# Web Application Attacks in Healthcare

July 21, 2022

# Agenda

- Background on Web Applications
- What Are Web Application Attacks?
- What Is the Impact to Health Sector?
- Mitigations for Common Attacks
- Free and Low-Cost Resources
- Conclusion and Major Takeaways

**Slides Key:**

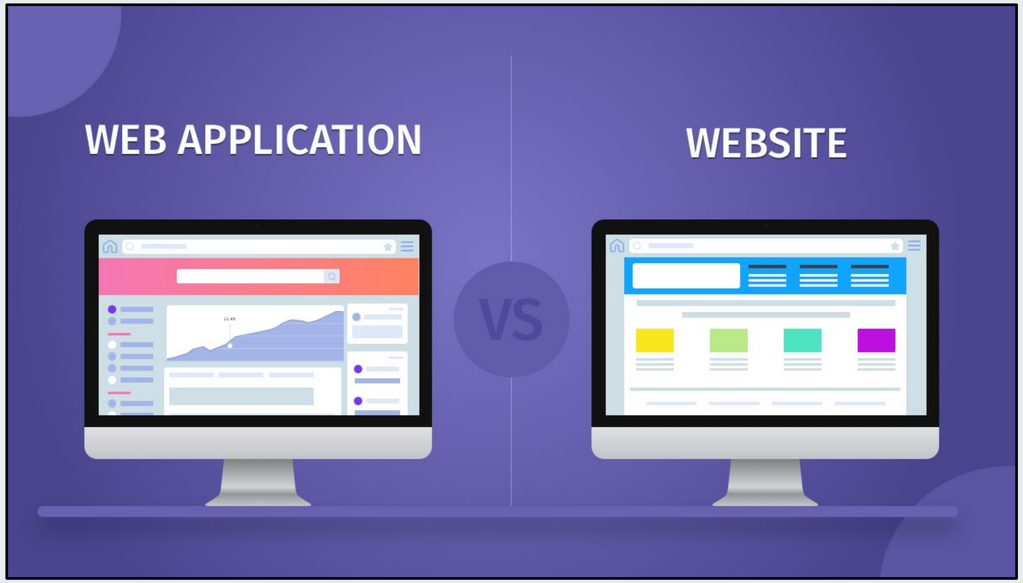
**Non-Technical:** Managerial, strategic and high-level (general audience)

**Technical:** Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

# What Are Web Applications?

## How do you define web application? What are considered web applications?

- A web application (or web app) is an application program that is stored on a remote server and delivered over the Internet through a browser interface.
- Web applications include online forms, shopping carts, word processors, spreadsheets, video and photo editing, file conversion, file scanning, and email programs such as Gmail.
- Unlike websites, web applications require user interaction and have a backend database with authentication and more.

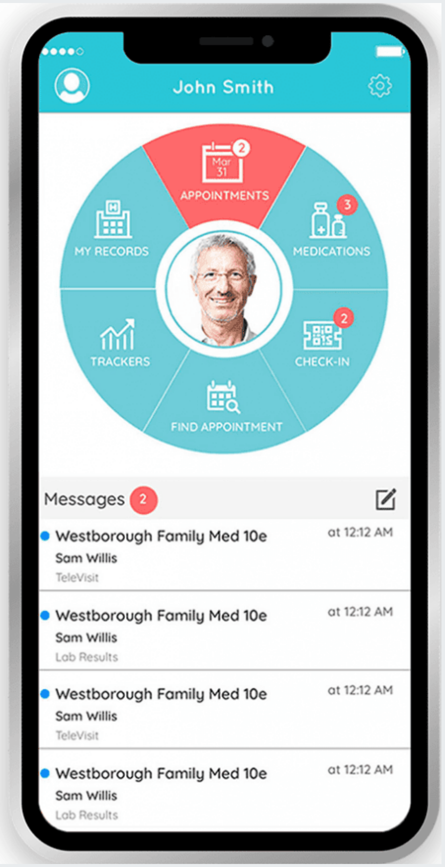


*Source: techuz.com*

# Examples of Web Apps in Healthcare

## What types of web applications are common in the healthcare sector?

- Patient Portals, Telehealth Services, and Online Pharmacies
- Electronic Health Record Systems
- Webmail for Hospitals and Clinics
- Patient Monitoring Applications with IoT Devices
- Medical Resources for Doctors and Clinical Decision Support
- Computer Aided Design (CAD) Systems for Dentists
- Health Insurance Portals
- Inventory Management in Hospitals



Westborough Family Med 10e at 12:12 AM
Sam Willis
TeleVisit

Westborough Family Med 10e at 12:12 AM
Sam Willis
Lab Results

Westborough Family Med 10e at 12:12 AM
Sam Willis
TeleVisit

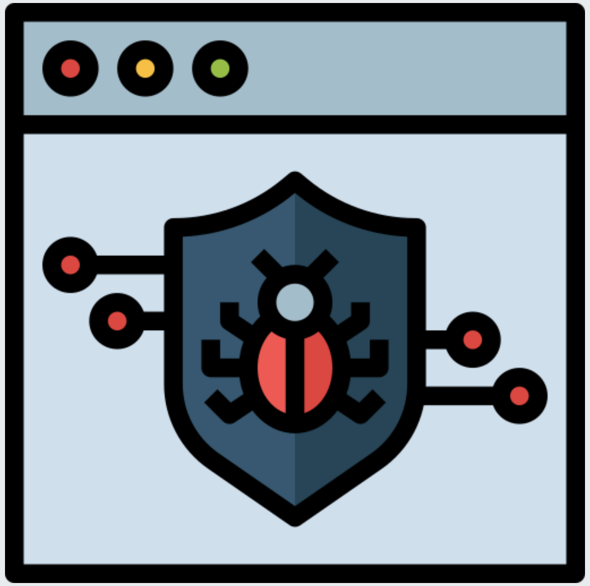
Westborough Family Med 10e at 12:12 AM
Sam Willis
Lab Results

