou extensão HTML, o servidor web processa o pedido e envia o arquivo para o navegador do usuário.
- Se o usuário solicita uma página web com uma extensão CFM, CFML, ou CFC, a solicitação deve ser processada pelo servidor da aplicação web.



OBS: Um arquivo CFM é uma página web que contém código ColdFusion ou CFML (ColdFusion Markup Language). Ele é executado dinamicamente por um servidor web ColdFusion quando a página é acessada por um usuário. Os arquivos CFM podem executar aplicativos e scripts do ColdFusion escritos no CFScript e podem referenciar informações do banco de dados, gerar formulários e criar relatórios PDF em tempo real.

Vetores de ataque em aplicações web

- **Manipulação de parâmetro**

O atacante fornece o valor de entrada errado para os serviços web e ganha o controle sobre os comandos SQL, LDAP, XPATH e shell. Quando os valores incorretos são fornecidos aos serviços web, eles se tornam vulneráveis e são facilmente atacados.

- **XML Poisoning**

Atacantes fornecem documentos XML manipulados que quando executado pode perturbar a lógica do método de análise no servidor. Quando enormes XML's são executadas na camada de aplicação, eles podem ser facilmente comprometidos pelo atacante para lançar o seu ataque e recolher informações.

- **Misconfiguration**

O atacante explora as vulnerabilidades nos servidores web e tentam burlar o método de validação e obter acesso aos dados confidenciais armazenados no servidor.

- **Validação de cliente**

A maioria das validações do lado do cliente tem que ser suportada pela autenticação do lado do servidor. As rotinas AJAX podem ser facilmente manipuladas, que por sua vez se torna uma maneira para os atacantes lidarem com injeção de SQL, injeção LDAP, etc. e negociar os principais recursos da aplicação web.

- **Web service routing issues/Problemas de roteamento do serviço da Web**

As mensagens SOAP são permitidas para acessar diferentes nós na Internet pelos WS-Routers. A exploração dos nós intermediários pode dar acesso às mensagens SOAP que são comunicadas entre os pontos finais.

- **Cross-site scripting**

Se qualquer código java script infectado for executado, os navegadores podem ser explorados para obter informações.

Ameaças de aplicações web

- **Cookie Tampering/Adulteração de cookie**

Adulteração de cookies é o método de envenenamento ou adulteração dos cookie do cliente. Os cookies persistentes e não persistentes podem ser modificados usando ferramentas diferentes.

- **Directory Traversal/Passagem de diretório**

Directory traversal é uma exploração de diretórios HTTP restritos através do qual os atacantes são capazes de acessar e executar comandos fora do diretório raiz do servidor web através da manipulação da URL.

- **Validação de input**

A fim de contornar o sistema de segurança, os atacantes adulteram as solicitações HTTP, URL, cabeçalhos, campos de formulário, campos ocultos, query strings e etc.

- **Cross-site scripting (XSS)**

Cross-site scripting é um método em que um atacante injeta tags HTML ou scripts em um site-alvo.

- **Form Tampering/Adulteração de Formulário**

Este tipo de ataque manipula os parâmetros trocados entre o cliente e servidor, a fim de modificar os dados da aplicação, tais como credenciais de usuários e permissões, preço e quantidade de produtos, etc.

- **SQL Injection/Ataques de injeção SQL**

Injeção SQL é uma técnica de injeção de código que usa a vulnerabilidade do banco de dados. O atacante injeta um código malicioso na string que é posteriormente repassada para SQL Server para serem executadas.

Ameaças de aplicações web

- Denial-of-Service (DoS)

Um ataque de negação de serviço é um método de ataque que pretende encerrar as operações de um site ou um servidor e tornar o acesso indisponível.

- Ataques de injeção de arquivos e validação de entradas

Ataques de validação entrada e de injeção de arquivo referem-se aos ataques realizados através do fornecimento de uma entrada não validada ou pela injeção de arquivos em uma aplicação web.

- Ataque Cross-Site Request Forgery (CSRF)

O navegador do usuário é solicitado por uma página web malicioso para enviar solicitações para um site malicioso, onde várias ações vulneráveis são realizadas.

- Ataques de buffer overflow

A maioria das aplicações web são designadas a sustentar certa quantidade de dados. Se esse montante for ultrapassado, a aplicação pode apresentar algum outro comportamento vulnerável.

OBS: Um **vetor de ataque**, ou **vetor de ameaça**, é uma maneira de os invasores entrarem em uma rede ou sistema.

Uma **superfície de ataque** é a combinação de todos os vetores de ataque disponíveis para um invasor. Quanto mais **vetores de ataque** uma organização tiver, maior será a **superfície de ataque**.

Uma **ameaça** em segurança da informação é qualquer fator ou ação capaz de interferir e causar danos à integridade, à confidencialidade, à autenticidade e à disponibilidades de dados e informações sobre uma empresa.

O **risco** é uma função das **ameaças** que exploram vulnerabilidades para obter, danificar ou destruir ativos. Portanto, ameaças (reais, conceituais ou inerentes) podem existir, mas se não houver vulnerabilidades, haverá pouco / nenhum risco.