*Source: Community Health Centers*

# What Are Web Application Attacks?

Verizon uses the term “Basic Web Application Attacks”, or BWAA.

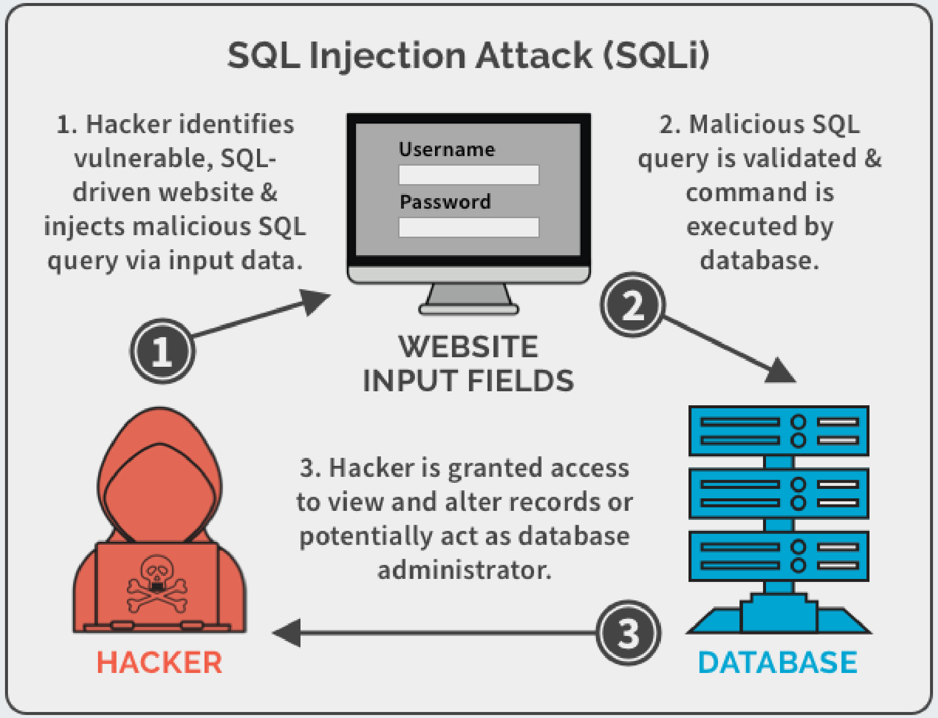
- Basic Web Application Attacks (BWAA) primarily involve attacks that directly target an organization’s most exposed infrastructure, such as web servers.
- Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior.
- These incidents commonly leverage stolen credentials or exploit a known vulnerability.



# Types of Web Application Attacks

What types of attacks aim to exploit web applications? Examples include the following:

- Cross-site scripting (XSS)
- SQL injection (SQLi)
- Path traversal
- Local file inclusion
- DDoS attacks
- Cross-site request forgery (CSRF)
- XML external entity (XXE)



SQL Injection Attack (SQLi)

1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.

2. Malicious SQL query is validated & command is executed by database.

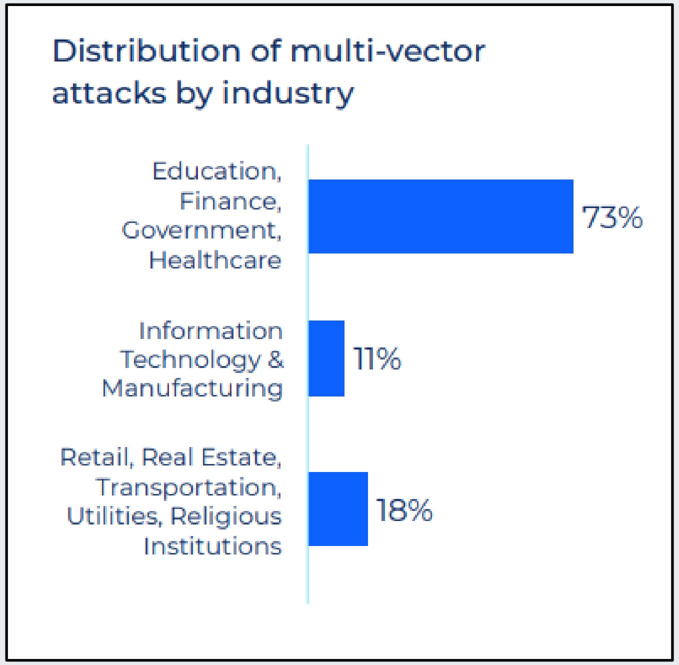
3. Hacker is granted access to view and alter records or potentially act as database administrator.

*Source: Spanning Backup*

# DDoS Attacks Impacting Web Applications

There are various possible drivers for Distributed Denial of Service (DDoS) attacks against healthcare organizations, such as political or hacktivist motivations and financial gain through extortion.

- According to Comcast Business, the healthcare sector faced the brunt of DDoS attacks last year, driven by COVID-19, school re-openings, and vaccine availability.
- The COVID-19 pandemic catalyzed a shift in targets from individuals to health and government infrastructure.
- DDoS attacks are extremely effective because they flood the victim's network with traffic, rendering network resources, such as web applications, unusable.
- DDoS attacks also may serve as a foothold for threat actors to deploy more sinister malware while distracting victims.



*Source: Comcast*

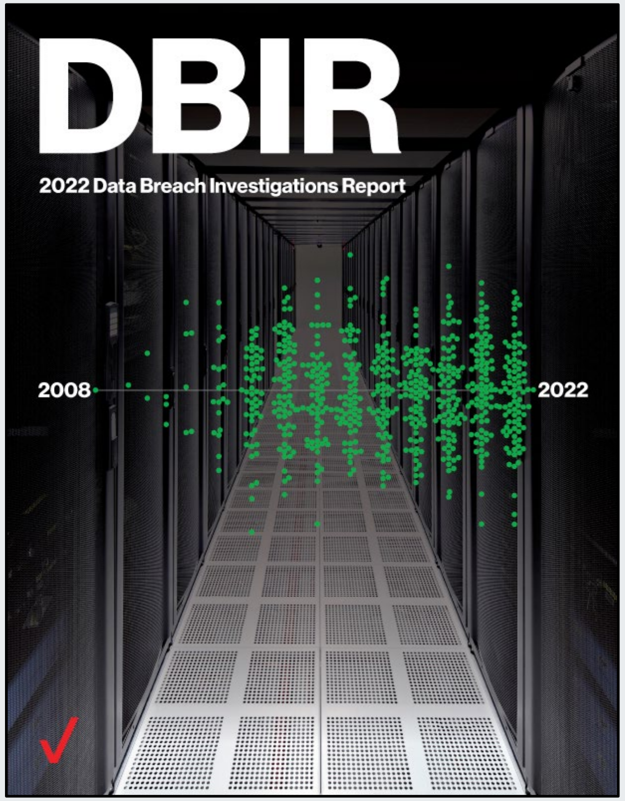
Office of **Information Security** Securing One HHS

**Health Sector Cybersecurity Coordination Center**

# What Is the Impact to Health Sector?

## Why are basic web application attacks a concern for the health sector?

- Verizon analyzed 849 total incidents, 571 with confirmed data disclosure in the healthcare sector in 2021 and found that web applications were the number one vector.
- Basic Web Application Attacks (BWAAs) have trended greater over the years in the healthcare sector and are more prominent than in other industries.
- Web application attacks targeting healthcare entities can impact the confidentiality, integrity, and availability of healthcare applications, systems, data, and resources.

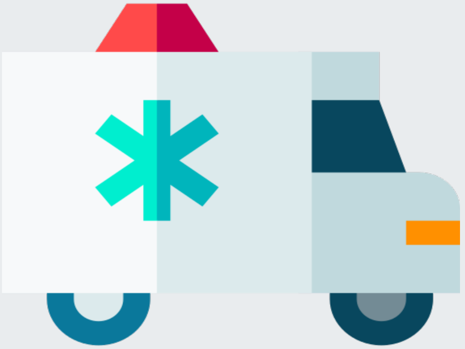


*Source: Verizon*

# Historical Incidents in Healthcare

What are some examples of historical cyber incidents involving web apps in healthcare?

- **May 2021:** California hospital system hit by ransomware attack, resulting in EHR downtime procedures and taking their patient portal offline.
- **January 2022:** Ransomware attack on HR and payroll vendor disrupted healthcare workforce paychecks, and even resulted in some discrepancies in paychecks.
- **April 2014:** Anonymous hacktivist group targeted a U.S. children's hospital with a DDoS attack after the hospital recommended a patient be admitted as a ward of the state and that custody be withdrawn from her parents, resulting in the appointment scheduling system, fundraising site and patient portal becoming unavailable to medical patients and personnel.



# Key MITRE ATT&CK® Enterprise Technique

MITRE ATT&CK® is a public knowledge base of adversary tactics and techniques based on real-world observations, which is used as a foundation for the development of specific threat models and methodologies.

**Exploit Public-Facing Application (ID: T1190)**

- ID: T1190
- Sub-techniques: No sub-techniques
- Tactic: Initial Access
- Platforms: Containers, IaaS, Linux, Network, Windows, macOS
- Description: Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior.