Input não validado



An attacker exploits input validation flaws to perform cross-site scripting, buffer overflow, injection attacks, etc. that result in **data theft and system malfunctioning**



`http://www.juggyboy.com/login.aspx?user=jasons@pass=springfield`

Browser Post Request

```
string sql = "select * from Users  
where  
user ='" + User.Text + "'  
and pwd='" + Password.Text + "'";
```

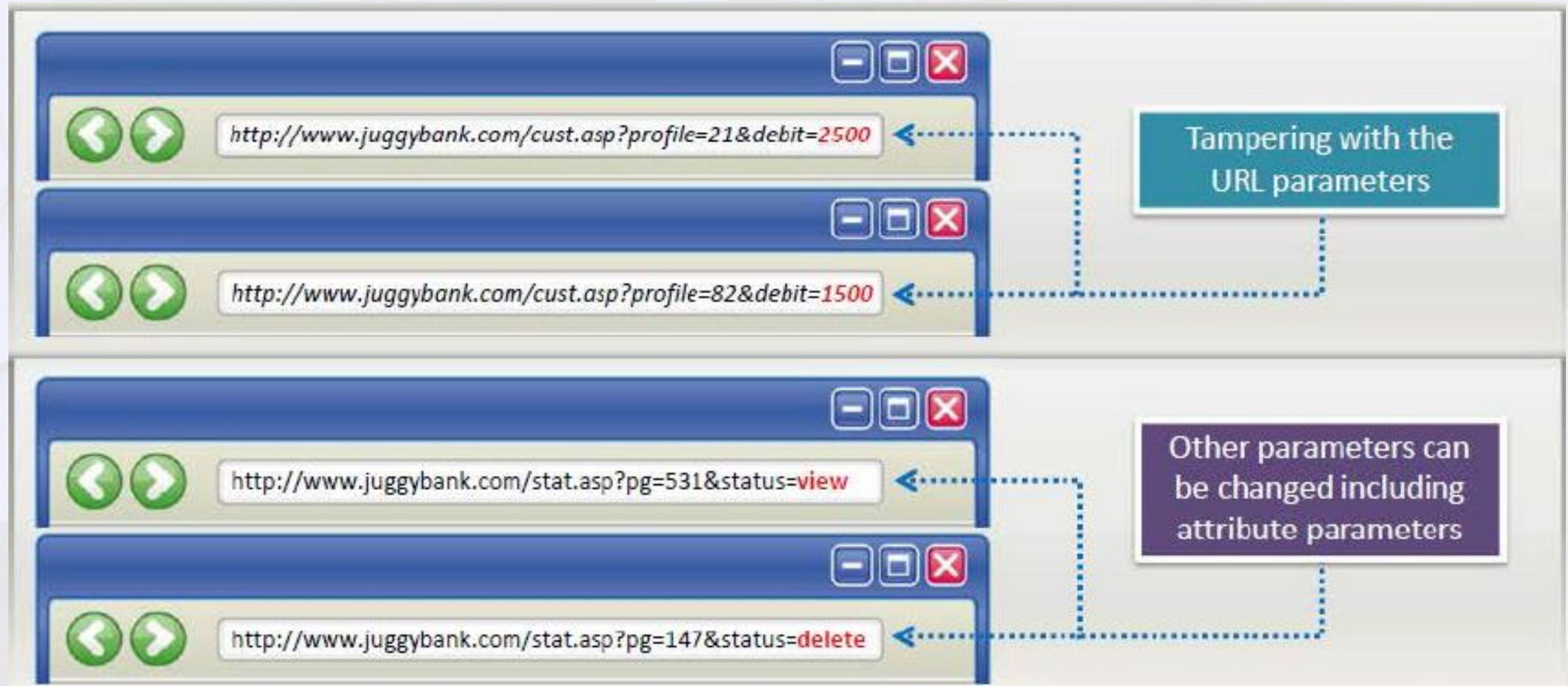
Modified Query



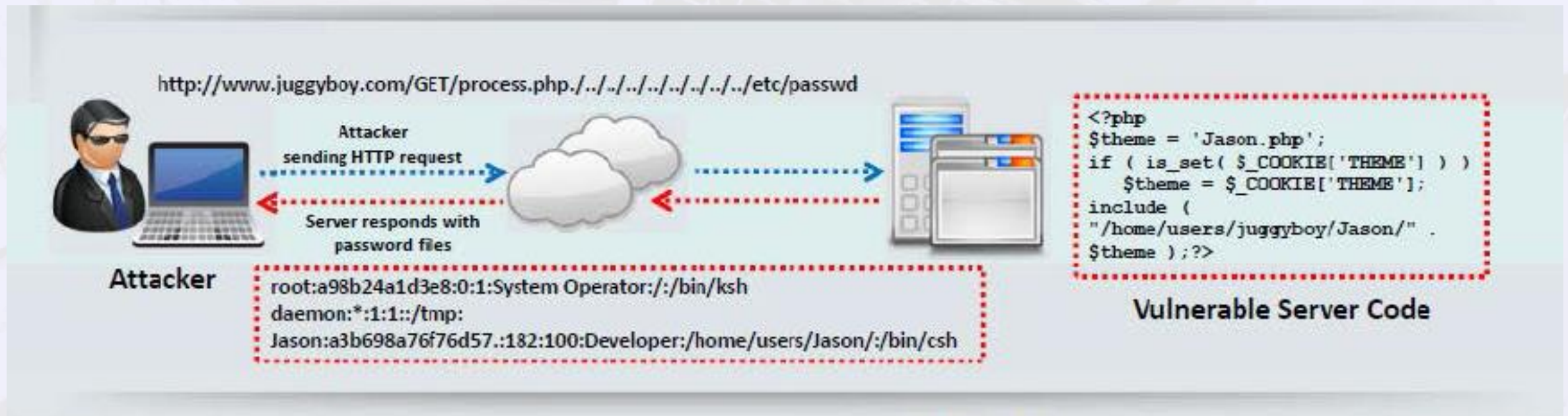
Database

Browser input not