ATT&CK®

*Source: The MITRE Corporation*

# Who Exploits Web Applications?

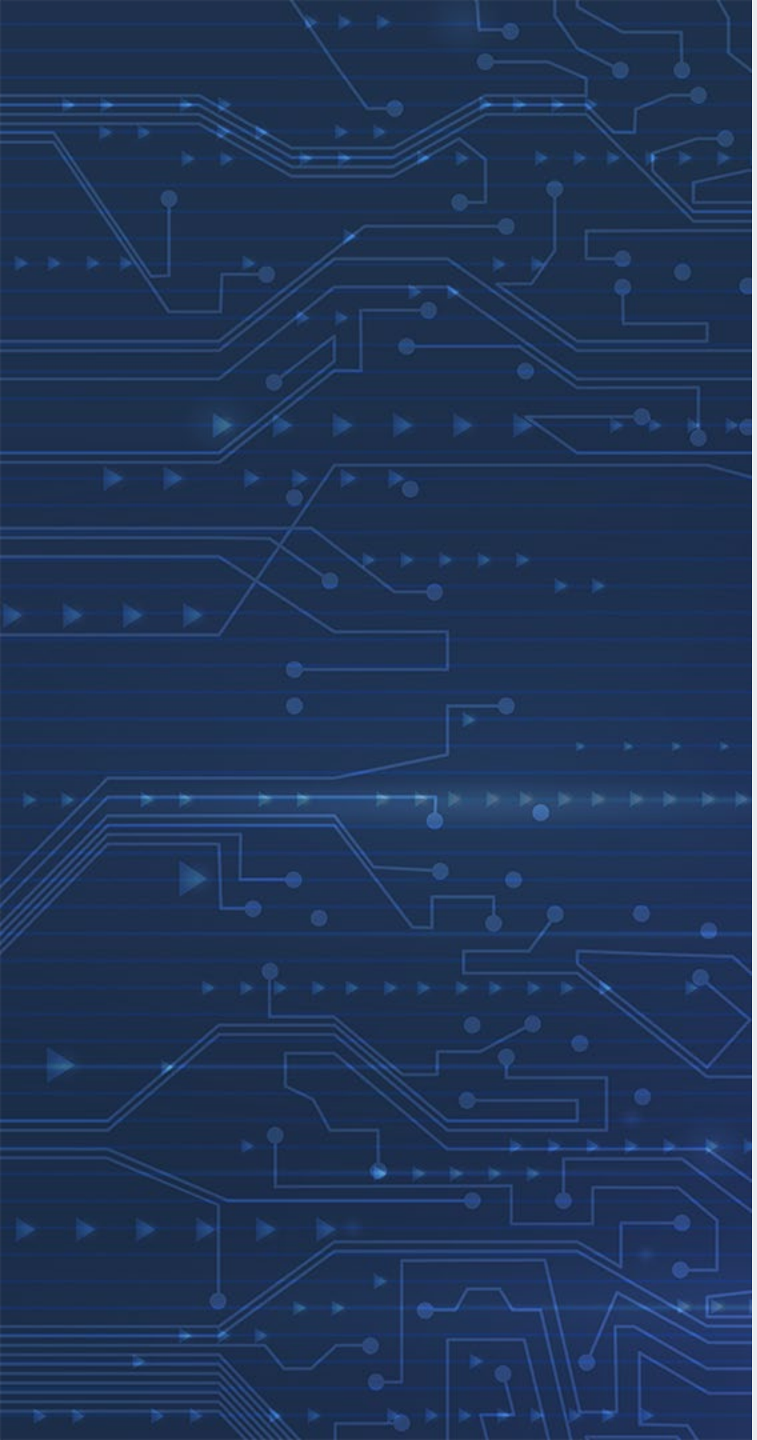
## What types of threat actors are exploiting web applications?

- Various state-sponsored APT groups and financially-motivated cybercriminal groups are known to exploit public-facing applications.
- Some examples of these threat groups include APT28, APT29, APT39, APT41, Axiom, BackdoorDiplomacy, BlackTech, Blue Mockingbird, Dragonfly, Fox Kitten, GALLIUM, GOLD SOUTHFIELD, HAFNIUM, Ke3chang, Kimsuky, Magic Hound, menuPass, Night Dragon, Operation Wocao, Rocke, Threat Group-3390, and Volatile Cedar, according to Mitre.

# Tools Used for Web Application Attacks

How do threat actors exploit public-facing applications? Here are just a few examples:

- **Havij** is an automatic SQL Injection tool distributed by ITSecTeam, an Iranian security company.
- **Siloscape** is a malware targeting Windows containers executed after the attacker gains initial access to a Windows container using a known vulnerability.
- **SoreFang** can gain access by exploiting a Sangfor SSL VPN vulnerability that allows for the placement and delivery of malicious update binaries.
- **sqlmap** can be used to automate exploitation of SQL injection vulnerabilities.
- **ZxShell** has been dropped through exploitation of CVE-2011-2462, CVE-2013-3163, and CVE-2014-0322.
- **China Chopper** is a web shell hosted on web servers to provide access back into an enterprise network that does not rely on an infected system, calling back to a remote C2 server.



# Mitigations

What are some mitigations to protect against web application attacks in the health sector?

# Web Application Security

## What is web application security?

- According to Synopsys, web application security (also known as Web AppSec) is the idea of building websites to function as expected, even when they are under attack. The concept involves a collection of security controls engineered into a web application to protect its assets from potentially malicious agents.
- Web applications, like all software, inevitably contain defects. Some of these defects constitute actual vulnerabilities that can be exploited, introducing risks to organizations. Web application security defends against such defects. It involves leveraging secure development practices and implementing security measures throughout the software development life cycle (SDLC), ensuring that design-level flaws and implementation-level bugs are addressed.

# Tips to Protect Against Web App Attacks

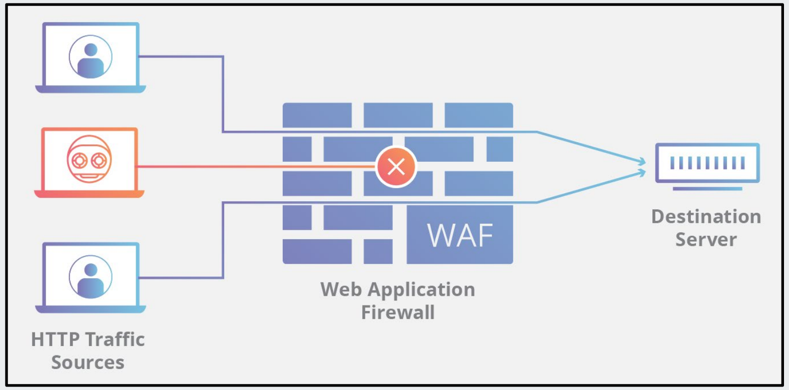
Even though there are a variety of web application attacks, there are also processes, technologies and methods to protect against them. Different approaches to web application security address different vulnerabilities.

- **Automated vulnerability scanning and security testing** helps organizations find, analyze and mitigate vulnerabilities and misconfigurations — hopefully before the actual attack occurs. This testing helps organizations identify security weaknesses that need to be resolved.
- **Web application firewalls** are hardware and software solutions that protect against application security threats by filtering, monitoring and blocking malicious traffic from traveling to the web application. These tools are continuously updated with new rules designed to catch the latest attack and exploitation techniques.
- **Secure development testing** is a practice in which security teams consider the threats and attacks that might have an impact on an application or product to help make it as secure as possible. Secure development testing can uncover the latest security risks and attack vectors early in the product's lifecycle. It also helps in developing effective approaches to preventing website attacks and minimizing the consequences of breaches.

# Web Application Firewalls (WAFs)

## How can web application firewalls (WAFs) help mitigate attacks?

- A WAF, or web application firewall, helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet.
- WAFs typically help protect web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection (SQLi), among others.
- A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks.

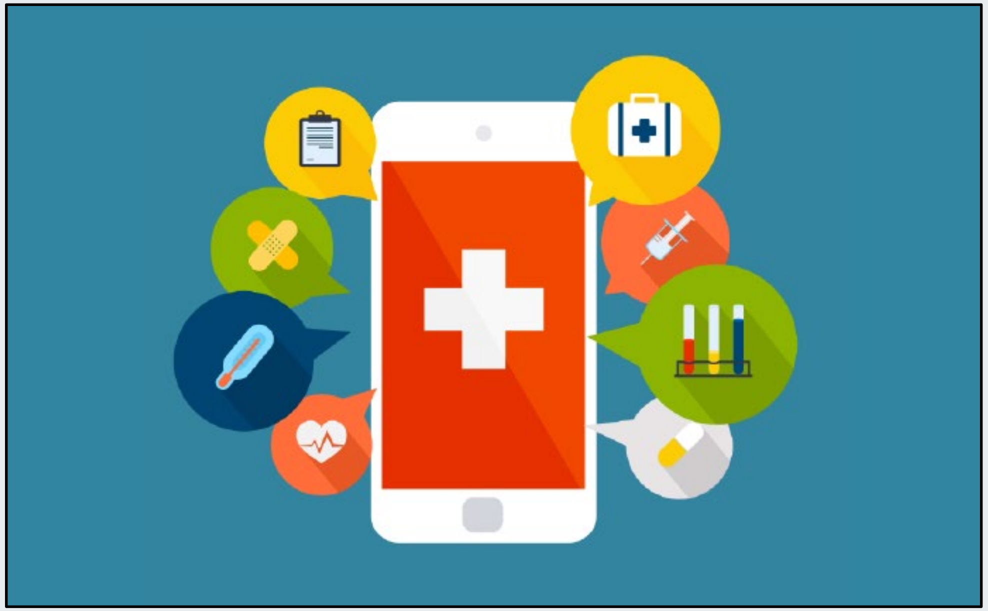


*Source: Cloudflare*

# Locking Down Patient Portals

What are some basic recommendations to help secure patient portals?

1. Implement a CAPTCHA
2. Establish a Login Limit
3. Use Login Monitoring
4. Screen for Compromised Credentials
5. Implement Multifactor Authentication (MFA)



*Source: PatientEngagementHIT*

# Corresponding Mitre ATT&CK Mitigations

The following Mitre ATT&CK mitigations address Exploit Public-Facing Application (T1190)

| ATT&CK ID | Mitigation | Description |
|---|---|---|
| M1048 | Application Isolation and Sandboxing | Application isolation will limit what other processes and system features the exploited target can access. |
| M1050 | Exploit Protection | Web application firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application. |
| M1030 | Network Segmentation | Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure. |
| M1026 | Privileged Account Management | Using least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system. |
| M1051 | Update Software | Update software regularly by employing patch management for externally exposed applications. |
| M1016 | Vulnerability Scanning | Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure. |

# Top 10 Web Application Security Risks

The OWASP Top 10 is a standard awareness document for developers and web application security.