validated by the web
application

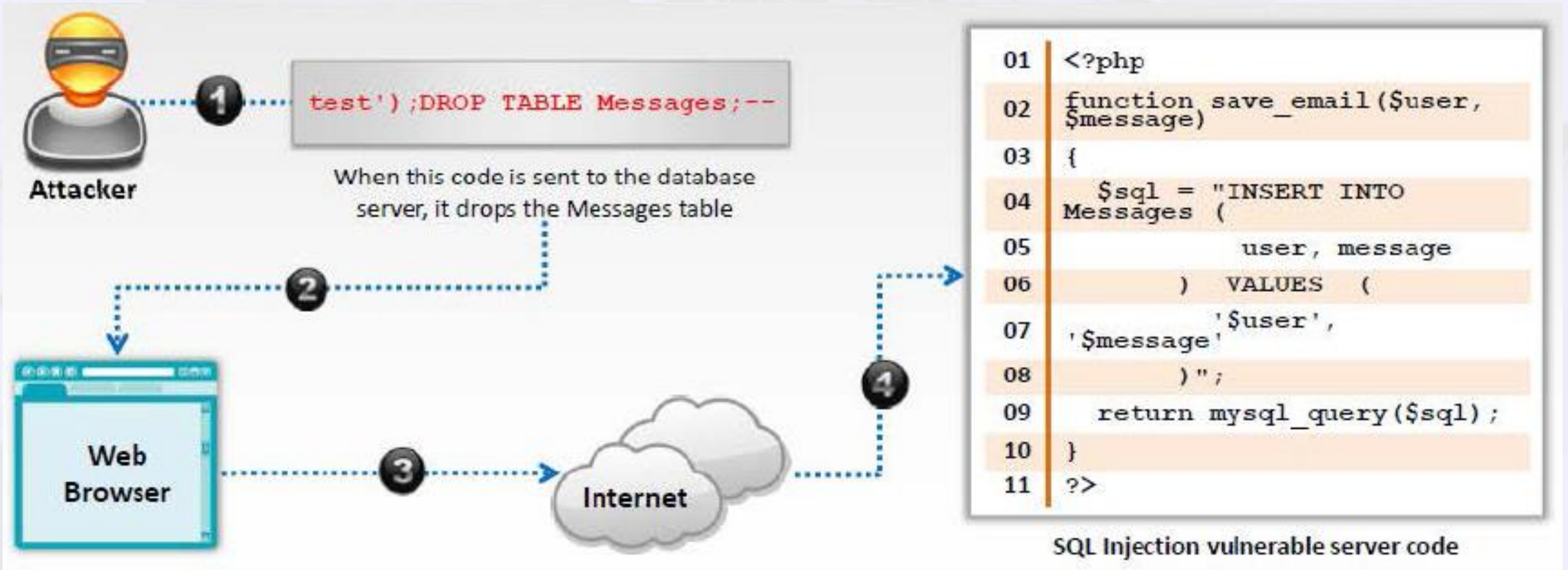
Adulteração de parâmetro



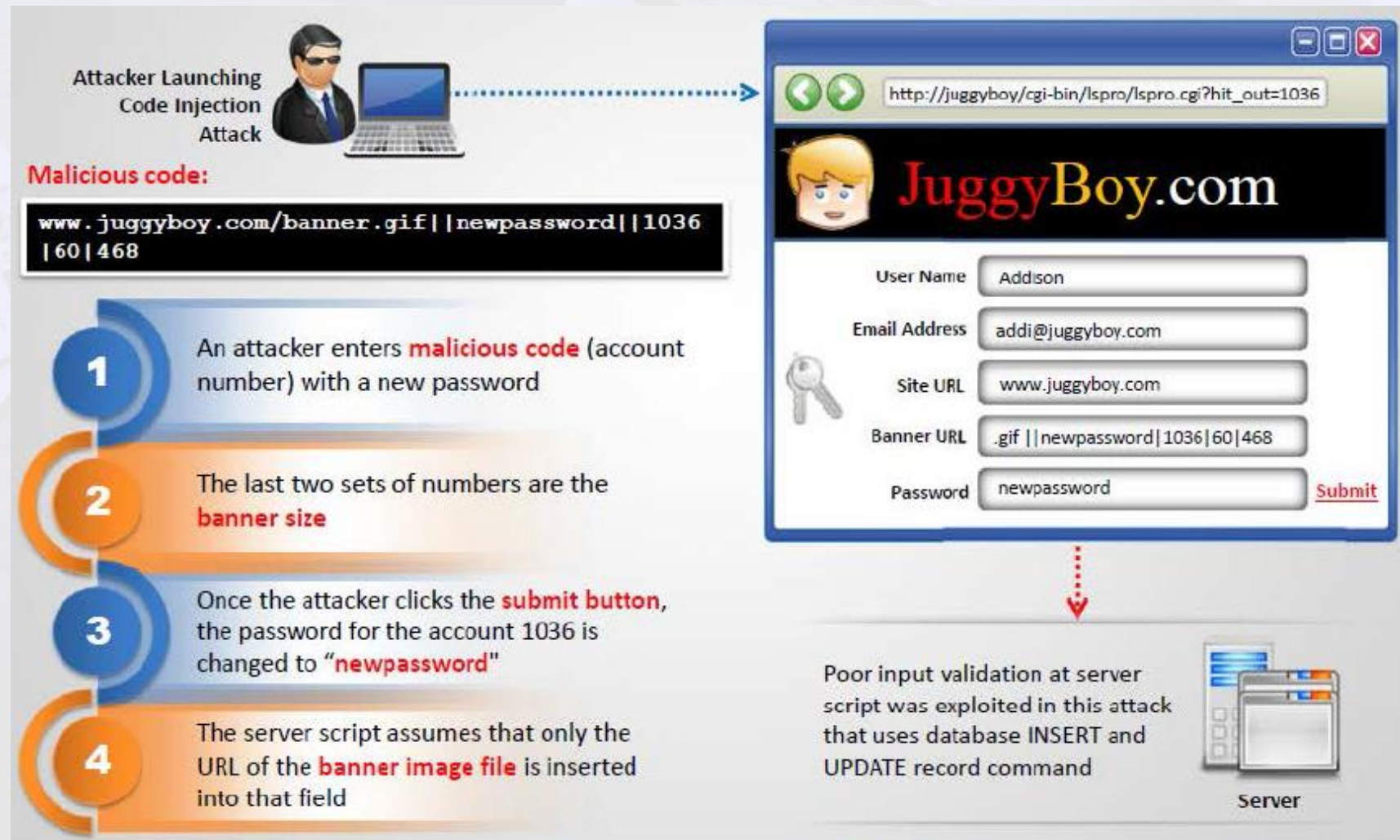
Directory Traversal



SQL Injection



Command Injection



Manipulação de campos ocultos

HTML Code


```
<form method="post"
  action="page.aspx">
  <input type="hidden" name=
    "PRICE" value="200.00">
  Product name: <input type=
    "text" name="product"
    value="Juggyboy Shirt"><br>
  Product price: 200.00"><br>
  <input type="submit" value=
    "submit">
</form>
```