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

Link: https://owasp.org/www-project-top-ten/

# CWE Top 25 Most Dangerous Software Weaknesses

- The 2022 Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses list (CWE™ Top 25) demonstrates the currently most common and impactful software weaknesses, which can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.
- Link: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

# HHS 405(d) HICP Best Practices

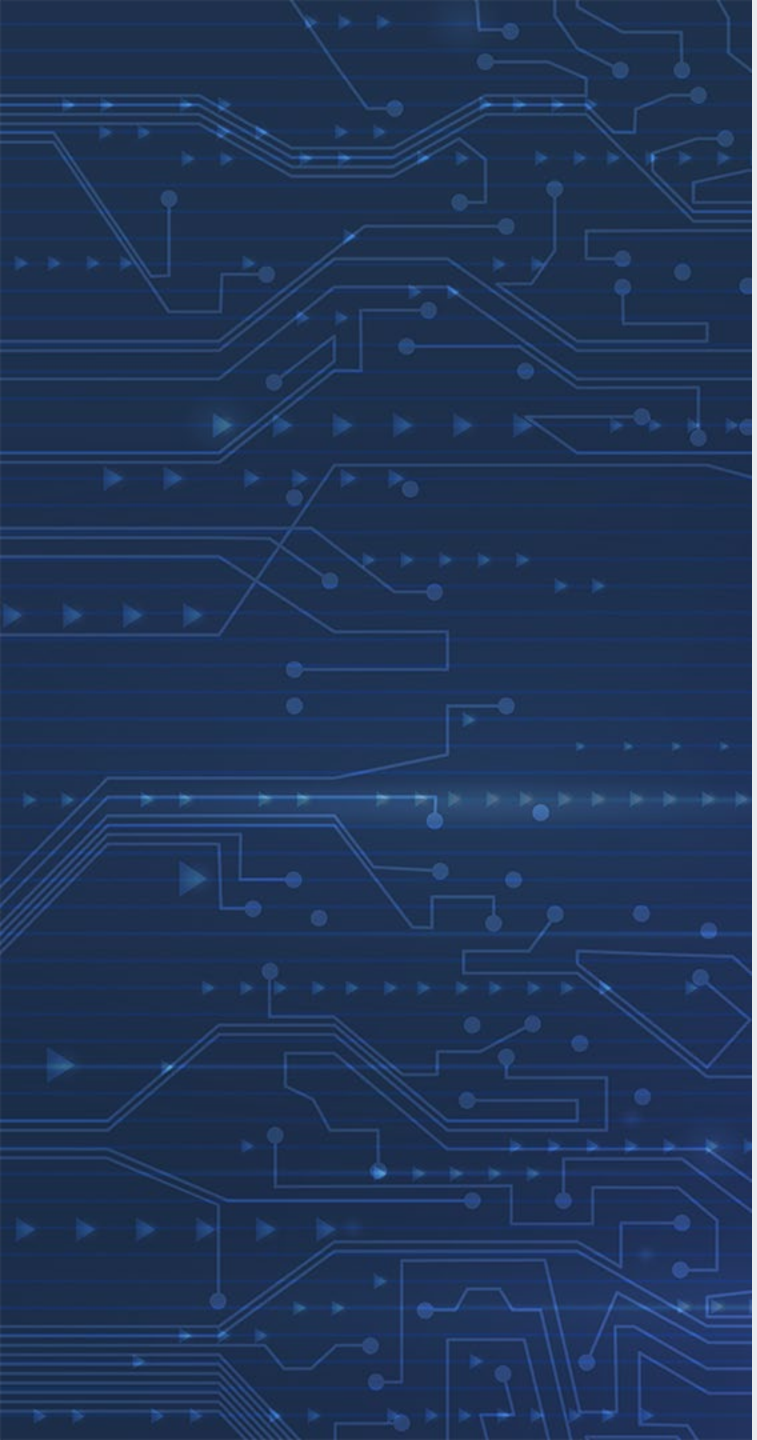
The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats, and the ten best practices to mitigate them. Below are examples from HICP that can be used to mitigate some common threats.

| 405(d) Reference | Description | NIST Framework Reference |
|---|---|---|
| 2.S.A | Basic Endpoint Protection Controls | PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS2, PR.AC-3 |
| 3.S.A | Basic Access Management | PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7 |
| 4.S.A | Policies | ID.GV-1, ID.AM-5 |
| 4.S.B | Procedures | ID.GV-1, PR.AT-1, PR.DS-2, PR.DS-5, PR.DS-1, PR.IP-6, ID.GV-3 |
| 5.S.A | Inventory | ID.AM-1 |
| 5.S.C | Decommissioning | PR.IP-6, PR.DS-3 |

# HHS 405(d) HICP Best Practices (cont.)

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats, and the ten best practices to mitigate them. Below are examples from HICP that can be used to mitigate some common threats.

| 405(d) Reference | Description | NIST Framework Reference |
|---|---|---|
| 6.S.A | Network Segmentation | PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3 |
| 6.S.C | Intrusion Prevention | PR.IP-1 |
| 7.S.A | Vulnerability Management | PR.IP-12 |
| 8.S.A | Incident Response | PR.IP-9 |
| 8.S.B | ISAC/ISAO Participation | DETECT ID.RA-2 |
| 10.S.A | Policies | IG.GV-1, ID.AM-6, PR.AT, PR.AT-1, RS.CO-1 |



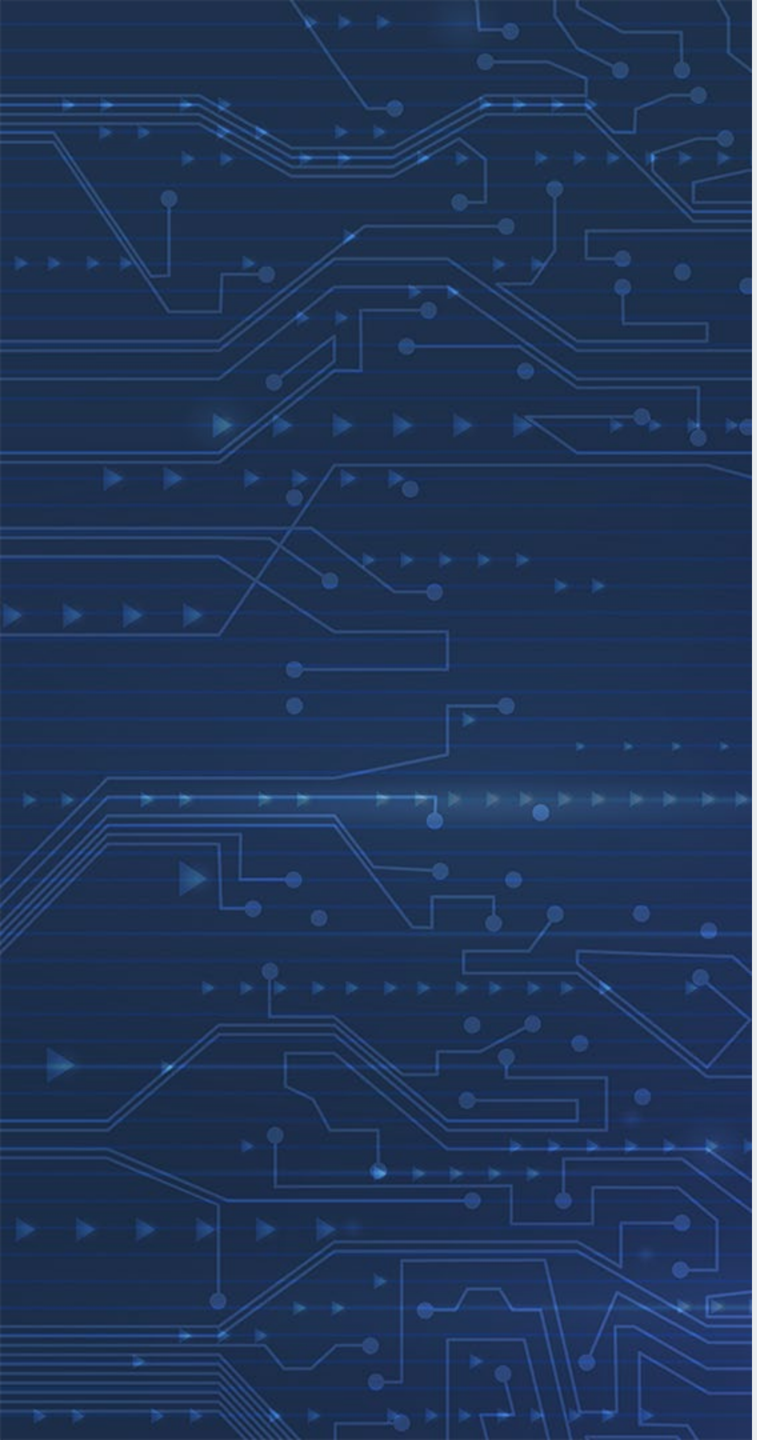
# Additional Resources

# Free and Low-Cost Technical Resources

| Title | Description | Location | Type |
|---|---|---|---|
| Web Application Hacker's Handbook | Handbook on everything web application penetration testing | https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470 | Resource |
| OWASP Web Security Testing Guide | Web application testing guide by OWASP | https://owasp.org/www-project-web-security-testing-guide/ | Resource |
| Portswigger XSS Cheat Sheet | List of XSS injections from Portswigger | https://portswigger.net/web-security/cross-site-scripting/cheat-sheet | Resource |
| Portswigger SQL Cheat Sheet | List of SQL injections from Portswigger | https://portswigger.net/web-security/sql-injection/cheat-sheet | Resource |
| OWASP XSS Filter Evasion Cheat Sheet | OWASP Cross-Site Script Filter/WAF evasion cheat sheet | https://owasp.org/www-community/xss-filter-evasion-cheatsheet | Resource |
| Hacker101 Web App Crash Course | Collection of short web application pentesting videos | https://www.hacker101.com/videos | Resource |
| Bug Bounty Report Writeups | Collection of bug bounty writeups from 2012 to 2020 | https://pentester.land/list-of-bug-bounty-writeups.html | Resource |
| Pentesting GraphQL | Article on pentesting GraphQL endpoints | https://prog.world/pentest-applications-with-graphql/ | Resource |