Normal Request

`http://www.juggyboy.com/page.aspx?product=Juggyboy%20Shirt&price=200.00`

Attack Request

`http://www.juggyboy.com/page.aspx?product=Juggyboy%20Shirt&price=2.00`



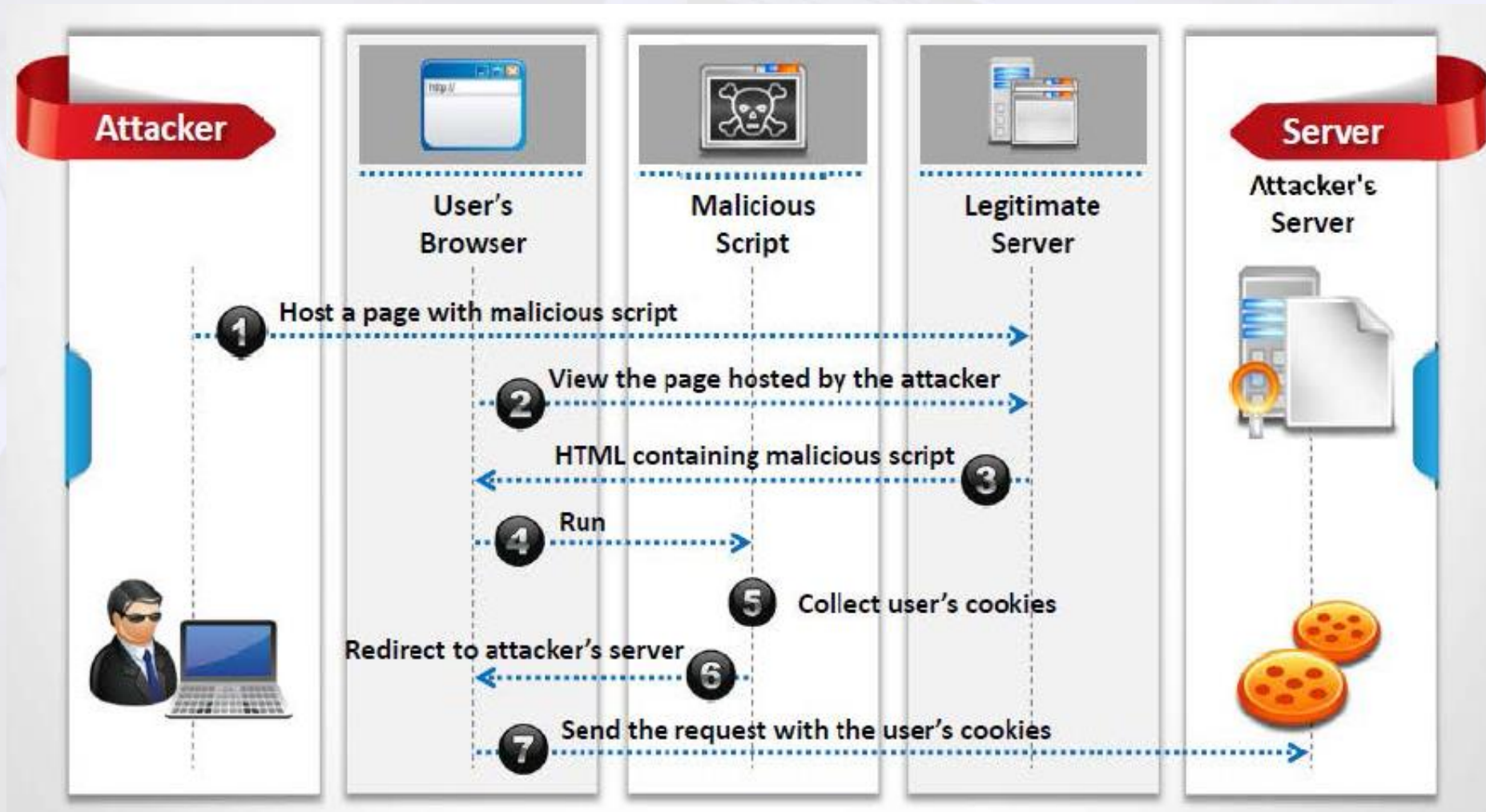
Product Name

Product Price

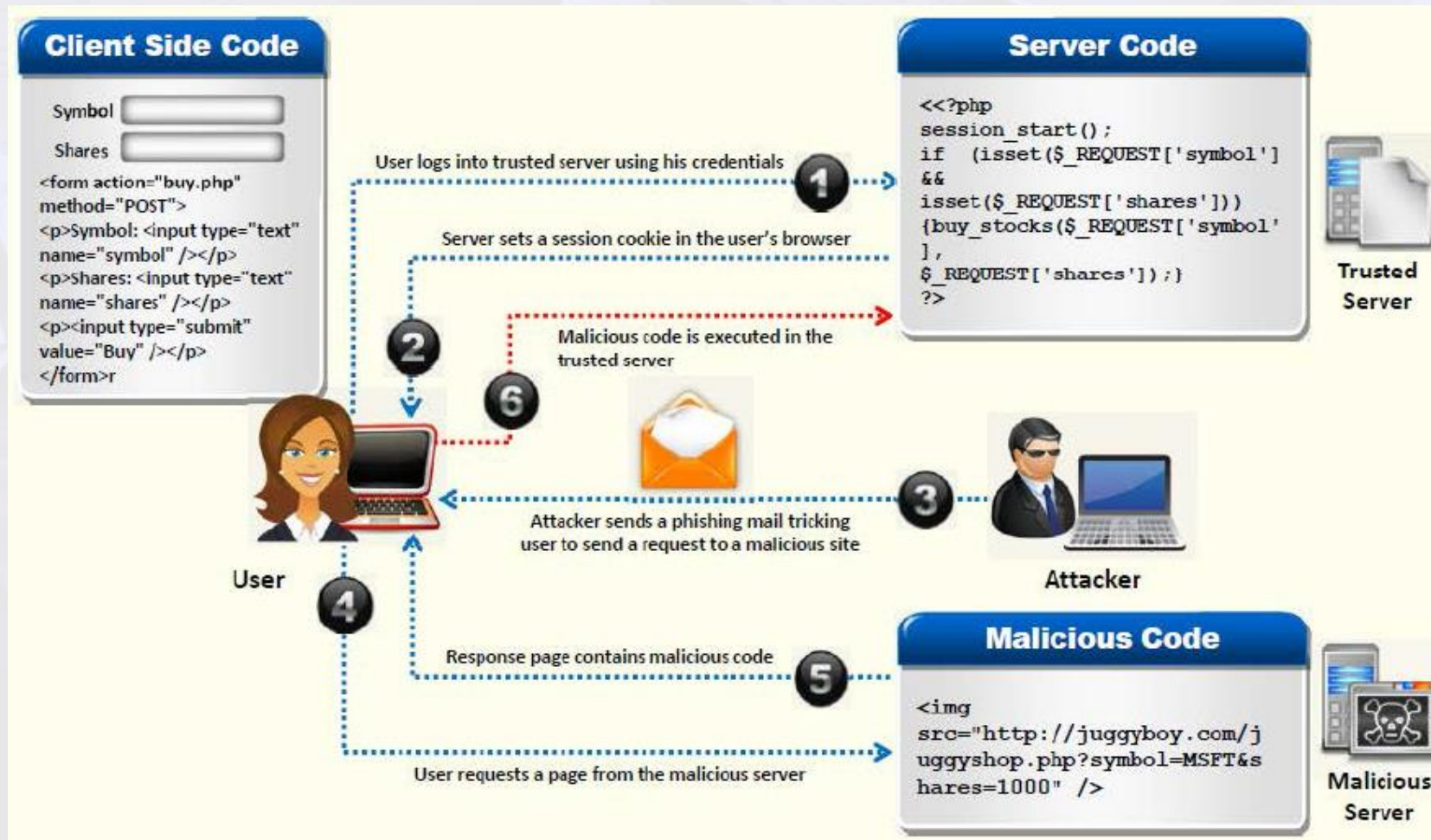
[Submit](#)

- When a user makes selections on an HTML page, the selection is typically stored as form field values and sent to the application as an **HTTP request (GET or POST)**
- HTML can also store field values as hidden fields, which are **not rendered to the screen** by the browser, but are collected and submitted as parameters during form submissions
- Attackers can examine the **HTML code of the page** and change the hidden field values in order to change post requests to server









Cross-Site Script - XSS



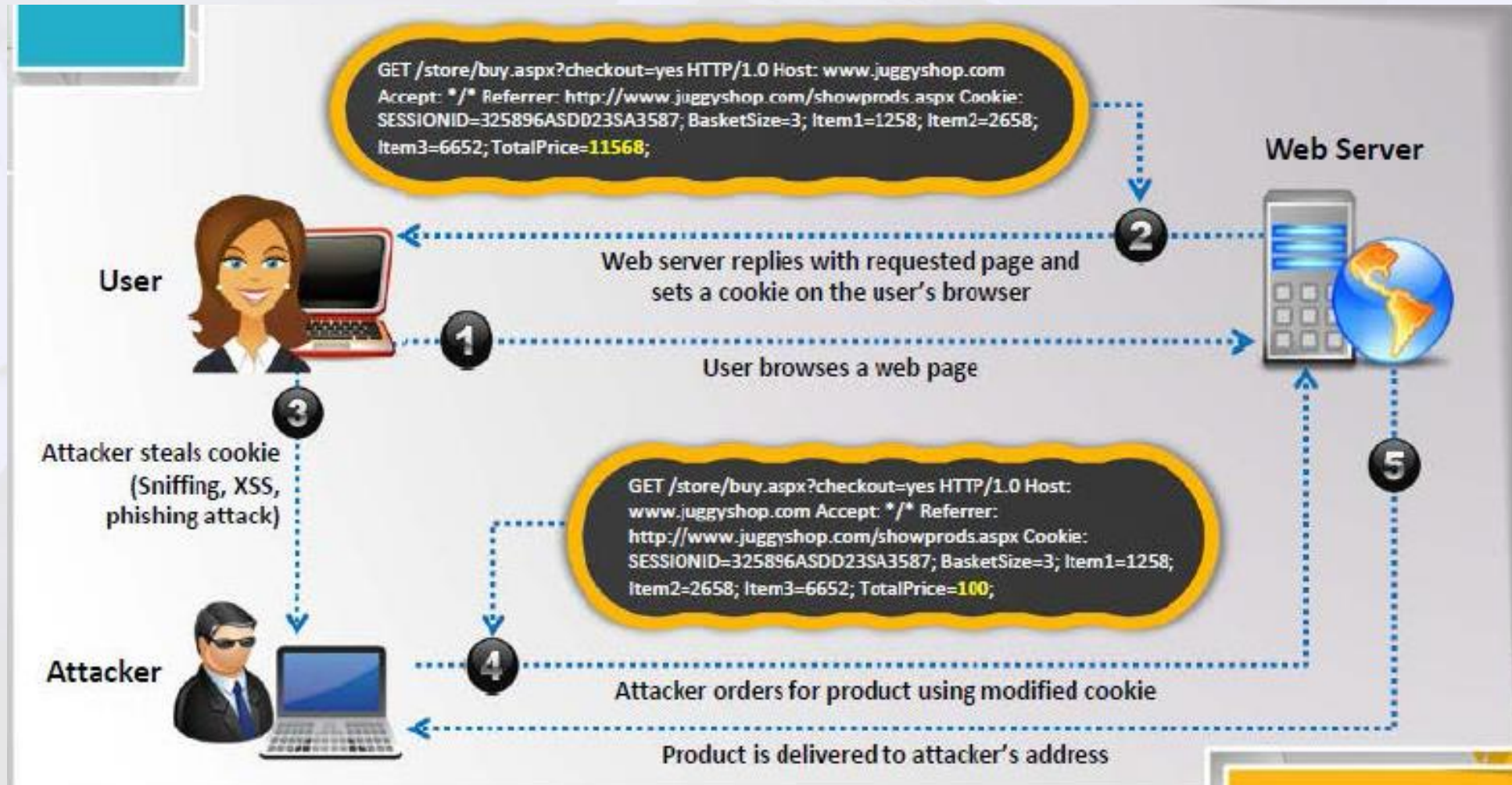
Cross-site request forgery - CSRF



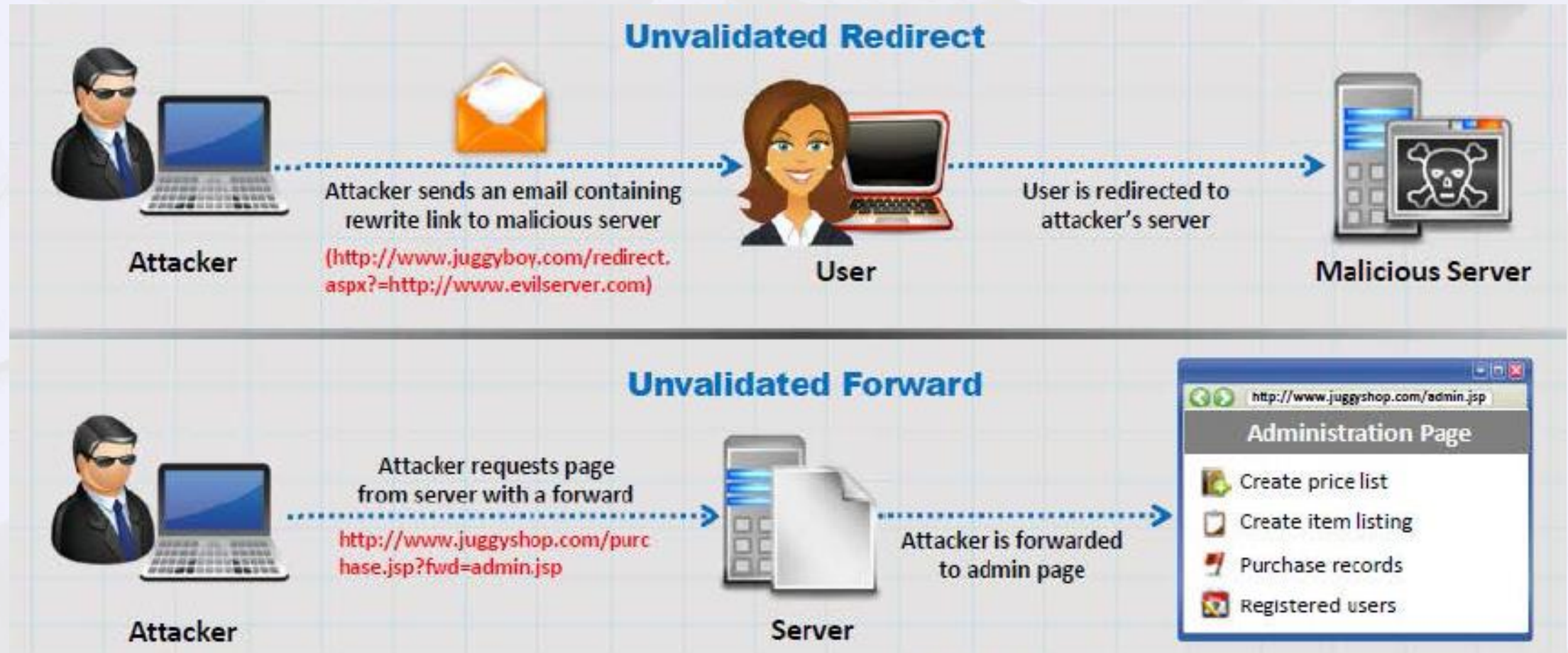
DoS

User Registration DoS 	 <p>The attacker could create a program that submits the registration forms repeatedly, adding a large number of spurious users to the application</p>
Login Attacks 	 <p>The attacker may overload the login process by continually sending login requests that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond</p>
User Enumeration 	 <p>If application states which part of the user name/password pair is incorrect, an attacker can automate the process of trying common user names from a dictionary file to enumerate the users of the application</p>
Account Lock Out Attacks 	 <p>The attacker may enumerate usernames and attempt to authenticate to the site using a username and incorrect passwords, which will lock out the user account after the specified number of failed attempts.</p>