# Free and Low-Cost Technical Tools, Trainings

| Title | Description | Location | Type |
|---|---|---|---|
| Bug Bounty Forum Tool List | Collection of web app/bug bounty open-source tools | https://bugbountyforum.com/tools/ | Tool |
| Altair GraphQL Client | GraphQL client that makes testing endpoints 10x easier | https://altair.sirmuel.design/ | Tool |
| Portswigger Academy | Free online web application security training/resources from creators of Burp Suite | https://portswigger.net/web-security | Training |
| Google Firing Range | Test bed for automated and manual web application testing | https://public-firing-range.appspot.com/ | Training |
| [Paid] Source Incite | [Advanced] Full Stack Web attack designed for experienced web testers to further their skills on cutting edge web attacks. | https://srcincite.io/training/ | Training |
| [Paid] MDSec | [Advanced] Designed for web testers to further skills on other cutting edge web attacks differently from the Source Incite training. | https://www.mdsec.co.uk/training/beyond-the-web-application-hackers-handbook-advanced/ | Training |



# Conclusion

What are the major takeaways?

# Major Takeaways

- Web applications were the number one vector for data disclosure in the healthcare sector in 2021, according to Verizon.
- Both state-sponsored and financially-motivated threat actors are responsible for web application attacks in the healthcare and public health (HPH) sector.
- Ransomware and DDoS attacks may indirectly or directly impact web applications used in the healthcare industry, such as patient portals or Electronic Health Record (EHR) systems.
- Types of web application attacks may include cross-site scripting, SQL injection, path traversal, local file inclusion, DDoS attacks, and more.
- Even though there are a variety of web application attacks, there are also processes, technologies and methods to protect against them.
- Some tips to protect against web application attacks include vulnerability scanning and penetration testing, secure development testing, and implementing web application firewalls.

# Reference Materials

# References

- Acunetix. n.d. What Is a Web Application Attack and how to Defend Against It. Accessed July 12, 2022. https://www.acunetix.com/websitesecurity/web-application-attack/.
- Burnham, Kristin. 2021. Defending Against Common Types of Web Application Attacks. November 18. Accessed July 12, 2022. https://www.mimecast.com/blog/web-application-attacks/.
- Center for Internet Security (CIS). n.d. DDoS Attacks: In the Healthcare Sector. Accessed July 12, 2022. https://www.cisecurity.org/insights/blog/ddos-attacks-in-the-healthcare-sector.
- Cloudflare. n.d. What is web application security? Accessed July 12, 2022. https://www.cloudflare.com/learning/security/what-is-web-application-security/.
- Davis, Jessica. 2021. Scripps Health EHR, Patient Portal Still Down After Ransomware Attack. May 10. Accessed July 12, 2022. https://healthitsecurity.com/news/scripps-health-ehr-patient-portal-still-down-after-ransomware-attack.
- Enzoic. 2021. Locking Down Patient Portals. December 2. Accessed July 12, 2022. https://securityboulevard.com/2021/12/locking-down-patient-portals/.
- Flashpoint. 2021. Compromised Credentials: Analyzing the 2021 Verizon DBIR and Its Most Sought-After Data Type. June 7. Accessed July 12, 2022. https://flashpoint.io/blog/compromised-credentials-analyzing-2021-verizon-dbir/.

# References

- Grim, Ryan. 2016. Why I Knocked Boston Children's Hospital Off The Internet: A Statement From Martin Gottesfeld. September 18. Accessed July 12, 2022. https://www.huffpost.com/entry/why-i-knocked-boston-childrens-hospital-off-the-internet-a-statement-from-martin-gottesfeld_n_57df4995e4b08cb140966cd3.
- HIPAA Journal. 2019. 10 Year Jail Term for Boston Children's Hospital Hacker. January 14. Accessed July 12, 2022. https://www.hipaajournal.com/10-year-jail-term-for-boston-childrens-hospital-hacker/.
- Hulme, George V. 2021. Top 5 Healthcare Cyber Attacks and Threats. September 29. Accessed July 12, 2022. https://businessinsights.bitdefender.com/top-5-healthcare-cyber-attacks-and-threats.
- Multi-State Information Sharing and Analysis Center (MS-ISAC). 2017. Technical White Paper – Guide to DDoS Attacks. November 1. Accessed July 12, 2022. https://www.cisecurity.org/insights/white-papers/technical-white-paper-guide-to-ddos-attacks.
- Muresan, Razvan. 2016. DDoS Attacks on the Rise—Here's What Companies Need to Do. December 28. Accessed July 12, 2022. https://businessinsights.bitdefender.com/ddos-attacks-what-companies-need-to-do.

# References

- Nehra, Mahipal. 2019. How Web Applications are Useful in Healthcare Industry? August 10. Accessed July 12, 2022. https://www.decipherzone.com/blog-detail/Use-of-Web-Applications-in-Healthcare-Industry.
- Synopsys. n.d. Web Application Security. Accessed July 12, 2022. https://www.synopsys.com/glossary/what-is-web-application-security.html.

# ? Questions

# FAQ

## Upcoming Briefing

- August 4 – The OWASP Top 10

## Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

## Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

### Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

# About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

## What We Offer

### Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

### Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

### Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Office of
**Information Security**
Securing One HHS

**Health Sector Cybersecurity Coordination Center**

# Contacts

🌐 HHS.GOV/HC3

@ HC3@HHS.GOV