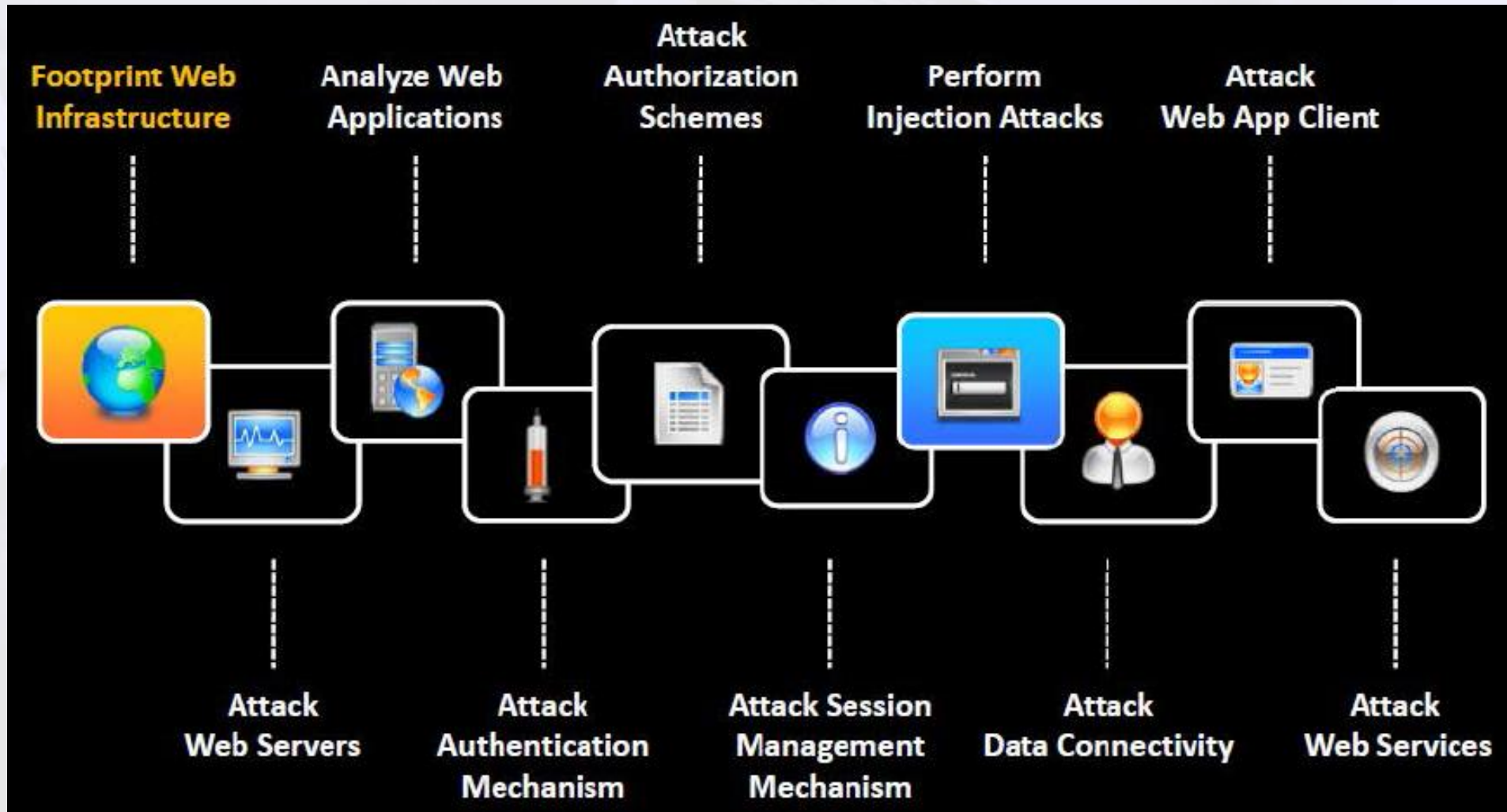
Cookie/Session Poisoning



Redirecionamentos não validados



Metodologia de análise em aplicações web



Footprint em infraestruturas Web

- Descoberta do servidor
- Descoberta de serviços
- Descoberta de conteúdo oculto
- Lookup Whois
- DNS Interrogation
- Port Scanning

Ataque em Servidores Web

01

After identifying the web server environment, **scan the server for known vulnerabilities** using any web server vulnerability scanner

02

Launch web server attack to exploit identified vulnerabilities

03

Launch Denial-of-Service (DoS) against web server

Tools used

1

UrlScan

2

Nikto

3

Nessus

4

Acunetix Web Vulnerability

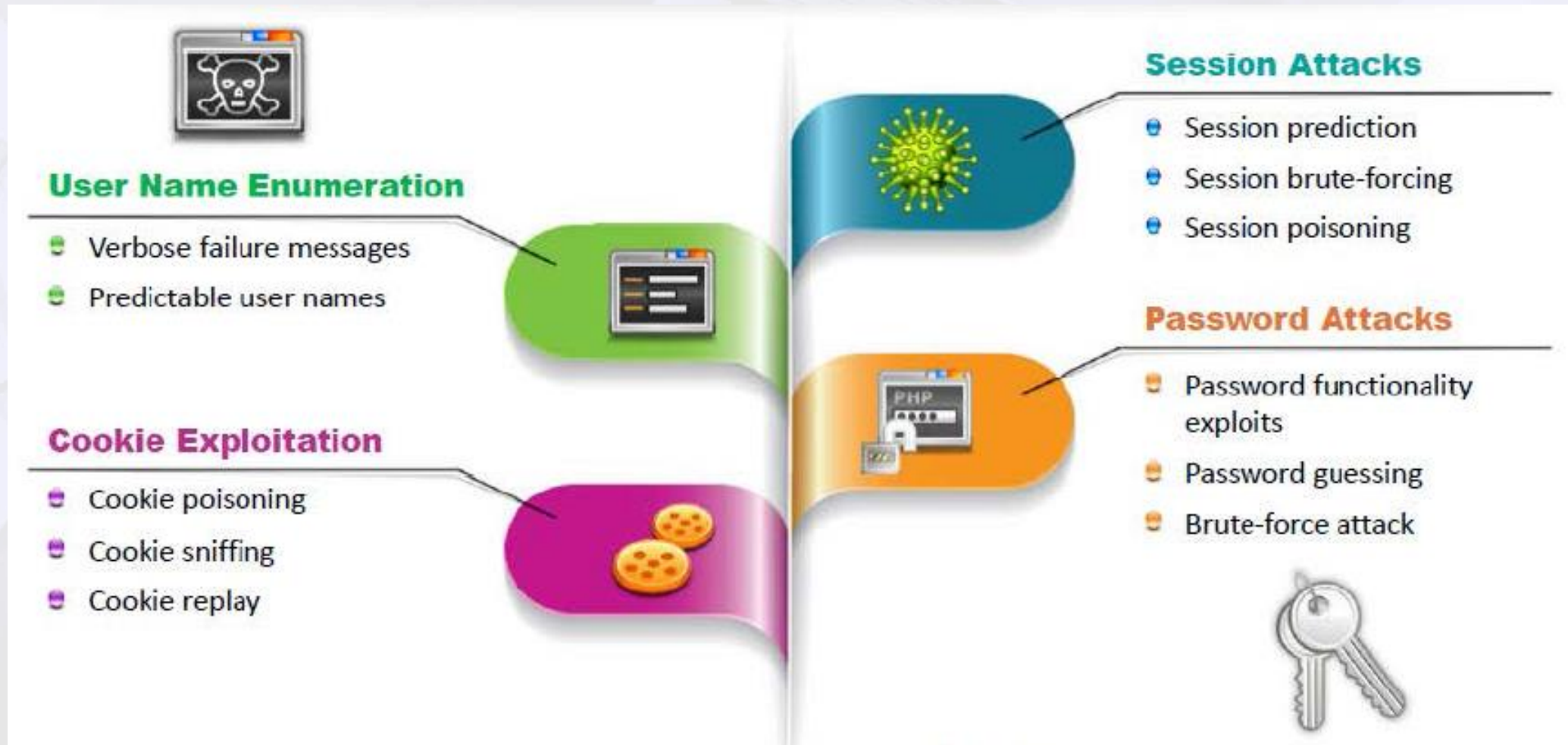
5

WebInspect

Análise de Aplicações Web

- Identificar pontos de entrada para input de usuário
- Identificar a funcionalidade do lado do servidor
- Identificar as tecnologias do lado do servidor
- Mapear a superfície de ataque

Ataque em Mecanismos de Autenticação



Ataque ao Esquema de Autorização

Em um ataque de autorização, o atacante primeiro encontra a conta com menor privilégio e em seguida, se autentica como usuário autêntico e lentamente escala privilégios para acessar recursos protegidos, os atacantes manipulam as solicitações HTTP para subverter os regimes de autorização da aplicação, modificando campos de entrada que se relacionam com ID de usuário, nome do usuário, grupo de acesso, custo, nomes de arquivos, identificadores de arquivo e etc.

Ataque ao Mecanismo de Gerenciamento de Sessão

O mecanismo de gerenciamento de sessão é o componente chave de segurança na maioria das aplicações web. Um intruso que burle o gerenciamento de sessão da aplicação pode facilmente contornar os controles de autenticação e mascarar-se como outro usuário da aplicação sem conhecer as suas credenciais.

A fim de gerar um token de sessão válido, o atacante executa:

- Previsão de token de sessão
- Manipulação de tokens de sessão

Uma vez que o atacante gera o token de sessão válido, ele tenta explorar a manipulação de token de sessão nas seguintes formas:

- Session Hijacking
- Session Replay
- Ataque man-in-the-middle

Executar ataques de injeção

Web Scripts Injection

Se a entrada do usuário é usada no código que é executado de forma dinâmica, digitar entradas maliciosas burlam o contexto dos dados e executam comandos no servidor.

OS Commands Injection

Explora o sistema operacional inserindo códigos maliciosos em campos de entrada se a aplicação utiliza a entrada do usuário em um comando de nível de sistema.

SMTP Injection

Injeta comandos SMTP arbitrários na aplicação e em conversas do servidor SMTP para gerar grandes volumes de spam.

SQL Injection

Insere uma série de consultas SQL maliciosos em campos de entrada para manipular diretamente o banco de dados.

LDAP Injection

Tira proveito de entradas não validadas na aplicação web para passar filtros LDAP para obter acesso direto às bases de dados.

Ataque em Dados de Conectividade




Before Injection

```
"Data Source=Server,Port; Network Library=IBMSSOCN; Initial Catalog=DataBase;  
User ID=Username; Password=pwd;"
```

After Injection

```
"Data Source=Server,Port; Network Library=IBMSSOCN; Initial Catalog=DataBase;  
User ID=Username; Password=pwd; Encryption=off"
```

Ataque ao Cliente de aplicação Web

Cross-Site Scripting		Redirection Attacks
HTTP Header Injection		Frame Injection
Request Forgery Attack		Session Fixation
Privacy Attacks		ActiveX Attacks



Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.